A Novel Approach to Symmetric Cryptographic Secured Communication Links for Real-Time Teleoperation and Telemetry

Robert David Sparrow

A thesis submitted in fulfilment of the requirements of the University of Greenwich for the Degree of Doctor of Philosophy

June 2018

Declaration

I certify that the work contained in this thesis, or any part of it, has not been accepted in substance for any previous degree awarded to me, and is not concurrently being submitted for any degree other than that of Doctor of Philosophy being studied at the University of Greenwich. I also declare that this work is the result of my own investigations, except where otherwise identified by references and that the contents are not the outcome of any form of research misconduct.

Student Signature:

First Supervisor Signature:

Second Supervisor Signature:

Acknowledgements

The undertaking of this thesis would not have been possible without thanks to those who had helped contribute towards the final outcome of this thesis. A special thanks to my first supervisor Dr Andrew Adekunle as his expertise, knowledge, kindness and influence helped guide myself throughout my academic career and for that I am forever grateful for his assistance. Additional thanks goes to my second supervisor Dr Robert Berry for support and guidance throughout the duration of the research.

Acknowledgement to all staff members in the faculty of Engineering and Science for guiding me for past seven years of my studies and presenting the opportunity to undertake research on behalf of the university. A special mention to academic colleges Janice Johnson who I have had the pleasure of collaborating with throughout the duration our undergraduate and postgraduate studies; colleagues of the Wolfson centre for contributing to a memorable experience to the research journey. A special thanks to Sean Edwards, Sean Stroud, Samantha King, Agnie Alexander, Carmen Piras, and Voula Kasapidou for being there throughout this journey, it has been a pleasure to share the experience with them all.

The most important acknowledgement goes to my parents David Sparrow and Lindsay Sparrow, my sister Gemma Sparrow, brother in law Chris Cocker, my grandparents Eiliene and William Hall, Audrey and Rodney Sparrow for providing me with the love and encouragement to carry on through tough times and reach the final goal. Without them the completion of this thesis would not have been possible and I am forever grateful for everything they have done.

Abstract

Communication links both wired and wireless can facilitate teleoperation and telemetry; however, contemporary security paradigms are not best suited for wired or wireless real-time teleoperation and telemetry as the strength of the security services provided increases the processing latency and energy consumption of utilised cryptographic platforms, resulting in a detrimental impact on real-time operational performance of teleoperation and telemetry.

The aim of this research is to derive a novel approach to symmetric cryptographic secured communication links that will have a reduced impact on the operational performance of the application utilising the communication link. The contributions of this research is the cryptographic synergy philosophy. The cryptographic synergy philosophy is presented in two sections; the intrinsic paradigm and the extrinsic paradigm. The intrinsic paradigm prioritises the internal security service with the reduction in the time to compute the process . The extrinsic paradigm prioritises the global security service to maintain the ephemerial privacy of the shared secret used for secure communication links.

The composite concept and speed-centric method derived from the intrinsic paradigm results in the design and implementation of new block cipher structures, designated the Permutation Substitution Network (PSN) and the Permutation Substitution Permutation Network (PSPN). Applying the PSN and PSPN structures enables the derivation of the Big Cat family of block ciphers which is a new design approach for lightweight block ciphers that focuses on speed of operation and sufficient cryptographic security for the specified time constraint; an instance of the approach is the presented Lightweight Encryption Operation Permutation Addition Rotation and Diffusion (LEOPARD) block cipher. The LEOPARD block cipher has a five per cent reduction per block call in its processing latency when compared to the National Institute of Standard and Technology (NIST) standardised AES-128 block cipher. The interdependency concept and privacy-based methods derived from the extrinsic paradigm are utilised with the derivation of the expert decision making system that resulted in the design and implementation of the Privacy Cryptographic Unit (PCU). The PCU contains an autonomous security expert logic rule set that controls the number of cryptographic key regeneration performed over the mission duration.

The outcome of this research is useful to practitioners involved with real-time teleoperation and telemetry, because the contributions presented achieved a reduction in detrimental operational performance on- teleoperation and telemetry applications with the LEOPARD block cipher; whilst the PCU achieves autonomous enhancement of the privacy associated with cryptographic secured communication links for- teleoperation and telemetry applications.

Contents

List of Figures

List of Tables

Nomenclature

A	Amps
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BCS	Binary Coded Signals
CA	Certificate Authority
CAA	Civil Aviation Authority
CAN	Controller Area Network
CBC	Cipher Block Chaining
CCM	Cipher Block Chaining with Message Authentication Code
CFB	Cipher Feedback Mode
CIA	Confidentiality, Integrity and Authentication
CL-AKA	Certificateless Authenticated Key Agreement
CLP	Constraint Logic Programming
CMAC	Cipher Based Message Authentication Code
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
dBm	Decibel-milliwatts
DDoS	Distributed Denial of Service
DES	Data Encryption Standard (1 key)
DES-3	Data Encryption Standard (3 keys)
DH	Diffie-Hellman
DoS	Denial of Service
DSA	Digital Signiture Algorithm

EAACK	Enhanced Adaptive Acknowlegement Protocol
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECLSC-TKEM	Efficient Certificateless Signcryption Tag Key Encapsulation Method
ECU	Electronic Control Unit
FPGA	Field Programmable Gate Arrays
FSM	Finite State Machines
Gbps	Gigabits per second
GCM	Galos Counter Mode
GMAC	Galos Based Message Authentication Code
HMAC	Hashed Message Authentication Code
IDS	Intrusion Detection System
IED	Intelligent Electrical Device
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
ISM	industrial, scientific and medical
ISO	International Organisation of Standards
IV	Initialisation Vector
JCM	Joint Cipher Mode
LEOPARD	Lightweight Encryption Operation Permutation Addition Rotation and Diffusion
m/s	Metres Per Second
MAC	Message Authentication Code

MANET	Mobile Ad-Hoc Network
MAV	Micro Aerial Vehicle
MAVlink	Mobile Aerial Vehicle Link
Mbps	Megabits per second
MD5	Message Digest 5
MIPS	Million Instructions Per Second
MIT	Massachusetts Institute of Technology
MITM	Man In The Middle
ms	Milliseconds
mW	Milliwatt
NIST	National Institute of Standard and Technology
NONCE	Number Only Used Once
NS-2	Network Simulator Two
OSI	Open Systems Interconnection
PCB	Printed Circuit Board
PCU	Privacy Cryptographic Unit
PESQ	Perceptial Evaluation of Speech Quality
PID	Proportional Intergral Derivative
PKI	Public Key Infrastructures
PSN	Permutation Subsitution Network
PSPN	Permutation Subsitution Permutation Network
QKD	Quantium Key Distribution
QoE	Quality of Experience
QoS	Quality of Service
RAM	Random Access Memory

RC4	Rivest Cipher Four
RFC	Request For Comments
RGB	Red Green Blue
RPA	Remotely Piloted Aircrafts
RSA	Rivest-Sharmir-Aldeman
RTP	Real-Time Protocol
RTS	Real-Time System
RTU	Remote Terminal Unit
SANS	Sysadmin Audit Network and Security
SHA	Secure Hash Algorithm
SPI	Serial Peripherial Interface
SPN	Subsitution Permutation Network
TCP	Transmission Communication Protocol
TQOS	Trustworthiness Quality of Service
TV-HORS	Time Valid Hash to Obtain Random Subsets
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UGV	Unmanned Ground Vehicle
USB	Universial Serial Bus
V	Volts
W	Watt
Wi-Fi	Wireless Fidelity
WNCS	Wireless Networked Control System
WSN	Wireless Sensor Networks
XOR	Exclusive OR

1 Introduction

The human race has philosophised about the supposed phenomenon of being in two places simultaneously; this is defined as bilocation. Accounts of the first instances of bilocation originated from religion with St Padre Pio; he was said to possess the ability to bi-locate, as it was reported that he visited people and places whilst remaining in an original location; a quote by Pio describes the ability of bilocation stating; *"They cannot know if the body or the soul moves, but they are very conscious of what happens and they know where they are going"* (Dallaire 2010). Contemporary adaption of bilocation is pervasive in modern society as it is applied in various scenarios that include space exploration, telepresence for remote business conferences, teleoperation to control devices from a remote location and telemetry to monitor the response of the action conducted.

Development of remotely operated devices has materialised as an approach to enable users to both interact and visualise the physical world remotely. The deployment of remotely operated devices in situations that are inaccessible to humans is growing in order to acquire knowledge of distant environments and to facilitate human interaction from a remote location.

1.1 Research Context

A recent survey conducted by the Pew Research Centre stated that workforce automation will be prominent in the future, two thirds of the Americans surveyed expected robots and computers to do much of the work currently done by humans within fifty years and expect robots and computers to be the future of workforce automation (Smith 2016); this indicates that the future trend of using manual, semi-autonomous or autonomous systems for routine tasks will become a more frequent occurrence in the future. There are three main configurations for remotely operated devices; manual control is where the human operator has full control over the operation; semi-autonomous control is where control of the system is shared between the human operator and the onboard computer. Fully-autonomous control is where the systems onboard computer has complete control of the operation (Huang 2004).

Communication devices have enabled humans to monitor and control tasks by means of real-time teleoperation and telemetry. Elaboration of specified applications and security issues associated with real-time teleoperation and telemetry in the context of this research are presented in the subsequent sub-sections.

1.2 Contemporary Applications of Real-Time Teleoperation and Telemetry

The application of human supervisory control enables the human to interact with a complex technical system to ensure efficiency and reliability of the operation in real-time (Inagaki & Stahre 2004). The use of human supervisory control has emerged in the agricultural sector with the development of machinery that can be operated remotely to complete agricultural tasks. Figure 1.1 illustrates the use of teleoperation to remotely operate machinery used in the agricultural sector.

Figure 1.1: The semi-autonomous concept vehicle used in the agricultural sector (Dvorsky 2016).

The semi-autonomous concept vehicle is an instance of a real-time teleoperation and telemetry device that is programmed by a human operator to conduct and monitor tasks through a mobile computing device. Teleoperation requires telemetry to monitor and collate data from an actuator to determine if the action performed was successful (Nohmi & Bock 2006); whilst the telemetry monitors the data obtained from the onboard cameras, radar and global positioning system (GPS) to control the speed of the vehicle which has a top speed of fifty kilometres per hour (thirty-one miles per hour).

Remote real-time teleoperation and telemetry data is frequently communicated over a wireless communication link to transfer data between the transmitter and the receiver through radio frequency; examples of systems that use wireless communication for real-time teleoperation and telemetry are remotely piloted aircraft (RPA) (aka Unmanned Aerial Vehicles (UAV)). Figure 1.2 pictures an UAV at the moment of launch.

Figure 1.2: A fixed-wing remotely piloted aircraft (Veen 2012).

The wireless communication medium facilitates the use of real-time teleoperation and telemetry as the UAV collects and transfers data whilst operating in scenarios that are hazardous or inaccessible to humans. The backbone of a UAV system is the wireless communication link between the aircraft and the ground control station (Winzer 2015). The communication link must be resistant to interference and unauthorised access to prevent attackers conducting malicious activity on data during propagation between the UAV and ground control base-station.

1.3 Security Incidents with Real-Time Teleoperation and Telemetry

The real-time nature of the data requires a task or procedure to be undertaken within a constraint period of time; in addition, the data must be kept on the move between devices, have predictable outcomes in action, instantaneous processing of the data in order to provide reliability and availability of the data (Stonebraker et al. 2005).

Current applications of real-time teleoperation and telemetry devices have been known to malfunction whilst in operation as a result of security vulnerabilities on the communication link. Recent incidents of a malfunctioned UAV during operation has been documented at the 2015 Ski World Cup championships in Alta Badia, Italy (Grez 2015); operational control the real-time teleoperation and telemetry was lost, this caused the UAV to be unresponsive and crash onto the ski course. The consequence of the malfunction resulted in the UAV causing potential injury to the competitors. Figure 1.3 pictures the close proximity of the crash.

Figure 1.3: UAV crash incident at the 2015 Ski World Cup event, Alta Badia, Italy (McFadyen 2015).

Safety critical processes in the bulk solids handling industry use real-time teleoperation and telemetry to mange plant systems to maintain safety, reliability and availability (Emerson 2014, Hultman 2015). The real-time requirements of the dust explosion plant system must not surpass the deadline as the consequent action could result in an uncontrolled explosion. An incident that compromised the safety, reliability and availability of a system was the Bosley wood mill explosion (Khomani 2015). A plausible cause of the explosion could have been due to the failure to complete the real-time teleoperation and telemetry in the constraints with specified to prevent the uncontrolled explosion. Figure 1.4 shows the blast damage at the Bosley wood mill.

Figure 1.4: Bosley wood mill dust explosion incident (Glendinning 2015).

Security research performed at the Keen Security Lab intercepted and influenced the operation of a real-time mobile ground vehicle, the Tesla model S car (Drozhzhin 2016).

The researched compromised the control of the actuators over a wireless communication link in real-time up to twelve miles away from the target. Safety critical features including the acceleration, braking and door locking mechanisms were in full operational control of the researchers attacking the vehicle; causing uncontrollable and unresponsive actions. Figure 1.5 shows the Tesla model S car.

Figure 1.5: Tesla model S car hacked by the Keen Security Lab (Zetter 2015).

1.4 Research Problem

Contemporary security measures use confidentiality, integrity and authentication (C.I.A) to secure communicated data in hardware or software; however, software methods derived for enterprise computer networks were not designed with consideration for real-time teleoperation and telemetry as implementations focused on non-real time constraints. The problem of balancing secure communications, real-time teleoperation and telemetry in software while maintaining minimal adverse operational performance on remote systems is multi-faceted, non-trivial and an open problem.

1.5 Scope of Research

The scope of this research is the investigation and provision of secure communication links for real-time teleoperation and telemetry applications using constrained platforms (e.g. 8-bit embedded microcontrollers). All wireless communications examined in the scope of this research are the standardised ISM bands for radio frequency (Union 2016). UAV that are within the Civil Aviation Authority (CAA) regulations are within the research scope to comply with the rules and regulations of UK based flight (CAA 2015). Methods of securing the end points fall outside the scope of this research as the focus in on the communication link only. Authentication methods are not within the scope of the research as it is assumed that authentication is achieved through successful decryption

and integrity check of the message using the same cryptographic key.

1.6 Research Assumptions

It is assumed in this research that the scheduling mechanism used is the first in, first out (FIFO) scheduling algorithm; this is because the focus of the research is on the real-time teleoperation and telemetry communication links and that the packetised data between the transmitter and receiver device would be processed based on a packet scheduler (Audsley et al. 1995). The instance of the packet scheduler examined in this thesis is the circular buffer as it is assumed that a fixed packet size has been selected and configured by the practitioner before implementation.

1.7 Research Aim

The aim of this research is to provide a novel approach to symmetric cryptographic secured communication links that will have a reduced impact on the operational performance of real-time teleoperation and telemetry in comparison to contemporary standardised symmetric cryptographic approaches to secured communication links.

1.8 Research Objectives

To achieve the aim of the research the following objectives have been identified:

- Research into existing published literature in order to ascertain the limits of current research knowledge relevant to the research scope;
- Investigate the impact of contemporary security paradigms and methods on real-time teleoperation and telemetry utilising secure communication links;
- Propose a philosophy to achieve the specified aim of this research;
- Validate the proposed philosophy and suggest future research directions.

1.9 Philosophical Methodology

The philosophical methodology undertaken in this thesis is presented in the following structure:

1. **Formulation of Questions and Problems:** Formulation of questions to be answered and problems to be solved. The problem is segmented into a series of questions in order to understand each aspect of the problem in order to ascertain a fundamental understanding of the research problem examined in this thesis as presented in Chapter 2.

2. **Problem Analysis of Research Gaps Identified:** Questions derived from the formulation of the questions and problems are investigated in detail through a series of experimentation and analytical reflection of the findings in order to identify variables and relationships that influences the problems, why this impacts the research context and how it could be remediate to reduce or overcome the problems examined as presented in Chapter 3, Chapter 4, Chapter 5, Chapter 6 and Chapter 7.

3. **Synthesis of Solution:** Knowledge collated from the examination and understanding of the questions proposed in the problem analysis is applied to synthesise and justify the proposed philosophical concepts and paradigms to overcome the specified research question as presented in Chapter 8 and Chapter 9.

4. **Validation of Synthesised Solution:** Instances of the methods derived from the philosophical framework are proposed to justify the philosophical thinking and how it compares with contemporary philosophical methodologies to address the problem specified with the conduction of a series of mini experiments as presented in Chapter 10.

5. **Conclusion:** Reflection of the synthesised solution derived to overcome the stated research problem is presented with identification of the benefits and the current limitations of the solution and the identification of the future research areas that have been identified as a result of the work conducted in this thesis; this is presented in Chapter 11.

The next section introduces the structure of the thesis based on the philosophical methodology stated.

1.10 Structure of Thesis

The structure of the rest of this thesis is as follows:

- **Chapter 2: Literature Review:** This chapter surveys the current literature relevant to the research problem with reference to standardised frameworks, contemporary security and communication approaches used to secure communications. An in-depth literature review of existing published literature is presented in order to ascertain the limits of current research knowledge relevant to the research problem scope and area, leading to the stated contributions.

- **Chapter 3: Investigation of Real-Time Teleoperation and Telemetry Communication Latency on Static End-Points:** This chapter examines how contemporary security paradigms identified in Chapter 2 impact on the communication latency of

real-time teleoperation and telemetry applications with analysis of the variables and fundamental relationships that contribute towards the problems investigated.

Analysis of the tests conducted in this chapter highlight the impact of secure communication on the latency generated instantaneous packet throughput recorded and the propagation method between the transmitter and receiver. Results presented show an increased in latency up to seven hundred milliseconds on the time required to complete a real-time teleoperation and telemetry task.

Further analysis identified the additional latency incurred had a significant reduction on instantaneous packet throughput over multiple-hop propagation. Contributions presented in this chapter include mathematical models to calculate the impact of secure communications on single and multiple hop propagation links and how mobile actuators contribute towards the multi-faceted problem investigated. Dissemination of three conference proceedings were achieved as a result of the analysis conducted in this chapter,

- **Chapter 4: Investigation of Real-Time Teleoperation and Telemetry Communication Latency on a Mobile End-Point:** This chapter examines how the communication latency induced from contemporary security constructs impact on real-time teleoperation and telemetry applications with mobile end-points. Findings obtained from the analysis undertaken is that security constructs contributes to the maximum distance travelled by the mobile end-point before responding to a teleoperation command.

The contribution presented in this Chapter include mathematical models to calculate the impact of secure communications on single and multiple hop propagation links with a mobile actuator and how mobile actuators contribute towards the multi-faceted problem investigated. Dissemination of two conference proceedings were achieved as a result of the analysis conducted in this chapter,

- **Chapter 5: Investigation of The Communication Link and Real-Time Task Scheduler:** This chapter examines how the real-time teleportation and telemetry messages are influenced by communication channel characteristics under ideal and non-ideal conditions and how real-time schedulers to process tasks contribute to the problems identified in Chapter 3 and Chapter 4.

Findings presented in this chapter show that the impact of a non-ideal communication link on the number of packets received over a period of time is a reduction

of up to thirty-four percent. The maximum communication range for real-time application from configuration of the transmission power, receiver sensitivity and the antenna placement is up to seventy-eight percent increase. Examination of the real-time schedulers demonstrated that the processing of periodic and periodic tasks using different real-time schedulers can impact on the latency recorded with a difference up to seven times greater recorded for the same security service selected.

Contributions presented in this chapter is the real-world analysis of the antenna placement towards the communication range for real-time applications.

- **Chapter 6: Investigation of Latency on Real-Time Teleoperation and Telemetry Applications:** This chapter examines how the communication latency induced from contemporary security constructs on the operational performance of real-time teleoperation and telemetry applications.

  Results presented in this chapter demonstrates that the impact of communication latency on the teleoperation of a mobile end-point is up to twenty-eight percent difference in the time to complete an real-time teleoperation process and the impact of latency of secure communication on the real-time telemetry link is up to sixteen times reduction in the speed of the mobile actuator in order to achieve the same number of telemetry captures as no security services. Analysis of the energy consumption of the cryptographic service, processing device and the communications also demonstrated significant impact on the real-time applications examined.

  The contribution presented in this Chapter is the analysis of how contemporary security services impact on static and mobile actuators contributes towards the multifaceted problem investigated.

- **Chapter 7: Analysis and Profiling of Cryptography:** This chapter analyses the research problem from the prospective of the cryptographic operations used by the standardised advanced encryption standard (AES) 128-bit block cipher. Profiling of the AES 128-bit block cipher is presented to ascertain its viability and the characteristics in the context of real-time teleoperation and telemetry.

  The second part of this chapter investigated the key-size used by the AES-128 block cipher with mathematical analysis based on possible attack vectors in relation to contemporary key management methods used; followed by the analysis of the implementation methods and application of cryptography in the context of real-time

teleoperation and telemetry.

Analysis of the AES-128 block cipher demonstrated that components used can increase the latency recorded up to thirty-eight percent and the number of iterations configured for the block cipher influences the cipher-text output metrics. Findings from the analysis of the key-size used for the AES block cipher is that the key length increases the time and resources required to brute force all possible cryptographic keys in a given search space at an exponential rate.

Specifications stated to overcome the problem based on the knowledge obtained from the problem analysis chapters is presented and used to derive the proposed philosophy in this thesis.

- **Chapter 8: Proposed Novel Philosophy: Cryptographic Synergy (Intrinsic):** This chapter introduces the first part of the cryptographic synergy philosophy synthesis and rationale of proposed philosophy based on the specification derived in Chapter 7. The cryptographic synergy philosophy emphasises speed as the priority whilst maintaining sufficient cryptographic strength for the specified context.

  The structural arrangement of the AES-128 block cipher is presented with two alternative structures proposed, named the Permutation Substitution Network (PSN) and the Permutation Substitution Permutation Network (PSPN). A composite concept is presented to fulfil the proposed speed-centric method by reducing the processing latency of the cryptographic process by combining cryptographic functions.

  The presentation of the Lightweight Encryption Operation Permutation Addition Rotation and Diffusion (LEOPARD) block cipher as an instance of the speed-centric method. The LEOPARD block cipher has a five per cent reduction per block call in its processing latency and energy usage when compared to the National Institute of Standard and Technology (NIST) standardised AES-128 block cipher. Dissemination of two conference proceedings were achieved as a result of the analysis conducted in this chapter,

- **Chapter 9: Proposed Novel Philosophy: Cryptographic Synergy (Extrinsic):** The second part of the cryptographic synergy philosophy emphasises on the extrinsic paradigm to maintain the privacy of the shared ephemeral cryptographic secret used for secured communications. The purpose of the extrinsic paradigm is to incorporate security services into the external application; this is achieved through the presentation of the interdependences concept that maintains the privacy

of the ephemeral shared secret dependent on internal and external factors.

The privacy-based method derived is based on the interdependency concept with a solution that makes decisions by sampling present information in order to make a future prognosis in real-time. An instance of the conceptual paradigm is achieved with the privacy cryptographic unit (PCU) that is a decision making unit to arrive at a diagnosis through the decision process derived from the expert logic to enhance the privacy of the shared secret between the communicating devices with variation of the key regeneration.

- **Chapter 10: Validation of The Synthisised Novel Cryptogrpahic Synergy Philosophy:** The novel approaches derived from the proposed cryptographic synergy philosophy are benchmarked and analysed against current philosophies in the context of the research problem of secure communication links for real-time teleoperation and telemetry.

  Analyses of the novel approaches are investigated in simulation, emulation and real-world environments to gauge the impact on the operational performance of real-time teleoperation and telemetry.

  Findings from the validation are applied to the validation scenario with benefits and limitation of the novel approaches discussed in relation to the research problem.

- **Chapter 11: Conclusion:** This chapter summarises the research undertaken in relation to the context area of real-time teleoperaiton and telemetry. Justification of the research aim and objectives specified are discussed with the findings presented from the completion of the objectives stated.

  Future research directions identified as a result of this research are presented with transferable generalised knowledge obtained in this thesis being applied into appropriate research fields. Conclusions of the findings and dissemination of the knowledge in peer reviewed publications collated throughout the duration of this research are specified.

- **References and Appendix are located after Chapter 11.**

1.11 Chapter Summary

This chapter introduced the context of real-time teleoperation and telemetry and its application in remotely operated scenarios to facilitate the completion of tasks from a remote

location. Recent incidents discussed indicate that the safety, reliability and availability could be compromised if the real-time teleoperation and telemetry is not performed in a constraint period of time. The problem statement specified that the communication medium is a security vulnerability that can influence the real-time teleoperation and telemetry data as it propagates; in addition, contemporary software security approaches were not designed for the real-time constants associated with this context.

The aim specified in this research is to provide a novel approach to symmetric cryptographic secured communication links that will have a reduced impact on the operational performance on real-time teleoperation and telemetry with a list of objectives stated. The next chapter introduces the literature review that surveys and examines the areas relevant to the problem statement specified in this chapter; an in-depth review of existing approaches and ideas presented by researcher in the field of secure communications for real-time teleoperation and telemetry is also presented.

2 Literature Review

2.1 Introduction

This chapter introduces literature relevant to the specified research problem stated in Chapter 1. The literature is categorised into three sections; the first section (2.2 to 2.13) disseminates a preliminary literature review of the individual areas that contribute towards secure communication for real-time teleoperation and telemetry. The second section (2.14 to 2.19.3) introduces a detailed literature review of the proposed research relevant to the specified research problem. The final section of this chapter (2.20 to 2.23) concludes the findings from the literature review and presents the authors' selected area of contribution with the proposition of a novel approach for secure communication links for real-time teleoperation and telemetry.

2.2 Preliminary Literature Review

The preliminary literature introduces the current frameworks, paradigms and methods applicable to overcoming the research problem. The structure of the preliminary review first examines standardised frameworks that provide recommended security services used for communication links; in addition, current methods of meeting the proposed frameworks criteria are discussed. Regulations and applications of teleoperation and telemetry are stated; followed by a discussion of the preliminary literature is presented.

2.3 Standardised Frameworks for Secure Communication

2.3.1 X.800 Framework

The X.800 framework is a standardised security architecture designed for the Open System Interconnection (OSI) network model (X.800 1991). The framework provides recommendations of general security architectures and the application of these recommendations. Security vulnerabilities specified in this standard are categorised from the viewpoint of passive and active attacks; the definition of a passive attack in reference to the X.800 standard is a non-modification to any information contained in the system where neither the operator nor the state of the system is changed; instances of passive attacks specified in this standard include tapping of the communication medium in order to observe data transmission as it propagates on the network.

An active attack is stated as an alteration of information contained in the system or changes to the state or operation of the system; attacks that are classified as an active attack in the X.800 framework are listed as:

- **Masquerade attacks:** where an entity pretends to be a different entity; replay attacks when a message or part of a message is repeated to produced an unauthorised effect;
- **Modification of messages:** where the content of the data transmitted is altered without detection and results in unauthorised effects;
- **Denial of service (DoS) attack:** when an entity fails to perform its proper function or acts in a way that prevents other entities from performing their proper function.

The X.800 framework specifies the application of the security services at each layer of the OSI model and enables practitioners to ensure appropriate security services are deployed for the layer to mitigate the aforementioned attacks identified. As the specified research problem investigates the data-link communication between the transmitter and receiver for real-time interoperation and telemetry, the recommended services specified in the X.800 standard is connection and connectionless confidentiality; the mechanism recommended to achieve this service is an encipherment mechanism.

2.3.2 X.509 Framework

The X.509 is a standardised framework for the use of public-key, attribute certificate and authorisation service in network systems (X.509 2014). Frameworks presented in the X.509 standard discuss the use of public key infrastructures (PKI) to provide confidentiality, integrity and authentication of data between the transmitter and receiver with asymmetric cryptographic approaches. Components that are required for the implementation of the PKI include digital certificates, certificate authority (CA) and asymmetric keys.

The digital signature binds the public-key material and the public-key certificate through a one way hash function and appends the hashed output to the message that was encrypted with the private key of the transmitter device before it is propagated to the receiver device. The recipient of the message verifies the validity of the signature by decrypting the signature appended to the message with the public key and passing the received information through an identical one-way hash function; the output is compared against the received hashed signature to validate if a legitimate device sent the message and determines whether to process the message based on the check of the signature. Result of the approach specified in the X.509 framework demonstrates the application of confidentiality, integrity and authentication to a communication link.

2.3.3 Section Summary

This section of the preliminary literature review introduced frameworks that provide recommendations for the controls required to achieve secure communications based on spe-

cified attack vectors. Analysis of the X.800 in relation to the problem scenario investigated in this thesis showed that the requirement for confidentiality and integrity services to communicated data to reduce the risk of the stated attacks compromising the communications used to facilitate in real-time teleoperation and telemetry applications. The next section investigate the contemporary secure communication paradigms used to achieve secure communications.

2.4 Contemporary Secure Communication Paradigms

2.4.1 IEEE 802.1AE MACSec Framework

The Media Access Control Security (MACSec) is an IEEE 802.1AE standardised framework for authentication and encryption of data packets between two devices (IEEE 2006). The MACSec protocol was designed to maintain correct network connectivity and services, isolation of DoS attack and secure communication between networks. The MACSec protocol was designed to provide confidentiality and integrity of data over a connectionless point to point symmetric communication link.

The default cryptographic construct specified to provide confidentiality and integrity to the packetised data is the Advanced Encryption Standard Galos Counter Mode (AES-GCM) 128-bit block cipher. The packet structure of the MACSec protocol comprises of a source and destination address for the MAC address fields, the medium access control protocol data unit encapsulates the MACSec security tag, secure data of the user and integrity check value.

Advantages of the MACSec protocol is the application of Authenticated Encryption with Associated Data (AEAD) constructs to provide confidentiality, integrity and authentication of associated data between each individual link on the network; however, the limitations of the proposed MACSec protocol is the use of the GCM-128 as the security vulnerabilities associated with this construct as specified in Section 2.6. In the application of the secured communication links for real-time teleoperation and telemetry, it is unknown what the impact of the GCM-128 cipher on the operational performance of the system and requires further analysis in the main section of the literature review.

2.4.2 IPSec Framework

The Internet Protocol Security (IPSec) is an Internet Engineering Task Force (IETF) Request For Comments (RFC) 6071 framework that specifies a suite of protocols to enable hosts to communicate in a secure manner (Clayton & Pandya 2016). IPSec was designed for the network layer of the OSI model with consideration for the data link layer, trans-

port layer and application layer. IPSec is designed to prevent attackers by protecting data between peer to peer communications, host to network gateway and gateway to gateway communications.

IPSec is comprised of three areas; the authenticated header, encapsulating security payload and internet key exchange. The authenticated header provides integrity protection of the payload of the message (Frankel et al. 2005). The encapsulating security payload adds a header and a trailer to the message before the encryption of the payload is performed as a means of confidentiality; an option of an integrity check is outlined with the attachment of the authenticated information field to store the calculated message authentication code (MAC) check. Cryptographic algorithms selected for encapsulating the security payload include AES-GCM, AES Counter mode with Cipher Block Chaining (CCM) and Triple Data Encryption Standard (3DES) operating in cipher block chaining mode (CBC) for confidentiality. Integrity algorithms presented are the Hashed Message Authentication Code (HMAC) with the Secure Hash Algorithm One (SHA1) 96-bit variant, AES-XCBC-MAC-96-bit variant and HMAC with the Message Digest Five (MD5) 96-bit variant. The internet key exchange was designed to create and manage security associations to preserve confidentiality, integrity and authentication (C.I.A) of the communication link through a variety of implementation methods (Frankel et al. 2005).

IPSec segments the confidentiality and integrity from the authentication of packetised data by the option of encrypted security payload (ESP) and authenticated headed (AH). The ESP is configurable in two different modes of operations, the encryption of the payload only and the encryption with authentication. Operation of the ESP encapsulates the packetised data with the addition of a header to store the security parameters and the trailer for the authenticated data. The AH is used to authenticate the packet between the transmitter and receiver device; this is achieved with the attachment of the hashed output of the IP fields of the packet and is attached to the header of the message.

Ciphers used by the IPSec protocol such as 3DES are not best suited for the context of real-time teleoperation and telemetry, this is because of the known security vulnerabilities associated with this cipher with meet-in-the-middle, known-plaintext and chosen-plaintext attacks and reduces the security to 112-bits and 80-bits (Merkle & Hellman 1981, Oorschot & Wiener 1990, Barker 2016*a*); furthermore, the confidentiality, integrity and authentication methods are achieved through separate algorithms and may not be suited to real-time systems with constrained resources (i.e. storage and memory).

2.4.3 Section Summary

Examination of the contemporary security services used for secure communication shows that MACSec and IPSec were not designed to conduct the confidentiality and integrity services as one operation as the standardised version of the protocols specify the ESP and AH can be enabled individual services. Newer paradigms have incorporated the ESP and AH concept used by the investigated protocols as a compulsory requirement in order to provide a complete secure communication link through confidentiality, integrity and authentication with the presentation of the authenticated encryption with associated data (AEAD) paradigm; this is reflected with the incorporation of the standardised AES-GCM-128 and AES-CCM-128 variants used by the IPSec protocol.

2.5 Authenticated Encryption with Associated Data Constructs

The IETF RFC 5116 outlines the AEAD paradigm as a form of encryption that provides confidentiality for the plain-text with the ability to check the integrity and authenticity of associated data (McGrew 2008). The AEAD approach is selected as the modern paradigm to provide C.I.A with the Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) cryptographic competition requesting new submissions of AEAD constructs (Bernstein 2016). Established AEAD paradigms that are currently used are the standardised Galois counter mode (GCM) and Counter with cipher block chaining message authentication code (CCM); newer implementations of the AEAD design that focused on energy conservation are EAX-Prime and Tiny Authenticated Encryption with Associated Data (TinyAEAD) (Dworkin 2004, 2007, Moise et al. 2011, Adekunle & Woodhead 2012).

GCM is a national institute of standards and technology (NIST) standard block cipher mode for AEAD (Dworkin 2007). The GCM construct is a two pass AEAD construct that undertakes confidentiality in one pass and integrity and authentication for the other pass with separate encryption keys. The components used in the design of the GCM construct are a secret key based on the bit length of the block cipher AES 128 and an initialisation vector (IV) size no greater than 64-bits for confidentiality. The plain-text input of the packet and additional authenticated data that is used for the integrity and authentication tag, known as the Galois message authentication code (GMAC) using multiplication fields of 2^{128} (aka Galois fields). Counter mode is selected as the block cipher mode of operation for GCM. The output from the GCM block cipher is the cipher-text which is the encrypted plain-text and the authentication tag.

The software implementation of GCM can use pre-computed multiplication tables to enhance the operational performance at the expense of 65,535 bytes of memory storage.

Hardware implementation of GCM does not have to trade memory for operational performance (NIST 2007) and the confidentiality and integrity and authentication streams are processed in parallel.

Security analysis of GCM conducted by Ferguson indicates that the authentication method used by GCM is susceptible to two security weaknesses; the short sized authentication tag is susceptible to successful forgery of the authentication tag and enables the attacker to obtain the authentication key (Ferguson 2005). Further research has been conducted based on Fergusons authentication key attack strategy with successful reduction of the security level of the GMAC authentication tag with 62-67-bits security level for a 32-bit tag and a 70–75 bits security level for 64-bit tag; which is below the NIST requirement of a 112-bit security (Saarinen 2012, Zhu et al. 2013, Yap et al. 2014, Mattsson & Westerlund 2015).

CCM is a NIST standardised AEAD design created by Whiting et al; (Dworkin 2004). The CCM construct uses AES 128-bit variant for confidentiality and a MAC for the integrity and authentication using a two pass method. The input for the operation requires an encryption key, a number only used once (aka nonce) to generate a different cipher-text output and the additional authenticated data for the message authentication tag. Security analysis undertaken by Rogaway and Wagner identified limitations with the CCM construct (Rogaway & Wagner 2003). The limitations discussed include efficiency issues as CCM is not an on-line block cipher and requires knowledge of the plain-text length and the associated data before it can proceed with encryption; parametrisation and complexity subtleties of variable length authentication tags that can impact the security of the approach if it is not implemented carefully as an attacker can forge small variable length authentication tags.

EAX-prime is an American National Standards Institute (ANSI) C12.22 standard cipher designed by Moise et al;. The EAX-prime cipher was designed to provide protection for small embedded devices for varying message sizes (Moise et al. 2011). EAX-prime uses a confidentiality-then-integrity framework to provide AEAD to packetised data. The operation of the EAX-prime cipher is categorised into three sections which are the encryption of the nonce, the confidentiality track for the data and the authentication track for the associated data.

Security analysis undertaken by Minematsu et al; demonstrates that EAX-Prime has known security vulnerabilities with forgery attacks, chosen plain-text distinguishers and chosen cipher-text plain-text recovery attacks which can be achieved using short packet size lengths of 16 bytes or less (Minematsu et al. 2012).

TinyAEAD is a block cipher AEAD operation designed by Adekunle and Woodhead (Adekunle & Woodhead 2012). The design of the TinyAEAD construct was developed for scenarios that have energy and memory constraint devices (e.g. wireless sensor networks). TinyAEAD is based on the derived Joint Cypher Mode (JCM) framework that uses a generic composite paradigm to enable individual selection of the confidentiality and authentication schemes. The JCM framework uses confidentiality-then-integrity for the authenticated encryption scheme; however, transposing the plain-text and cipher-text string positions changes the construct to an integrity-then-confidentiality construct.

Adekunle and Woodhead JCM framework is advantageous as the generic composition paradigm used can be applied for the design of appropriate symmetric encryption schemes and message authentication schemes independently and can be combined to derive new AEAD construct designs. The components specified in the JCM framework for confidentiality are a cryptographic nonce (number only used once), a salt to modify the ciphertext generated by the confidentiality algorithm in order to mitigate pre-computation attacks and the plain-text data. Items classified for the integrity scheme include the initialisation vector (IV) which is generated per data frame processed for confidentiality and integrity schemes, header, cypher-text data and the metadata.

The TinyAEAD approach allows the practitioner to adjust the operation of the AEAD scheme through multiple parameters with underlying block ciphers lengths of 64-bit or 128-bit operation and the number of rounds selected for the block cipher. The reduction of the number of rounds used by the block cipher increases the processing speed of the construct. A schematic of the TinyAEAD construct is presented in Figure 2.1.

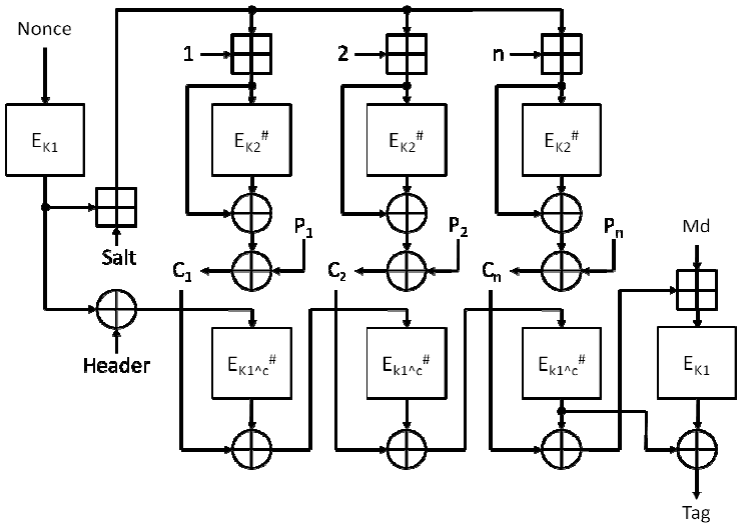


Figure 2.1: Schematic diagram of TinyAEAD construct using associated data inclusive integrity configuration (Adekunle & Woodhead 2012)

The mechanism of the TinyAEAD scheme is a two pass construct that processes the confidentiality and integrity separate. Initialisation of the construct passes the number only used once (NONCE) through a block call of the underlying block cipher; The output of the encryption call is used differently for the confidentiality and integrity tracks; the confidentiality track uses an addition of the encrypted nonce with a salt value to prevent against pre-computed attacks; whilst the associated data (the header) is exclusive or (XOR) with the NONCE value for the integrity track in order to protect the initial value passed into the construct.

Operation of the confidentiality track for the data uses counter mode to add an incremented value to the initial input of the block cipher; the output of the addition with the counter value is copied and used with the XOR logic gate at the output of the block to screen the cipher-text. The plain-text and cipher-text positions can be transposed to operate in cipher-feedback mode or plain-text feedback mode. The output of the confidentiality track per round is XOR'd with the output of the integrity track of the associated data per block round call; the value obtained from the XOR screen is then feedback into the next round of the integrity; this process is repeated for the number of rounds used by the underlying block cipher until the final round call. The final round of the integrity track combines the metadata to the output of the XOR screen of the previous round before passing the data through the final integrity round, the output is XOR'd with the unscreened cipher-text of the final round to obfuscate the attacker from deriving the values used for the final round XOR screen.

Benchmark comparative analysis conducted by Adekunle and Woodhead demonstrates that the TinyAEAD construct consumed the least processing and integrity check latency in comparison to CCM and EAX-Prime and had the largest processing throughput and processing efficiency for the sampled byte sizes. This was achieved through the reduction of the number of iterations used by the underlying block cipher (AES-128) as a measure of reducing the energy consumption of the cryptographic operation.

2.5.1 Section Summary

Presentation of the AEAD paradigms investigated in this thesis demonstrate two design considerations are proposed for contemporary AEAD paradigms with standardised AEAD constructs focused on the security, whilst TinyAEAD prioritised energy conservation as the main design consideration; this raises the question to which AEAD security service is best suited for the context of real-time teleoperation and telemetry application and their impact on the research problem investigated.

Analysis of the AEAD construct presented shows that the cipher selected to provide con-

fidentiality and integrity services is the AES-128 block cipher; this raises the question of what are the alternative ciphers available to provide the require services specified from the X.800 framework. The next section introduces the contemporary block cipher designs derived to achieve confidentiality and integrity services.

2.6 Contemporary Block Cipher Designs

This section introduces the contemporary block ciphers that are used to provide confidentiality and can be integrated with the AEAD constructs identified in the aforementioned section. The block ciphers examined in this thesis are derived from the AES competition (Nechvatal et al. 2000). The goal of the Advanced Encryption Standard (AES) competition was to specify "an unclassified, publicly disclosed encryption algorithm capable of protecting sensitive government information well into the next century" (NIST 2014).

The AES competition evaluated entrants based on three individual criteria which are the security of the block cipher, cost of operation and algorithm implementation using key bit-sizes of 128, 192 and 256-bits. Cipher entrants for the AES competition consisted of a combination of block and stream cipher with entrants including RC6 and MARS ciphers. Three block ciphers finalists Rijndael, Serpent and Twofish of the competition are reviewed in this section.

The Rijndael block cipher is a symmetric key substitution permutation network (SPN) block cipher developed by Daemen and Rijmen and was selected as the winner of the NIST AES competition (Daemen & Rijmen 2002). The SPN structure consists of three operations; the substitution-box that replaces byte value input with a new byte value output to create confusion, the permutation is achieved through shiftrows and mixcolumns to offset the byte position of the input message and mix the data from each column to create diffusion. The number of iterations used by the Rijndael block cipher is set to ten rounds.

The selection of the Rijndael block cipher as the winner of the AES competition was due to its versatility and adequate level of security, flexible implementation in software and low cost of operation; this is further reinforced in section “block cipher design and contemporary secure communication paradigms” as the majority of the proposed schemes and ciphers incorporate the de-facto standardised AES-128 block cipher; furthermore, in the context of a secure communication link for real-time teleoperation and telemetry systems.

The flexible implementation in software and low cost of operation suggests this cipher could be a suitable candidate for the application of a secure communication link for real-

time teleoperation and telemetry; however, further investigation of the Rijndael block cipher is required in the literature review to ascertain what existing research has disseminate on the suitability of this as a suitable cipher scheme.

The Serpent block cipher is a SPN structure design presented by Anderson et al; and was the runner up of the AES competition (Anderson et al. 1999). The Serpent block cipher operates on four 32-bits of data in parallel to generate a block size of 128-bits. Eight substitution boxes consisting of four by four bit-sizes are used on the 32-bits data inputs; logical operators are used to create permutation through rotations, shifts and XOR. Thirty two rounds are selected for the serpent block cipher.

The security service of the Serpent block cipher was rated as strong by the NIST in comparison to Rijndael medium rating based on the number of reduced rounds-variants of the block cipher (e.g. differential cryptanalysis and meet-in-the-middle attacks); however, the implementation and cost of operation was not comparable in software against the Rijndael block cipher as it was reported that the Serpent block cipher required 126,074 clock cycles to compute in comparison to the 9,464 clock cycles processed by the Rijendal block cipher on an 8-bit processor.

This could be problematic as a component selected for secure communication for real-time teleoperation and telemetry as the instruction cycles required to compute the block cipher is up to thirteen time greater than the Rijndael cipher; consequently, this means the computational device would have more instruction to compute per block cipher call; this could also transfer to additional latency and increased energy consumption.

Twofish is a block cipher designed by Schneier et al; that uses a sixteen rounds Feistel structure (Schneier et al. 1998). The substitution box is selected to generate confusion with addition, XOR, rotation, maximum distance separable matrices and pseudo-Hadamard transforms are used for permutation.

The Twofish block cipher was ranked third place behind Rijndael and Serpent in the AES competition; similar to Serpent block cipher, Twofish security service was rated a strong by NIST in comparison to Rijndael medium rating based on the number of reduced rounds-variants of the block cipher; however, the performance of the algorithm and the key scheduler were reasons to why this was not selected as the winner of the competition.

The performance aspect could also contribute towards performance issues of real-time teleoperation and telemetry devices in terms of network and hardware performance in terms of how much data is processed in a given time and the latency required to process

the cipher; this could be problematic in real-time systems that have stringent deadlines in safety critical systems as specified in Chapter 1, sections 1.1, 1.2 and 1.4.

Alternative structural arrangement of the SPN design paradigm was presented by Sugita et al; during their cryptanalysis of word orientated block ciphers using differential, truncated differential, impossible differential cryptanalysis. The presented alternative structure was the permutation substitution network (PSN) structure (Sugita et al. 2000); however, they did not extend this to a full and piratical block cipher.

The arrangement of the SPN structure follows a linear transformation layer, non-linear transformation layer and a linear transformation layer; whilst the PSN design follows a non-linear transformation layer, linear transformation layer and a non-linear transformation layer. Findings presented by the authors demonstrate that the PSN is not at a disadvantage against SPN with differential and truncated differential cryptanalysis.

Dunkelman et al.; introduce a variation of the Even-Mansour cryptographic scheme with a permutation addition network (PAN) scheme know as the Addition Even-Mansour (AEM) (Dunkelman et al. 2012). The proposed scheme replaces the exclusive-or (XOR) logic operators with modular additional functions. Analysis of the AEM scheme by Dunkelman et al.; state that lower bound security proof holds for this scheme against differential attacks and slide-attacks.

2.6.1 Section Summary

Literature presented in this section examined the AES block cipher finalist selected by the NIST. Review of the ciphers presented shows that the Rijndael block cipher is the best suited design as its flexible implementation in software and low cost of operation in comparison to other cipher schemes presented appears to make it a suitable candidate in the context of real-time teleoperation and telemetry applications; however, it is difficult to ascertain its suitability without further investigation to context investigated in this thesis. Additional consideration as a result of the aforementioned review conducted is the consideration of newer lightweight block cipher schemes that were designed for constraint devices; as the scope of this research is focused on constrained embedded devices, the next section of this preliminary literature review investigated lightweight block ciphers.

2.7 Lightweight Ciphers

This section of the literature review presents the contemporary lightweight block ciphers proposed by researchers; the areas analysed in this section are the design consideration of the proposed solutions in relation to the research scope and the implementation method

selected.

2.7.1 PRESENT Block Cipher

The PRESENT block cipher is presented by Bogdanov et al; as an ultra-lightweight block cipher (Bogdanov et al. 2007). The authors' state that current cryptographic primitives are unsatisfactory for resource-constraint environments in terms of energy and power consumption. The solution presented is the PRESENT block cipher, a hardware optimised SPN structure with an 80-bit key length designed with the consideration of energy and power constraints without compromising security. Analysis of the PRESENT block cipher was undertaken with performance analysis of present against AES-128, DES and Camellia hardware implementations. Results show that PRESENT is comparable to the contemporary approaches selected with a reduced area required to implement.

2.7.2 Piccolo: An Ultra-Lightweight Block Cipher

Shibutani et al; introduce Piccolo, an ultra-lightweight block cipher (Shibutani et al. 2011). The authors' state that low resource devices such as radio frequency identification (RFID) and wireless sensor network are becoming more frequently used and the requirement of lightweight cryptography to secure the communication and meet the constraints associated with this environment. The Piccolo block cipher is presented by the authors' as the solution to overcome and meet the limitations specified. The design of the piccolo block cipher is a hardware implementation that concentrates on a secure and compact design that uses a generalised Fiestel structure with key lengths of 80-bits and 128-bits.

Tests conducted compared the Piccolo variants against existing algorithms that include AES-128, PRESENT and DESXL. The comparison of the algorithms was achieved in hardware implementation with focus on the number of cycles used, energy per bit and area required to implement. Results show that the Piccolo block cipher is comparable to existing approaches in hardware for the same number of iterations selected.

2.7.3 KLEIN: A New Family of Lightweight Block Ciphers

Gong et al; introduce a new family of lightweight block ciphers for resource constrained embedded systems (Gong et al. 2012). The problem specified by the authors' is the requirement of resource efficient cryptography for embedded systems to reduce the cost of operation and preserve the limited energy supply. The KLEIN block cipher suite was proposed as a software efficient block cipher to overcome the aforementioned problem specified. Implementation of the KLEIN block cipher suite is a SPN structured block

cipher with 64-bit, 80-bit and 96-bit length key variants.

Two tests were presented to validate the KLIEN block cipher variants against existing approaches that include AES-128 and PRESENT block ciphers on an 8-bit ATMEGA128L microcontroller and a 16-bit TelosB microcontroller and a comparison of implementation in hardware. Items examined for the software test was the processing speed per block call and the memory usage; the hardware test examined the area required to implement the block ciphers.

Results presented show that the KLIEN 64-bit key variant recorded a reduced latency in comparison to AES-128 on the ATMEGA128L only whilst a higher latency was recorded for all KLIEN variants on all other platforms; however, KLIEN performance in comparison to PRESENT show a considerable improvement in software. Hardware comparison shows the KLIEN variants required less area than AES-128 with a gate equivalent of 1365 recorded for KLIEN in comparison to AES-128 of 2400 gate equivalent; however, the PRESENT block cipher had the smallest impact on the area required in comparison to KLIEN and AES with a gate equivalent of 1075 recorded.

2.7.4 The SIMON and SPECK Lightweight Block Ciphers

Beaulieu et al; presented the SIMON and SPECK lightweight block ciphers (Beaulieu et al. 2015). The aim of the research discussed by the authors' was to design a lightweight block cipher to overcome the needs of computational limited devices and provide flexibility of the implementation of the lightweight block cipher with the authors' specifying that contemporary lightweight block ciphers do not consider flexibility.

The solution presented in their research is the SIMON and SPECK Feistel structured lightweight block ciphers; the presented approaches enable variable block and key size implementations to meet the requirements of the scenario presented. The authors' state the SIMON block cipher is a hardware variation and SPECK is a software variation. Limitation of the SIMON block cipher is the increased number of rounds required to overcome the weak cryptographic output, whilst the SPECK block cipher is not as efficient as the SIMON block cipher due to the propagation of the carries from the ADD logic function. No real world testing is presented in this paper.

2.7.5 RECTANGLE: A Bit-Slice Lightweight Block Cipher Suitable for Multiple Platforms

The Rectangle block cipher is presented by Zhang et al; as a suitable block cipher for multiple platforms (Zhang et al. 2015).The problem presented by the authors' is that

small embedded devices have strong cost constraints in terms of energy consumption of hardware and low memory and the requirement of providing cryptographic protection of this application. The proposed solution presented in this research is the Rectangle block cipher. Rectangle uses a SPN structure with a bit slicing technique to facilitate lightweight operation with claims of a low cost of implementation in hardware and competitive performance in software.

Tests undertaken benchmarked Rectangle 80-bit and 128-bit variations against existing lightweight block ciphers of AES-128, PRESENT and Piccolo in VHDL and in C++ to represent hardware and software approaches. Result of the hardware analysis shows Rectangle is comparable in the area use and throughput measurement recorded against existing approaches. Analysis of software based implementation on an Intel 2.5 GHz i5 processor shows that the number of cycles required for one block encryption call and multiple parallel encryption per cycle is reduced in comparison to PRESENT and Piccolo.

A final test of the performance of the software variant of the Rectangle block cipher on an ATtiny45 8-bit microcontroller analysed the key management approaches of static, fixed and on-the-fly key scheduling. Implementation was achieved in assembler language with the encryption, decryption and key schedule are one round unrolled. Results show that the static key method has the least number of cycles for encryption and decryption but required the most memory to implement, whilst on-the-fly keying has the smallest code size but highest number of cycles to encrypt and decrypt with the key scheduler.

2.7.6 Section Summary

Examination of the literature presented for lightweight cryptographic ciphers demonstrates that the main design considerations is focused on the energy conservation. The ciphers presented in this section utilise hardware implementation method over software variants; this indicates that the implementation method may have an influence on the real-time teleoperation and telemetry communication but may require further investigation in order to ascertain if the security service selected has an impact on the context investigated in this thesis.

Analysis of the findings presented in the literature conducted in this section does not appear to explicitly demonstrate the resilience of the proposed lightweight cipher schemes against known cryptanalysis techniques used to identify weaknesses with ciphers; therefore, the next section introduces established cryptanalysis methods used to analyse cipher designs.

2.8 Cryptanalysis Methods

This section of the background literature introduces the contemporary cryptanalysis techniques used to analyse block and stream cipher designs; cryptanalysis methods examined include linear and differential cryptanalysis, frameworks for algebraic fault attacks and slide attacks.

Linear cryptanalysis is a probabilistic statistical cryptanalysis technique developed by Matsui and Yamagishi; to identify the relationship between the input and the output of a block cipher algorithm and derive linear equations that yields information about the bits of the key used to encrypt them (Matsui 1992). The methodology presented by the authors constructs linear expressions to relate the known plain-text input to the cipher-text output and the key string used for encryption. An instance of a linear expression is presented in Formula 1.

$$P[i_1, i_2, ...i_a] \oplus C[j_1, j_2, ..., j_b] = K[k_1, k_2, ..., k_c] \quad (1)$$

Formula 1. Linear expression for a given cipher algorithm (Matsui 1992)

The linear approximations determine if the known plain-text input and the cipher-text output combination produce a bias in the result (e.g. greater or less than $\frac{1}{2}$ probability); the further away the bias is from a half probability, the more successful the linear approximation is in deriving the key bits used by the block cipher; this method is also referred to as a parity check to determine the probability of a non-linear output. This cryptanalysis method was successful against block cipher designs that used linear components to generate a cipher-text output; instances include the data encryption standard (DES) and the fast data encryption algorithm (FEAL) (Matsui 1992).

Limitations of the linear cryptanalysis approach is the number of known plain-text and cipher-text pairs required to derive the correct linear approximation for the key as Matsui computed 2^{43} pairs for DES; this translates to a file size of four terabytes of known plain-text and cipher-text pairs that requires an eight byte input; consequently, this is not a feasible form of attack as the probability of an attacker attempting four terabytes of plain-text to derive the key value is remote and the increased number of rounds used by a cipher can mitigate these forms of attacks as presented.

Differential cryptanalysis follows a similar concept to the linear cryptanalysis as it is a probabilistic statistical cryptanalysis methods. The differential cryptanalysis was proposed by Biham and Shamir and focused on the differences when a known plain-text is modified and how this impact the corresponding cipher-text output (Biham & Shamir

1991). To measure the differences in the values of the XOR values of the plain-text and cipher-text; the mathematical notation is presented in Formula 2.

$$\Omega_x = (X_1 \oplus X_2) \Rightarrow \Omega_y = (Y_1 \oplus Y_2) \tag{2}$$

Formula 2: Differential cryptanalysis of input differences (denoted by X) and the output differences (denoted by Y) (Swenson 2008)

Analysis of the differences is undertaken through the investigation of the bias of the difference between the known plain-text input and the cipher-text output; however, the objective of this cryptanalysis is to identify areas of non-random behaviour within the block cipher and use the bias of the behaviour to derive the know cryptographic key used. Limitations of the differential cryptanalysis method are inherited from the linear cryptanalysis as the number of known plain-text and cipher-text pairs required to derive the cryptographic key used and can be mitigated with the increased number of rounds used by the cipher; in addition, as the linear and differential methods are probabilistic approaches, both linear and differential attacks assume that the attacker has prior knowledge of the mechanism of the cipher and that the attacker has the ability to manipulate the plain-text input into the cipher (Swenson 2008); this may not be applicable in the context of real-time teleoperation and telemetry systems as devices could be mobile or placed out of the attackers range and the configuration of the cipher may not be in its standardised form or is not a standardised implementation; resulting in incorrect configuration of the attackers cipher for the attack.

The slide attack is cryptanalysis technique implemented by Biryukov and Wagner and built upon Grossman and Tuckermans initial attack of block ciphers with cyclic key schedulers (Biryukov & Wagner 1999). The concept of the attack is to negate the number of rounds used by a cipher to encrypt data which mitigates differential attack vectors by analysing the key scheduler of the cipher and exploiting weaknesses associated with the key scheduler and general structure of the cipher; this is achieved as the cipher is viewed as a permutation with a fixed secret key value.

Application of the slide attack is undertaken with known plain-text or chosen plain-texts and initiates the periodic nature of the key scheduler; as the cipher is viewed as a permutation function with a fixed key value, the known plain-text and related cipher-text pairs are used to extract the secret key value by identifying slid pairs of plain-text and cipher-texts that fulfil the criteria of $F(P) = P'$ and $F(C) = C'$. The complexity of the attack against bit-block ciphers has been stated as $0(2^{n/2})$ and $0(2^{n/4})$ for a feistel structure. Prevention against a slide attack is achieved by removing the self-similarity of the iterative process

through the inclusion of iterative counters or fixed random constants to remove similarity of the cryptographic process per round.

A side-channel attack is an attack vector that acquires information based on physical implementation of the cryptographic operation. The NIST FIPS-140 standard identified that a side channel attack is generally categorised into three groups; control over the computational process, the way of accessing the model and the method used in analysis process (Zhou & Feng 2005). Instances of side-channel attacks include timing attacks where the attacker analyses the variation in time to complete a cryptographic operation in order to derive the users secret information to power analysis of the cryptographic process to profile the how much power the functions of the cipher consume and derive cryptographic key of the system. Alternative side-channel attacks identified in the NIST FIPS-140 standard were acoustic attacks, visible light attacks, error attacks, cache based attacks, scan based attacks and frequency attacks.

Fault attacks observe hardware faults and errors during cryptographic operation and the impact of intentionally corrupted input data on the attacked module. The procedure for this type of side-channel attack is to first inject a fault into the system based on the hardware; once the fault has been injected, the final step exploits the unexpected behaviour of the hardware in relation to the fault injection. Implementation of fault attack can be achieved using algebraic fault analysis with differential fault analysis; this approach aids cryptanalysis by identifying the difference in cipher-text output from the system under normal operation conditions and abnormal operation condition.

Side-channel attacks presented target the physical properties of the system in order to obtain information about the cryptosystem; this differs from the aforementioned methods presented in this section that concentrate on mathematical methods to approximate or derive bit values of the cryptographic key; however, limitations of the side-channel attacks is the requirement of the attacker to physically obtain the device with the cryptographic system stored in order to conduct the attack; therefore, the attacker has an infinite amount of time to profile and break the cipher and the defender would be aware that the node has been physically compromised and would likely change the cryptosystem parameters, cipher or hardware selected to account for possible side-channel attacks. In the context of the research scope; the physical compromise of the transmitter or receiver device is outside the scope of this research as the focus is on the secure communication link between the two communicating entities.

2.8.1 Section Summary

This section introduced a variety of approaches to demonstrate the resilience of a cipher designs. Examination of the techniques presented in this section indicates that the linear and differential cryptanalysis are the most commonly used techniques to analyse a cipher; however, contemporary literature investigated up to this point does not explicitly demonstrate the viability of lightweight cipher designs unlike the AES-128 NIST standardised block cipher. This further raises the question of the types of key management methods and their applicability to the cipher resilliance to known cryptanalysis techniques; therefore, the next section investigates the symmetric and asymmetric key management techniques.

2.9 Symmetric and Asymmetric Key Management

The NIST 800-57 standard specifies the recommendation of key management (Barker 2016*b*); components discussed in the standard are key exchange, key agility, key storage and key use. The two instances of key management techniques that are discussed in this standard are symmetric key management and asymmetric key management techniques. The requirement for symmetric key management is to generate and establish cryptographic keys for confidentiality, integrity and authentication purposes similar to that in the X.800 standard, whilst asymmetric key management approaches are more commonly found in reference to the X.509 standard for digital signatures.

The Wired Equivalent Privacy (WEP) was the standardised 802.11 security measure for wireless networks (IEEE 1997). WEP selected the stream cipher Rivest Cipher four (RC4) to provide confidentiality to plain-text messages transmitted across a wireless link. The key generation scheme of WEP used key sizes of 40-bit and 104-bit key length with a 24-bit initialisation vector attached to prevent repetition from the output of the RC4 stream cipher and can use up to four pre-computed cryptographic keys that rotate after a set number of times a key is used or use a static key implementation.

A weakness identified with the WEP key management mechanism is that brute force attack can be undertaken against the specified 40-bit key size variant. The size of the initialisation vector has been noted as a vulnerability as the 24-bit size limits the number of streams of the key to 2^{24} as the initialisation value is transmitted in plain-text to the receiver node, this results in the reuse of a previous key stream which enables an attacker to conduct a passive attack to collate the initialisation vectors used to derive the cryptographic key (Borisov et al. 2001).

Asymmetric key management methods are an alternative to static and pre-computed key approaches used in symmetric key systems. The Rivest-Shamir-Adlemen (RSA) crypto-

graphic key management system is a public-key cryptosystems (Rivest et al. 1978). The principle of the key generation technique used by RSA is based on prime numbers and modular arithmetic to derive the public and private cryptographic key used. Limitations of this approach are the large prime numbers required to be chosen in order to prevent brute force attacks that may not be best suited for the context of real-time teleoperation and telemetry systems as a result of computational and time constraints may impact on the latency generated to process the mathematical operation in comparison to the static and pre-computed symmetric key methods presented with WEP.

Literature presented by Coppersmith et al; shows that the RSA cryptographic key generation technique is susceptible to brute force attacks when the public encryption key is small or partial knowledge of the secret key is acquired (Coppersmith et al. 1996); alternative attack methods such as Wiener's attack uses continued fraction method to find the private key when the size of the private key is small (Blomer & May 2004); this is because the Wiener method observed that information encoded in the public exponent might help to factor the primes of an equal-bit size used for the RSA keys; the authors state that Wiener showed that every public exponent that corresponds to a secret exponent yields a factorisation of the modulus in time polynomial; thus, the authors extended the Wiener attack that leads to a much larger class of secret keys which are insecure; consequently, this increases the probability of compromising the secret keys used for secure communications.

The Diffie-Hellman (DH) key exchange protocol was derived by Whitfield Diffie and Martin Hellman as an IETF RFC 2631 standard symmetric cryptographic key exchange protocol (Rescorla 1999). The design of the DH key exchange protocol was derived as a key exchange protocol to generate a new secret between devices over an unsecure public communication link. The mechanism used by the DH key exchange protocol uses modulus and exponential arithmetic to derive the same secret value used by communicating nodes in order to obfuscate attackers from intercepting the key used for secure communications over an unsecure communication link and intercept and receive communicated data between the transmitter and receiver. In the context of real-time teleoperation and telemetry systems; the application of the a DH key exchange may not be best suited as a result of the real-time constraints associated with the problem scope specified in Chapter 1, section 1.5 and shares similar limitations as the RSA key management method.

Kerberos is a RFC 4120 standard computer network authentication protocol designed by the Massachusetts Institute of Technology as an approach to authenticate client and server application for symmetric and asymmetric cryptography methods (Neuman et al. 2005). The mechanism used by Kerberos to achieve authentication between the client and server is achieved by the three exchange processes between the ticket generator service, the

authentication server and the client/server exchange. Figure 2.2 illustrates the exchange process used by Keberos to achieve client/server authentication.

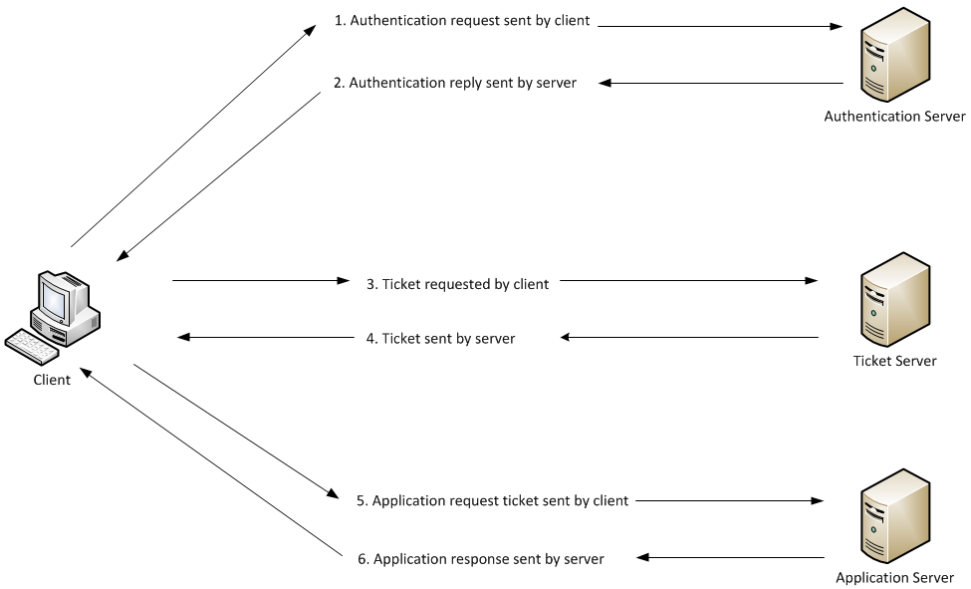


Figure 2.2: Kerberos authentication protocol between client/server applications on enterprise networks adapted from (Al-Janabi & s. Rasheed 2011).

The operation of the Kerberos authentication protocol uses asymmetric cryptography to authenticate the client device to the application server through the use of shared secrets to verify the identity of the client or server through the confirmation of the communicating entity that knows the secret; this is achieved using a symmetric key method to ensure authentication is achieved as the single key must be capable of encryption and decryption; therefore, both parties are mutually authenticated if the encrypted information received by the device can be decrypted and thus achieve trust on an untrusted network. The process of achieving secure communications with Kerberos is achieved in three sections as outlined in Figure 2.2; the authentication server, the ticket server and the application server.

The client initiates the Kerberos protocol with a request to the authentication server by transmitting information unique to its owner (e.g. username) in an encrypted format to authenticate with the authentication server. The Authentication server uses the shared secret associated with that user to decrypt the request; if the decryption is successful, a reply encapsulating a ticket granting ticket is transmitted back to the client for the next phase of the Kerberos process; otherwise, the request is classified as an unauthorised source and is discarded. The client sends the acquired ticket granting ticket to the ticket server as proof of successful authentication; the ticket server locates the shared secret used for the authentication process and decrypts the client unique information with the shared secret to validate the client before the session ticket is provided. The session ticket is encrypted with the session key that is only known by the services and transmits to the client device.

The final step of the Kerberos process integrates the asymmetric cryptography element as the service ticket can not be decrypted by the client as the session key used is only known between the ticket server and the application server; however, the client and the application can still communicate using the users shared secret as this is known by both parties; therefore, the initial application request is decrypted using the same symmetric key and the service ticket is decrypted using the known session key between the ticket and application servers. Once the client is mutually authenticated with the application server, the client can access the server with the permissions set by the application server.

Limitation of the Keberos network authentication protocol include caching authenticators, secure time services, spoofing logins, chosen plain-text attacks and various other variations of vulnerabilities as disseminated by (Bellovin & Merritt 1990). In the context of secure communication links for real-time teleoperation and telemetry; the implementation of the Kerberos system would not be best suited as the cost of implementation of three separate servers would not be viable in terms of financially viable in comparison to alternative key management methods presented in this section; in addition, its impact on the real-time nature of the context examined in this thesis and the computational storage of the system would not be significant if the number of real-time devices on the network is of a large volume; especially in scenarios that use networked real-time embedded systems (i.e. microcontrollers).

Elliptic Curve cryptography (ECC) is an ANSI X9.62 standard for asymmetric public-key cryptosystem (Johnson et al. 2001). The operation of the ECC uses algebraical mathematical notation to prevent attackers from obtaining the private key used; this is achieved by using the elliptic curve to derive the key value. Classification of curve sizes has been specified in the NIST P-192 standard (NIST 1999). Dot multiplication of intersection points along an elliptic curve enables the derivation of the value used for the public and private key of the system. An elliptic curve is the set points satisfying an equation in two variables with degree two in one of the variables and three in the other and described by the Weierstrass normal form presented in Formula 3:

$$y^2 = x^3 + ax + b \tag{3}$$

Formula 3 : Weierstrass normal form for elliptic curves adapted from (Corbellini 2015)

The properties of the elliptic curve are suitable in the context of cryptography as it has horizontal symmetry across the x-axis and non-vertical lines intersect the elliptic curve

across three places; these properties are used in the cryptographic system to derive the intersect value at the their point of the elliptic curve; at this initial intersection point, the intersection line follows a linear intersection across the x-axis until it intersects with the symmetric curve line that is above or below the x-axis; this process is repeated a number of times using dot multiplication to derive to the final intersection point across the elliptic curve, which is used as the private key value for the system.

The advantages of the ECC cryptosystem is the simplicity of deriving the private key value from the same elliptic curve profile for the two communicating entities using the same dot multiplication process to ascertain the private key value used; this process if referred to as a trap door function as an attacker would have no knowledge of how many times the dot multiplication of the intersection point was conducted before it had derived to the correct intersection value; unlike the factoring methods used for RSA cryptosystems; in addition, the discrete logarithm problem is significantly harder to solve in comparison to factoring methods.

Application of the ECC as a component for the secure communication link for real-time teleoperation and telemetry systems would not be best suited as the computational resources required to compute the process would results in an increase in the processing time to calculate all the intersection points and the dot multiplications to calculate the value for the private key; resulting in a direct impact on the real-time nature of the system.

The Elgamal cryptosystem is an asymmetric public key cryptosystem created by Thaer Elgamal (Elgamal 1985). The Elgamal cryptosystem uses the Diffie-Hellman protocol to exchange the private key secret between both parties over a non-secure communication link. The Elgamal cryptosystem differs from asymmetric methods such as RSA in the use of the prime numbers to obfuscate attackers but also in addition to the computation of discrete logs, this is where the exponent used to derive the output of the equation is unknown and prevents the attacker deriving the secret key as used by ECC.

Operation of the Elgamal key generation is conducted in a series of operations; the first process is to select a large prime number and generate the multiplicative group values; the second stage selects the private key by selecting an integer from the generated multiplicative groups at random under the constraints that the value is greater than one and less than the prime number minus one. The third stage of the Elgamal key generation process is the public key assembling, this is where the public key part of the asymmetric cryptography is calculated by using the prime number, generated multiplicative number selected and the outcome of the generated multiplicative number raised to the private key value modulus the prime number. The calculated public key is exchanged with the recip-

ient communication device in order to participate in secure communications.

Benefits of the Elgamal cryptosystem are that the same plain-text input would derive a different cipher-text output each time the message is encrypted (Kaur Grewal 2015); in addition, the key sizes used for encryption and decryption of data can be reduced in size as a result of the discrete log problem which shares resemblance with ECC. Limitations of the Elgamal cryptosystem is that the cipher-text is twice as long as the plain-text and requires large prime numbers to compute (Kaur Grewal 2015); as a result of this may not be suited to the real-time teleoperation and telemetry systems as the time to conduct the mathematical operation may influence the time constraints associated with real-time systems and the memory requirements to store a larger quantity of data may not be feasible for computationally constrained devices used in real-time teleoperation and telemetry systems.

2.9.1 Section Summary

The literature survey undertaken in this section presented a variety symmetric and asymmetric key management techniques used for cipher designs. Analysis of the survey conducted indicates that both symmetric and asymmetric could be viable option for the context of real-time teleoperation and telemetry applications; however, it is unknown what the impact of the contemporary key management methods would have on the real-time applications investigated in this thesis; therefore, the next section of the literature review introduces the application of contemporary key management techniques in real-time applications.

2.10 Cryptographic Key Management Techniques

This section of the literature review presents the cryptographic key management techniques proposed to frustrate the attacker from conducting passive and active attacks whilst considering variables that impact the human operation of the real-time teleoperation and telemetry application.

2.10.1 Energy and Mobility Based Group Key Management in Mobile Ad-Hoc Networks

Priyadharshini et al; introduce an energy and mobility based group key management in mobile ad-hoc networks (Priyadharshini et al. 2014). The problem discussed by the authors' is the issue of applying secure communications to mobile MANETs as the energy and mobility constraints and a requirement of an efficient key management scheme is required. The areas of consideration presented are segmented into four areas; the cluster

management, link stability, mobile prediction and group key management. The proposed solution presented by the authors' is the energy and mobility based group key management which is an identification based key management scheme. The scheme is comprised of two sections the cluster head formation and the efficient key management in the clusters.

Tests undertaken on the proposed scheme was undertaken in the simulation NS2. Results presented by the authors' show the number of nodes participating in the MANET increased the latency generated for the key generation; this trend was also present for the energy consumption. The stability of the communication link was investigated in relation to overhead, the more stable the communication link was, the less overhead incurred by the MANET. Comparison of the link stability and number of cluster head and key updataion shows an exponential decay trend as the link stability increases; furthermore, the more cluster heads present in the MANET, the less key updates were required.

The authors' state the system would be extended to the application of real-time systems, however, it is unknown if this approach would be best suited for this context as the processing frequency of the device has not been accounted for, therefore, it is assumed that the findings from the simulator are based on the processing speed of the computer and may not reflect the real world impact on a real-time system in terms of latency and energy consumption.

2.10.2 Authentication of Mobile Aerial Vehicle Communication using Caesar Cipher Cryptography

Rajatha et al; research focused on the authentication of Micro Aerial Vehicles (MAV) communication using Caesar cipher cryptography (Rajatha et al. 2015). The authors' proposed a methodology for data encryption and authentication of MAV protocol messages between the ground station and the MAV using the Caesar cipher; this was achieved using a shift operator to rotate the character positions by a fixed number, referred to as a key. Authentication between the ground station and the MAV is proposed through the same chosen fixed number. The methodology selected by the authors' is known to be vulnerable to modern cryptographic techniques used due to the widely known security vulnerabilities associated with the Caesar cipher. Test methodology and results have not been explicitly stated.

2.10.3 Section Summary

Analysis of contemporary key management techniques utilised for the context of real-time application demonstrates that the schemes presented prioritised energy conservation

or authentication of packetised data between the ground station and a mobile end-point. It is not explicitly stated how the stated methods impact the context investigated in this thesis and if the cryptographic key lengths specified by the authors are suited for the context investigated in this thesis and raises the question of what the appropriate length of the cryptographic key should be for real-time communications.

2.11 Regulations and Applications of Teleoperation and Telemetry Systems

The communication medium facilitates data propagation between the transmitter and receiver. The medium selected to propagate data is achieved through two methods, wired and wireless communication mediums. Wired communication medium uses cabling to interconnect devices together (e.g. fibre optics); benefits of using the wired medium is dedicated bandwidth between devices and improved protection against factors that impact the channel characteristics. Wireless communication medium generally uses radio frequency (RF) to broadcast data to devices on the same frequency; advantages of the wireless communication medium is low cost and ease of implementation (Chand et al. 2010).

The method of communication between the transmitter and receiver can be implemented in three configurations which are simplex, half-duplex and full-duplex. Simplex communication is selected for scenario where the transmitter communicates with the receiver in one direction only; this method of communication is similar to the user datagram protocol (UDP) as the operation is connectionless (i.e. no acknowledgement of message arrival is sent from the receiver to the transmitter). Half-duplex communication method operates similar to simplex communication; however, the receiver can communicate back to the transmitter if the communication channel is clear for transmission. Full-duplex communications is a method that enables the transmitter and receiver to communicate over the same communication channel at the same time. Figure 2.3 illustrates communication method between two nodes.

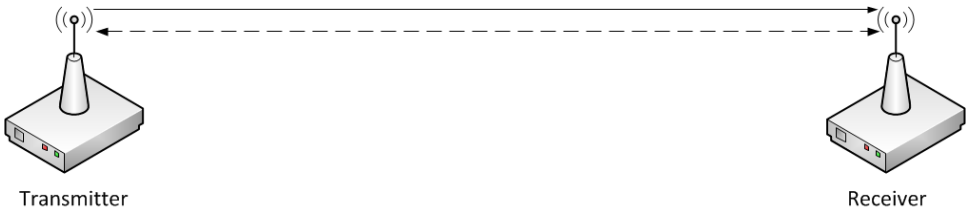


Figure 2.3: Simplex communication (solid line) and duplex communication (dashed link) between transmitter and receiver (Author, 2017).

The propagation of data between the transmitter and the receiver can be achieved through

two methods, single-hop and multiple-hop propagation. The single-hop propagation is a direct link between the transmitter device and the receiver device; this is normally implemented for systems that are in close proximity for point-to-point communications. Multiple hop propagation is a technique used to propagate data between the transmitter and receiver through intermediate node or relays; this method is selected when the transmitter and receiver are not within direct communication range and require neighbouring nodes to propagate data to the intended destination. Figure 2.4 illustrates single-hop and multiple-hop propagation methods for data communications.

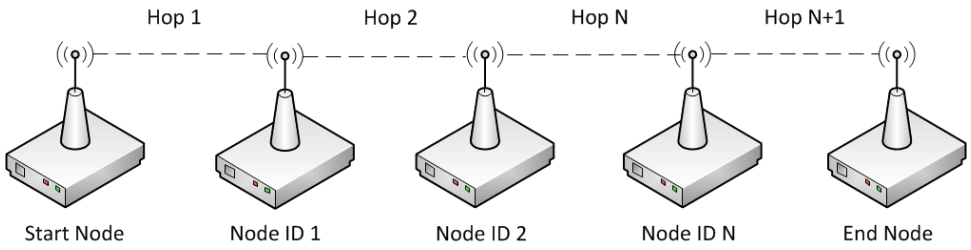


Figure 2.4: Data communication methods for propagation of data. Single hop propagation is represented as the data travelling from the Start Node to Node ID 1. Multiple hop propagation is represented as the data travelling from the Start Node over multiple intermediate nodes to the End Node. (Author, 2017).

The communication protocols used for real-time teleoperation and telemetry vary dependent on the application. Automotive and manufacturing scenarios select fieldbus protocols for data communications between the transmitter and receiver (Sundell et al. 2016). Instances of a fieldbus protocol include the International Organization for Standardization (ISO) 11898-1 Controller Area Network (CAN) protocol (ISO 2015); Profibus and Profinet. The structure of a standardised Profinet 802.3 industrial Ethernet fieldbus protocol Profinet is presented in Figure 2.5.

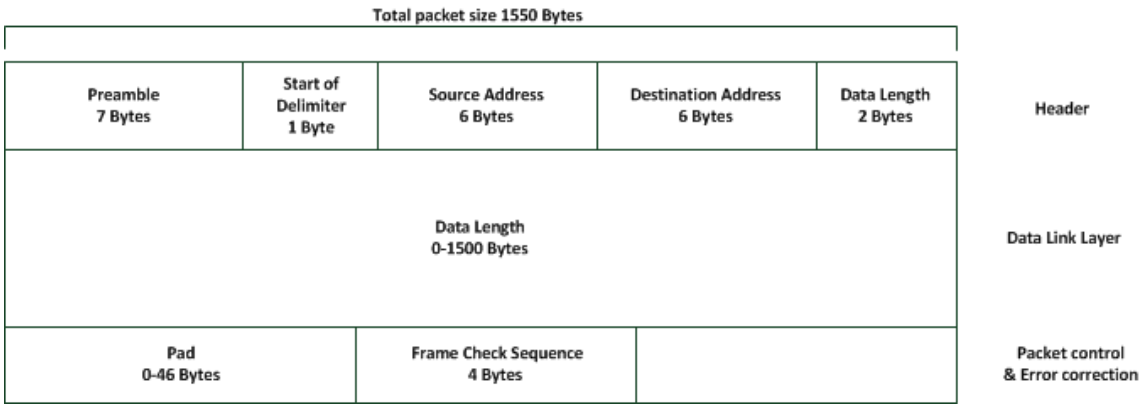


Figure 2.5: Packet structure of an 802.3 standard Profinet fieldbus protocol adapted from (Siemens 2010).

Protocols selected for mobile end points select different protocols commonly used in static scenarios. Mobile platforms such as unmanned vehicles select protocols that have small

packet size due to increased overhead. The Micro Air Vehicle link (MAVlink) protocol is an example of a protocol that is used to communicate with UAV. Figure 2.6 illustrates the structure of a MAVlink protocol

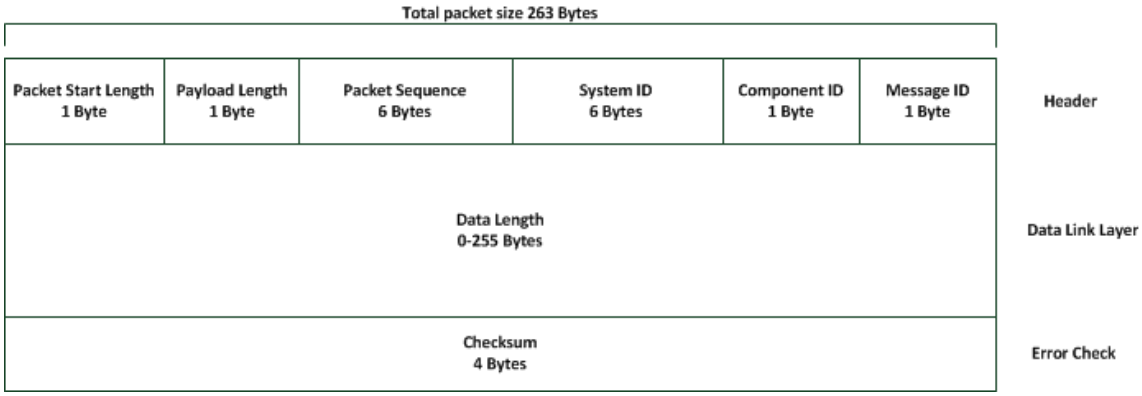


Figure 2.6: Packet structure of Micro Aerial Vehicle link protocol for mobile endpoints adapted from (QGroundControl 2016).

The operation of an UAV is dependent on the mission type as the pilot is limited based on their flight licence (CAA 2015). For the context of this thesis there are three classifications of mission types which UAV are deployed for; Table 2.1 categorises the types of mission and what is classified in each mission category.

Table 2.1: Unmanned Aerial Vehicles mission classifications adapted from (GlobalSecurity 2015).

Mission	**Characteristic of the mission type**
Tactical	• Up to one hour duration • Range up to 50 Km
Operational	• Eight to ten hour duration • Range up to 200 Km
Strategic	• Over twenty four hours duration • Range over 200 Km

The Civil Aviation Authority (CAA) guidelines state that the tactical UAV for civilian applications can only be operated within a line of sight of up to five hundred metres horizontally and one hundred metres vertically (CAA 2015); therefore, the tactical scenario investigated in this research is limited to the CAA regulations. The application of tactical

fixed wing UAV are used in military and civilian applications to conduct various tasks. Figure 2.7 pictures the variation in the tactical fixed wing UAV used for military and civilian applications.

Figure 2.7: Tactical fixed wing UAV Raven RQ-11 used by the UK military (left) (Aeroviroment 2017) and the Parrot Disco drone used for civilian applications (right). (Jarvis 2016)

Features associated with the tactical drones are the dual communication links that enables real-time teleoperation and telemetry simultaneously (i.e. control the plane operation and receive live video stream). The total cost of a tactical UAV used for military applications is £240,000 (Kasper 2014); whilst the civilian drone would cost approximately £1,149 (Parrot 2017); therefore, it is feasible for civilians to purchase tactical UAV in situations that require remote surveillance.

The implementation methods used for real-time teleoperation and telemetry can be viewed as four different permutations as the transmitter and receiver are either static or mobile. Table 2.2 tabulates the possible ordering for the transmitter and receiver.

Table 2.2: Variations of static and mobile teleoperation and telemetry from the prospective of the transmitter and receiver (Author, 2017).

Transmitter	**Receiver**
Static	Static
Static	Mobile
Mobile	Static
Mobile	Mobile

2.11.1 Section Summary

The literature survey identified that there are multiple methods to provide communication for real-time teleoperation and telemetry applications with single and multiple-hop communications and the type of communications selected between the transmitter and receiver (i.e simplex, half-duplex or full-duplex); however, it is unknown how the communication methods impact on the real-time nature of the teleoperation and telemetry application and raises the question of how multiple-hop communication methods contribute towards the problem investigated. The next section presents literature on the real-time systems.

2.12 Real-time Systems

This section of the background literature introduces the fundamental concepts associated with real-time system. The structure of this section is as follows; first, an introduction to the computational deadlines of a real-time system are presented and segmented into specific classifications, followed by the components required to facilitate a real-time system. The function requirements to process and compute the computational tasks for the application is examined, followed by an introduction to the real-time schedulers used in real time systems. The final section discusses the analytical techniques applicable to real-time system.

As real-time systems require a task or an operation to be executed in a constrained period of time; deadlines are specified to ensure predictable behaviour in order to maintain reliability and availability of the system. Classification of real-time system deadlines has been presented by (Shin & Ramanathan 1994); into three categories which are:

- **Hard real-time:** The consequences of not meeting the deadline can be catastrophic; normally associated with periodic tasks.
- **Firm real-time:** The results produced by the corresponding task cease to be useful as soon as the deadline expires but consequences of not meeting the deadline are not very severe; normally associated with aperiodic tasks.
- **Soft real-time:** The utility of results produced by a task with a soft deadline decreases over time after the deadline expires.

The selection of the three deadlines specified is dependent on the application as specified by Shin et al.; however, the consideration of additional non-real time constraints is specified by the authors'; areas identified include resource constraints (i.e. communication networks, database, input/output devices); precedence constraints where a task must wait for previous tasks to be completed before it can be executed and performance constraints in order to meet the reliability, availability and performance constraints in addition to the design considerations and functional requirements stated throughout this section.

Real-time systems are applied in multiple applications that require real-time teleoperation and telemetry, instances range from pacemakers to autonomous control of a vehicle (Shaw 2001); design requirements for each scenario varies depending upon the context to ensure safety, reliability and availability of the system. Design considerations that constitute to a definition of real-time systems and their functional requirements are presented in Table 2.3.

Table 2.3: Categorisation of design and functional requirements for real-time systems (adapted from (Williams 2006)).

Design Consideration	**Functional Requirements**
Timing	• Response latency does not exceed specified deadline for the application. • Transform unpredictable, asynchronous demands into scheduled synchronous processing
Interrupt driven	• React to an event driven interrupt immediately.
Hardware considerations	• Understand hardware components used in the real-time system and their functional role in relation to software systems
Volatile data	• Software must be structured to check for changes at the correct rate to prevent data loss.
Multi-tasking	• The inter-relationship of tasks required by the real-time system to be computed and their influence the behavioural characteristics of the system.
Run-time scheduling	• The ordering of tasks to be computed by the real-time system and the scheduler system required for the application specified.
Unpredictability	• Consideration of the events analysed, unpredictable environments and interactions.
Life-critical code	• Ensure safety, reliability and availability of the system to prevent potential life threatening situations.

The functional requirements of a real-time system may require tasks to be processed in parallel whilst providing a fast response in the completion of these tasks; however, in some instances, a real-time system may only require a simple looping programme to achieve its operation; as long as the response is good enough for the application, no further complexities need to be introduced; however, if a large number of data inputs are being monitored

by a single computational device or are complex, then a multi-tasking solution would be required (Williams 2006).

Areas specified in this section are important in the context of real-time teleoperation and telemetry; this is because the combination of the context and the non-real time factors contribute towards the multi-faceted, non trivial research problem stated in Chapter 1, section 1.4; this is because the variable application, context, resources and performance constraints contribute to the impact of the operational performance of the real-time teleoperation and telemetry; consequently, the application of secure communication links could further influence the identified variables in terms of resources consumed, impact on the performance of the system and the number of tasks completed for all classification stated and requires further analysis in the literature review section.

2.12.1 Real-Time Schedulers

Real-time schedulers are used in the context of real-time systems to achieve two objectives; to maximise the resource use of the system and provide fairness in the allocation of resources to complete the tasks (Arpaci-Dusseau 2015). As the focus of the research is on the secure communication link for real-time teleoperation and telemetry; the scheduling algorithms investigated in this section are related towards the handling of the communications of packetised data (i.e. packet switched networks) between the transmitter and the receiver.

The First In First Out (FIFO) scheduler is a prioritises the completion of tasks based on the task arrival into the process (Cummings 2002). The FIFO scheduler is used in queueing theory to model the completion of tasks based on the first come, first serve principle. Implementation of the FIFO is achieved through the storage of tasks into a circular ring buffer (i.e circular queue) based on the time of the task arrival; the stored data is processed in a sequential manner and follows a continuous loop until there are no tasks remaining in the queue.

The benefits of a FIFO scheduler are the time of the task arrival is set as the priority as tasks are completed upon arrival and its simplicity in implementation; however, a limitation of this approach is the time required to complete the task is not factored into consideration, this could be problematic in applications that prioritise the number of tasks completed in a given time period (i.e. increased latency in the system). Alternative methods derived from the FIFO scheduler are the Last In First Out (LIFO) scheduler which prioritises the completion of task that arrived last into the system; however, this method inherits benefits and limitations of the FIFO approach as the time of task arrival is set as priority.

The Round Robin (RR) scheduler is a pre-emptive method that allocates the full resources of the system to tasks through equal time periods (Stallings 2015). Operation of the round robin scheduler divides the time period (a.k.a time quantum) into equal sections (i.e 200 ms per task) and allocated full resources to the task for the specified period of time before the next task has allocation to the systems resources; this process uses a circular ring buffer to store and select tasks.

Application of the round robin scheduler has been used in networked system with the IEEE 802.5 token ring network (Cisco 1999); each node communicates whilst in possession of the token; once the data has been transmitted, the token is then released by the node and is passed onto the next node awaiting to communicate in the network.

The benefits of the round robin scheduler is the allocation of resources is distributed fairly across tasks through equal time allocation of tasks, unlike the FIFO and LIFO schedulers that prioritise the arrival of the task into the system; however, the limitation with the round robin approach is the time required to complete varying sized tasks impacts the operation of the system (i.e. tasks that require an increased time period to the resources in order to process the task will have an increased latency in the completion of the operation; therefore, a delay in the execution of a process or operation).

Priority driven schedulers can be configured to be pre-emptive or non-pre-emptive in operation and designates the order of tasks completion based on the priority value set (Goossens et al. 2003). The calculation of the priority value assigned to a task is derived based on operation requirements of the task; instances of the factors that influence the priority calculation include the memory requirements to store the task or the time requirement to process the task.

The advantages of a priority driven scheduler include the ordering of tasks based on the resources or time to execute and reduces the latency for mission critical tasks; however, a limitation of this method is the low priority tasks would incur an increased latency to complete if the scheduler is configured in a pre-emptive mode as low processing tasks would be interrupted as higher priority tasks arrive.

Instances of schedulers that modify the concept of priority based scheduling are the shortest time remaining that processes tasks with the smallest time first (Cobham 1954, Coffman & Kleinrock 1968). The shortest time remaining scheduler is a pre-emptive scheduler that allocates the priority of the task based on the time remaining to complete the task (e.g. tasks that are closer to completion are set as priority); whilst shortest time

first scheduler is a non-pre-emptive that prioritises tasks with the shortest time to complete its whole task. Limitations of the shortest time remaining and shortest job first schedulers is the restriction of resources for long tasks and the process execution time must be known for the methods to be applicable.

2.12.2 Real-Time System Analysis Techniques

The discussion of the real-time system timing analysis techniques are presented in this section with emphasis on code conformance for the context of real-time teleoperation and telemetry. Literature presented by Wilhelm et al;. categorised the analysis of the time required to complete the execution of a real-time task into two areas; the best case execution time as the shortest time required to complete the operation and the worst case execution time, the longest time to complete the operation (Wilhelm et al. 2008). As the context of this thesis is focused on the impact of secure communication links for real-time teleoperation and telemetry; the worst case execution time analysis methods are investigated to account for the worst case guarantee of the implementation of secure communication links.

The authors present two classes of analytical methods for worst case execution time with static and measurement-based methods. The static timing analysis methods mathematically model the task code and the possible path the code follows based on the hardware architecture used to complete its execution without the requirement of real-hardware or simulations; instances of the static timing analysis include value analysis to statically analyse the effective memory address location at run time, control-flow analysis to gather information about the possible execution paths; processor-behaviour analysis the occupancy state of the processor and estimate calculations.

The measurement-based methods analyse the observed time for a task or set of tasks to be completed based on various input variables in a simulation or real-world hardware implementation; the minimum and maximum observed execution times are derived to profile the behaviour of the code and used as the worst case execution time. Measurement of the time required to execute the code is achieved through intrusive methods (i.e. time-stamp or CPU cycles required to execute the code) and non-intrusive methods with logic analysers or oscilloscopes to time the execution of the code from start of execution to the end of execution.

Wilhem et al.; further describe the benefits and limitations of the two approaches with the static analysis described as a suitable methods for behaviour of real-time systems with specific processors as the model accounts for the all possible context dependencies and does not require real-world equipment to conduct the timing analysis; however, the limit-

ation is that each model is processor dependent and is suited for the bespoke scenario and could be invalid for systems using alternative processors. Measurement-based methods are more suited for the worse case execution time analysis when the processor behaviour of the system does not require modelling and precise measurement of the worse case execution time is required, which is a limitation of the static methods but requires implementation and numerous tests to reduce error in the results obtained from the measurement-based timing analysis.

The application of static and measurement-based methods are applicable towards the in the context of real-time teleoperation and telemetry; this is because the measurement-based methods are applicable for the collection of the worst case execution time for the overall operation and for each individual component required for the secured communication like (i.e. the cryptographic algorithm). Static methods are also applicable as the time analysis obtained from the measurement-based methods can be formalised to model the tasks of each component required by the secure communication link from an abstract prospective in terms of overall system behaviour.

2.12.3 Section Summary

In the context of real-time teleoperation and telemetry, the FIFO scheduler can be used for the storage and transfer of data packets between the transmitter and receiver as the teleoperation data is sequentially processed upon arrival to the receiver to operate the actuator and the telemetry data is displayed based on the arrival of the data.

Alternative approaches prioritise the equal sharing of resources in terms of time spent per task for round robin schedulers or the urgency of the operation to be completed for priority based schedulers; this could be problematic in the context of real-time secure communication links as the security service selected may influence the scheduler to prioritise the operation before or after the prerequisite tasks (i.e. teleoperation command or telemetry sample) are complete or cause a bottleneck in the processing throughput for round robin methods and raises the question of how the real-time task schedulers contribute towards the problem statement.

2.13 Discussion of Preliminary Literature Review

The AEAD security paradigm provides C.I.A that can be categorised into two paradigms which are the security paradigm and energy paradigm; the earlier implementations of AEAD provided cryptographic strength to the message with standardised approaches GCM and CCM using the full specified number of block cipher iterations (rounds) for AES. The second paradigm of energy is presented with TinyAEAD where the number of

block cipher iterations has been reduced to limit the energy consumption.

Initial findings from the preliminary survey indicate that the energy paradigm is a suited paradigm as it takes into consideration the computational and energy constraints; this is beneficial for the context of secure communication links for real-time teleoperation and telemetry as an implicit by-product of the reduction of the energy consumption using the energy paradigm was the reduction of the time required to process the cryptographic construct; this differentiates from existing designs presented in the preliminary literature review that consider the security as the main priority; however, further research is required in the literature review to disseminate if there is contemporary research that investigates secure communication for the context of real-time teleoperation and telemetry devices.

Identification of symmetric and asymmetric methods for secure communication links have been identified in the preliminary literature review. Limitations of asymmetric is the requirement of large prime numbers and may not be suited to applications with limited computational constants as the time required to complete the process would have a possible impact on the total latency required to complete real-time teleoperation and telemetry.

2.14 Literature Review

This section introduces research relevant to the initial research problem stated in Chapter 1, section 1.4. The literature review is categorised into four section based on the configuration methods presented in section 2.11, Table 2.2 of the preliminary literature review to reflect static and mobile real-time systems. The second section reviews the psychology of an attacker and their motives for initiating a security attack against a system, followed by an in-depth review of the cryptographic key methods used for secure communications. The final section reviews the current lightweight block ciphers used for secure communications. The presentation of the papers in each section is in chronological order.

2.15 Static to Static End-Points

2.15.1 A Security-Enhanced Encryption Scheme on Power System Real-Time Data Communications

Jing et al; introduce power system real-time data encryption on a networked environment (Jing & Xi 2012). The problem identified by the authors' is the increased interconnection of real-time systems over a networked communication link as the data transmitted is sent in plain-text. The authors' state that measures applicable to computer network information security are not transferable to power systems as the contemporary approaches are not suited to the context of real-time data communication constraints.

The requirements identified in this research are to provide: encryption to management data and economic data to maintain confidentiality of sensitive information, downlink and uplink data to mitigate passive and active attacks against the real-time communication link and ensure confidentiality of communicated data during propagation. The real-time features that have been highlighted are latency and network connection time to reduce the timing overhead to process data in the real-time system, authentication to verify if the device is authorised to participate in communications, encryption in addition to decryption and data packing and unpacking. In the context of the scope of this thesis; the most important factor is the latency of the real-time latency incurred as a result of the proposed scheme.

The proposed solution presented by the authors' is the Quantum Key Distribution (QKD) with a one-time pad to provide end to end network security in the real-time system. Three implementation methods have been proposed which are the QKD link encryption where a symmetric block or stream cipher is used with the QKD to secure the link, the QKD links which terminates the communication link between the master and remote terminal unit (RTU) and the QKD key distribution server that supplies cryptographic keys to host on the network. No test methodology or results have been explicitly stated in this research as the authors' only present the concept of the QKD method; therefore, this may require further analysis in terms of how it impacts the real-time teleoperation and telemetry, how key management aids the derivation of a secure communication link and a method of validating a symmetric key management system.

The authors' of this paper have identified variables that have influence on the real-time constraints specified in this research with network communication latency and processing of data through encryption and decryption algorithms and the requirement of security services to plain-text data in power systems. The communication link is specified as a problem that required investigation with the uplink and downlink specified as factors susceptible to security attacks which is an important aspect to consider as system may use dual-channel or half-duplex communication methods.

The proposed ideas in this research attempts to secure the link between two nodes and a method of cryptographic key distribution; however, the key distribution server technique is susceptible as it is a single point of failure (e.g. if the key distribution service is compromised, the attacker has the cryptographic key pairs for each device on the network) and with no test results presented, it is difficult to infer if this method is suited to real-time teleoperation and telemetry.

2.15.2 Co-design Techniques for Distributed Real-Time Embedded Systems with Communication Security Constraints

Jiang et al; consider confidentiality for internal communication for distributed real-time embedded systems (Jiang et al. 2012). The authors' research concentrated on security measures for securing real-time embedded systems as the interconnection of embedded systems to network communication links has increased through wireless fidelity (Wi-Fi). The internal communications between the embedded devices was the main focus in their research.

The problems identified in this research consider the number of Field Programmable Gate Arrays (FPGA) units required to achieve a level of confidentiality whilst meeting real-time and resource constraints. Preliminary analysis of the number of rounds used by the encryption algorithm demonstrate that software implementations of AES can meet the constants of the authors' contrived scenario if the number of iterations used by the AES block cipher is reduced to three rounds. The authors' specify that the software implementation is not satisfactory solution; therefore, an investigation of a hardware method that processes the full ten round iterations of AES is required.

Two hardware design optimisation methods are proposed by the authors' using FPGA, the heuristic constraint logic programming (CLP) method and the heuristic programmable dynamic reconfiguration (PDR). The authors' proposed heuristic methods were compared against the original design optimisation methods of CLP and PDR. Experiments were conducted on a Linux quad-core machine (Xeon Central Processing Unit (CPU)) operating at 2.6 GHz and 8 GB Random Access Memory (RAM) using the Eclipse software programme. Tests factored the number of FPGA processors and the number of individual applications.

Results from the experiments demonstrate that the CLP technique required a longer time to process in comparison to the heuristic CLP method for the same number of applications. The PDR heuristic method had a reduced time for the same number of applications in comparison to the CLP heuristic method. The hardware expenditure was analysed using the authors' average additional hardware expenditure formula; the CLP heuristic method had less hardware expenditure in comparison to the PDR heuristic method.

The research considers the problem of the communication link between devices on a network and identified similar problems as discussed by (Jing & Xi 2012) with focus on securing the internal communication channel. The methods of implementation using hardware were explored and the method of implementation appears to influence the over-

head generated by the security algorithm. Hardware implementation was discussed by the authors' with the main consideration of the design optimisation of the processes used for encryption and decryption, however, the justification for dismissing software AES methods was not demonstrated as it had been stated that the software variation met the constraints of the scenario with a reduced number of iterations used by the AES block cipher.

2.15.3 Performance Evaluation of MAC Algorithms for Real-Time Ethernet Communication Systems

Czybik et al; analysed the performance and evaluation of message authentication code (MAC) algorithms for real-time Ethernet communication systems (Czybik et al. 2013). The problem analysed by the authors' is the communication protocols used for real-time systems were not designed with consideration of confidentiality, integrity or authentication as the real-time data is communicated. The research investigated the performance of MAC algorithms and their influence in the context of real-time data communications.

Test methodology selected for this research compared the theoretical run-time of the MAC algorithms based on a 32-bit CPU architecture against the real-world measurements on an ARM-9 100 MHz microprocessor. The three MAC authentication methods that were benchmarked for the tests were the Key-Hashed Message Authentication Code (HMAC) with SHA-256 algorithm, Cipher-based Message Authentication Code (CMAC) and Giga Multiply-Accumulate operations (GMAC). AES-128 was selected as the block cipher operating in cipher block chaining (CBC) mode using 128-bit key length. Data input size of one hundred bytes was selected.

Results presented from the test suggests that the CMAC-AES-128 algorithm was theoretically calculated to be the fastest algorithm at 57 microseconds in comparison to HMAC-SHA-256 at 66 microseconds and GMAC-AES-128 at 218 microseconds; however the real-world tests show that the HMAC-SHA-256 was the fastest algorithm with a time recorded of 96 microseconds whilst CMAC-AES-128 recorded a time of 110 microseconds and GMAC-AES-128 at 265 microseconds. There was discrepancy with the estimated calculated time and the real-world calculation time with all variants examined.

The research identified how different MAC based schemes induce latency on the communication protocol and the impact this would have on real-time data communication; this differs from (Jing & Xi 2012, Jiang et al. 2015) as their focus was on the method of encryption. Small packet sizes were sampled to mimic the protocol sizes commonly used in real-time system and how the impact of confidentiality, integrity and authentication is affected in terms of latency. It is stated in this research that software implementations

are applicable for real-time applications but could be problematic in contexts that have hard real-time constraints (e.g. microseconds time constraints) and recommends hardware methods to reduce the delay incurred.

2.15.4 Securing RTP Packets Using Per-Packet Selective Encryption Scheme for Real-Time Multimedia Applications

Jung et al; attempt to secure the Real-time Protocol (RTP) using per-packet selective encryption scheme for real-time multimedia (Jung & Festijo 2013). The problem investigated by the authors' is the trade-off between the security strength of the session key used for encryption and the latency generated from the key size used. The solution proposed by the authors' is to generate a session key per packet whilst satisfying the real-time requirements with the selective packet key encryption scheme that does not reuse the same key for the encryption of new packets in the same session. The main consideration in this research was to identify the latency and security strength of reduced digits of the key; key sizes examined range from three digits and up to ten digits. An instance of the proposed approach was implemented with the Diffie-Hellman (DH) key generation with the RC4 stream cipher.

Three tests were conducted; first, the latency for encryption and decryption was tested with different sized key lengths for the DH-key generation over an average of five hundred measurements of video streamed data. The second test benchmarked the impact of the selective packet encryption scheme on the average latency caused by packet key exchange. The final test investigated the strength of security for selective packet key encryption scheme by computing the time taken for an attacker to decrypt the message with various key length sizes.

Results of the tests demonstrates that the latency for encryption and decryption tests was influenced by larger sized key lengths for the DH key generation with the biggest increase on latency recorded for the same sized video stream sampled; the encryption rate influence the average latency recorded with a logarithmic trend-line identified for all variations sampled. The results of the second test shows an exponential decay trend as the higher encryption rates have a greater impact on the Perceptual Evaluation of Speech Quality (PESQ) with lower quality received. The results of the computation time taken for an attacker to decrypt the message with various key lengths indicates that the larger sized key lengths requires a longer time period to break in comparison with smaller sized key lengths and follows a linear growth trend-line as the number of queued decrypted packets increases.

The authors' research focused on real-time system targeted towards the RTP used in ap-

plication that use voice communication in real-time. The methodology presented emphasised constraints that are commonly associated with enterprise networks with tests undertaken on platforms with high computational power and larger packet sizes selected. The implementation of the authors' approach used a stream cipher over a block cipher due to its increased performance in speed (Singhal & Raina 2011); however, the RC4 stream cipher has known security vulnerabilities that could be exploited by an attacker (Maitra & Paul 2008).

Trends identified from this research are that the size of the encryption key has an influence on the encryption operation and the additional latency generated; this could influence the proposed key distribution system presented by (Jing & Xi 2012) as the time required to process the key-length impacts on the latency generated.

2.15.5 A Secure but still Safe and Low Cost Automotive Communication Technique

Zalman et al; examine a secure but still safe and low cost automotive communication technique (Zalman & Mayer 2014). Problems identified by the authors' include the interconnection of wireless modules on traditional onboard communications for automotive environment (e.g. Controller Area Networks (CAN)). The requirements specified for this scenario are targeted at the integrity of data to prevent data modification is prevented, ensuring data arrives in the specified real-time constraints and authenticity of the data from an authorised trusted user on the system.

The proposed solution presented by the authors' attempts to address the limitations identified for the pre-shared symmetric key message authentication code (MAC) which included no time related information in the message, therefore enabling message delay attacks, the MAC and CRC combined add significantly to the message lengths and the time to calculate the MAC in real-time. At the transmitter a time-stamp is added and used in the MAC calculation for the tag, the MAC is added to the payload of the message with a CRC before transmitting to the receiver node. No test methodology or results have been presented.

The application of real-time systems presented in this research is focused on the automotive applications that use fieldbus communication protocols; this continues from the research discussed by (Czybik et al. 2013) who discussed these requirements with the addition of confidentiality. With no test methodology or results stated; there is no indication that this method is suited to meeting the constraints associated with real-time systems in the automotive sector, however, the research presented by (Czybik et al. 2013) suggests that the additional latency may impact on the safety critical nature of the automotive

environment (e.g. stopping the vehicle).

2.15.6 A Secure Communication Architecture for Distributed Microgrid Control

A secure communication architecture for distributed microgrid control is presented by Kounev et al; (Kounev et al. 2015). The research problems specified by the authors' are the real-time nature of the communication, resource limitations of intelligent electrical devices (IED) and distributed nature of microgrid systems. The IED has been identified as the bottleneck of the system and impacts the communication overhead due to the computational limitation of processing and storage and that the execution cycles of such controllers must be considered in the design of a security architecture as they limit the type of confidentiality and integrity methods employed.

The proposed solution presented by the authors' of this research is a microgrid security architecture that uses the principles of MAC-based incomplete-set schemes with symmetric cryptography. The first section of the microgrid security architecture uses key bootstrapping to initiate secure communications; the secure communications is achieved with preinstalled bootstrap keys on the IED to communicate with their key management server and other IED on the network; the proposed method selects AES 192-bit key length variation. The second section of the security architecture proposes the communication security with an encrypt-then-MAC method selected for unicast and multicast communications.

The test methodology used in this research applied theoretical calculation of the performance of the bootstrapping and key size selected with comparative performance of the methods benchmarked in the tests. The selected confidentiality and integrity scheme by the authors' based on their security architecture is AES-CMAC using a 192-bit key size and a 96-bit key size variant. The proposed solution was benchmarked against Rivest-Shamir-Adleman (RSA) public-key cryptosystem using 2048-bit key size, Digital Signature Algorithm (DSA) using a 256-bit key size and Time Valid Hash to Obtain Random Subsets (TV-HORS) using a 500 KB key size. A microprocessor of 600 MHz was selected to calculate the results based on a 42 byte message payload.

Results presented demonstrate that their proposed method of AES-192 with CMAC was the quickest with 0.008 milliseconds recorded for transmission, whilst RSA had a time of 312 milliseconds, DSA time of 91 milliseconds and TV-HORS 0.0015 milliseconds. The time to process the receiver message indicated that TV-HORS and AES-192 was the fastest implementation CMAC with 0.016 milliseconds recorded whilst RSA had an induce delay of 9 milliseconds and DSA had a delay of 111 milliseconds.

Simulation of the maximum end-to-end delay was examined. The simulation of the power

system was conducted in MATLAB and the microgrid communication network was tested in Omnet++; a custom adaptive scheduler was selected to interface between the two simulators. Two test were conducted, first a comparison of the maximum end-to-end delay for varying number of multicast receivers using AES-192 CMAC and AES-96 CMAC. Results obtained indicate that the maximum end-to-end delay increases with the number of receivers on the system; the end to end delay increased at a higher rate for AES-192 CMAC in comparison to AES-96 CMAC with both methods following a linear growth in the latency recorded as the number of receivers on the network increased.

The final test examined the maximum distributed control loop delay using AES-192 CMAC, AES-96 CMAC, RSA and DSA. The same simulated test platform used for the second test was selected for this test and results were compared to the authors' theoretical distributed control loop delay calculations. Results show that CMAC-192 and CMAC-96 methods had a simulated delay of 1,128 milliseconds, whilst RSA had a delay of 2,093 milliseconds and DSA 4,424 milliseconds. The theoretical delay for CMAC methods was 1,080 milliseconds, RSA calculated delay was 1,805 milliseconds and DSA calculated delay was 2,485 milliseconds. Results of the RSA and DSA methods would cause instability to the proposed system.

The research presented has similarities with (Jing & Xi 2012, Jiang et al. 2012) with problems identified with the communication link and the computational limitation of embedded devices. The method and implementation draws comparison to (Czybik et al. 2013) research with MAC based schemes are selected and the examination of the additional latency induced by their proposed schemes; in addition; (Kounev et al. 2015) report statistics on the latency recorded for asymmetric and symmetric cryptographic schemes.(Kounev et al. 2015) research is targeted at secure communications at the network layer and not the data link layer of the OSI model. The proposed solution was benchmarked against asymmetric methods only, alternative symmetric cryptographic paradigms were not taken into consideration.

2.15.7 Analysis of the Trade-Off Between Compression Ratio and Security Level in Real-Time Voice

Analysis of the trade-off between the security level and compression ratio of real-time voice communication was researched by Attie et al; (Attie et al. 2015). The problem identified by the authors' focused on voice compression as an attacker can reconstruct the digital representation of the signal without requiring the original voice signal. The proposed solution to this problem is to rely on constant bit-rate compression or to pad the sent frames to a multiple of sixteen, thirty-two, or sixty-four bytes. To address the problem, data encryption had been identified as an approach to providing data confidentiality for

the compressed voice message as it eliminates the structure from the compression output.

A test platform was created on a Linux Ubuntu operating system using the C programming language. The voice encoder selected by the authors' was Speex and the encryption algorithm chosen operated in cipher block chaining (CBC) mode from the OpenSSL libcrypto package. Data samples of the voice messages were sampled at 16 KHz with 16-bit linear sampling. AES block sizes of 128-bits and 256-bits were chosen for AES and a 512-bit variant was sampled with a combination of 256-bit operation and manual padding. Stream encryption scheme was also sampled for the test procedure. Protocol selection for the test was the real-time protocol with a polling time of 20 milliseconds (ms) with two separate streams for transmitter and receiver.

Results presented by the authors' indicates that the block size selected influences the quality of the compressed voice; the authors' suggest that there is a trade-off between selecting the strength of the security algorithm to the quality of the compressed voice (i.e. the higher the security strength, the lower the quality of the compressed voice). It was noted that the size of the block cipher impacted the overhead incurred with 512-bit variant reporting the largest overhead in comparison to the lowest overhead using the 128-bit variant. The configuration of the voice encoder has an impact on the quality of the voice message and the additional overhead incurred with wideband compression reporting an improved output in comparison to narrowband compression.

The research presented by (Attie et al. 2015) attempts to prevent the attacker from reconstructing the voice message. The research differs from (Jung & Festijo 2013) as the authors' select a block cipher implementation with the standardised AES selected instead of the stream cipher RC4 selected by (Jung & Festijo 2013); discussion of stream ciphers were stated by (Attie et al. 2015) but elaboration on the specific implementation was not specified. The authors' discuss a method of applying confidentiality to the data only with the analysis of AES-128 and AES-256 bit variants with no consideration for integrity or authentication methods; this is problematic as integrity and authentication are key components required to fulfil the requirement of a secure communication link; otherwise, an attack could conduct forgery or replay previous packetised data and participate in unauthorised communication with devices on the network.

2.15.8 Safety Can Be Dangerous: Secure Communications Impair Smart Grid Stability Under Emergencies

Wei and Wang; analyse how secure communications impair on smart grid stability under emergencies (Wei & Wang 2015). This research identifies that the interconnection of cyber-physical systems to the internet has enabled attackers to target critical infra-

structures. The authors' state that existing security countermeasures that are theoretically feasible have not been validated in relation to the performance of smart grids and the impact of security attacks against the system. Two case scenarios are presented in this research, cyber attacks under plain-text communication and cyber attacks under cipher-text communications.

The test methodology examined the latency of the cryptography in an emulated environment. Components selected for this test were an ARM9 500 MHz microcontroller as an intelligent electronic device (IED) and a Linux Ubuntu Intel i7 2.9 GHz CPU as the emulated control centre. The encryption and decryption algorithm selected for this test was AES in cipher feedback mode (CFB); message size of two hundred and forty bytes was selected to emulate a maximum Modbus packet size. The communication protocol selected for this test was Ethernet using the User Datagram Protocol (UDP) method of transportation. The test was completed five thousand times and factored the propagation delay into the results. The results presented shows that the cryptographic process takes up to eighty per cent of the overall time (3.8 milliseconds latency).

The authors' conducted a simulation of the two scenarios to identify the impact of plan-text and cipher text communications in terms of transmission delay only and transmission and processing delay. Results demonstrate that the additional time generated from the cryptography has an impact on the system as the clear-text response time of 0.318 milliseconds was simulated to have a voltage collapse on the power system of two point three per cent; whilst the cipher-text implementation had a combined 4 milliseconds delay; a simulated impact on the power system with a voltage collapse of twenty-six per cent as a result of the time required to encrypt and decrypt the message; this indicates that the security service contributes towards the real-time system behaviour and has an impact of the safety, reliability and availability of the system as a result of increased latency in comparison to the processing latency of a message without security services applied.

The authors' reinforce the problems highlighted by (Jing & Xi 2012, Jiang et al. 2012, Zalman & Mayer 2014) of the interconnection of devices to real-time systems to networked devices can facilitate security attacks. The methodology of the test has similarities with the aforementioned researchers approach with latency examined; however, the authors' analyse the impact of the transmission delay and the processing delay of the cryptographic method chosen and how the additional delay influences the performance of the systems from the perspective of safety. Confidentiality of the message was analysed only in this research.

2.15.9 Lightweight Authentication for Secure Automotive Network

Mundhenk et al; present a lightweight authentication for secure automotive networks (Mundhenk et al. 2015). The problems identified by the authors' are the increased interconnection between inter-communication and intra-communication used for automotive systems are susceptible to security attacks as the internal communication was not considered with security in mind.

The proposed solution is a lightweight authentication framework which combined symmetric and asymmetric authentication schemes. The asymmetric authentication is used to authenticate the electronic control unit (ECU) with the security module and is non-real-time and is achieved whilst the vehicle is not operational; the symmetric authentication is selected for real-time data streams whilst the vehicle is operational. Implementation of the framework was achieved using a modified version of Kerberos two stage set up for authentication. RSA was selected as the mechanism for confidentiality for the asymmetric implementation and AES for the symmetric cryptographic implementation.

Tests were conducted on an ARM Cortex-M4 STM32F415RG microcontroller operating at 16 MHz. A random number generator was used to generate input data for the encryption schemes. Results from the tests show that the asymmetric method induced a significant amount of latency to process the encryption and decryption process with the combined time for the public and private key operation with a 512-bit key length was 1 second; whilst a key length of 2048-bit key length would require 35 seconds to compute.

Symmetric cryptography was benchmarked using hardware and software AES in cipher block chaining mode (CBC) of operation. Results demonstrate that hardware AES induces less latency than software AES for the same input length; however, the trend for encryption and decryption between hardware and software follows a linear growth profile as the number of input bytes into the block cipher increases, this is because the increased number of bytes passed into the block cipher requires more block cipher calls in order to encrypt or decrypt the whole message. The data rate of the communication system was reported by the authors' to impact the cryptographic method chosen with low data rates unsuited for secure communication due to the additional time required to transmit, and process the security service.

(Mundhenk et al. 2015) discuss the requirement of lightweight authentication methods as a prevention method against attackers with emphasis on the impact of safety if exploited. The selection of asymmetric key cryptography for non-real-time communications and symmetric key for real-time communications suggests that the selection of the secur-

ity approach is an important aspect to factor as an incorrect method can impact on the system; this further reinforces findings presented by (Kounev et al. 2015) who analysed the performance of asymmetric cryptographic approaches on distributed smart grids with real-time requirements. Implementation and analysis of hardware and software implementations of the proposed solution had not been taken into consideration by (Zalman & Mayer 2014); furthermore, the analysis was undertaken on a test platform that is more commonly found in the automotive sector. Latency of the system is factored only and the impact of the latency is not explicitly stated.

2.15.10 Secure IoT Framework and 2D Architecture for End-to-End Security

A secure internet of things (IoT) framework and 2D architecture for end-to-end security is presented by (Choi et al. 2016). The problem discussed is the requirement of fulfilling end-to-end security. It is stated that intermediate security issues are required in scenarios that include real-time healthcare monitoring to ensure privacy of patient's data. The requirement for a lightweight protocol is specified in this research as IoT devices have constrained communication and computational ability.

The solution proposed by the authors' is an attribute based encryption with a certificate authority scheme with AES selected as the symmetric block cipher. Tests were conducted on three IoT specifications which were IoT application (PC Intel i7 CPU 3.6 GHz 8 GB RAM PC), IoT broker (ODROID ARM Cortex quad-core 2.0 GHz 2 GB RAM) and an IoT device (Raspberry Pi ARM11 700MHz 512 MB RAM). The test sampled the total time for the IoT application node to transmit the encrypted message to the IoT broker node and relay the data to the IoT device to decrypt. The tests sampled times for unencrypted communication and encrypted communication. Results indicate that the proposed scheme induced double the response time in comparison to the non-encrypted response time sampled.

The authors' of this research identify that a lightweight security protocol is required to meet the real-time constraints, this correlates with (Mundhenk et al. 2015) who propose an asymmetric method concept for automotive networks; whilst research conducted by (Jing & Xi 2012, Wei & Wang 2015) were targeted towards power grid systems that select the same computational devices with symmetric cryptographic methods. (Choi et al. 2016) discuss the use of different computational platforms over multiple hops communications. End-to-end security was the main objective of this research which differs from the point-to-point secure measures. The results presented are for the latency of the encrypted and non-encrypted messages only.

2.15.11 Section Summary

Analysis of the findings presented in contemporary literature demonstrates that the focus of the research is on the application of security services from the viewpoint of the latency required to process symmetric and asymmetric cryptographic services.

The common theme presented in this section of the literature review is that the security services investigated are implemented on microprocessor devices and only consider the latency induced by the security service only and the security services examined by researchers are not utilising contemporary security paradigms.

The questions raised from this review are what is the impact of contemporary security services on the communication latency incurred by static devices (transmitter and receiver) used for real-time teleoperation and telemetry using embedded microcontroller devices and how does the latency induced by contemporary security services influence the operational performance characteristics (i.e. packet throughput) of the real-time teleoperation and telemetry application.

2.16 Static to Mobile End-Points

2.16.1 Performance Evaluation of Security Communication in Critical Embedded Systems

Salla et al; conduct a performance evaluation of security communication in critical embedded systems (Salla et al. 2012). This research discussed the context of critical embedded systems that collect and exchange data among devices which included environmental monitoring, military and agricultural monitoring through the use of aerial and ground autonomous vehicles and unmanned vehicles.

The problem stated in this research is the application of cryptographic approaches has an increased impact on the response time of a task to be executed; it is stated that the increase in the strength of the cryptographic construct has a decrease impact on the performance of the system. The authors' specify that the communications between UAV and UGV requires security services to information sent between devices in real-time.

The experiment conducted by the authors' investigated the impact of varying the size of the message in relation to the distance and cryptographic algorithm selected. The block cipher chosen for this experiment was AES using a 256-bit key and the stream cipher RC4 using a 128-bit key. Message sizes of 105 KB and 322 KB were sampled. Distance of 1 metre between the communication devices represented close range communication

and 9 metres for long ranged communication. Tests were conducted thirty times. All tests were conducted using an ARM Cortex-A8 processor with the 802.11b/g wireless standard selected.

Results presented demonstrate that the message size has the biggest impact on the response time with a 322 KB message recorded a higher latency measurement in comparison to a 105 KB message size for AES and RC4. The AES block cipher at 1 metre range recorded the least latency for the same message size sampled; however, at a 9 metre distance, the RC4 cipher was recorded to have the least latency measured to process the message sizes sampled.

The authors' take into consideration characteristic of a secure communication channel between the transmitter and receiver and its impact of additional latency on the performance of the UAV. Confidentiality and integrity have been presented as a proposed solution to prevent eavesdropping and malicious intended modification of data during propagation. The size of the messages selected for this test are not commonly selected for mobile real-time systems and it is unclear to how the distance between the communicating devices has a detrimental impact on the behaviour of the security service selected and raises the question whether the experimental methodology was appropriate for the test conducted.

2.16.2 A Secure Communication Framework for Large-Scale Unmanned Aircraft Systems

Bian et al; propose a secure communication framework for large-scale unmanned aircraft systems (Bian et al. 2013). The problem discussed by the authors' is the security threat models that can be used by an attacker against the unmanned aircraft system; threats include eavesdropping, spoofing, masquerade, man-in-the-middle and DoS attacks. The proposed countermeasure by the authors' is the unmanned aircraft system collaborative wireless network (UAS-CWN) which uses one way encrypted hash key-chain and symmetric cryptography selected for confidentiality service and asymmetric key cryptography for the integrity and authentication service. Key management methods selected in this research is the pre-distributed approach as the authors' state the configuration of the keys is applied at the base-station before launch.

The test platform selected was a simulated environment with the implementation of the Erdös-Rényi random graph model to mimic the communication links between unmanned aerial systems. A mesh network topology was created with a hundred random interconnected devices on the network. Test conducted show that the number of UAV on the network does not have significant influence on the operation of the system in data recovery failure rate; however, the increased strength in security does influence the data

recovery failure rate. Simulation and cryptographic methods are not explicitly stated.

The authors' identified security vulnerabilities associated with mobile real-time platforms with passive and active attacks specified. The proposed solution presented in this research requires time to process through the asymmetric key hash algorithm and viewed the problem from the priority of the mission (e.g. more important the mission, the stronger the security used) that is unsuited to the context of real-time systems as (Salla et al. 2012) established the impact of security services on embedded systems; furthermore, research presented in the static-static context identifies the additional delay of the operation of hashed based asymmetric approaches as discussed by (Czybik et al. 2013, Zalman & Mayer 2014, Kounev et al. 2015).

2.16.3 The Vulnerability of UAV to Cyber Attacks - An Approach to the Risk Assessment

The vulnerability of UAV to cyber attacks is presented by Hartmann and Steup (Hartmann & Steup 2013). The authors' investigate the security vulnerabilities associated with UAV; attack vectors identified in this research focus on spoofing attacks and the weakness of the communication channel due to its wireless broadcast nature. A proactive risk assessment scheme is proposed to evaluate the risks against UAV which takes into consideration each component using a probability based evaluation of confidentiality, integrity and authentication.

Factors examined for the risk assessment include the environment, communications, sensors, data storage and fault handling mechanisms. The application of the authors' risk assessment is applied to two UAV which are the AR.Drone and MQ-9-reaper. Results from the framework indicate that confidentiality and integrity appear to be the most susceptible to risks with the communication link and sensors.

The authors' identifications of potential risks correlated with Salla et al; with the importance of confidentiality and integrity service stated; whilst Jing et al; view a similar problem from the context of internal communication between devices in a static scenario. The proposed framework and risk analysis undertaken by the authors' is based on probability theory to determine the likelihood of a successful attack.

2.16.4 HAMSTER - Healthy, Mobility and Security-based Data Communication Architecture for Unmanned Aircraft System

Pigatto et al; present a healthy, mobility and security based data communication architecture (Pigatto et al. 2014). The scenario examined by the authors' was for unmanned

aircraft systems where information exchange is achieved in real-time and requires low latency and security mechanisms to meet the basic requirements of the unmanned aircraft system. The proposition presented by the authors' is a specification of the healthy, mobile security communication architecture (HAMSTER) with the main objective of the architecture being to help developers of unmanned aircrafts to efficiently implement communications in UAS by considering the internal and external communications.

The derivation of the HAMSTER framework incorporates the operations of the ground-station and aircraft in terms of real-time, near real-time or non real-time communications. The central security service specification is stated as a method of authenticating aircraft peripherals through storage of the public-keys of all components on the system, similar to a certification authority. Authorised modules on the system participate in an e-voting system to determine the authenticity of the modules on the system. The design, configuration and application of confidentiality, integrity and authentication security services are not specified. No testing of the proposed solution was undertaken in their research.

The proposed framework presented by the authors' discusses authentication of internal module devices on the network; but does not take into consideration confidentiality and integrity methods as presented in (Salla et al. 2012, Jiang et al. 2012, Czybik et al. 2013) research; however, the segmentation of the real-time processes and tasks stated in this literature show the consideration of the operation of the real-time system with suggestion to approaches to best suit these requirements. Discussion of asymmetric approaches has been mentioned in this research with a variant of a certificate authority but the research discussed in the static environment demonstrates the impact of latency on a system that deploys asymmetric cryptographic methods.(Pigatto et al. 2014) have identified the importance of the communication link from the perspective of the uplink and downlink between the base-station to the air vehicle or air vehicle to air vehicle and categorised the types of traffic transmitted between the two devices.

2.16.5 An Assessment of Recent Attacks on Specific Embedded Systems

Ali Alheeti and McDonald conducted an assessment of recent attacks on specific embedded systems (Ali Alheeti et al. 2014). This research focused on security attacks against mobile phones, wireless sensor networks and unmanned aerial and ground vehicles in the context of mission critical applications. Attack vectors presented are classified into two sections which are physical and logical security. Ramifications of a physical or logical security exploit has been stated by the authors' with vulnerabilities that include forged information, information theft, network intrusion and sensor manipulation.

Vulnerabilities of wireless sensor networks and unmanned aerial and ground vehicles

mentioned by the authors' include spoofing data from sensors, replay attacks, injection attack through web applications and man-in-the-middle attacks. Countermeasures identified by the authors' prioritises encryption to mitigate the attacks. The authors' conclude that future work on security systems needs to be customised to specific characteristics of the embedded system.

Despite the authors' not conducting any tests to validate their proposed countermeasures; the identification of the attack vectors against a mobile device is presented with the message propagation between the transmitter and receiver as the weakness which is reinforced by (Bian et al. 2013, Pigatto et al. 2014). The future work presented by the authors' indicates the requirement for context specific security countermeasures which correlates with the concepts presented by (Jing & Xi 2012, Wei & Wang 2015); who specify that current cryptographic services were not designed for the context of real-time systems.

2.16.6 Section Summary

Findings presented from the literature review undertaken in this section shows that the primary focus for static to mobile scenarios is on the communication links between the transmitter and receiver device with consideration of low latency secure communications. Countermeasures proposed by the authors in this research have identified confidentiality, integrity and authentication schemes to mitigate the identified attacks against mobile endpoints.

Security services proposed by authors in this section of the literature review is a combination of symmetric and asymmetric cryptographic services to mitigate against stated security attack vectors; however, as identified in the static to static analysis, the additional latency incurred by specified security services would have an impact on total delay time recorded and solutions proposed may not be best suited for the context investigated in this thesis.

Consideration for the communication range for the mobile end-point using security services has been discussed in the literature presented; however, the impact of security services in relation to the mobile end-point characteristics has not been explicitly stated. This raises the questions of what the impact of contemporary security services on the latency incurred by mobile real-time teleoperation and telemetry applications and what influences the maximum communication range between the transmitter and receiver devices used for mobile real-time teleoperation and telemetry applications.

2.17 Mobile to Static End-Points

2.17.1 Data Communication in Linear Wireless Sensor Networks using Unmanned Aerial Vehicles

Jawhar et al; investigate data communication in linear wireless sensor network using unmanned aerial vehicles (Jawhar et al. 2014). The authors' examine the scenario of wireless sensor network and the impact of multiple hop relays on the energy consumption of the sensing and relay nodes.

The solution proposed in this research uses a hierarchical network topology to facilitate the flow of data using various links throughout the hierarchical topology (i.e. zigbee protocol between sensor and relay nodes and WiMAX between relay node and UAV); categories of the devices are segmented into four section which are sensor nodes that take measurements of the data obtained, relay nodes which interfaces with the sensing node to obtain and propagate data on the network, the UAV that is mobile to collate data from the relay node and carries the data to the sink device which collates and passes the data to the network control centre. Factors considered in this research include the length of the network, distance between the nodes, height of the UAV and nodes, transmission rate and communication range.

Tests were conducted in simulation and investigated the delivery ratio and the average delay of the messages from the sensor node to the sink node for three UAV speeds of movement which are constant speed UAV, adaptive speed UAV and variable speed UAV in relation to the buffer size and timeout value. Results presented in this research demonstrate the increased buffer size and timeout time increases the delivery ratio of the packets transmitted; however, the average latency recorded increased as a by-product. The authors' state the speed algorithms selected by the UAV has a different performance characteristics on the packet delivery ratio and average delay recorded.

The authors' have taken into consideration the impact of multiple hop communication in relation to the energy consumption of each node on the network. The speed of the mobile actuator has been factored and indicates that there is a relationship between the mobile device and the performance characteristics; in addition, the network and communication metrics on the mobile platform has been factored with the inclusion of the physical speed of the mobile end-point.

2.17.2 A Secure Communication Protocol for Drones and Smart Objects

Won et al; present a secure communication protocol for drone and smart objects (Won et al. 2015). The problems discussed in this research are targeted towards the communic-

ation links used to transmit and receive data between the drone and the smart objects (e.g. sensors). The authors' state that the drone could be susceptible to attacks which include impersonation, manipulation and interception of data as the drone flies unattended over possible hostile environments. The second problem identified is the key management issues as the devices are computational constrained limited flight time and mobility. The last problem discussed focused on the prevention of information leakage if a device is physically captured.

The proposals presented by the authors' are the efficient certificates signcryption tag key encapsulation method (eCLSC-TKEM); a dual channel strategy to undertake eCLSC-TKEM with smart objects as a method to conserve drone energy and the secure communication protocol for drone applications. The test environment utilised an AR.Drone 2.0 quad-copter using 2.4 GHz Wi-Fi transmission links. The drone has a 1 GHz 32-bit ARM cortex A8 CPU and 1 Gbit DDR2 RAM operating a Linux operating system. A linear network topology was chosen with a 5 metre distance between each smart object over a total distance of 80 metre. The start point of the drone was set 30 metre away from the first smart object in the topology at an altitude of 10 metre.

The eCLSC-TKEM protocol was benchmarked against CLSC-TKEM, Sun's certificateless authenticated key agreement (CL-AKA) and Yan's CL-AKA. The first test investigated the mission completion time of the four benchmarked protocols using different Elliptic Curve Cryptography (ECC) key lengths of 128-bit, 160-bit and 192-bit. Results from the test show that the size of the key has an impact on the completion size as the largest key size incurred a longer time to complete in comparison to the smaller key sizes. The method selected influenced the mission completion time with the eCLSC-TKEM method recorded the quickest completion times for all three key bit lengths selected.

The impact of the intervals between radio wake-ups was also tested in relation to the impact on mission completion time. A range of 1 to 9 second wake-up interval times were sampled. Results presented indicate that the eCLSC-TKEM method incurred the least time to complete the mission. The final test focused on the impact of eCLSC-TKEM with 128, 160 and 192-bit key sizes using the dual channel strategy and the impact on mission completion time. Results from the test suggest that the dual channels approach takes less time to complete the mission in comparison to a single communication link.

The authors' have investigated the impact of secure communication in relation to security and efficiency of a mobile system with consideration for the efficiency of the proposed solution on constrained energy resources with proof of security and reduction of time required to compute through experimentation and analytical methods. The research

presented by (Won et al. 2015, Jawhar et al. 2014) who focused on the speed of the mobile actuator; however, (Jawhar et al. 2014) factored multiple-hop propagation of data between the transmitter and receiver which correlates with experimentation undertaken by (Won et al. 2015) but different performance metrics were analysed. The emphasis of the security service provided in this research analysed authenticated key agreement methods that reduce the computational overhead.

2.17.3 A New Adaptive Security Protocol for UAV Network

Zouhri et al; introduce a new adaptive security protocol for UAV network (Zouhri et al. 2017). The authors' examined the teleoperation and telemetry communication between the ground control station and the UAV over a wireless communication link using the UAVNET protocol. The problems identified in this research is that current security protocols that currently exist are not designed for this environment in terms of the constraints of limited energy, bandwidth and computational resources in addition to a dynamically changing environment make it difficult to apply established protocol in this context; finally, modification or unauthorised data transmitted to the UAV could impact on the safety of civilians as a UAV could be used as a weapon. The proposed solution presented in this research is the derivation of new architecture that allows for secured communication between the UAV and the ground control station through cryptographic approaches to the data whilst taking into consideration the constraints and limitations of the scenario.

The instance of the new architecture is focused on the confidentiality, integrity and authentication of the data messages between the UAV and ground control station with the presentation of SPUAV. The architecture is divided into four sections; the authentication protocol that initialises the UAV to the ground control station and security parameters selected; the transfer protocol that provides data transfer to the UAV and ground control station with confidentiality and integrity of the message transmitted; the monitoring protocol that detects potential attacks and archives the attacks to prevent it occurring in the future and the security database that audits the protocols and session keys used for the system. No tests have been explicitly stated in this research.

Zouhri et al; have identified problems that correlate with areas identified by (Jawhar et al. 2014, Won et al. 2015) with the vulnerability of data transmission over unsecure communication links and the constraints associated with mobile applications. The consideration of the security service was discussed by (Zouhri et al. 2017) and stated that contemporary security approaches such as transport layer security and Kerberos were not designed for this context as the consideration for resource constraints and dynamic situations was not factored; therefore, this indicates that a new approach is required for this scenario; however, the proposed framework presented in this research is susceptible to a single point

of failure as the attacker could compromise the security database to obtain the security configurations for all devices on the network.

2.17.4 Section Summary

The next section of the literature review examines mobile to mobile end-point and how contemporary security services impact on the stated scenario. Research presented in this section of the literature review has identified the communication link as the problem as real-time teleoperation and telemetry data is propagated over unsecure communication links.

Variables associated with the problem include the limited computational and energy resources for the mobile end-point; however, security services proposed by authors in this section of the literature focus on asymmetric security services that appear to be not best suited for this context as a result of the additional processing and communication latency incurred as presented in the static to static section of this chapter.

Consideration for the multiple hop communication links to relay data between the static and mobile endpoints has been discussed in the literature; however, the focus of the multiple hop propagation of data was viewed from the perspective of the energy consumption of the computationally constrained devices. This raises the question of what the impact of security services are on the real-time teleoperation and telemetry applications over a multiple hop communication link and how the cryptographic service selected impacts on the energy consumption of the real-time teleoperation and telemetry application.

In addition, research presented has introduce single and dual communication links between the transmitter and receiver and how this interlinks with the latency measurements recorded; measurements recorded indicate that dual communication links have a reduced impact on the latency recorded; however, this raises the question of what the cost of communication is in relation to the cost of processing from an energy perspective and a requirement to validate the stated findings to confirm dual communication links have a reduced impact on the latency measurements.

2.18 Mobile to Mobile End-Points

2.18.1 Enhancing Mobile Ad-Hoc Network (MANET) Security using Hybrid Techniques in Key Generation Mechanism

A mechanism for enhancing MANET security using hybrid key generation techniques is presented by Dhanalakshmi et al; (Dhanalakshmi et al. 2014). The problems identified by

the authors' are that MANETs are susceptible to passive and active security attacks due to the infrastructureless nature of the wireless network. The proposed solution presented by the authors' is an intrusion detection system (IDS) to obfuscate the aforementioned security vulnerabilities.

The proposed IDS comprised of three components; the end-to-end acknowledgement scheme to identify and prevent a malicious node from communicating on the network by selecting the enhanced adaptive acknowledgement protocol (EAACK). The EEACK protocol consists of an acknowledgement protocol for regular communications, the secure acknowledgement protocol that checks for malicious activity at every third intermediate node on the network and the misbehaviour report authentication to confirm the authenticity of the reported misbehaving node. Digital signature schemes are selected as a method of integrity and authentication to all acknowledgement packets before transmission, the scheme selected by the authors' is the digital signature scheme (DSA). A key generation scheme is proposed by the authors' that use symmetric key generation for all nodes on the network when a node participates in communication on the network to reduce memory overhead; all cryptographic keys are pre-distributed before use to alleviate communication cost.

The test methodology used by the authors' selected 50 nodes for the MANET with a maximum mobile speed of 20 metres per second; the network field size selected was 1,500m x 300m. The packet size selected was 512 bytes with the IEEE 802.11 protocol selected to communicate with the nodes on the network. The UDP protocol was selected as the transport layer protocol. Tests conducted by the authors' were achieved using the network simulator (NS-2). Results from the simulation are inconclusive with the data not clearly presented to the reader.

(Dhanalakshmi et al. 2014) research presents a hybrid of symmetric and asymmetric cryptographic methods for secure communications between MANET devices. Integrity and authentication schemes have been considered by the authors' and correlates with (Czybik et al. 2013, Kounev et al. 2015, Mundhenk et al. 2015, Choi et al. 2016) however, the implementation differs from the aforementioned research as the context of the application is for IDS system. Limitations of the proposed approach for the context of real-time systems is the limited constraints of the system could prevent the implementation of the scheme as the latency, computational power and energy requirements as identified in aforementioned research (Czybik et al. 2013, Kounev et al. 2015, Mundhenk et al. 2015, Choi et al. 2016) would cause unreliable operation of the system as a result of the increased latency incurred from using asymmetric schemes.

2.18.2 Enhancing Security of MAC Protocol in MANET using Trust Based Engine

Pandey et al; research an enhancing security of medium access layer protocol in MANET using trust based engine (Pandey & Singh 2015). The authors' discussed the problem of securing MANETs without impeding on performance and resource constraints. The proposed solution is a specification based detection engine based on the IEEE 802.11 medium access control protocol to provide confidentiality and authentication of messages.

The detection engine was implemented with finite state machines (FSM) to represent the sequence of the operation. Three scenarios are introduced which are idle node design, transmitter design and receiver design. The idle node design views an idle node as either two states, preparing a packet for transmission or is receiving a packet from another node on the network. The transmitter design is grouped into two sections, the request to send and clear to send. The request to send design checks if the communication medium is available to transmit by retrieving a Distributed co-ordination function Inter-Frame Space (DIFS) initialisation time parameter; if the node attempts to transmit before the timer value has exceeded the timer parameter; the action is deemed as malicious behaviour and the node is prevented from transmitting the packet; if the activity is not malicious then the packet size is checked to determine if the correct size is used before transmission of the message is achieved; if the size is not valid the behaviour is reported as malicious.

The clear to send design checks the short Inter-Frame Space (SIFS) to determine if a clear to send message is legitimate; if the clear to send message was sent after the SIFS timer had expired, the message is classified as malicious, otherwise the clear to send changes state to await an acknowledgement from the transmitter node. The receiver design uses the same system as the clear to send to determine malicious activity, however, if no malicious behaviour is detected, the node monitors the network for incoming messages until the message is received or a timeout occurs. No test procedure or results of tests had been explicitly stated in this research.

The authors' present FSM and elaborate on their proposed trust based engine for securing the medium access protocol; this contrasts from the research presented by Dhanalakshmi et al; as their research proposed an intrusion detection system for MANET. The security discussed by the authors' of this research is based on a series of decisions that relate to the frame space arrival time and overlooks the conventional application of security methods for the medium access control protocol.

2.18.3 Energy Optimisation of Security-Critical Real-Time Applications with Guaranteed Security Protection

Jiang et al; research energy optimisation of security-critical real-time applications with guaranteed security protection (Jiang et al. 2015). The authors' investigate the problem of the design of a secure and energy efficient real-time embedded system with the objective of minimising energy consumed based on the energy constraints on mobile applications such as UAV. The proposed approximation approaches presented by the authors' are the round to ceiling, round to floor, round randomly and round to nearest.

The test platform selected by the authors' was simulated based on the measurements obtained from a preliminary test of the time and energy readings of various security algorithms sampled on an ARM S3C2440 CPI operating at 500 MHz and 64 MB of RAM. Results from the preliminary results indicate that stream cipher RC4 consumed the least time and energy whilst triple data encryption standard (3DES) consumed the longest time and energy consumption. The security algorithms sampled were classified in order of security level based on the result of this test with the fastest and least energy consuming ranked the lowest level (i.e. RC4) and the slowest and most energy consuming ranked the highest (i.e. AES-128).

The four approximation approaches are benchmarked in a series of tests that measured energy consumption and security risk ratio. The authors' presented five tests which were the impact of risk bound, security risk evaluation, data size of the message and the number of tasks. Summary of the test undertaken indicate that the round to nearest approximation was better suited than the other approaches to meeting the requirements specified in their research; however, this approach has the highest computation time.

Jiang et al; present a performance comparison of security services in terms of latency and energy consumption which correlates with (Salla et al. 2012) who also undertook similar analysis as both authors' investigated block and stream cipher variants. (Jiang et al. 2012) analysed the behaviour of their proposed approximation approaches in relation to the energy consumption and security risks; this correlates with research by (Won et al. 2015) who analysed a similar problem in an emulated environment; however, no mathematical modelling to predict the impact was presented by (Won et al. 2015).

2.18.4 Impact of Trust-Based Security Association and Mobility on the Delay Metric in MANET

Nguyen et al; research the impact of trust-based security association and mobility on the delay metric in MANET (Nguyen et al. 2016). The problem discussed by the au-

thors' is the broadcast delay induced from broadcast authentication between devices on the MANET and the impact of the delay on the overall system. The proposed solution presented in this research is a mathematical model for analysing the delay of epidemic broadcasts in MANET. Variables considered for the mathematical model include the network metrics, mobility of the device, the trust of each node on the network and end-to-end delays.

The test methodology selected by the authors' used a simulated environment to validate their mathematical models. Four simulations were conducted that focus on the density of nodes in an area and the velocity of the mobile nodes. The test undertaken examines the delay induced from the security handshake and the total end-to-end delay. A hundred nodes were randomly placed at the beginning of each simulation with a trust link state of 0.5 which evolves over the course of the simulation using the trust model presented by the authors'. The security packets are given random security values and the security handshake delay was set to one second. The simulations are written in the C programming language. All tests undertaken were repeated two hundred times with the average of the results presented.

Results presented by the authors' indicates that the mathematical model and the simulation correlate for fixed density of nodes at varying velocities with larger delays reported at lower velocities. The density of nodes in an area influences the delay induced with larger density of nodes reducing the delay incurred. The security handshake delay measured indicated that the simulation results have a reduced impact on the delay measured in comparison to the mathematical model results.

The authors' present a mathematical analysis of the impact of security association on the mobility of MANET systems; this continues from (Jawhar et al. 2014) who specifies the network metrics and some operational characteristic into consideration of their problem and Won et al; who investigated packet delivery ratios and timeout delays.

2.18.5 Section Summary

The literature presented in this section introduces the mobile to mobile real-time applications. Problems presented by authors focus on performance of the mobile end-point from the perspective of the impact of security services on energy consumption or latency incurred by the real-time application.

Security services investigated in this section of the literature considered symmetric and asymmetric approaches to provide confidentiality, intergrity and authentication to packetised data over an unsecure communicaiton link; however, it is not explicitly stated what

the impact of the presented security services have on the mobile to mobile rean-time application. This further raises the question of what the impact of contempoary security services on a mobile to mobile real-time applicaiton.

The next section of the literature review investigates the psychological factors that motivates an attacker to undertake security related attacks and how humans interact with real-time teleoperation and telemetry applications.

2.19 Psychological Factors of Security and Real-Time Teleoperation and Telemetry

This section of the literature review present research of the psychological aspect of security and real-time teleoperation and telemetry. The literature discussed in this section of the review analyses the human with investigation of the impact of response times between human interaction and machine response and the motives for humans to conduct attacks against systems.

2.19.1 Response Time and Display Rate in Human Performance with Computers

Shneiderman et al; conduct an investigation of the response time and display rate in human performance with computers (Shneiderman 1984). The problems analysed in this research consider the importance of response time between a human and a computer to complete a task; the authors' specify that short or long system response times increase errors in a process, make ill considered decisions, lower comprehension and understanding of the situation. The authors' discuss the relationship between short-term human memory and sources of error with particular emphasis on the short-term memory and working memory and how volatile the memory is with disruptions causing loss in memory, errors and delays with the presence of interpretation of sensory distraction (e.g. visual or audio disturbance).

The authors' further elaborate on the issues of display rates and how this contributes towards the users expectation and attitudes in shaping their subjective reaction to the computer system response time that include previous experience, variation in individuals response time and the human adaption to the situation. Examination of human performance with computer was presented through previous case scenarios undertaken by other researchers in the field; aspect investigated include variation in response times between human and computer and how this impacts the productivity of the human. Summary of the research presented in this article demonstrates that response times under one second increase productivity of a human; however, the number of errors incurred is either increased or decreased dependent on how difficult the error it is to detect the error; this

suggests that there is a trade-off between the response speed of the computer and the human performance based on the number of errors incurred.

The paper analysed the impact of response time on human performance; however, consideration of the additional processing time on the impact of the human performance was not discussed as the focus was on time of response. As real-time teleoperation and telemetry processes examined in this thesis are inter-linked to human reaction time as the human that has manual operational control of real-time teleoperation and telemetry system; this correlates with literature presented by Woods et al; that human response time vary between one hundred to two hundred milliseconds (Woods et al. 2015). This further reinforces the research presented by Shneiderman et al; as the trends identified in this research shows the errors increases if the variation between the mean response time is plus or minus fifty percent and that there is no general rule to which approach is more suitable but that it is context driven and dependent on the situation (e.g. new or experienced workers).

2.19.2 Get Your Head Around Hacker Psychology

Gold analyses the psychology of a hacker and the motivation behind their decision to hack (Gold 2014). The author categorises hackers into three groups, white hats hack systems to identify and overcome flaws within a system to prevent malicious attacks; black hats that compromise IT systems for their own beneficial gain or choice and the grey hats that ethically hack to seek additional methods to defend their network.

Gold elaborates on the differences in techniques used by a hacker from the 1970's and 1980's to the modern concept of a hacker. The techniques used by hackers previously focused on 'phreaking', the concept of experimentation with telecommunication equipment and network systems; whilst modern techniques are targeted towards social engineering and client side exploits. An interview with ex-hacker Kevin Mitnick reveals that it is easier to attack a system than defend it; Mitnick states that the weakest link of the system is the human element through the use of social engineering rather than the misuse of technology as humans are susceptible to manipulation of their own emotions.

The perception of a hacker is also discussed by the author as the social view of a hacker in the 1970's and 1980's was viewed as electronic joyriding and portrayed as a Robin Hood approach to electronic devices; whilst modern society takes the view of hacking as in inexcusable crime against society as the number of people that have been exploited to viruses and online hacking has increased. Gold states that the sociological view of hackers has been facilitated by the use of media and governments to protect their own agendas; however, with the increase in understanding of the technology and hacking concept, activists seek to use hacking to expose the covert activities undertaken by the government

with reference to the case scenario of Gary McKinnon.

Psychological behaviour and profiling of hackers is discussed throughout the literature with comparison of autistic spectrum disorder (ASD) through subjective observation by the author. The author states that social and psychological elements have moulded a person to become a hacker (e.g. difficulty in social situations, focuses on the facts). Methodologies presented to overcome the hacker mindset has been presented by Gold through the use of Neuro-Linguistic programming (NLP); this method uses language to programme a humans behaviour and change the mindset; however it is argued that this is only possible if the person is willing to change their mindset. In addition, the requirement of hackers is discussed as defence organisations are actively recruiting hackers to prevent cyber attackers or terrorism with the UK ministry of defence used as the case scenario.

2.19.3 Understand Insider Threat: A Framework for Characterising Attacks

Nurse et al; introduce a framework for characterising insider attacks for enterprise systems (Nurse et al. 2014). The authors' have identified that the insider attack has become an increased threat to organisational security with a reported fifty-eight per cent of security incident was recorded to be an insider attack. A profile of an inside attacker stated by the authors' is an employee that is currently or previously worked for the company, contractor or trusted third party that has privileges to the network. Two categories of insider attacker have been presented in this literature, legitimate inside attackers who seek to gain privileges of the system for their own personal gain and accidental insider attackers that unintentionally caused threat to the confidentiality, integrity and authentication of the network.

The proposed solution presented by the authors' is a framework for characterising insider attacks based on real-world data and existing literature. The framework considers four elements based on psychological elements which are the catalyst, actor's characteristics, attack characteristics and organisation characteristics. Each section is further categorised by the authors'; the catalyst is discussed as the precipitating event that initialised the cause of the insider attack; actors characteristics comprise of the psychological factors of the employee in terms of their psychological past and present attitudes; in addition, the actor characteristics include the motivation, skills and opportunity presented to undertake an inside attack and their role to the company. Attack characteristics which are attacks used by the actor, the objective of the attack and the steps required to achieve the desired goal; organisation characteristics look at the asset under attack and the impact of exploitation of the vulnerability.

The conceptual framework presented by (Nurse et al. 2014) introduces an indication to

the logical process of an insider attacker form the cause to the end outcome of the attack; however, the authors' have specified limitation with their approach as the current framework does not consider the personality characteristic or motivation of the attacker, how the data can be used to predict an insider attack and what level of revenge is required before action is taken; this is presented in Gold's paper (Gold 2014) that classifies the motivation through the variation of attacker types (e.g. black, grey and white hats).

2.19.4 Section Summary

Analysis of the motives behind an anti-persona conducting an security attack against a system is derived for a variety of underlying factors. Understanding the reasons to why an anti-persona is undertaking the attack enables proportionate security controls and countermeasures to be deployed to overcome the problem investigated in this thesis.

Examination of the interaction between the human and a real-time application indicates that the latency between real-time teleoperation and telemetry commands influence the response time for a human to react to the information presented and conduct the task presented. This raises the question of how the real-time task schedulers and the latency incurred by security services impacts on the manual control of real-time applications.

2.20 Discussion of Literature Review

The literature reviewed identified three areas of current research, the hardware implementation method of cryptographic methods; application of enterprise methods in the context of real-time teleoperaiton and telemetry and the key management mechanism used. The hardware implementation approaches presented by research propose claims of meeting real-time requirements with minimal impact on the performance of the system; but, the limitations of this approach is the fixed nature and the amount of room required to implement the solution.

Security service used by researchers throughout the literature are commonly found in enterprise computer network environments that were not designed with the consideration of real-time teleoperation and telemetry; in addition, the specified recommendations in the X.800 standard states the requirement for connection and connectionless security services for data-link communications with decipherment techniques; however, findings obtained in the literature select methods that are computational intensive, are not suited for the context of real-time teleoperation and telemetry (i.e. asymmetric authentication schemes) and are bespoke to a particular scenario only.

Examination of the threats investigated in contemporary research reviewed demonstrates

that the main threats considered by researcher is the communication link between the transmitter and receiver as current real-time applications transmit data without the consideration of security services or with security solutions that are not best suited for this context; this is of particular concern in the context of static to static scenarios as the impact of an attacker conducting passive or active attacks against the real-time teleoperation and telemetry and is transferable to static to mobile and mobile to static scenarios where the problem becomes multi-faceted as a results of the mobile nature of the end-points and the limited resources and time constraints of the real-time teleoperation and telemetry system.

Factors considered to overcome the problems specified by authors throughout the literature survey focus on confidentiality and authentication schemes. Confidentiality methods proposed varied between the standardised AES-128 block cipher with different variations analysed and stream ciphers using a Fiestel strictures; however, the variation of schemes proposed to achieve confidentiality are limited with designs proposed for enterprise systems considered which appear to be unsuited for real-time teleoperation and telemetry applications as proposed schemes have an impact on the performance of the real-time teleoperation and telemetry in terms of energy consumption, latency incurred and its ease of implementation; this is also present in the analysis of authentication schemes and indicates that asymmetric methods are not best suited in comparison to symmetric schemes as a result of the additional latency recorded.

There is minimal consideration for the integrity of the data as it is propagated across the communication link and is an important factor to include in order to achieve a secure communication link with most research concerned on confidentiality and integrity; this is an issue that is required to be addressed especially for real-time teleoperation and telemetry data as intentional or unintentional modification of data packets for either teleoepration or telemetry could result in incorrect telemetry reading and unknown commands sent to the actuator; this is further exemplified in applications where mobile systems are selected as the mobile end-point would continue to travel before the next legitimate command is received.

Alternative factors presented in the literature review are related to key management and key distribution between the communicating entities. Approaches presented by researchers tend to follow an identical approach to key management as found in the literature review with static key implementation or pre-computed keys generated and rotated after a fixed period of time; in addition, the challenge of performing a key exchange over an unsecure communication link is negated as the majority of methods presented do not elaborate on the mechanism of invoking a key regeneration between transmitter and receiver.

Research identified in the background literature and literature review demonstrates that contemporary security services derived to secure real-time teleoperation and telemetry communications were designed with two main considerations; the security (i.e. resilience or strength against attack vectors) and the energy conservation of the block cipher.

Approaches that focused on the resilience of the block cipher against attack vectors are not best suited in this application as the time required to compute the cryptographic operation; this was particular prominent with propositions that used asymmetric cryptographic methods with reported latency measured are reported in the seconds range; whilst reported latency measured for symmetric cryptographic methods were within the millisecond range; this demonstrates that symmetric cryptographic methods are better suited for the application of real-time teleoperation and telemetry as the additional latency incurred is reduced in comparison to asymmetric cryptography; with variations of lightweight block ciphers that have been designed for constraint devices.

Analysis of the lightweight block cipher presented in existing literature demonstrates that the objective of the designs presented were targeted to maintain the cryptographic strength of the cipher and reduce the energy consumption of the operation as demonstrated across all the block ciphers reviewed; however, these methods do not take into consideration the latency of the cryptographic process and in the context of real-time teleoperation and telemetry this is priority to ensure specified deadlines of the system are met.

The implementation method selected for the majority of the specified ciphers reviewed was hardware with only KLEIN and SPECK as software variations; it is known that hardware implementations have less impact on latency than software approaches; however, it is not known if the real-time deadlines can be achieved with software block ciphers variants and requires an in-depth investigation to ascertain its viability in the context of real-time teleoepration and telemetry.

Contemporary AEAD constructs identified in the background literature were designed to simultaneously provide confidentiality, integrity and authentication assurances on data; however, in recent literature reviewed, the existing research and lightweight cipher schemes presented segment the component of the secure communication channel into separate cryptographic operations; this is because the AEAD paradigm integrates the process in order to achieve the cipher-text output in one or two passes; therefore, it is beneficial in terms of reduced latency as demonstrated by Adekunle and Woodhead benchmark analysis of TinyAEAD against EAX-Prime.

Further analysis of the literature indicates that the consideration of the AEAD paradigm

has been overlooked in favour of methods found in an enterprise network or with the defined lightweight block ciphers reviewed in this literature; however, it appears that the contemporary AEAD scheme devised are a feasible solution in the context of real-time teleoperation and telemetry but there is limited literature that analyses the application of this solution to a real-time context; therefore, the requirement of a problem analysis on the selection of AEAD constructs in real-time teleoperation and telemetry scenarios is required in order to understand if this method is best suited for this situation.

Trade-offs appears to be a frequent occurrence throughout the literature with analysis of the time required to process the secure communication process and how its implementation with software and hardware variants contribute towards the problem in terms of latency; however, there is limited understanding of how this transfers into the context of real-time teleoperation and telemetry from the prospective of network metrics, impact on the mobile end-point performance and the consequence in terms of safety, reliability and availability of the system; therefore, further in-depth analysis is required to understand the problem and determine if it is feasible to implement a secure communication link whilst meeting the performance requirements of the real-time teleoperation and telemetry.

Literature undertaken in Chapter 2 demonstrates that the majority of contemporary research undertaken has measured the cost of security services from the perspective of the additional processing latency incurred by the real-time application; however, investigation of the impact of the additional latency incurred on the real-time application has not been explicitly disseminated in literature reviewed in this thesis. In addition, the consideration of the real-time task schedulers in relation to security services has not been explicitly stated in the literature presented in this thesis.

Contemporary research investigated throughout the literature review has considered elements of the communication link in terms of the maximum transmission power used by the transmitter; however, the consideration of a non-ideal communication link and the arrangement of the components used for communication is not explicitly stated. This indicates that there are grounds to conduct further investigation to ascertain how a non-ideal communication link and the configuration of the components required to facilitate communications interplay with the real-time teleportation and telemetry applications.

The components that contribute towards the secure communication link for the context of real-time teleoperation and telemetry requires in-depth analysis in order to ascertain how the individual components contribute towards the secure communication link for real-time teleoperation and telemetry and understand the underlying cause to why contemporary solution are not adequate for this context; this is also applicable towards the key manage-

ment used for symmetric cryptographic systems as this component of the block cipher is the shared secret between the communicating entities and is therefore an area that requires further research in order to determine how this influences the problem in the context of secure communication links for real-time teleoperation and telemetry.

2.21 Selected Areas of Contribution

The stated areas of contribution from the literature review undertaken are as follows:

- Propose a cryptographic primitive to fulfil the constraints associated with real-time teleoperation and telemetry as existing methodologies were not designed for this context;
- Propose a philosophy that provides secure communication links whilst fulfilling the constraints associated with real-time teleoperation and telemetry applications as contemporary cryptographic approaches used in enterprise networks are not suited for this context;
- Implement a novel approach to securing real-time teleoperation and telemetry applications as current philosophies of implementing secure communication links are focused towards the strength of the cryptographic output or energy consumption of the algorithm.

2.22 Proposed Questions

Analysis of the literature review undertaken has highlighted five areas to be investigated in the problem analysis. The areas of investigation and the proposed questions derived for the problem analysis are as follows:

2.22.1 Investigation of Real-Time Teleoperation and Telemetry Communication Latency on Static End-Points

- What is the impact of contemporary security services on the communication latency incurred by static devices (transmitter and receiver) used for real-time teleoperation and telemetry?
- What is the impact of contemporary security services on the communicated packet throughput of each device (transmitter and receiver) used in static real-time teleoperation and telemetry applications?

2.22.2 Investigation of Real-Time Teleoperation and Telemetry Communication Latency on a Mobile End-Point

- What is the impact of contemporary security services on the latency incurred by devices (transmitter and receiver) used in mobile real-time teleoperation and telemetry applications?
- What is the impact of contemporary security services on the maximum communication range between the transmitter and receiver devices used for mobile real-time teleoperation and telemetry applications?

2.22.3 Investigation of The Communication Link and Real-Time Task Scheduler

- What is the impact of real-time teleoperation and telemetry on instantaneous packet throughput under non-ideal communication links?
- How does the antenna placement and receiver sensitivity influence the operational range of the real-time teleoperation and telemetry application?
- How does the selection of real-time task schedulers impact on the latency measurements recorded?

2.22.4 Investigation of Latency on Real-Time Teleoperation and Telemetry Applications

- What is the energy cost of processing and communications on real-time teleoperation and telemetry applications?
- What is the impact of cryptographic services on the energy consumption for real-time teleoperation and telemetry applications?
- How does the implementation method of the cryptographic services impact on real-time teleoperation and telemetry applications?

2.22.5 Analysis and Profiling of Cryptography

- What is the operational performance profile of the standardised AES-128 block cipher?
- What key implementation methods are used by the AES-128 block cipher and how does each approach frustrate an attacker from compromising the cryptographic key?

2.23 Chapter Summary

The chapter presented a preliminary literature review of individual areas that are related to the research problem specified in Chapter 1; areas discussed in this section analysed standardised frameworks derived to present recommendation of security services in relation to the OSI network model and the implementation of asymmetric PKI. Security paradigms that apply security services of confidentiality, integrity and authentication have been identified with the MACSec and IPSec protocol and the presentation of the contemporary AEAD paradigms with examination of constructs designed for the context of security and energy conservation. Implementation methods for the security services, communication links and real-time devices have been identified and categorised.

The literature review examined research areas that incorporated the areas presented in the preliminary literature review. Analysis of the current research demonstrated that current security services for real-time applications are not best suited as the impact on the operational performance of the system is significant and the current approaches presented are not designed based on the recommendations of the standardised frameworks. Methods of block cipher designs that are classified as lightweight consider the requirement of energy conservation only and are generally implemented in hardware to meet real-time constraints. Selected areas of contribution based on the findings of the literature review have been presented.

The discussion of the literature review identified that the focus of current research examined the problem from three viewpoints; the hardware implementation of security services; the application of enterprise security methods used in the context of real-time teleoperation and telemetry and the investigation of cryptographic key management techniques used. Consideration of the impact on the transmitter and receiver devices with the consideration of the communication channel characteristics has not been fully investigated and the proposed cryptographic approaches are bespoke to the requirements of the individual scenario; therefore, the next section of the thesis presents the problem analysis.

The problem analysis is segmented into four chapters; Chapter 3 examines the problems associated with communication latency on real-time teleoperation and telemetry of the transmitter and receiver devices; Chapter 4 investigates the communication latency on the real-time teleoperation and telemetry with mobile end-points. Chapter 5 examines the communication link and real-time schedulers used by real-time applications using teleoperaiton and telemetry and Chapter 6 investigates latency on the real-time teleoperation and telemetry applications. Chapter 7 analyses contemporary cryptography methods. The next chapter introduces the problem analysis of the transmitter and receiver.

3 Investigation of Real-Time Teleoperation and Telemetry Communication Latency on Static End-Points

3.1 Introduction

As discussed in Chapter 2; ideally, teleoperation and telemetry communication links should be able to move as much data as is required instantaneously without any loss of data. In reality this is unachievable, as the physical laws of reality introduce communication delay which impacts on packetised data throughput.

The purpose of this chapter is to ascertain the fundamental relationships associated with real-time teleoperation and telemetry links utilising contemporary security services to mitigate against attacks. The areas investigated in this problem analysis are communication latency and throughput from the viewpoint of a static transmitter and receiver used in real-time teleoperation and telemetry applications.

In this chapter, the problem analysis undertaken is based on the following questions:

- What is the impact of contemporary security services on the communication latency incurred by static devices (transmitter and receiver) used for real-time teleoperation and telemetry?
- What is the impact of contemporary security services on the communicated packet throughput of each device (transmitter and receiver) used in static real-time teleoperation and telemetry applications?

The structure of this problem analysis undertaken is as follows; section 3.2 introduces the investigated problem scenarios to provide context to the analysis undertaken; section 3.3 presents the analysis of the impact of security services on the latency for a single, simplex communication link and for a dual, half-duplex communication link. Sections 3.4 presents the impact of homogeneous and heterogeneous transmitter and receiver configurations on the real-time teleoperation and telemetry applications over a point to point communication link and a multiple hop communication link. A discussion of the findings obtained from the investigations undertaken is presented in section 3.5. A chapter summary concludes in section 3.6.

3.2 Investigated Problem Scenarios

To aid in the examination and quantifying of communication latency in a static-to-static situation, a problem scenario is described to contextualise the problem investigated in this chapter. The scenario presented is an open loop control system that is used to automate a

safety critical process for the prevention of dust explosions. Dust explosions in bulk solids powder handling can result in personal injury or death and loss of the processing plant. The adoption of legislation to mitigate the impacts of such events is now widespread and many technical approaches can be applied to ensure plant safety. The scenario assumes the use of these counter-measures commonly found in industry. Figure 3.1 illustrates a schematic of a pneumatic system found in industry along with the type of explosion suppression typically utilised.

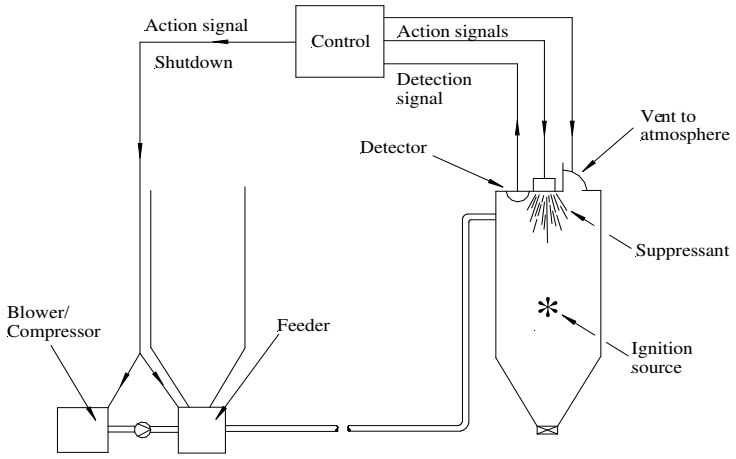


Figure 3.1: Schematic of a dust explosion suppression system typically incorporated into a process plant for powder handling.

The preliminary analysis of the static to static real-time application indicates that real-time teleoperation and telemetry are the most significant aspect to be taken into consideration as the telemetry data from the sensor (i.e. detector) and its interpretation for teleoperation response is crucial in order to prevent a firm real-time application from failing (i.e. opening the vent in time).

Secure communications between the communicating entities in the system is normally used in order to hinder cyber attacks against the application; such as passive attacks where communicated teleoperation and telemetry traffic can be monitored without modification to the contents and an active attack where data is intercepted and modified during propagation. The motivation for selection this scenario is the additional processing cost of utilising contemporary security service methods that could result in a catastrophic failure of this form real-time application.

3.3 Analysis of Communication Latency on Real-Time Teleoperation and Telemetry

The communications required in Figure 3.1 are presented as three teleoperation tasks, they are the operation of the vent on the silo to release pressure, the control of the suppressant to dampen an explosion and the shutdown command to the compressor and feeder system. The real-time telemetry task identified in this scenario is the periodic measurements (dust concentration level) relayed to the controller; where it is processed and used to determine the teleoperation action to perform (e.g. operates the vent to reduce the pressure within the silo).

The consequence of the static to static real-time teleoperation and telemetry not meeting timing constraints could be server implication on the safety of employees and reliability of the system. This problem scenario can be classified as a hard real-time system (Shin & Ramanathan 1994); consequently, for this scenario the tasks are computed in a periodic order whilst meeting the specified hard real-time constraints. Research presented by Hienrich (Hienrich 1988) states that the real-time requirement for a dust explosion scenario is twenty-five milliseconds before the pressure begins to reach dangerous levels; therefore, this value is used in this investigation as the real-time deadline.

3.3.1 The Impact of Communication Latency on Real-Time Teleoperation Over a Single Communication Link

This section investigates the communication latency in a single hop simplex communication link. The previous analysis of the static to static real-time teleoperation and telemetry scenario demonstrates that there are multiple tasks that are required to be computed to prevent an uncontrolled dust explosion scenario. This analysis focuses on the simplex communication link between the controller and an actuator that performs certain tasks in the system (i.e. to initiate the suppressant) in order to control an event (i.e. dust explosion).

A task analysis of the real-time teleoperation and telemetry used in this scenario is conducted to specify the timing requirement for each operation. The tasks are presented in three categories; the input tasks, processing tasks and output tasks in order to quantify the real-time application; it is assumed in this analysis that the timing requirements are undertaken in reference to the twenty-five milliseconds deadline specified for this case scenario (see section 3.3) and the tasks analysed are focused on the worst case execution time for the real-time application. Appendix A tabulates the timing requirements for each task of the static to static real-time application.

For this scenario the order of tasks specified follow a first in first out (FIFO) scheduling that processes each task in sequential order; once the controller reacts to the dangerous level of dust concentration detected within the silo. It is be assumed that the examination of the worst case execution time of the FIFO scheduler on the operation of the static-to-static scenario is the maximum hard real-time deadline of the system

The literature review in Chapter 2 showed that the security services examined impacted on real-time applications; therefore, the area investigated in this section of the analysis is the impact of additional communication latency incurred over a single-hop simplex communication link on the static to static real-time application scenario, when utilising data confidentiality and integrity security services.

The problem examined in this section of the thesis is segmented into three areas; the transmitter node, the receiver node and the communication link. Variables identified in the three areas examined are as follows: the processing frequency of the computing device; the transmission rate between the transmitter and receiver, the propagation method between the communication devices; the security service selected and the size of the packet used for real-time teleoperation and telemetry data. In order to acquire a deeper understanding of the additional latency incurred, a mathematical model has been derived to calculate the total latency incurred for the stated scenario and is presented in Formula 4.

$$\tau dl = (\triangle(\eta + \delta + \psi)) + \frac{\nu}{\ell} \tag{4}$$

Formula 4: Secure communication latency model for a single hop link.

To calculate the total communication latency (τdl) for a single hop link, the equation calculates a subtotal of the instruction cycle time (δ) (at a specified crystal frequency) for a microcontroller to process and transmit one byte of data across to the receiving microcontroller; the time to transmit the data (η) and the time to process a byte of data though the security algorithm (ψ). The size of the packet $(\bigtriangleup)$ is multiplied by the sub-total acquired from $(\eta + \delta + \psi)$, to acquire the latency for the desired packet length in bytes. The propagation delay is calculated by dividing the speed of the transmission method (ν) (e.g. radio frequency communication speed of $2.99 * 10^8$m/s) by the distance of the link in metres (ℓ).

The model presented in Formula 4 is used to forecast the impact (i.e. additional latency) of security services on the communication latency over a single hop simplex communication link; the parameters for this analysis are listed in Table 3.1.

Table 3.1: Parameters selected to model the impact of security services on the communication latency over a single hop simplex communication link.

Independent Variable	**Dependent Variable**
Variable	**Value**
Packet Size	36 bytes
Transmission Delay	8 milliseconds
Propagation Delay	300 nanoseconds
Communication Distance	100 metres
Instruction Cycle	1 microseconds
Delay Per Instruction Cycle	**Trial 1:** 25 microseconds **Trial 2:** 100 microseconds **Trial 3:** 400 microseconds

Analysis of the forecast obtained from the model is presented in Table 3.2.

Table 3.2: Forecasted impact of security services on the communication latency over a single hop simplex communication link using mathematical modelling

Independent Variable	**Dependent Variable**
Security Service Sample	**Total Delay (ms)**
Trial 1	288
Trial 2	292
Trial 3	302

Results presented in Table 3.2 demonstrates that the increased time to process the security service does have an impact on the total delay measured. Further analysis of the findings presented in Table 3.2 demonstrates that the delay per instruction cycle does contribute to the total delay recorded; the difference in the time recorded is four milliseconds when Trial 1 and Trial 2 are compared and fourteen milliseconds when Trail 1 and Trail 3 are compared. The findings presented in this table indicate that the difference in the total delay recorded is dependent on the time-base selected; this is because the time-base determines the severity of the difference (i.e from milliseconds difference to seconds difference).

Validation of the mathematical model is conducted through benchmark analysis against results obtained from a simulated environment. The tests simulated the end-to-end communication latency of two communicating microcontrollers. Three Serial Peripheral Interface (SPI) divisor settings of four, sixteen and sixty-four were selected to examine how the transmission rate influenced the latency. Packet sizes of thirty-six, fifty-two and eighty-four bytes were selected to represent small-sized packets used in real-time teleoperation and telemetry. The structure of the packet is a follows, the header is sixteen bytes in length; followed by a variable length payload; a four byte message integrity check is applied to the trailer of the packet. This packet format is used for all experiments in this

thesis.

Crystal frequencies of 1 MHz (0.25 Million Instructions Per Second), 4 MHz (1 Million Instructions Per Second) and 8 MHz (2 Million Instructions Per Second) were selected to represent crystal frequencies used by the PIC18F45K22 microcontroller. Appendix B illustrates the schematic of the test platform. Figure 3.2 graphs the total latency recorded (obtained from the simulator) for a thirty-six byte packet size with no security services, varying transmission rates and crystal frequencies.

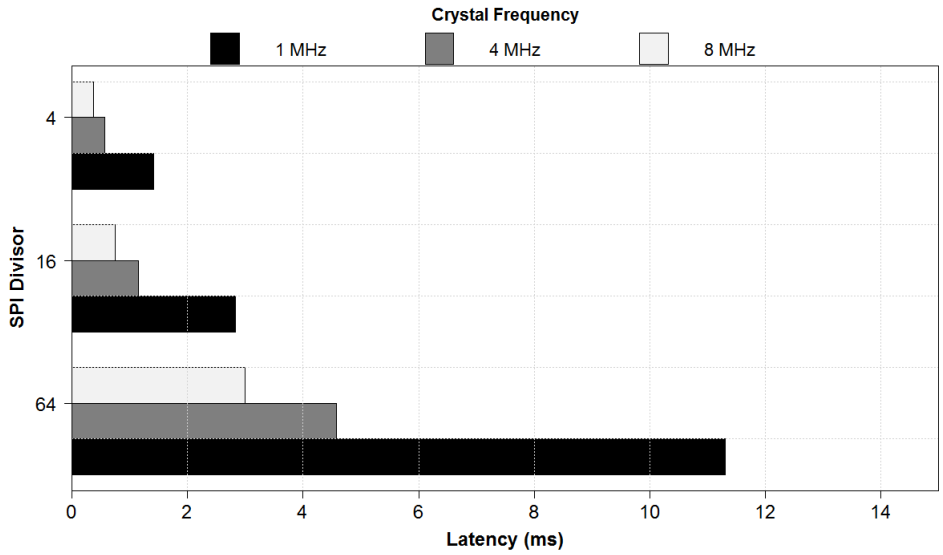


Figure 3.2: Communication latency for a simulated single hop simplex link without security for a thirty-six byte packet length. Transmission rate is calculated by dividing the crystal frequency by the SPI divisor.

Results presented in Figure 3.2 shows that the crystal frequency selected for the microcontroller contributes to the total latency recorded with higher crystal frequencies recording a reduction in the total latency incurred in comparison to lower crystal frequencies. The transmission rate contributes to the latency with an increased latency recorded for lower transmission rates in comparison to higher transmission rates.

Analysis of the findings presented shows that all of the configuration settings meet Hienrichs twenty-five millisecond real-time constraint for the dust explosion scenario specified. The next test examined the latency incurred with the inclusion of security services utilised to mitigate cyber attacks.

AEAD (Authenticated Encryption with Associated Data) constructs were selected as the security constructs utilised in this problem analysis; they are the contemporary approach to providing confidentiality and integrity security services to packetised data. Three

AEAD constructs utilising the Advanced Encryption Standard (AES) block cipher are examined in this thesis; CCM-AES-128 and GCM-AES-128 constructs are selected as they are NIST standardised AEAD constructs that were designed with security as a primary design consideration. The final AEAD construct examined in his thesis is the TinyAEAD-AES-128 construct, this is because this construct's main design consideration is focused on energy conservation (see Chapter 2, section 2.5).

For this test the null hypothesis is that security constructs will have no impact on the communication latency in a single hop simplex communication link. The alternative hypothesis is that the security construct will have an impact on the communication latency in a single hop simplex communication link. Figure 3.3 graphs the total latency measured using the simulator to process various packet sizes with AEAD security constructs at crystal frequencies of 1 MHz, 4 MHz and 8 MHz and a SPI divisor of four.

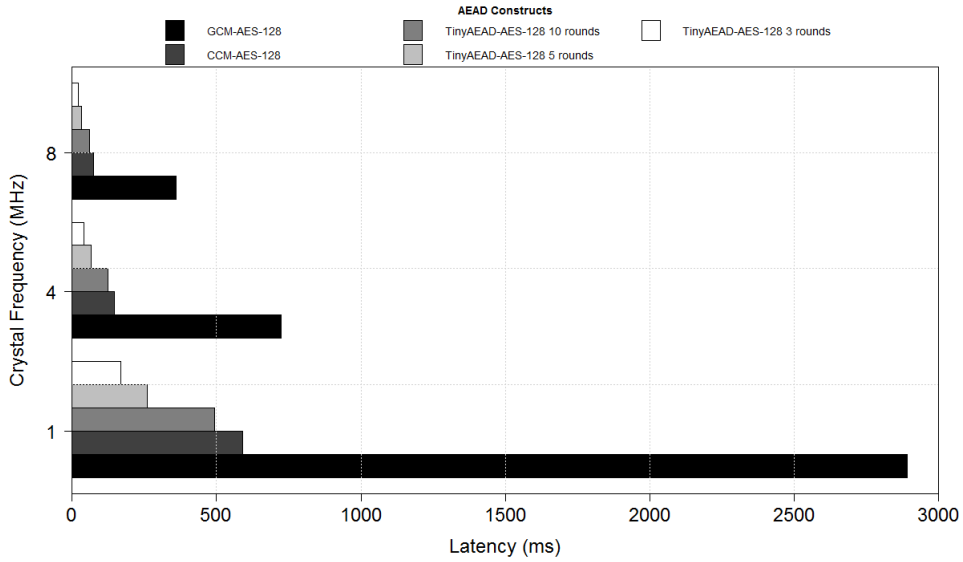


Figure 3.3: End to end communication latency for specified AEAD constructs on a simulated single hop simplex communication link for a thirty-six byte packet size. Transmission rate is calculated by dividing the crystal frequency by the SPI divisor of four

Results displayed in Figure 3.3 shows that the TinyAEAD-AES-128 construct at three rounds induced the least latency whilst GCM-AES-128 recorded the highest latency. The frequency of the crystal influenced the latency measured as higher crystal frequencies had a reduced latency in comparison to lower crystal frequencies. Further analysis of TinyAEAD-AES-128 and CCM-AES-128 with fifty-two and eighty-four byte packets is presented in Table 3.3; for this test the GCM-AES-128 construct was not selected; this is because the comparison undertaken between CCM-AES-128 and software implementation of GCM-AES-128 for a thirty-six byte packet size shows that GCM-AES-128 is not suited for real-time teleoperation and telemetry in contrast to CCM-AES-128; there-

fore, the CCM-AES-128 construct is selected as the benchmarked standardised AEAD construct for the rest of the problem analysis and this thesis.

Table 3.3: Simulated end to end communication latency for TinyAEAD-AES-128 and CCM-AES-128 constructs on a simulated single hop link for a fifty-two and eighty-four byte packet size at 8 MHz crystal frequency (2 Mbps transmission rate).

Independent Variable	**Dependent Variables**			
Packet Size (Bytes)	**TinyAEAD-AES-128 3 rounds (ms)**	**TinyAEAD-AES-128 5 rounds (ms)**	**TinyAEAD-AES-128 10 rounds (ms)**	**CCM-AES-128 (ms)**
52	31.1	48.4	92.1	103.6
84	51.5	80.4	153.0	162.8

Results presented in Table 3.3 demonstrates that the TinyAEAD-AES-128 construct at three rounds has the smallest impact on latency whilst CCM-AES-128 has the largest impact latency recorded. The size of the packet has an influence on the latency incurred with the eighty-four byte packet size recording a higher latency measurement in comparison to the fifty-two byte packet for all constructs sampled. Examination of the findings between the no security and security results demonstrates that the majority of security services examined would not fulfil the real-time requirements specified by Hienrich (i.e 25 milliseconds).

The difference between the TinyAEAD-AES-128 construct and the CCM-AES-128 constructs for the same number of rounds used by the underlying block cipher demonstrates that there is marginal difference a twelve percent reduction between TinyAEAD-AES-128 and CCM-AES-128 for a fifty-two byte packet and a six percent for an eighty-four byte packet. Analysis of the investigated AEAD constructs indicates that the construct has an implicit impact on the communication latency recorded; the underlying block cipher demonstrates an explicit impact on the communication latency incurred as the TinyAEAD-AES-128 construct configured at three rounds incurred a reduction of two point three times reduction for a fifty-two byte message and a two point six times reduction for an eighty-four byte packet.

Analysis of the packet size selected for secure communications between the transmitter and receiver demonstrates that the size of the packet impacts on the communication latency incurred with a difference on average of thirty-nine percent between the fifty-two and eighty-four byte packet analysed.

In the context of this research, the combination of the number of rounds used by the underlying block cipher and the size of the real-time teleoperation and telemetry packets are the two explicit variables that contribute to the communication latency incurred and the AEAD construct has an implicit impact; this means the configuration of the security service and the protocol used for communicating data will influence the real-time application and the time to complete a tasks or operation.

A benchmark comparison of the mathematical model against the simulation was conducted to validate the proposed model presented in Formula 4. The simulated microcontroller selected (PIC18F45K22) used a crystal frequency of 20 MHz. Packet sizes of thirty-six, fifty-two and eighty-four bytes were selected. TinyAEAD-AES-128 operating at three rounds was selected as the security construct, as previous tests have demonstrated that this construct has induced the least communication latency. Table 3.4 presents the results of the mathematical model and the simulation.

Table 3.4: Results of model versus simulation for software implementation of TinyAEAD-AES-128 at three rounds at a 20 MHz crystal frequency (5 MIPS) and a transmission rate of 5 Mbps.

Independent Variable	**Dependent Variables**	
Packet Size (Bytes)	**Model Results (ms)**	**Simulation Results (ms)**
36	8.64	8.64
52	12.79	12.78
84	21.34	21.30
Mean	**14.26**	**12.24**
Standard Deviation	**6.47**	**6.45**
Coefficient of Variance	**45.37**	**52.56**

Results presented in Table 3.4 shows that the error between the mathematical model and simulation increases as the packet size increases, however, the significance of the difference for the same packet size examined is within one standard deviation (binomial distribution); furthermore, the findings obtained from the mathematical model and simulation comparison follow a strong positive correlation as the latency recorded increases as the packet size is increased for the same security service examined.

Further analysis of the mathematical model and the simulation results was conducted with the coefficient of variance analysis; this is to determine the variance between the mathematical model results and simulation results. The coefficient of variance demonstrates that there is not a significant difference between the mathematical model and simulation results.The standard deviation between the two sets of results are near identical; however,

the mean of the mathematical model values obtained is offset from the actual simulation measurement recorded.

3.3.2 Section Summary

Findings obtained from the analysis of the simulation and mathematical model demonstrates that the alternative hypothesis presented in this analysis holds true as the selection of the security service does impact on the communication latency over a single hop simplex communication link; this is mainly due to the time required by the underlying block cipher used by the AEAD constructs to process the security service. It was shown that reducing the number of rounds of the block cipher results in a lower impact on communication latency.

The AEAD paradigms investigated in this analysis implicitly impact on the communication latency incurred by the real-time application; however, AEAD constructs designed with security as the main design consideration (i.e. GCM-AES-128 and CCM-AES-128) do not have a significant difference in comparison to AEAD constructs designed with energy as the main design consideration (i.e. TinyAEAD-AES-128), when the number of rounds for the utilised block cipher is not reduced.

Additional factors that further contribute towards the problem are the processing speed of the microcontroller as the rate a task can be computed dictates the latency recorded. The packet size also contributes to latency as the increased number of bytes results in additional processing needing to be undertaken; however, this raises the question of how the impact of latency would influence a static to static real-time application with dual communication links as a real-time teleoperation packet in the presented scenario requires an acknowledgement packet to be sent to the controller to ensure that the teleoperation packet has been received. The next section investigates the impact of latency on real-time teleoperation over half-duplex links.

3.3.3 The Impact of Latency on Real-Time Teleoperation over Half-Duplex Dual-Communication Link

This section investigates the phenomena of the communication latency over a single hop half-duplex dual communication link. The communication between the controller (e.g. micro-controller) and actuator in the static scenario is connected in the following way: Command and control packets are transmitted from the controller to the actuator; the actuator sends back acknowledgement packets to the controller on successful completion of any operation. Figure 3.4 illustrates a conceptual overview of the problem scenario investigated in this section.

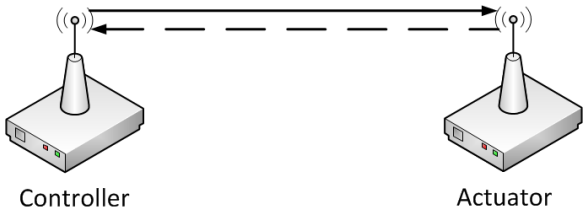


Figure 3.4: Illustrative concept of a half-duplex dual communication link used for real-time teleoperation and telemetry communication between the controller and actuator for the dust explosion scenario. The solid line represents the dedicated real-time teleoperation link and the dashed line represents the dedicated real-time telemetry link.

Real-time applications may utilise a dedicated communication link for specific tasks in order to reduce latency from transmitting and receiving data over the same communication link; in this instance, the teleoperation link from the controller to the actuator is for command and control tasks and is denoted as the uplink. The telemetry link is used to relay acknowledgement or data acquisition information from the actuator back to the controller to notify an action has been completed, this is denoted as the downlink.

Analysis of this scenario indicates that the inclusion of an additional communication link may impact on the latency incurred by the real-time application; this is because the communication and processing latency will increase as a result of both communicating devices conducting the processing and transmission of real-time teleoperation and telemetry packets; therefore, further investigation is undertaken to ascertain if this behaviour is true.

Modification of the mathematical model presented in Formula 4 in section 3.3.1. was undertaken to model the communication latency introduced by security constructs for a single hop dual-communication link; it is assumed that the behaviour of cryptographic services on the real-time application follows the same relationship as presented in section 3.3.1 with the inclusion of the RTT (Round Trip Time) to send an acknowledgement of a packet back to the transmitter node. Formula 5 present the mathematical model for a single hop dual-communication half duplex link.

$$\tau l = (\triangle(\eta + \delta + \psi)) + \frac{\nu}{\ell} + F \tag{5}$$

Formula 5: Secure communication model for a single hop dual-communication half duplex link.

The model uses the same variables as described in Formula 5 with the inclusion of the time for the receiver to complete the operation and transmit the telemetry feedback to the transmitter this is represented by the variable(F). Validation of the mathematical model proposed was conducted through benchmark analysis against a simulated environment to

ascertain if the observation holds true. A test was conducted to validate the mathematical model presented. The test used the model to predict the latency with secure communications applied and is used as a benchmark for the simulation test using the same parameters.

The null hypothesis is that the security constructs will not impact on the communication latency recorded for a real-time teleoperation and telemetry application with half-duplex dual communication links; the alternative hypothesis to this is that the security construct will have an impact on the communication latency recorded for a real-time teleoperation and telemetry application with half-duplex dual communication links.

The test investigated the total latency of the RTT when utilising secure communications. Packet sizes of thirty-six, fifty-two and eighty-four bytes were sampled to reflect real-time teleoperation packet sizes. The crystal frequency selected was 8 MHz (2 MIPS) with a SPI divisor of four selected (2 Mbps) for maximum data throughput for both communication links. AES-128 was selected as the block cipher used by the specified AEAD constructs to showcase how the number of rounds configured for the block cipher influence the time to process the cryptographic algorithm. Appendix C presents the schematic used for the test platform. The first test investigated the latency measured for an unsecured half-duplex dual communication link. Table 3.5 states the latency measurements obtained from the simulator for this test.

Table 3.5: Communication latency for a simulated single hop closed loop unsecured half-duplex dual communication link. (2 MIPS and 2 Mbps transmission rate).

Independent Variable	**Dependent Variable**
Packet size (Bytes)	**Time (ms)**
36	180.4
52	180.7
84	181.7

The results presented in Table 3.5 shows that the thirty-six byte packet size has the lowest time measured for latency, whilst the eighty-four byte packet size has the highest time for latency measured; this indicates that the size of the packet with no security services does not have an significant impact on the communication latency recorded.

Analysis of the findings presented indicates that the time to process a byte of data and transmit the packet over the SPI communication link are not a significant factors as the difference in the latency recorded is within the microsecond range; therefore, this suggests that the packet size may not be a significant variable that impacts the communication latency for real-time teleoperation and telemetry communications with no security

services applied. The results obtained in Table 3.5 are used as a benchmark measurement for the real-time requirements in this section of the analysis.

Figure 3.5 graphs the results obtained for software AEAD security constructs for various packet sized packets.

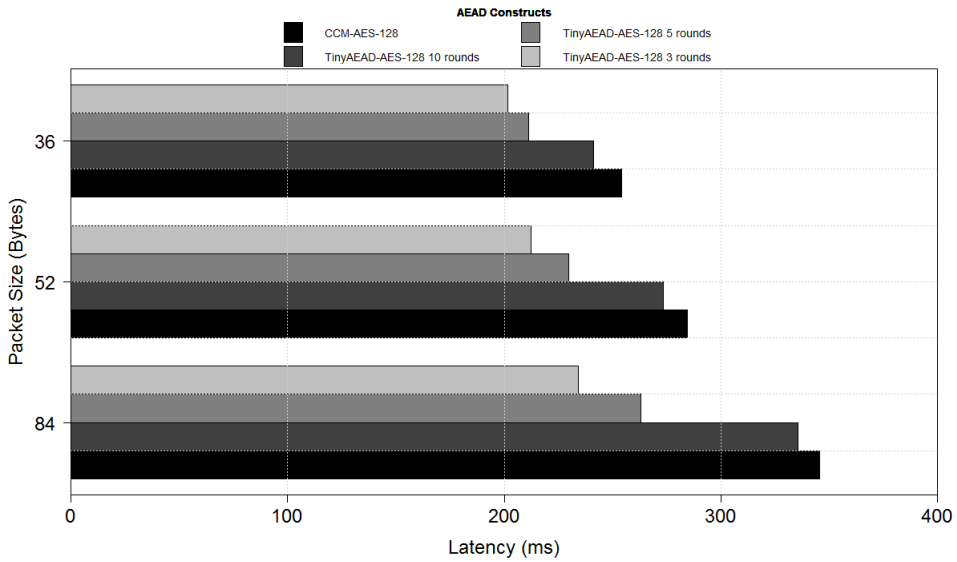


Figure 3.5: Secured communication latency for a simulated single hop half-duplex dual-communication link at an 8 MHz (2 MIPS) crystal frequency and SPI transmission rate of 2 Mbps.

Results presented in Figure 3.5 shows that the security constructs have an impact on the latency measured for the half-duplex dual-communication link as CCM-AES-128 measured the longest latency times for the three packet sizes sampled whilst TinyAEAD-AES-128 at three rounds had the shortest latency times for the three packet sizes sampled. The smallest packet size of thirty-six bytes has the lowest latency measured, whilst eighty-four byte packet sizes has the highest latency measured for the same security construct selected.

Information obtained from the test conducted shows that security constructs have an increased impact on the latency recorded with CCM-AES-128 recording a forty-eight per cent increase in latency in comparison to thirty-three per cent recorded for TinyAEAD-AES-128 at three rounds per eighty-four byte packet processed. The packet size influenced latency with smaller packet sizes having a reduced impact on latency with security measures applied as CCM-AES-128 had on average a twenty-nine per cent increase on latency, whilst TinyAEAD-AES-128 at three rounds had a twelve per cent increase for a thirty-six byte packet size packet processed.

Correlation between the packet size and latency recorded for CCM-AES-128 and the TinyAEAD-AES-128 variants tested follow a strong positive correlation; the relationship between the packet size and the latency recorded for both cryptographic constructs increases as the size of the packet increases, this is because the number of encryption calls to the block cipher is increased to encrypt a larger size payload; resulting in an increased time required to process the cryptographic operation.

Investigation of the mathematical model against the simulation test platform is undertaken to validate the mathematical model presented and identify if the null or alternative hypothesis holds true. This test selects CCM-AES-128 and TinyAEAD-AES-128 at three rounds as the security constructs. Packet sizes of thirty-six, fifty-two and eighty-four bytes are chosen. The crystal frequency used was 64 MHz (16 million instructions per second). Figure 3.6 graphs the comparison between the mathematical model and simulation.

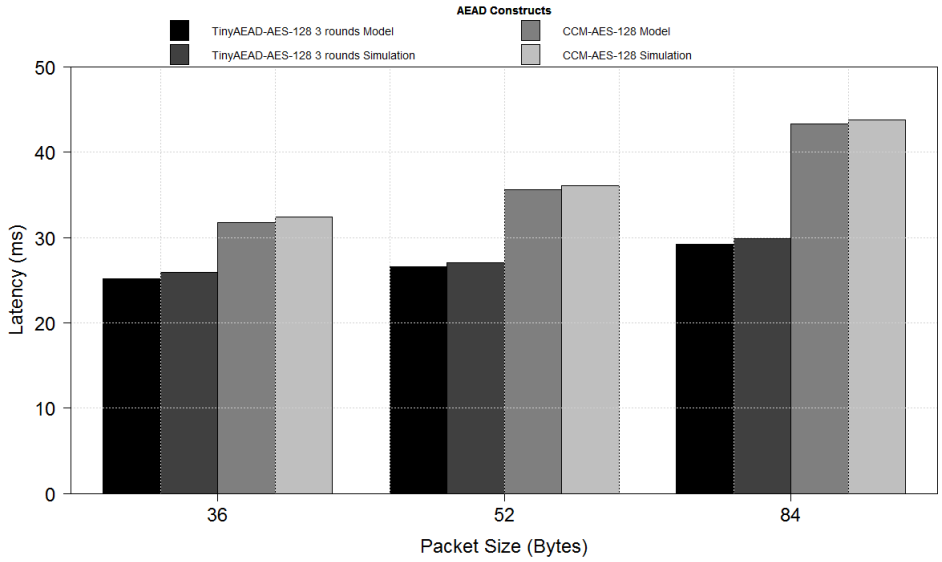


Figure 3.6: Comparative results of mathematical model and simulation for software implementation of TinyAEAD-AES-128 three rounds and CCM-AES-128 at a 64 MHz crystal frequency (16 MIPS) and a transmission rate of 16 Mbps.

Data presented in Figure 3.6 shows that the results obtained from the mathematical model and simulation are correlated for the two security constructs selected with the difference between the mathematical model and simulation falling within one standard deviation (binomial distribution).

3.3.4 Section Summary

The findings obtained from this experiment shows that security services do have an impact (i.e incurred latency) on the communication latency with half-duplex dual communication links, this is because the security service selected requires a finite amount of time

to process the data as demonstrated with the number of block cipher rounds selected for TinyAEAD-AES-128.

The processing frequency selected influences the latency recorded as this determines the rate that the instruction cycles are executed as demonstrated in the aforementioned analysis on the single, simplex communication link; however, with the inclusion of the half-duplex dual communication link, both transmitter and receiver nodes are required to perform the encryption and decryption operation in order to participate in two way communications; consequently, this result in an increase in the latency recorded and proves the alternative hypothesis to hold true for this analysis undertaken.

Applying of the findings to the research undertaken in this thesis further reinforces the summary presented from the analysis conducted in section 3.3.1. The findings presented in this section and section 3.3.1 indicates that the rate at which the real-time teleoperation and telemetry packet is transmitted, or processed is a contributing factor to the problem investigated. This is because the mathematical models presented in each analysis examine the problem from the perspective of time; therefore, this suggests there must be an underlying relationship between the rate an action is complete and the latency incurred. To validate this initial hypothesis, an analysis of the security services on the instantaneous packet throughput over a multiple hop communication link is conducted in the next section.

3.4 Analysis of the Impact of Security Constructs on Instantaneous Packet Throughput over Single and Multiple Hop Communication Link

This section of the problem analysis investigates the instantaneous packet throughput recorded by the transmitter and receiver node with homogeneous and heterogeneous processing and transmission rates over a point to point communication link. The rationale for the investigation was to ascertain how the processing and transmission rate contributes towards the number of observed instantaneous packet throughput recorded by the receiver node over a specific period of time.

In this thesis, throughput is separated into two classifications which are, instantaneous and average throughput. The instantaneous throughput is the rate (at any instance of time) at which a node is receiving data. The average throughput is the size of the packet divided by the time it takes to receive all of it.

In the following problem analysis, the focus is on instantaneous throughput with real-

time teleoperation, it is desirable to have a low delay and an instantaneous throughput consistently above a required threshold as evidenced in the investigations conducted in section 3.3. Analysis of the problem using instantaneous packet throughput is undertaken in this section to identify how the number of intermediate nodes on a communication link and the cryptographic construct selected impact on the instantaneous packet throughput recorded.

3.4.1 The Impact of Homogeneous and Heterogeneous Configuration on the Instantaneous Packet Throughput Over a Point to Point Communications Link

Analysis of the static to static problem scenario (i.e. dust explosion) shows that there is point to point communication between the controller device (transmitting teleoperation commands) and the actuator. Figure 3.7 draws the conceptual overview of the point to point simplex communication link used for the real-time application.

Figure 3.7: Illustrative concept of a point to point link used to propagate communicated data between the controller and actuator for the dust explosion scenario.

The use of different computational devices or communication could be feasible in this scenario investigated (i.e different embedded microcontroller selected or communication bit rates); in this thesis, two configurations are examined, homogeneous configuration is where the processing and communication rates are the same between communicating nodes. Heterogeneous configuration is where the processing and communication rate are not the same between the communicating nodes.

The analysis conducted in sub-sections 3.3.1 and 3.3.3 demonstrated the impact of security services from a latency perspective using homogeneous configurations for the processing and transmission rates; however, under certain situations, it is likely that the configuration of the hardware used could be heterogeneous as a result of different manufacturer specifications; consequently, it is forecasted that this would impact on the number of instantaneous packets received in a sampled period of time.

The test constructed for this analysis counted the instantaneous packet throughput over a number of intermediate nodes with homogeneous and heterogeneous transmission and processing rates. Packets were sent continuously from the transmitter and counted at each hop to measure how many instantaneous packets arrived at each hop within a sixty second time interval.

The null hypothesis is that the heterogeneous configuration of the processing and transmission rate would not have an impact on the number of instantaneous packets recorded by the receiving device in comparison to the homogeneous configuration. The alternative hypothesis is that heterogeneous configuration of the processing and transmission rate would have an impact on the number of packets recorded by the receiver in comparison to the homogeneous configuration.

Configuration of the components selected are as follows, a crystal frequency of 2 MHz (0.5 MIPS) and 4 MHz (1 MIPS) was selected with a packet size of thirty-six bytes sampled. The Universal Asynchronous Receiver Transmitter (UART) was selected as the serial communication method between the transmitter and receiver. It is assumed that there is no flow control nor queueing buffers utilised between the transmitter and receiver. Details of the test platform and the configuration parameters set for this experiment are located in Appendix D. Table 3.6 tabulates the instantaneous packet throughput recorded with homogeneous processing and transmission rates over a sixty-second time frame.

Table 3.6: Simulation results of homogeneous processing and transmission rates on the instantaneous packet throughput recorded for a thirty-six byte packet over a point to point communication link in a sixty second time frame. (9600 bps transmission rate).

Independent Variable	**Dependent Variable**	
Configuration Method	**Number of Packets Transmitted**	**Number of Packets Received**
Homogeneous	428	425

Results presented in Table 3.6 demonstrates that homogeneous processing and transmission rates does not influence the instantaneous packet throughput recorded; this is because the transmitter and receiver process the same number of instruction cycles at the same rate and are synchronised in their communication.

Examination of this finding is undertaken in further detail in order to ascertain if this hypothesis is correct; this is achieved by creating a heterogeneous configuration between the transmitter and receiver nodes. In this instance of the analysis the transmitter processing frequency is configured to 4 MHz (1 MIPS) and the receiver node was configured to 2 MHz (0.5 MIPS). Table 3.7 and Table 3.8 tabulates the instantaneous packet throughput

recorded with heterogeneous processing and transmission rates over a sixty-second time frame.

Table 3.7: Simulation results of heterogeneous processing rates on the instantaneous packet throughput recorded for a thirty-six byte packet over a point to point communication link in a sixty second time frame. (4 MHz crystal frequency (1 MIPS); 9600 bps transmission rate).

Independent Variable	**Dependent Variable**	
Configuration Method	**Number of Packets Transmitted**	**Number of Packets Received**
Heterogeneous Processing Rate	428	282

Table 3.8: Simulation results of homogeneous and heterogeneous transmission rates on the instantaneous packet throughput recorded for a thirty-six byte packet over a point to point communication link in a sixty second time frame. (Transmission rate of 9600 bps for transmitter and a receiving rate of 4800 bps for the receiver).

Independent Variable	**Dependent Variable**	
Configuration Method	**Number of Packets Transmitted**	**Number of Packets Received**
Heterogeneous Transmission Rates	428	282

Results presented in Tables 3.7 and Table 3.8 demonstrates that heterogeneous processing and transmission rates do have an impact on the instantaneous packet throughput recorded by the receiver with a difference of one hundred and forty six packets were recorded. This demonstrates that heterogeneous processing and transmission rates have a significant influence on the instantaneous packet throughput recorded by the receiver. The rate that data is transmitted or received dictates the number of instantaneous packets that are lost; because, if the packet is still being processed whilst the next packet arrives, the arriving packet is discarded in this instance as the data buffer is full with the previous packet as no additional queueing buffer is used for continuous streamed data in this scenario.

3.4.2 Section Summary

Application of the knowledge obtained from this analysis on the static to static real-time scenario shows that the heterogeneous configuration of the processing and transmission rate would impact on the number of instantaneous packets received in a given period of time. This is because the packets are dropped by the receiver node as it is still acting on the previous command sent; resulting in a reduction in the instantaneous packet throughput recorded; therefore, the findings support the alternative hypothesis presented in this

section of the problem analysis.

Examination of the findings presented in the analysis undertaken demonstrates that the rate at which the processing or transmission is undertaken impacts on the instantaneous packet throughput recorded over a point to point communication link; however, in certain situations, there is a possibility that real-time teleoperation and telemetry packets require multiple hop propagation to relay packets between two static end-points that are not within direct communication range; therefore, the next section of the problem analysis investigates the impact of multiple hop propagation with homogeneous and heterogeneous transmission and processing rates on instantaneous packet throughput

3.4.3 The Impact of Multiple Hop Propagation with Homogeneous and Heterogeneous Transmission and Processing Rates on Instantaneous Packet Throughput

The propagation of packetised data may occur over multiple hop communication for real-time teleoperation and telemetry in situations where real-time teleoperation and telemetry of the application is undertaken remotely. Figure 3.8 presents an illustrative concept of a static to static real-time teleoperation and telemetry multiple hop situation.

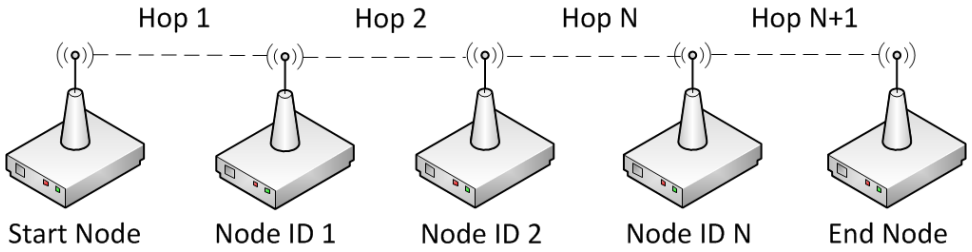


Figure 3.8: Illustrative concept of a circuit switched linear multi-hop topology for real-time teleoperation and telemetry scenario.

Analysis undertaken has focused on a point to point communication link between the transmitter and receiver device; therefore, the analysis conducted in this section focuses on how homogeneous and heterogeneous configuration of the intermediate nodes impacts on the number of instantaneous packets received over a multiple hop communication link in an emulated environment.

The test counted the instantaneous packet throughput over a number of intermediate nodes with homogeneous and heterogeneous transmission and processing rates and how multiple hop propagation impacts on the instantaneous throughput recorded. Packets were sent continuously from the transmitter and counted at each hop to measure how many instantaneous packets had arrived at each hop within a sixty second time interval.

The null hypothesis presented is that the increased number of nodes on the communication link will not have an impact on the number of instantaneous packets received for homogeneous and heterogeneous configuration methods. The alternative hypothesis is that the increased number of nodes on the communication link will have an impact on the number of instantaneous packets received for homogeneous and heterogeneous configuration methods.

Two tests were conducted in this analysis; the first test examined, the homogeneous and heterogeneous processing rates of the computational devices and its impact on the instantaneous packet throughput recorded over a multiple-hop communication link. The second test investigated how homogeneous and heterogeneous transmission rates influence the instantaneous throughput recorded over multiple-hop propagation.

Crystal frequencies of 5 MHz, 4 MHz, 3 MHz, 2 MHz and 1 MHz was selected with packet sizes of thirty-six bytes sampled for the processing rate test. The Universal Asynchronous Receiver Transmitter (UART) was selected as the serial communication methods between the transmitter and receiver with baud rates of 9,600, 4,800 2,400, 1,200, 600 and 300 symbols per second selected. It is assumed that there is no flow control or queueing buffers utilised between the transmitter and receiver nodes. Table 3.9 and 3.10 tabulates the configuration of the homogeneous and heterogeneous processing and transmission rates for the multiple hop scenario investigated.

Table 3.9: Configuration parameters for homogeneous processing and transmission rates for the multiple hop test.

Independent Variable	**Dependent Variable**	
Intermediate Node Number	**Crystal Frequency (MHz)**	**Transmission Rate (Bps)**
Start Node	5	9600
1	5	9600
2	5	9600
3	5	9600
4	5	9600
End Node	5	9600

Table 3.10: Configuration parameters for heterogeneous processing and transmission rates for the multiple hop test.

Independent Variable	**Dependent Variable**	
Intermediate Node Number	**Crystal Frequency (MHz)**	**Transmission Rate (Bps)**
Start Node	5	9600
1	5	4800
2	4	2400
3	3	1200
4	2	600
End Node	1	300

Additional details of the test plan, platform and the configuration parameters set for this experiment are located in Appendix E. Figure 3.9 illustrates the instantaneous packet throughput recorded for homogeneous and heterogeneous processing rates over multiple intermediate nodes in a sixty second time frame.

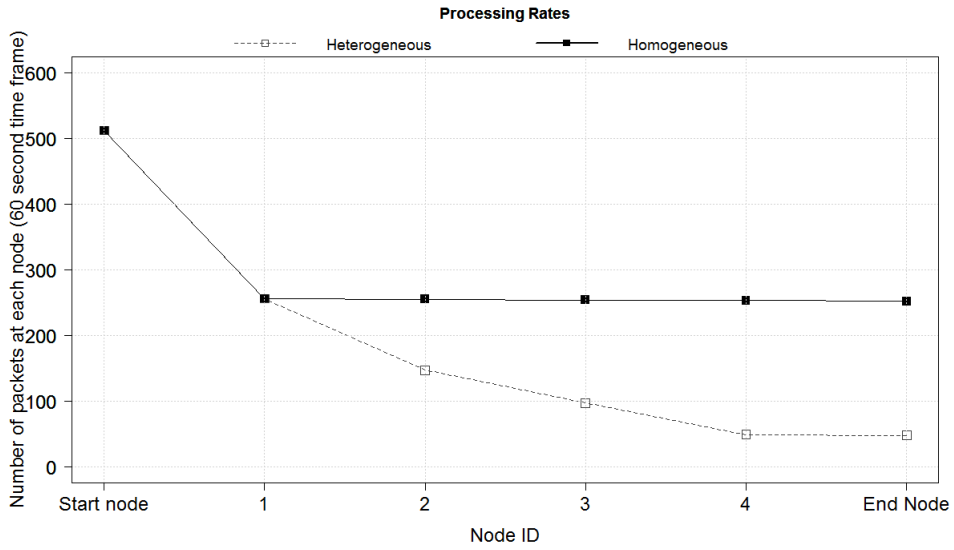


Figure 3.9: Simulation results of homogeneous and heterogeneous processing rates on the instantaneous packet throughput for a thirty-six byte packet over multiple intermediate nodes in a sixty second time frame.

Information presented in Figure 3.9 demonstrates that the homogeneous processing rate follows a linear profile after the first intermediate node; this is because the intermediate nodes have to call the decryption function to check the integrity of the packets is legitimate and the encryption function to encrypt the packet before propagation to the next node; whilst the start node calls the encryption function only. As the intermediate nodes execute the same number of instruction cycles, no packets are dropped as it is propagated across the link.

The results for the heterogeneous processing rate test shows an exponential decay profile for the number of instantaneous packets received at each hop, this is because the processing rate at each hop (i.e. reduced processing frequency) has increased the time to process the received packet and retransmit to the next intermediate node; consequently, the additional latency results in increased packet drops as the processing device is undertaking encryption or decryption tasks on the previous packet. Figure 3.10 illustrates the instantaneous packet throughput recorded for homogeneous and heterogeneous transmission rates over multiple intermediate nodes in a sixty second time frame.

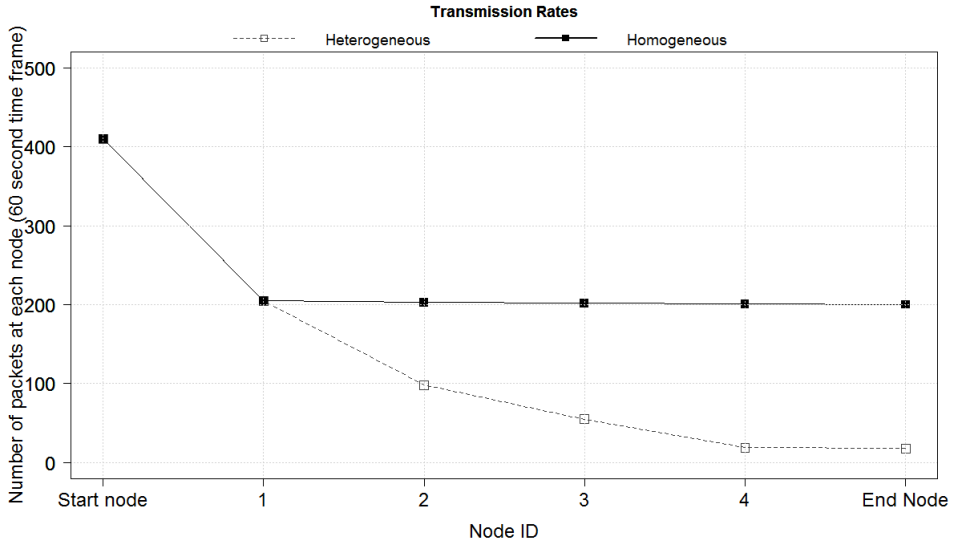


Figure 3.10: Simulation results of homogeneous and heterogeneous transmission rates on the instantaneous packet throughput for a thirty-six byte packet over multiple intermediate nodes in a sixty second time frame (5 MHz crystal frequency used for all nodes on the network).

The results presented in Figure 3.10 shows that the heterogeneous transmission rate between intermediate nodes on the network has a significant impact on the reduction of instantaneous packet rate recorded at each node in comparison to a homogeneous transmission rates; this correlated with the data presented in Figure 3.9 and further reinforces that the processing or transmission rate influences the instantaneous packet throughput recorded and is further showcased with the increase of intermediate nodes on the communication link for heterogeneous scenarios: This partially proves the alternative hypothesis as the increase number of nodes on the communication link will have an impact on the number of instantaneous packets received for heterogeneous configuration methods only.

3.4.4 Section Summary

Analysis of the findings presented in this section demonstrates that the multiple hop propagation impacts on the instantaneous packet throughput recorded for a communica-

tion link with heterogeneous processing or transmission rates. In the real-time dust explosion scenario examined in this thesis, a reduced number of packets received when using multiple-hop propagation with heterogeneous configuration; this may result in teleoperation and telemetry packets not meeting the real-time constraints and result in a delayed reaction to events (e.g. readings from sensors)

The underlying cause of this problem identified from the analysis undertaken in section 3.4.1 and section 3.4.3 is the rate at which real-time teleoperation and telemetry packets can be processed and transmitted from each intermediate device on the communication link; this is because the time required to conduct a specific task determines the rate that the packets can be processed and transmitted across the communication link; therefore, the reduction of the packets observed in the analysis undertaken is as a result of a bottleneck in the processing and transmission rate of the real-time teleoperaiton and telemetry packets.

The findings obtained interlink with the configuration of the number of rounds for the underlying block cipher as this directly affected the rate at which real-time teleoperation and telemetry packets could be transmitted; therefore, this suggests that the cause of the problem is the time to undertake a task (i.e security service or transmission of data).

The change in the packet throughput recorded follows an exponential decay curve as a result of the asynchronous nature of the configuration applied; this indicates that this trend could be mathematically modelled to derive a forecast of the number of instantaneous packets received in a given period of time; therefore, the next section of the problem analysis investigates the impact of multiple hop propagation on instantaneous packet throughput with heterogeneous processing rates.

3.4.5 The Impact of Multiple Hop Propagation on Instantaneous Packet Throughput with Heterogeneous Processing Rates

The static to static real-time teleoperation and telemetry application scenario highlighted that the heterogeneous configuration of the processing and transmission rate has a significant impact on instantaneous packet throughput recorded. Analysis of the findings shows that the rate at which a task is conducted is the underlying cause of the phenomena examined.

To validate the findings obtained, a mathematical model has been derived to profile the instantaneous packet throughput at each hop. Figure 3.11 illustrates the conceptual overview of the problem investigated in this section of the problem analysis.

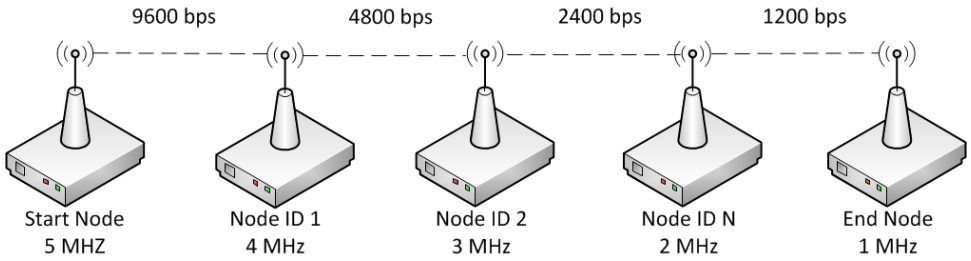


Figure 3.11: Illustrative concept of a circuit switched linear multi-hop topology for real-time teleoperation and telemetry applications with heterogeneous processing and transmission rates stated.

The test observed in this section of the problem analysis examined the instantaneous packet throughput over a number of intermediate nodes with and without AEAD software security measures applied and how multiple hop propagation with heterogeneous processing rates would have an impact on the instantaneous packet throughput recorded in a given period of time.

The mathematical model presented uses the exponential decay function to calculate the change of instantaneous packet throughput over time for each hop. This model assumes that the wireless nodes would have no knowledge of the previous packet arrival (i.e. the amount of packets arrived at the previous hops), thus making the process memoryless. It is assumed that the packet arrivals do not occur simultaneously; therefore, orderliness has been factored into this model.

The model calculates instantaneous throughput by adding the initial packet throughput value for the initial start hop (N_o) divided by the time frame selected in seconds(t) to calculate the packet arrival rate. The inverse of the value is obtained using -1/$(\frac{N_o}{t})$ before using the value with the exponential function (e). The value obtained is then multiplied by the total throughput value of the previous wireless hop packet throughput (N_o) to calculate the rate change in packet throughput (r). Formula 6 presents the instantaneous throughput rate of change per wireless hop model.

$$r = N_o e^{(-1/(\frac{N_o}{t}))} \tag{6}$$

Formula 6: Formula for estimating instantaneous throughput rate of change per hop.

The final calculation is to subtract r from N_o to derive the new instantaneous packet throughput measurement for N_{o+1} as formulated in Formula 7.

$$N_{o+1} = N_o - r \tag{7}$$

Formula 7: Calculation for estimating instantaneous packet throughput per hop.

Application of the mathematical model is undertaken to ascertain a baseline profile and identify trends in the relationship between the instantaneous packet rate and the number of packets recorded at each intermediate node over a multiple hop communication link. The input parameters were derived from the aforementioned analysis conducted in section 3.4.1. Figure 3.12 presents the results derived from the mathematical model for a thirty-six byte packet length over multiple intermediate nodes with heterogeneous processing rate in a sixty second time frame.

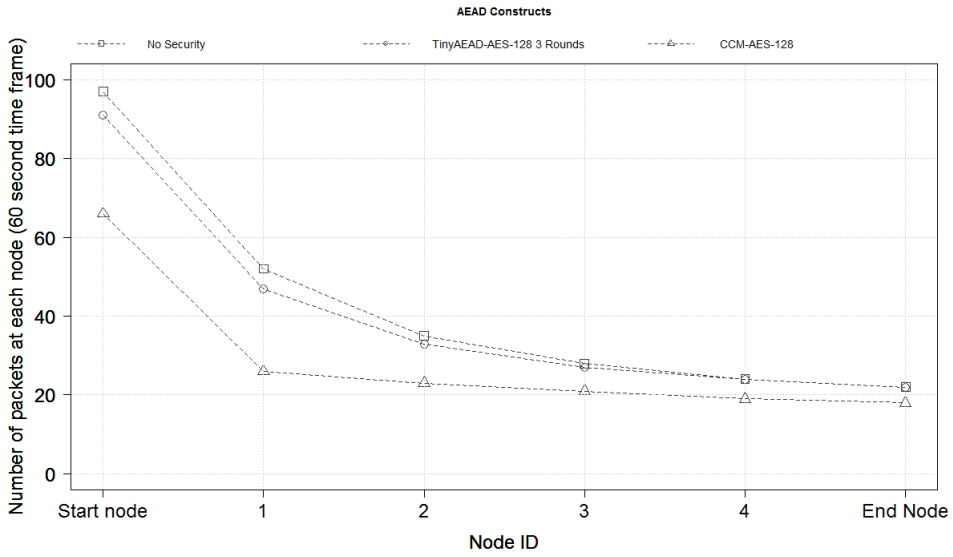


Figure 3.12: Mathematical model results for a thirty-six byte packet length over multiple intermediate nodes with heterogeneous processing rate in a sixty second time frame.

Analysis of the findings presented in Figure 3.12 demonstrates that the selection of the cryptographic services influences the number of packets recorded as a result of the time required to process the cryptographic operation as presented in section 3.4.3. Examination of the results presented demonstrates that the number of packets recorded between the start node and the first intermediate node is reduced by half; furthermore, there is a relationship between the number of packets received transmitted from the start node and the number of intermediate nodes on the communication link as the packet throughput recorded at the start node is divisible by the intermediate node to derive the expected packet throughput.

Investigation of the processing rate across multiple intermediate nodes using the mathematical model indicates two findings; the first finding is the cryptographic service selected offsets the initial number of packets transmitted by the start node in a given period of time; this suggests that the cryptographic operation contributes towards the packet rate

and as a result in the time required to process the service.

The second findings obtained from the use of the mathematical model is the reduction in the rate of change as the number of intermediate nodes is increased with the most significant reduction observed between the start node and intermediate node one; in addition, the rates for all three cryptographic services begin to converge as the number of intermediate nodes increases. The following investigation examines if the mathematical model represent the true behaviour of the relationship with benchmark comparison of the mathematical model to results obtained from a simulated environment.

The null hypothesis presented for this investigation is that the security service selected will not have an impact on the number of instantaneous packets recorded at each intermediate node on the communication link. The alternative hypothesis is that the security service selected will have an impact on the number of instantaneous packets recorded at each intermediate node on the communication link.

The method for this experiment is a follows; the transmission of packets between the transmitter and receiver is a continuous operation (i.e. where there is no interruption of the main routine in the real-time application) at its fastest transmission rate and that each task in the system is conducted in a sequential manner based on the principle of a first in first out scheduler system (i.e. has full dedication of the computational resources for an individual task and computes tasks in periodical fashion). Packets were sent continuously from the transmitter and counted at each hop to measure how many instantaneous packets have arrived at each hop within a sixty second time interval.

The test varied the number of intermediate nodes on the linear network, starting from one node to the maximum of five nodes; in this instance of the analysis, three microcontrollers were used, one as the transmitter device, one for the receiver device and an intermediate microcontroller for the number of intermediate nodes on the link. The variation of the number of intermediate number of nodes on the network was conducted using one microcontroller that was configured to loop through its configured process a number of iterations (i.e. 3 loop iterations to represent three hops) before transmitting the packet to the end receiver node.

Configuration of the components selected are as follows, a crystal frequency of 4 MHz (1 Million Instructions Per Second) was selected, as the PIC18F45K22 microcontroller required four clock cycles per instruction. Packet sizes of thirty-six and eighty-four bytes sampled. A SPI divisor of sixteen is chosen to replicate a transmission rate of a wireless communication link of 250 Kbps (Instruments 2014). Metrics used for the experiment-

ation are seconds for the time frame sample. Appendix F illustrates the schematic of the simulated test platform. Figure 3.13 graphs the total instantaneous packet throughput measured in sixty seconds for packet size of thirty-six and eighty-four bytes.

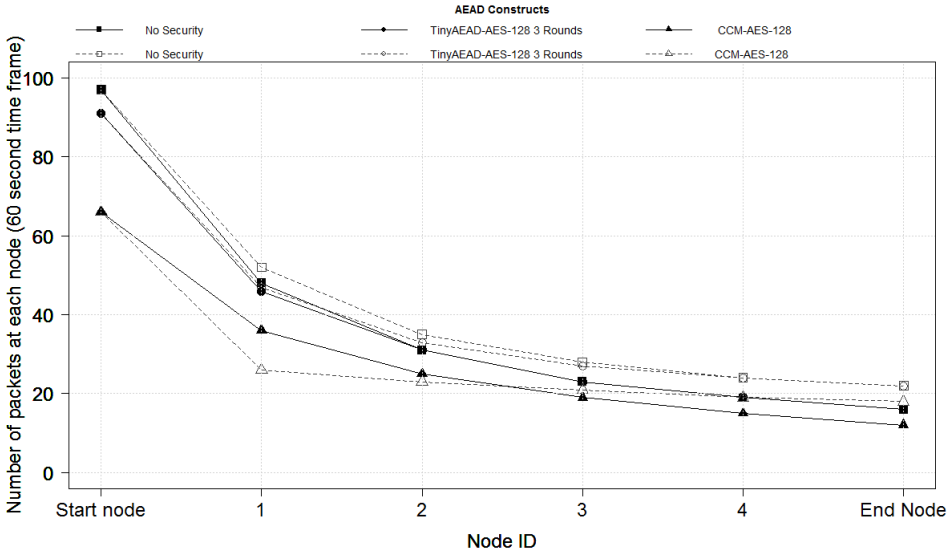


Figure 3.13: Simulation results for thirty-six and eighty-four byte packet lengths over multiple intermediate nodes with heterogeneous processing rate in a sixty second time frame.

Results presented in Figure 3.13 demonstrates that the number of intermediate nodes influenced instantaneous packet throughput for thirty-six and eighty-four byte packets with one hop showing the largest instantaneous packet throughput recorded and five hops showing the smallest instantaneous throughput. TinyAEAD-AES-128 at three rounds has a smaller impact on instantaneous packet throughput than CCM-AES-128 when benchmarked against no security. The packet size contributes to the instantaneous packet throughput recorded with larger packet sizes having a greater reduction than smaller size packets.

The number of rounds for the utilised block cipher used by the AEAD constructs has an impact on instantaneous packet throughput as the AEAD constructs operating at reduced number of rounds increased the number of instantaneous packets received in comparison to the standardised specified maximum number of rounds in the same period of time; this means less data is processed in the same period of time and results in a longer period of time required to obtain the full data-set for the measurement.

The quantity of intermediate nodes between the source and destination has an influence on instantaneous packet throughput as an increased number of intermediate nodes present on the communication link has a greater impact on the instantaneous packet throughput recorded. The AEAD constructs have a significant impact on the instantaneous packet

throughput as CCM-AES-128 and TinyAEAD-AES-128 at three rounds reduced the instantaneous packet rate each intermediate node performs across the link; this is because the additional time to required to process the encryption and decryption function impact on the total number of packets transmitted in a given period of time. The exponential decay profile displayed in Figure 3.13 represent the heterogeneous processing rate of the intermediate nodes and it is identified that packets are dropped between each intermediate node as a result of a reduced processing rate at each hop; this is demonstrated in the point to point communication tests presented in section 3.4.1.

The trend identified from the analysis of the results is an exponential decay as the instantaneous packet throughput decreases at a set rate between each node; however, the rate of degradation still increases at a reduced rate as a larger quantity of hops are introduced to the network. The mathematical model was benchmarked against the simulation environment to validate the findings obtained. The aforementioned test methodology for the wireless multi-hop test is selected, the packet size chosen was thirty-six bytes; AEAD constructs CCM-AES-128 and TinyAEAD-AES-128 at three rounds were selected. Figure 3.14 illustrates the comparison of the instantaneous packet throughput recorded for the mathematical model and simulation with no security applied.

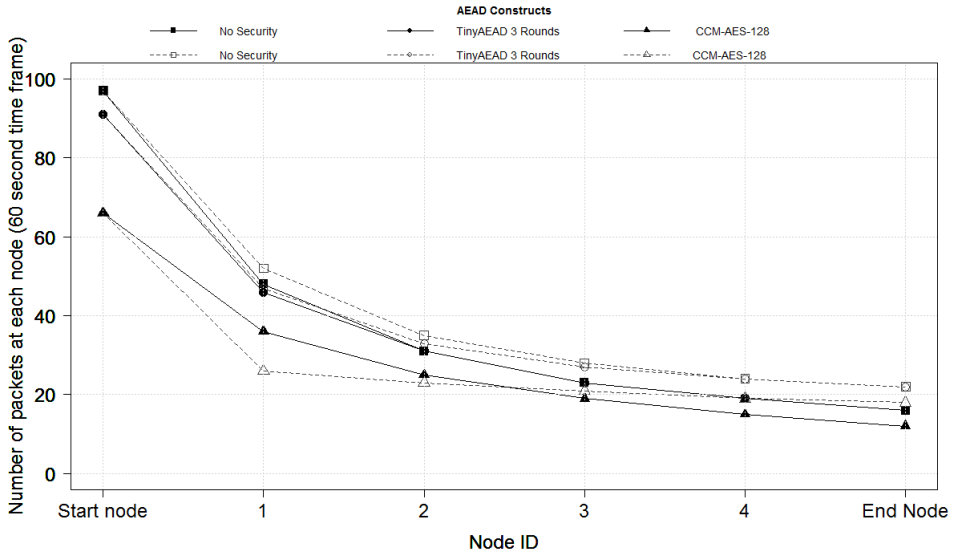


Figure 3.14: Comparison of instantaneous throughput recorded between the proposed mathematical model (dotted lines) and simulation results (solid lines) with no security, TinyAEAD-AES-128 at three rounds and CCM-AES-128 for a thirty-six byte packet size.

Results presented in Figure 3.14 shows that the mathematical model and simulation results predict an exponential decay trend for the instantaneous packet throughput over a sixty second time frame.

The benchmark comparison of the proposed model and simulation results shows that the mathematical model is correlated with the simulation results up to three intermediate nodes and is better suited for modelling the results for a fewer number of intermediate nodes; this is because the rate of change at each intermediate hop is affected at a reduced rate in the simulated results; whilst the mathematical model rate of change has not factored the reduction of the change with an increased number of intermediate hops on the network; therefore, the error increases in the rate of change with the addition of more intermediate nodes on the network.

From the results of the comparison presented, the model could be used to predict the instantaneous packet throughput over a longer period of time and with more intermediate nodes. To test this theory two tests were devised to validate the proposed mathematical model as a predictive tool, the first test varied the number of intermediate relay nodes between the transmitter and receiver to calculate the predicted instantaneous packet throughput; the number of intermediate nodes selected for this test was six, seven, eight and nine nodes to forecast the trend over an increased number of hops, CCM-AES-128 and TinyAEAD-AES-128 were selected as the security constructs. Table 3.11 tabulates the comparison between the mathematical model and simulation results.

Table 3.11: Mathematical model versus simulation results for instantaneous packet throughput recorded over increased multiple nodes.

Independent Variables			**Dependent Variables**	
Number of nodes	**Security construct**	**Packet size (bytes)**	**Model results (Packets)**	**Simulation results (Packets)**
6	CCM-AES-128	36	11	16
7	TinyAEAD-AES-128 3 rounds	52	12	19
8	TinyAEAD-AES-128 5 rounds	84	7	12
9	TinyAEAD-AES-128 10 rounds	36	8	14

The data presented in Table 3.11 shows that the proposed model follows the same trend in results in relation to the simulation, however, the proposed model is not suited for the prediction of instantaneous packet throughput over five intermediate nodes as the discrepancy between the model and simulation results increases as the error in the results accumulates over an increased number of intermediate nodes on the network.

The second test assessed the viability of the model by varying the packet size, time frame, number of hops and rounds used by TinyAEAD-AES-128. The tests used the mathematical model as a predictive tool to calculate the exponential trend based on the parameters selected as presented in Table 3.12.

Table 3.12: Mathematical model versus simulation results for instantaneous packet throughput measurements at various sampling times.

Independent Variables				**Dependent Variables**	
Number of nodes	**Security construct**	**Packet size (bytes)**	**Sampling Times (s)**	**Model results (Packets)**	**Simulation results (Packets)**
2	TinyAEAD-AES-128 3 rounds	36	120	93	92
3	TinyAEAD-AES-128 5 rounds	52	180	76	80
4	TinyAEAD-AES-128 10 rounds	84	240	62	63

Data presented in Table 3.12 shows that the predictive results obtained from the proposed model correlates with the simulation results for different sampling times, packet sizes and number of intermediate hops chosen; this demonstrates that the model is suited based on the findings presented from the small sub-sample in Table 3.12 and therefore can be used to calculate a wider range of parameter values used within an acceptable margin of error.

3.4.6 Section Summary

The findings from the test demonstrates that the propagation method between the transmitter and receiver has an impact on the instantaneous packet throughput measured with the increased number of intermediate nodes has a reduced impact on the number of packets received by the end node; this is because the processing of the packet at each intermediate node impacts the instantaneous rate of packet transmission. The selection of the security construct impacts the instantaneous packet rate; Figure 3.15 illustrates the impact of the security construct on the instantaneous packet rate obtained from the simulation.

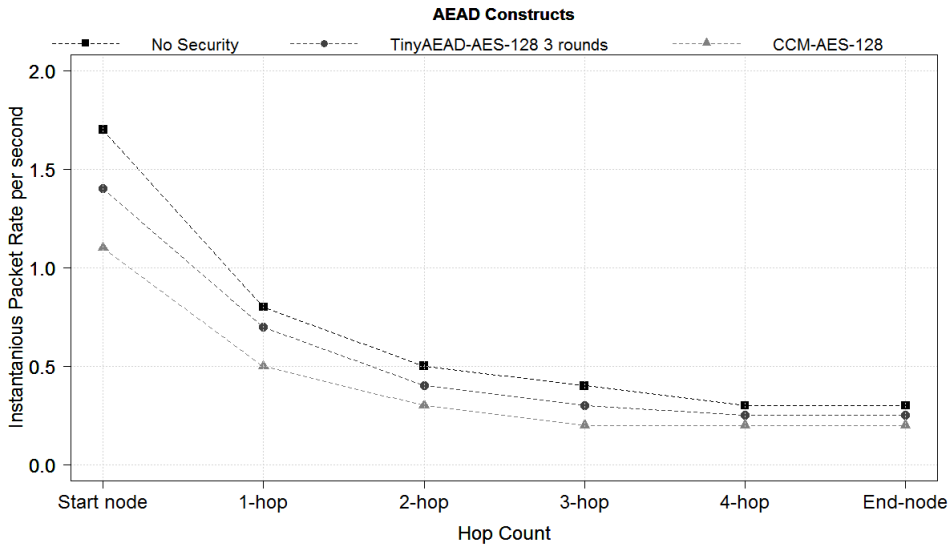


Figure 3.15: Instantaneous packet rate per second measurements for thirty-six byte packet lengths over a sixty second time frame.

Results presented in Figure 3.15 shows that the implementation of security constructs influences the instantaneous rate of packets received in the given time frame as no security has the highest instantaneous packet rate per second, however, the selection of the security algorithms also influences the instantaneous packet rate as TinyAEAD-AES-128 at three rounds outputs 0.3 packets per second faster than CCM-AES-128 from the initial start hop. The percentage change between no security and CCM-AES-128 from the start node is thirty-five per cent whilst the percentage change between TinyAEAD-AES-128 and no security is nineteen per cent. The initial impact of security algorithms on instantaneous packet throughput is offset from the start node and propagates over multiple hops.

Analysis of the findings presented in this section of the problem analysis demonstrates that the security service selected does have an impact on the instantaneous packet throughput recorded over a multiple hop communication link with heterogeneous processing rates; this is because of the additional latency generated by the cryptographic process impacts on the number of packets processed per second and result in a reduced number of packets received for the same sample time examined; therefore, this validates the alternative hypothesis proposed in this analysis.

3.5 Discussion

Analysis of the impact of cryptographic services over a single and dual communication link found that the time to process the cryptographic service contributes towards the overall latency induced by the real-time teleoperation and telemetry system and proves the null hypothesis that security constructs will have an impact on the time required to compute

the security operation for single and dual communication links. The consequence of the increased number of block cipher rounds was the time required to compute the operation as the number of calls to the underlying block cipher accumulate; therefore; an in-depth analysis of the profile of the AES-128 block cipher is required to ascertain the underlying cause of the latency from the cryptographic service.

The rate that the cryptographic operation and real-time teleoperation and telemetry packet is processed and transmitted between the transmitter and receiver nodes adds further complexity to the problem analysed as heterogeneous communications contribute towards the impact on the real-time teleoperation and telemetry applications; this is because the rate at which the real time teleoperation or telemetry command is processed or transmitted influences the total duration of time required to complete the operation as demonstrated in sections 3.4, 3.4.1, 3.4.3 and 3.4.5. The consequence of this is the reduction in instantaneous throughput recorded in a given period of time and therefore reduces the number of packets recorded by the transmitter and receiver nodes as the packets are dropped or overwritten in the buffer as a result of the latency induced and proves the null hypothesis stated in sections 3.4, 3.4.1 and 3.4.3.

Application of the cryptographic service over a multiple-hop communication link adds further complexity towards the multi-faceted problem analysed in this thesis as each intermediate node is required to conduct the confidentiality and integrity service on the packet before the packet is encrypted and relayed onto the next intermediate node in order to provide secure point to point relay of communicated data. This has an impact on the total latency induced for real-time teleoperation and telemetry communications as the worst case execution time is increased as a result of the additional latency induced by secure communications as demonstrated in sections 3.4, 3.4.1, 3.4.3 and 3.4.5. Further analysis is required to ascertain how the mobile end-point influences the problems identified and how the findings interlink for this scenario.

The problem analysis conducted in Chapter 3 demonstrated that the communication latency recorded with contemporary security constructs had a significant impact on the communication latency recorded. Table 3.13 tabulates the communication latency recorded for the static to static problem scenario investigated.

Table 3.13: Simulated end to end communication latency for TinyAEAD-AES-128 and CCM-AES-128 constructs on a simulated single hop communication link for a thirty-six byte packet size at 8 MHz crystal frequency and the equivalent processing frequency measured (2 Mbps transmission rate).

Independent Variable	**Dependent Variables**			
Packet Size (Bytes)	**TinyAEAD-AES-128 3 rounds (ms)**	**TinyAEAD-AES-128 5 rounds (ms)**	**TinyAEAD-AES-128 10 rounds (ms)**	**CCM-AES-128 (ms)**
36	20.9	32.5	61.5	73.9
Equivalent Processing Rate	**0.047**	**0.030**	**0.016**	**0.013**
Equivalent Processing Frequency	**376 KHz**	**240 KHz**	**128 KHz**	**108 KHz**

The results presented in Table 3.13 demonstrate that the selection of the AEAD cryptographic services has a significant impact on the static to static real-time application scenario investigated; this is because of the additional processing time required to compute the number of rounds configured for the underling block cipher (AES-128). Applying these findings to the impact of the static to static real-time application showed that the dust explosion scenario analysed would be susceptible to a failure of the safety, reliability and availability of the system as a result of the additional communication latency induced.

Examination of the equivalent processing rate and frequency of the security constructs investigated in this chapter demonstrates that the application of security services has a significant impact on the processing rate of the microcontroller, this is because of the additional latency incurred from processing the security services.

Further investigation into the findings presented shows that the inclusion of security services utilises a maximum of up to five percent of the microcontrollers available processing frequency; this signifies that the security services selected will reduce the utilisation of any processing device regardless of the processing frequency specified; therefore, the security services are an underlying cause to additional latency incurred for real-time communication and application investigated in this thesis.

Knowledge collated from the in-depth problem analysis undertaken throughout this chapter demonstrates that the main problem identified is the time required to undertake a process (i.e security service or transmission of packetised data). The impact of the additional time incurred from communication latency is the reduction in the number of packets transmit-

ted in a given period of time; the consequence of this in the context of real-time communications is the reduction in the number of teleoperation and telemetry packets received in a given period of time.

Examination of the time required to undertake an operation is the reoccurring theme between all of the experiments conducted throughout the analysis as time determines the rate at which things can be achieved; inclusion of security services into the context affects this rate as a result of the increased time to process the packet through the AEAD construct; consequently, this directly impacts the number of packets transmitted and received in a given period of time.

Application of the knowledge obtained from the analysis to the context of this research investigated in this thesis is that the security services investigated would delay the teleoperational and telemetry commands; this has significant repercussion for hard and soft real-time constraints as the additional communication latency would delay the end point receiving the teleoperational or telemetry packet; this could result in a mission critical process failing and causing harm or damage to workers operating the application.

Analysis of the knowledge and its application to the context investigated in this thesis demonstrates that time is the most important aspect to take into consideration; as the security services investigated in this investigation contributed the most significant impact on the latency recorded with the number of rounds selected by the block cipher; therefore, a main consideration is to reduce the time to process the underlying block cipher.

Conclusion of the knowledge obtained from the preliminary experiments conducted in this section of the problem analysis indicates that the source of the problem is the duration required to process the block cipher and that the speed of the cryptographic service is the main requirement for the specification as the additional latency has considerable impact on the operational performance of the real-time teleoperation and telemetry communications; the number of rounds selected for the underlying block cipher for the AEAD constructs significantly influenced the latency and instantaneous packet throughput recorded from the subsequent experiments conducted in this chapter.

3.6 Chapter Summary

This chapter presented the problem analysis from the prospective of the real-time teleoperation and telemetry with the application of contemporary security services identified in Chapter 2. The questions investigated in this problem analysis examined the impact of contemporary security services on the communication latency incurred by static devices

(transmitter and receiver) used for real-time teleoperation and telemetry from the perspective of latency and packet throughput.

Knowledge obtained from the preliminary tests undertaken in this section of the problem analysis demonstrates that the latency incurred from the transmitter and receiver processing the contemporary cryptographic approaches impacts real-time teleoperation and telemetry; the processing frequency chosen influences the amount of latency generated. Instantaneous packet throughput of real-time teleoperation and telemetry data over multiple hop communications shows an exponential decay trend with the increased number of intermediate devices between the transmitter and receiver for heterogeneous systems.

Application of the mathematical models presented throughout the analysis has assisted with the clarification of the relationship between variables investigated in this analysis. Dissemination of the mathematical models and the analysis undertaken through this chapter has been presented at the following conferences:

- Simulating and Modelling the Impact of Security Constructs on Latency for Open Loop Control - IEEE 6th Computer Science and Electronic Engineering Conference (CEEC) 2014, Colchester, Essex - 26th September 2014.
- Simulating and Modelling the Impact of Secure Communication Latency for Closed Loop Control - IEEE 6th International Conference on Internet Technologies & Applications 2015, Wrexham, Wales - 11th September 2015.
- Study of Two Security Constructs on Throughput for Wireless Sensor Multi-Hop Networks - IEEE 38th International convention on information and communication technology, electronics and microelectronics, Opatija, Croatia - 27th May 2015.

Copies of the disseminated conference papers are located in Appendix sections R, S, and T.

The different categories of real-time applications have different variables to account for with static to static systems prioritising the latency of the process; whilst static to mobile and mobile to static systems requires consideration of the physical properties of the mobile device and adds complexity to the problem. Justification for an extensive analysis of the impact of security services on real-time telemetry that use mobile end-points is because contemporary real-time teleoperation and telemetry communications is applied in mobile scenarios (i.e Unmanned Aerial and Ground Vehicles) that travel at varying speeds; therefore, the next chapter presents the problem analysis of the impact of security services on real-time teleoperation and telemetry applications that use mobile end-points.

4 Investigation of Real-Time Teleoperation and Telemetry Communication Latency on a Mobile End-Point

4.1 Introduction

As discussed in Chapter 3; the application of security services on static to static real-time teleoperation and telemetry scenarios has a significant impact on the communication latency generated. While the scenarios investigated in the previous chapter considered the transmitter and receiver device to be static; there are situations where one or both end-point are mobile, therefore, the purpose of this chapter is to analyse how the mobile end-points influences the multi-faceted research problem investigated for this thesis and what its impact is on the problem scenarios examined in this chapter.

Building on the knowledge gained from the investigations undertaken in Chapter 3, the analysis undertaken in this chapter is based on the following questions:

- What is the impact of contemporary security services on the latency incurred by devices (transmitter and receiver) used in mobile real-time teleoperation and telemetry applications?
- What is the impact of contemporary security services on the maximum communication range between the transmitter and receiver devices used for mobile real-time teleoperation and telemetry applications?

The structure of this problem analysis undertaken is as follows; section 4.2 introduces the investigated problem scenarios; section 4.3 presents the relationship between speed of the mobile end-points, the communication time window and latency; in addition to investigating the maximum communication distance of a mobile end-point utilising various AEAD cryptographic constructs. Section 4.5 conducts an analysis of communication latency on a mobile end-point over a single hop communication link. A discussion of the investigating findings is presented in section 4.6. A chapter summary concludes in section 4.7.

4.2 Analysis of the Mobile End-Point Problem Scenario

This section of the problem analysis investigates the relationship between the speed of the mobile end-point and how it influences the time available to communicate real-time teleoperation and telemetry packets between the transmitter and receiver over a wireless (i.e. radio frequency) multiple-hop communication link.

The analysis undertaken uses the concept of a communication time window, the window is the time duration that a mobile end-point would be in communication range of a node

to transmit and receive real-time teleoperation and telemetry packets.

The communication time window makes the analysis application agnostic, as the analysis mainly focuses on the mobile end-points speed, distance and direction. Initial null hypothesis is that the faster the mobile end-point travels away from the transmitter the shorter the communication window will be, consequently, the number of packets will be low.

Intuitively, it can be seen that the opposite would be true. This analysis shows that there is a correlation between the number of communicated packets and the speed plus direction of the mobile end-point. When analysing communication with a mobile end-point, the problem of hand-off needs to be considered. In the context of this analysis, hand-off occurs when a mobile end-point changes its association (i.e communication) from one transmitting node to another during a communication session.

Hand-off may occur for a number of reason, which could include (1) the signal between the current transmitter and the mobile end-point may have deteriorated to an extent that could cause the communication link to be in danger of being dropped; (2) the mobile end-point is travelling from a communication window into another. No matter how the hand-off is accomplished, it will contribute additional latency to communication which will reduce the instantaneous packet throughput (see Chapter 3, section 3.4) and lower average packet throughput (e.g. transmission of photographic telemetry).

4.3 Investigated Problem Scenarios

The problem scenarios presented in this section are categorised into three areas which are static to mobile, mobile to static and mobile to mobile real-time teleoperation and telemetry applications over a single and multiple hop communication link. The problem scenarios presented in this section are generalised to showcase an instance of the scenarios investigated in this chapter.

The UK Civil Aviation Authority's (CAA) policy states that line-of-sight maximum operating distances of the UAV are five hundred metres (one thousand six hundred and forty feet) horizontal and one hundred and twenty metres (four hundred feet) vertical (CAA 2015). The classification of a tactical UAV in this thesis is based on the guidelines of the CAA regulations. The regulations stipulated are applicable to both static to mobile and mobile to static scenarios investigated in this problem analysis.

In this section of the problem analysis, it is assumed that the problem scenarios investigated are using a first in first out (FIFO) real-time scheduler to process tasks to enable

simplicity of the analysis conducted; analysis of the stated problem scenarios presented with a different real-time task scheduler is presented in Chapter 5. A presentation of the individual tasks required for the mobile real-time teleoperation and telemetry application is tabulated in Appendix G.

4.3.1 Static to Mobile and Mobile to Static Scenario

The scenario selected for static to mobile and mobile to static real-time teleoperation and telemetry is one where a fixed wing tactical unmanned aerial vehicle (UAV) is remotely piloted from the ground station using radio frequency communications. Figure 4.1 illustrates the concept of the static to mobile and mobile to static scenario.

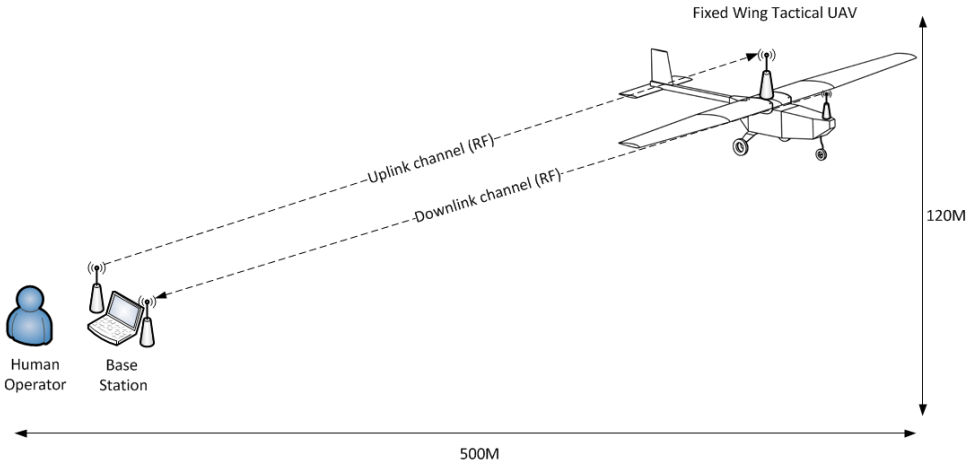


Figure 4.1: Illustrative concept of a point to point link for fixed wing UAV communication under CAA regulations.

Communications between the operator and the tactical UAV is achieved over two individual links; one of the links is designated as the uplink and represents a static to mobile system where command and control packets are transmitted between the base-station and UAV; the other link is assigned as the downlink and represents a mobile to static system that is streaming data (e.g. sensor readings) from the UAV to the base-station.

The second scenario investigated in this chapter is a static to mobile and telemetry application, where a fixed wing UAV is remotely piloted from the ground station using radio frequency over multiple hop simplex communication link. Figure 4.2 presents the illustrative concept of the second scenario investigated.

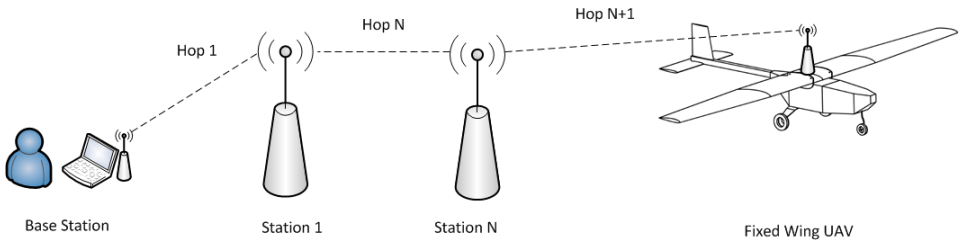


Figure 4.2: Illustrative concept of a multiple-hop communication link for a mobile end-point

In this scenario command and control packet are transmitted at regular intervals from the controlling device (i.e. base-station) to the UAV through a varying number of intermediate nodes. Figure 4.3 presents the illustrative breakdown of the mobile to mobile problem scenario investigated in this analysis.

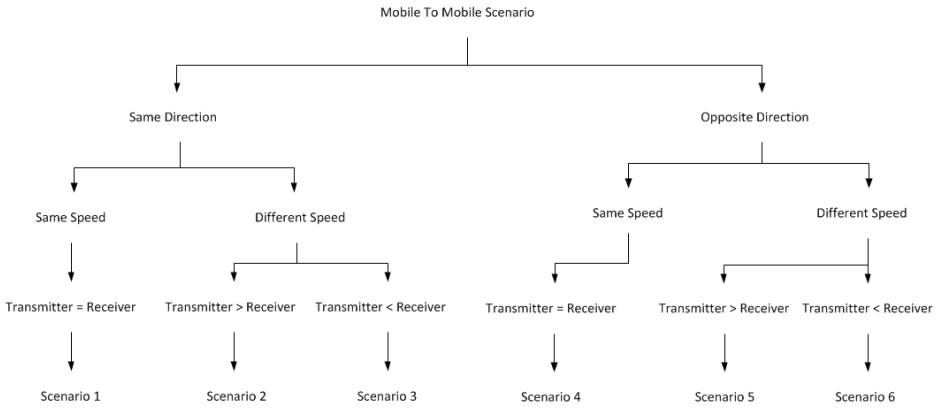


Figure 4.3: Illustrative concept of the mobile to mobile problem investigated

It is assumed in this analysis that mobile to mobile devices travelling in opposite directions are directly one hundred and eighty degrees opposite to each other. Analysis of the mobile to mobile scenario indicates that the problem can be analysed as a static to static scenario for Scenario 1; this is because the mobile end-points are travelling at the same speed in the same direction; therefore, the speed of the mobile end-point is negated as the distance between the two devices is constant and the communication time window would remain constant. Scenarios 2 and Scenario 3 are analysed as a static to mobile scenario as one device is consistently moving away from the other, this reflects a mobile device moving from a static device.

The communication time window for Scenario 2 would increase as the mobile end-point as the transmitter and receiver are within closer proximity per time epoch examined (at an non-linear rate dependent on the speed of the mobile end-points); whilst the communication time window for Scenario 3 would reduced (at an non-linear rate dependent on the speed of the mobile end-points) as the receiver device is faster than the transmitter device,

resulting in a reduction in the time both device are within proximity. The communication time window for Scenario 4 would reduce at a linear rate as both end-point are travelling in different directions at a fixed speed. The time window for Scenario 5 would decrease at a non-linear rate as a result of the different speed of the mobile end-points, whilst the time window for Scenario 6 would increase at an non-linear rate.

Analysis of the communication time window from the viewpoint of balancing the latency and the instantaneous packet throughput recorded is undertaken. In this thesis, the term balance point is defined as "*a situation in which different elements are equal or in the correct proportions*" (Dictionary 2018*a*); whilst the term optimise is defined as "*the best or most effective use of (a situation or resource)* (Dictionary 2018*b*)". The difference between the two concepts is essential in order to undertake the analysis in this thesis; this is because the communication time window problem is classified in this thesis as a multiple variable problem.

Classification of a multiple variable problem is presented in two sections, a multiple variable problem with infinite values, this is not best suited in this form of the analysis as the an infinite number of possibilities are applicable to solving the proposed problem investigated. The selected method for the communication time window analysis is a multiple variable problem with a finite number of values as this enables the problem to be analysed on a smaller scale that can be adjusted proportionately dependent on the number of finite variables that are under investigation; therefore, this facilitates an understanding of the multiple variable problem as a result of reducing the bounds used for the mathematical models derived in this analysis.

4.4 Validation of the Mathematical Models Derived for the Communication Time Window

This section of the problem analysis introduces the mathematical models derived for the analysis of the communication time window to transmit and receive data between the mobile end-point and the static base-station. The rationale for the analysis undertaken in this section is two-fold: (1) to understand when does a mobile end-point begin to become unresponsive; (2) the relationship between the speed of the mobile end-point, the security construct selected and the number of instantaneous packets received.

Validation of the scenario is conducted with an analysis of the speed of the mobile end-point in relation to the size of the communication time window for a mobile end-point over multiple hop propagation. Two formulas were used to obtain the time communication window; the first is the time, distance and speed formula and the second formula

using the packet transmission time. Formula 8 and Formula 9 present the mathematical models.

$$T = \frac{D}{S} \tag{8}$$

Formula 8: Time, distance, speed calculation

$$P_t = \lfloor P_r \cdot T \rfloor \tag{9}$$

Formula 9: Communication time window calculation.

Calculation of the time (T) is derived by dividing the distance of each intermediate node (D) by the speed of the mobile vehicle (S). Once the communication time window has been derived; the value is multiplied by the packet rate per second (P_r) at each intermediate node of the window in order to ascertain the number of theoretical packet transmissions obtained at each node associated on the communication link (P_t).

Leading on form the mathematical model presented in Formula 8 and Formula 9; the following hypothesis have been derived to validate the relationship between the number of messages transmitted in relation to the communication time window. The null hypothesis is that the communication time window will not change dependent on the security service and speed of the mobile end-point selected for the real-time teleoperation and telemetry applications. The alternative hypothesis is that the the communication time window will change dependent on the security service and speed of the mobile end-point selected for the real-time teleoperation and telemetry applications.

The tables presented in this section showcase the impact of the AEAD cryptographic constructs on the operation of an unmanned vehicle in terms of the number of communicated real-time teleoperation and telemetry packets in the communication time window as a result of the speed of the mobile vehicle using Formula 8 and Formula 9. Table 4.1 tabulates the communication time window of a mobile vehicle at a speed of thirteen and sixty metres per second with no security service selected at a crystal frequency of 4 MHz (1 million instructions per second).

Table 4.1: The communication time window for an unmanned vehicle at various speed before responding to the telecommand utilising no security services at a crystal frequency of 4 MHz (1 MIPS), a transmission rate of 250 Kbps and a packet size of thirty-six bytes.

Independent Variable	**Dependent Variables**
Mobile Actuator Speed (m/s)	**Communication Window (Seconds)**
13	7.7
60	1.6

Data obtained in Table 4.1 demonstrates that the speed of the mobile actuator influences the communication time window to transmit and receive real-time teleoperation and telemetry packets as the mobile end-point travelling at sixty metres per second has a reduce period of time to communicate with the static end-point in comparison to the the mobile end-point travelling at thirteen metres per second.

Examination of the findings presented in Table 4.1 indicate that the difference between the communication time window for the two speeds examined is up to five times greater; this is because the speed of the mobile end-point determines the duration that the mobile actuator is in communication range of the devices (i.e. 100 metres); this is derived by dividing the speed of the mobile end-point by the maximum communication range of the devices.

The findings presented demonstrates that the time, distance and speed formula model is applicable in order to derive the time for the communication time window; however, the impact of cryptographic services on the communication time window has not been factored into the problem. To ascertain the impact of cryptography and its relationship with the communication time window; Table 4.2 and Table 4.3 tabulates the number of packets received at each intermediate node over a heterogeneous communication link for a thirty-six byte packet with TinyAEAD-AES-128 at three rounds and CCM-AES-128 using the mathematical models presented in Formula 8 and Formula 9.

Table 4.2: The number of communicated packets from the mobile end-point at each intermediate node on the communication link at a speed of thirteen metres per second with TinyAEAD-AES-128 at three rounds and CCM-AES-128 (crystal frequency of 4 MHz (1 MIPS), a transmission rate of 250 Kbps and a packet size of thirty-six bytes).

Independent Variable	**Dependent Variable**	
Number of Hops	**TinyAEAD-AES-128 (3 rounds)**	**CCM-AES-128**
1	11	7
2	5	3
3	3	2
4	2	1
5	2	1
6	2	1

Results presented in Table 4.2 demonstrates that the number of packets transmitted follows an exponential decay trend for both TinyAEAD-AES-128 at three rounds and CCM-AES-128 as the number of intermediate nodes increases; this is because the nature of the heterogeneous communication link across each intermediate node and the security service selected has resulted in a reduction in the packet rate per second obtained at each intermediate node; in addition, the speed of the vehicle has reduced the communication time window to transmit and receive the number of packets between the transmitter and receiver.

Analysis of the information presented in Table 4.2 shows that the time required to process the security service contributes towards the the number of communicated packet received in the communication time window with a difference of four packets for one intermediate node on the communication link using TinyAEAD-AES-128 at three rounds and CCM-AES-128; this is because of the time required to process the cryptographic operation as presented in the analysis undertaken in Chapter 3.

Examination of the number of packets received over a heterogeneous multiple hop communication link shows that there is an offset between the number of packets received by TinyAEAD-AES-128 at three round and CCM-AES-128; this is because the processing delay for the cryptographic services has the same offsets across the intermediate nodes; however, the accumulation in the processing delay of the cryptographic services reduces the communication time window as the processing latency accumulates per intermediate node on the communication link and directly impacts on the packet rate recorded at each hop. Table 4.3 tabulates the comparison of the number of transmitted packets with TinyAEAD-AES-128 at three rounds and CCM-AES-128 with a mobile end-point travelling at a speed of sixty meters per second.

Table 4.3: The number of communicated packets from the mobile vehicle to each intermediate node on the communication link at a speed of sixty metres per second with TinyAEAD-AES-128 at three rounds and CCM-AES-128 (crystal frequency of 4 MHz (1 MIPS), a transmission rate of 250 Kbps and a packet size of thirty-six bytes).

Independent Variable	**Dependent Variable**	
Number of Hops	**TinyAEAD-AES-128 (3 rounds)**	**CCM-AES-128**
1	2	1
2	1	0
3	0	0
4	0	0
5	0	0
6	0	0

Findings obtained from the mathematical analysis undertaken demonstrates that the speed of the mobile vehicle impacts on the available time to communicate data; this is because the speed of the mobile vehicle influences the total time that the mobile vehicle is within range of the intermediate node on the network, as demonstrated by Table 4.2 and Table 4.3.

4.4.1 Section Summary

Application of the findings to the static to mobile and mobile to static scenarios demonstrates that three variables influences the instantaneous packet throughput recorded, they are: the selection of the cryptographic service, the speed of the mobile end-point and the number of intermediate nodes on the communication link.

The time allocated to communicate data between the mobile end-point and the static receiver is achieved in a communication time window that is variable based on the speed of the mobile end-point and the cryptographic services selected; however, the current analysis undertaken has assumed that the communication link between the transmitter and receiver is under ideal conditions (i.e no packet loss); therefore, this raises the question of what the impact of a non-ideal communication link is on the real-time application scenarios investigated.

Further examination of the findings indicate that privacy of the shared secret used for secure communication is an important factor to consider; this is because the duration of the communication time window is for a limited period, this limits the attacker to a constrained period of time to conduct an attack against the communication link as a result of the real-time constraints associated with the context investigated.

Findings presented in this analysis demonstrates that the alternative hypothesis presented is correct and that the communication time window does change dependent on the security service selected and speed that the mobile end-point is travelling. The current analysis undertaken focused on the impact of the speed and the cryptographic services to the mobile end-point and not on the distance that the mobile end-point could travel before becoming unresponsive. The next section of the problem analysis investigates the maximum communication distance that a mobile end-point can travel with using secure communications before falling under a specified packet threshold.

4.4.2 The Maximum Communication Range of a Mobile End-Point with Various Cryptographic Services

The rationale for this analysis is to understand what the maximum communication range is for the mobile end-point before the number of real-time teleoperation and telemetry instantaneous packets falls below a specified threshold.

Findings obtained from the aforementioned analysis conducted shows that the speed of the mobile actuator and the cryptographic service both contribute towards the mobile scenarios examined as the cryptographic service chosen affects the rate that packets are transmitted in a given time period and the speed of the mobile end-point influences the time that the mobile end-point is within communication range.

Analysis is undertaken to ascertain if the relationship between the speed of the mobile end-point and the cryptographic services does have an impact on the maximum communication range of a mobile end-point from the viewpoint of meeting a specified threshold for the number of packets received by the mobile end-point. Formula 10 presents a mathematical model that can be used to the expected number of packets received at a specified distance of the communication link.

$$P_f = \frac{1}{\left(\frac{P_l \cdot H_n}{\left(\frac{T_w}{S}\right)}\right)} \tag{10}$$

Formula 10: Calculation for the expected number of packets received at a specified distance of the communication link.

The number of forecasted packets (P_f) is calculated by multiplying the latency to process one packet at the start node (P_l) by the number of intermediate hops (H_n) to derive the total latency over the number of hops specified. The sample time (T_w) is divided by the speed of the mobile vehicle (S) to obtain the communication time window; this is divided

by the sub-total of the previous calculation to obtain the latency per second. The inverse of the sub-total is used to derive the number of forecasted packets transmitted at a particular intermediate node for the instance of time examined.

Leading on form the mathematical model presented in Formula 10; the following hypothesis have been derived to validate the maximum communication range for the mobile end-point before the number of real-time teleoperation and telemetry packets falls below a specified threshold. The null hypothesis presented in this analysis is that the selection of AEAD constructs will not have a significant impact on the maximum communication range before falling under the specified packet threshold. The alternative hypothesis is that the selection of AEAD constructs will have a significant impact on the maximum communication range before falling under the specified packet threshold.

Input parameters for the mathematical model are as follows; a thirty-six byte packet size was selected as an instance of a real-time teleoperation message used for communications between the transmitter and receiver device utilising cryptographic services TinyAEAD-AES-128 and CCM-AES-128 operating at a crystal frequency of 4 MHz (1 million instructions per second) processing frequency and a transmission rate of 250 Kbps. In this instance of the analysis; the packet rates derived from the multiple-hop propagation test in Chapter 3, section 3.4.5, Figure 3.15 are used to formulate the expected outcomes. Table 4.4 tabulates the configuration set for each variable of the mathematical model, based on the configuration parameters specified.

Table 4.4: Processing latency of TinyAEAD-AES-128 and CCM-AES-128 at a 4 MHz crystal frequency (1 MIPS), a transmission rate of 250 Kbps and a packet size of 36 bytes

Independent Variable	**Dependent Variable**
AEAD Construct	**Latency (milliseconds)**
TinyAEAD-AES-128 3 rounds	11
CCM-AES-128	14

Analysis of the results presented in Table 4.4 demonstrates that the cryptographic construct selected contributes towards the time required to process the message per intermediate node and reinforces findings presented in the problem analysis conducted in Chapter 3.

Validation of the cryptographic services impact on the maximum communication range for a mobile end-point before falling under a specified packet threshold is conducted to ascertain if there is a relationship between the additional latency incurred by cryptographic services and the speed of the mobile end-point on the number of instantaneous packets

received in a given period of time,

Investigation conducted in this section examines two variables; they are: (1) the number of instantaneous packets recorded in relation to the communication time window at each intermediate hop; (2) the maximum communication distance of a mobile end-point with various configurations for a specified number of packets. Values presented in Table 4.4 are used as the input parameter into the mathematical models derived for the analysis undertaken.

The scenario for the tests is as follows: A communication range of each intermediate hop is a hundred metre radius with a coverage of a fifty metre radius either side of the node placement in an omni-directional pattern. The protocol chosen for this scenario is a UDP like protocol, where there is no acknowledgement of successful packet delivery or packet loss. It is assumed in this scenario that the wireless broadcast range of each intermediate node does overlay with neighbouring intermediate nodes in order to facilitate multiple hop communication; in addition, there is no communication hand-off between the intermediate nodes as the UAV travels from one intermediate node's communication time window to another.

4.4.3 The Number of Instantaneous Packets Recorded by a Mobile End-Point Across a Multiple-Hop Communication Link

This section of the analysis investigates the number of instantaneous packets recorded by a mobile end-point across a multiple-hop communication link. The rationale for the analysis undertaken is to identify how the communication time window and the number of instantaneous packets recorded are influenced by the speed of the mobile actuator across a heterogeneous multiple hop communication link with comparison of a static to static and mobile to static scenarios.

Benchmark analysis of the mathematical model presented in Formula 10 was undertaken against a simulated environment as described for the multiple hop propagation test presented in Chapter 3, section 3.4.5. Appendix F presents the test plan and the schematic of the simulated test platform. Table 4.5 tabulates the expected number of packets over a varying number of intermediate nodes for a 36 byte packet size using TinyAEAD-AES-128 at three rounds for a static to static scenario.

Table 4.5: Comparison of the number of packets received from the simulator and mathematical model for a static to static scenario using TinyAEAD-AES-128 at three rounds at a 4 MHz crystal frequency (1 MIPS) and a 36 byte packet (timings as presented in Appendix A).

Independent Variable	**Dependent Variables**	
Number of Hops	**Simulation packets recorded**	**Model packets calculated**
Start Node	91	91
1	45	45
2	30	30
3	22	22
4	18	18

Results presented in Table 4.5 demonstrates that the mathematical model and the simulation give the same results; this shows that the mathematical model and the simulation are correlated for the number of packets recorded for a specific time frame sampled.

Validation of the findings presented was undertaken using CCM-AES-128 in order to ascertain if the mathematical model would hold true in comparison to the simulation results for a different AEAD construct. Table 4.6 tabulates the results using the same specifications as the previous experiment.

Table 4.6: Comparison of the number of packets received from the simulator and mathematical model for a static to static scenario using CCM-AES-128 at three rounds at a 4 MHz crystal frequency (1 MIPS) and a 36 byte packet.

Independent Variable	**Dependent Variables**	
Number of Hops	**Simulation packets recorded**	**Model packets calculated**
Start Node	70	70
1	35	35
2	23	23
3	17	17
4	14	14

Data presented in Table 4.6 shows that the number of packets recorded by the simulator and the mathematical model are correlated for the number of intermediate nodes examined in this analysis; this demonstrates that the mathematical model can be used to forecast the expected number of packets at each intermediate node on the communication link; however, the question of what is the maximum distance that could be travelled before the instantaneous packet throughput recorded in a given period of time falls below a specified threshold is still unanswered; therefore, the next section of this investigation examines the maximum distance that a mobile end-point can travel before the number of instantaneous packet throughput received by the mobile end-point falls below a specified number of packets.

4.4.4 The Maximum Communication Distance of a Mobile End-Point with Various Configurations for a Specified Number of Packets

Leading from the aforementioned analysis conducted in the previous sub-section, the focus of the analysis undertaken in this section is on the the maximum communication distance of a mobile end-point with various configurations for a specified number of packets. In order to conduct this analysis, a transposition of Formula 11 is required in order to identify the maximum distance traveled before the threshold is met.

$$\lfloor D \rfloor = (\frac{P_s}{P_t}) \cdot D_u \tag{11}$$

Formula 11: Calculation of the maximum communication distance for a specified number of packets and sample time.

Calculation of the distance traveled (D) is derived by dividing the start packets (P_s) by the total number of packets of the start of the communication window (P_t); The value represents the number of intermediate nodes required to propagate the date between the start and end node; in order to convert this value into a distance, the unit used to measure the distance per hop (D_u) is multiplied by the number of intermediate nodes in order to ascertain D.

The assumption is that the distance between each intermediate node is one hundred meters in distance; therefore, the number of intermediate hops derived from the calculation of $(\frac{P_s}{P_t})$ is multiplied by one hundred. This formula can also be transposed to calculate the time required to transmit a specified number of packets by dividing the sample time by the number of intermediate nodes.

The parameters from the aforementioned analysis conducted in section 4.4 are used to calculate the maximum communication distance before falling below a specified packet threshold; this is a sample time of sixty seconds and the starting number of packets is ninety one packets for TinyAEAD-AES-128 and seventy packets for CCM-AES-128 (see Table 4.5 and Table 4.6). The packet threshold stipulated in this instance of the analysis is forty packets. Table 4.7 tabulates the maximum communication range for TinyAEAD-AES-128 at three rounds and CCM-AES-128 for a threshold of forty packets for a static to static scenario.

Table 4.7: Maximum communication range for TinyAEAD-AES-128 at three rounds and CCM-AES-128 for a static to static scenario with a packet threshold of forty packets (a crystal frequency of 4 MHz (1 MIPS), transmission rate of 250 Kbps and packet size of 36 bytes.).

Independent Variable	**Dependent Variable**
AEAD Construct	**Maximum Communication Distance (Metres)**
TinyAEAD-AES-128 3 rounds	227
CCM-AES-128	175

Results presented in Table 4.7 demonstrates that the maximum communication distance before the specified packets required falls beneath its threshold is greater for TinyAEAD-AES-128 at three rounds in comparison to CCM-AES-128 with a difference of fifty-two metres; this is because the time required by the cryptographic constructs increases the latency required to encrypt and decrypt packetised data at each intermediate node; this demonstrates that the additional latency incurred from the security constructs and the multiple hop heterogeneous communication link influences the packet rate and consequently reduces the maximum distance travelled before the packet threshold for the specific time period is no longer met.

The outcome of the additional latency incurred by the security service lowers the packet rate per second as the additional latency reduces the instantaneous packet throughput for a static to static scenario; this is noticeable for CCM-AES-128 in comparison to TinyAEAD-AES-128 as the number of rounds used by the underlying block cipher is reduced; this is related to the time required to process the security service. The final part of this analysis investigates if the speed of the mobile end-point contributes towards the problem examined.

The parameters and assumptions stated in the aforementioned tests conducted were selected for the mathematical model presented in Formula 10. The speed of the mobile end-point examined in this analysis was thirteen metres per second. Table 4.8 tabulates the expected number of packets over a varying number of intermediate nodes for a 36 byte packet size using TinyAEAD-AES-128 at three rounds.

Table 4.8: The number of packets forecasted from the mathematical model results using TinyAEAD-AES-128 at three rounds and CCM-AES-128 for a mobile end-point traveling at 13 metres per second (4 MHz crystal frequency (1 MIPS), 250 Kbps transmission rate and a 36 byte packet size.).

Independent Variable	**Dependent Variables**	
Number of Hops	**TinyAEAD-AES-128 3 rounds packets recorded**	**CCM-AES-128 packets recorded**
Start Node	91	70
1	7	5
2	3	2
3	2	1
4	1	1

Results presented in Table 4.8 demonstrate that the selection of the cryptographic construct has an impact on the number of instantaneous packets received in a given period of time; however, with the inclusion of the speed of a mobile end-point, the number of received packets at each intermediate hops is significantly reduced, this is because the communication time window to transmit and receive packetised data between the mobile end-point and the intermediate node is reduced as a result of the continuous fixed speed of the mobile end-point.

The consequence of the inclusion of the mobile end-point traveling at a fixed speed with cryptographic services applied is demonstrated with the analysis of the distance tavelled by the mobile end-point before the number of packets received falls under a specified threshold; in this instance of the analysis, the packet threshold has been set to forty five packets. Table 4.9 tabulates the maximum communication distance for a mobile end-point traveling at thirteen metres per second with TinyAEAD-AES-128 at three rounds and CCM-AES-128 for a threshold of forty packets at a processing frequency of 4 MHz (1 MIPS) and packet size of 36 bytes.

Table 4.9: Maximum communication range for a mobile end-point traveling at thirteen metres per second with TinyAEAD-AES-128 at three rounds and CCM-AES-128 for a threshold of forty packets (crystal frequency of 4 MHz, 250 Kbps transmission rate and packet size of 36 bytes.).

Independent Variable	**Dependent Variable**
AEAD Construct	**Maximum Communication Distance (Metres)**
TinyAEAD-AES-128 3 rounds	17.5
CCM-AES-128	13.4

Results presented in Table 4.9 demonstrates that the speed of the mobile actuator and the cryptographic services selected impacts on the maximum communication range for

a mobile end-point before it falls beneath a specified packet threshold; therefore, this supports the alternative hypothesis that the the selection of the AEAD construct will not have a significant impact on the maximum communication range before falling under the specified packet threshold.

4.4.5 Section Summary

Findings presented in this section of the problem analysis has identified that the mufti-faceted relationship between the speed of the mobile end-point; the cryptographic services selected and the packet throughput all contribute towards the problem investigated in this thesis. The speed of the mobile end-point influences the communication time window as the time that the mobile end-point is within communication range is affected by the speed of the device; this directly influences the number of communicated packets that are received in a given period of time.

Examination of the findings presented in this section of the problem analysis discussed the impact of security services on the maximum communication range of the mobile end-point before the specified packet threshold is no longer met; however, the consideration of the communication link and the components used to facilitate communications has not been factored; therefore, this raises the question of how the communication components influence the maximum communication range attainable by the real-time teleoperation and telemetry application.

Additional information obtained from the analysis undertaken is that the cryptographic service impacts on the packet rate as the additional latency incurred reduces the number of packets that can be transmitted in a given period of time; therefore, this indicates that this is a contributing factor that impacts the real-time teleoperation and telemetry problem investigated in this thesis; however, it is not visabilly clear how the findings impact the mobile end-point, therefore, an investigation of the impact of a secure communication link on the operational performance of a semi-autonomous mobile end-point is undertaken to ascertain the impact of the communication delay identified on a mobile end-point.

4.5 Analysis of Communication Latency on a Mobile End-Point over a Single Hop Communication Link

This section of the problem analysis investigates the speed of the mobile end-point and how it influences the time available to communicate real-time teleoperation and telemetry messages between the transmitter and receiver over a single-hop communication link. Analysis conducted in section 4.2 has identified the impact of the security services on a

mobile end-point over a multiple hop communication link using mathematical modelling.

Findings collated from the aforementioned section in this problem analysis demonstrates that the mobile end-point is affected with the selection of security service applied with the reduction in the instantaneous packet throughput recorded. The impact of this finding on the real-time teleoperation and telemetry communications is that the mobile end-point would travel further before the teleoperation command is executed as a result of the communication latency incurred; whilst telemetry communications is affected with the reduction in the number of packets communicated within a set period of time. To exemplify the impact of security services on the mobile end-point, this section of the analysis presents the impact of security services on the teleoperation of a mobile end-point in a controlled simulated environment.

4.5.1 The Impact of a Secure Communication Link on the Operational Performance of a Semi-Autonomous Mobile End-Point

Real-time application scenarios examined in this thesis demonstrate that a variety of methods are applicable to teleoperate the mobile end-point. Analysis conducted has focused on scenarios where the mobile end-point is operated by a human; observation of the mobile end-point identifies that there are multiple methods to teleoperate the mobile end-point, these include semi-autonomous and fully autonomous systems. The analysis presented in this section investigates the impact of a secure communication link on a mobile ground vehicle to derive what the impact of the secure communication link is on different mobile platforms.

The mobile end-point in the analysis undertaken using the simulator uses a script to conduct a series of tasks in a sequential order (i.e. a First In First Out (FIFO) task scheduler). After each task conducted, the task for the next mobile end-point will be delayed by the communication latency recorded to process the investigated cryptographic service before conducting the next task in the script; this is to reflect the delay of a human operator transmitting a real-time teleoperation message over a secure communication link.

The null hypothesis presented is that the secure communication link would not have the same impact on the responsiveness between the command sent and the action undertaken based on the command sent to the mobile ground vehicle. The alternative hypothesis is that the secure communication link will have the same impact on the responsiveness between the command sent and the action undertaken based on the command sent to the mobile ground vehicle.

The test platform selected for this experiment was a simulated environment with the robot

simulator software selected (Papini 2016). The operation of the robot in this scenario was an autonomous mobile ground vehicle that followed a series of commands to drive from the start position to the exit point in a maze. Input delays of twenty-one milliseconds and one hundred and ninety milliseconds and seven hundred milliseconds was implemented into the semi-autonomous script to reflect the additional delay incurred from the autonomous vehicle to process TinyAEAD-AES-128 at three rounds, CCM-AES-128 and GCM-AES-128 per task conducted in the pre-computed script used by the semi-autonomous mobile end-point. The same start position is initiated for each test with the delay of the AEAD constructs applied per command initiated from the command script used for all tests.

Measurement recorded of the path taken by the semi-autonomous ground vehicle and the time required to complete the task. The start and exit positions for the robot to exit the maze were the same for all tests conducted. All timings were taken from a real-world clock. Configuration of the test platform, test procedure and methodology are presented in Appendix H. Table 4.10 tabulates the time required by the semi-autonomous ground vehicle to exit the maze with different security measures.

Table 4.10: Time required by the semi-autonomous ground vehicle to exit the maze with different security measures.

Independent Variables	**Dependent Variables**	
Security Service	**Average Time (Seconds)**	**Difference in Time (Seconds)**
No Security	42.8	0.0
TinyAEAD-AES-128 (3 rounds)	43.1	0.3
CCM-AES-128	44.7	1.9
GCM-AES-128	77.4	34.6

Results presented in Table 4.10 for the robot using security services show that the time required for the semi-autonomous mobile ground vehicle to complete the tasks was at its lowest with TinyAEAD-AES-128 three rounds selected; whilst the time required to complete the same operation with GCM-AES-128 recorded the highest time. The statistical analysis of the data presented in Table 4.10 shows that the comparison of time recorded for no security with TinyAEAD-AES-128 at three rounds and CCM-AES-128 is within one standard deviation (normal distribution); whilst the comparison of no security and GCM-AES-128 is within two standard deviations; this demonstrates that GCM-AES-128 has a significant impact on the latency recorded for the mobile end-point in comparison to other variants investigated. Figures 4.4, 4.5, 4.6 and 4.7 illustrate the trace-lines of the autonomous mobile ground vehicle with various cryptographic services applied.

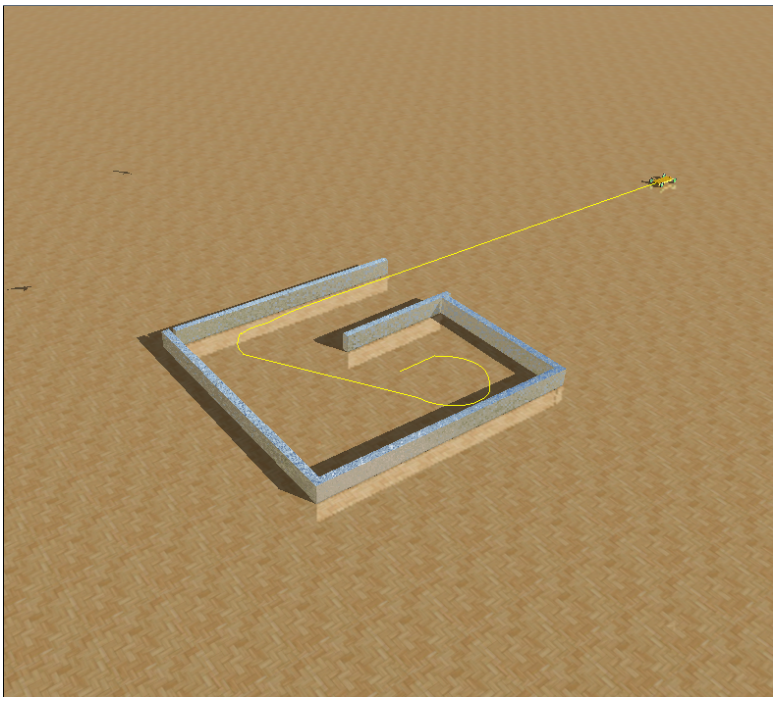


Figure 4.4: Recorded path taken by the semi-autonomous mobile ground vehicle to exit the maze with no security services applied.

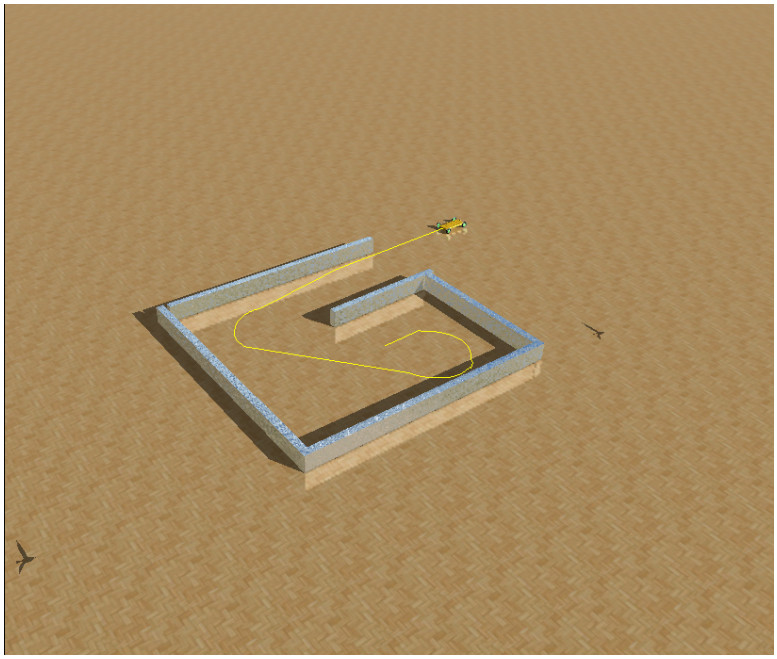


Figure 4.5: Recorded path taken by the semi-autonomous mobile ground vehicle to exit the maze with TinyAEAD-AES-128 at three rounds.

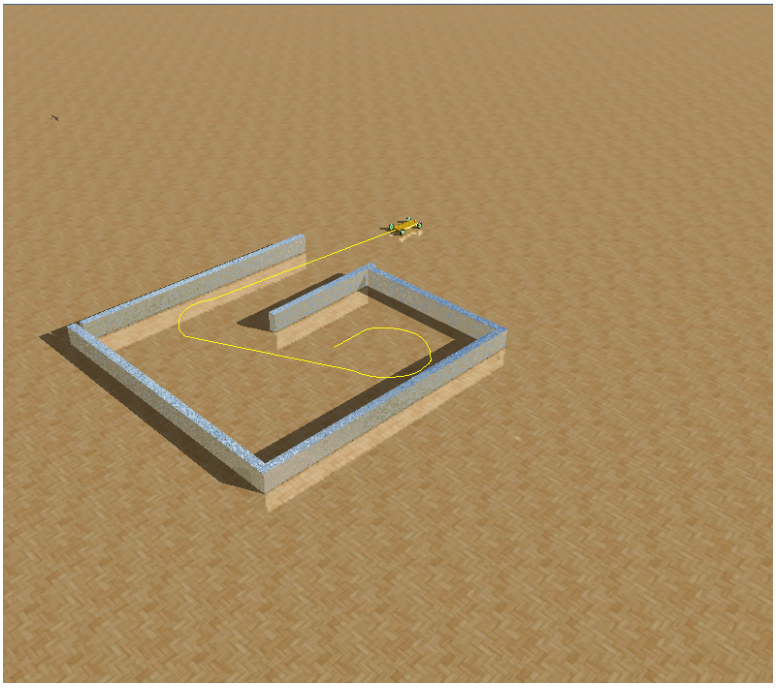


Figure 4.6: Recorded path taken by the semi-autonomous mobile ground vehicle to exit the maze with CCM-AES-128.

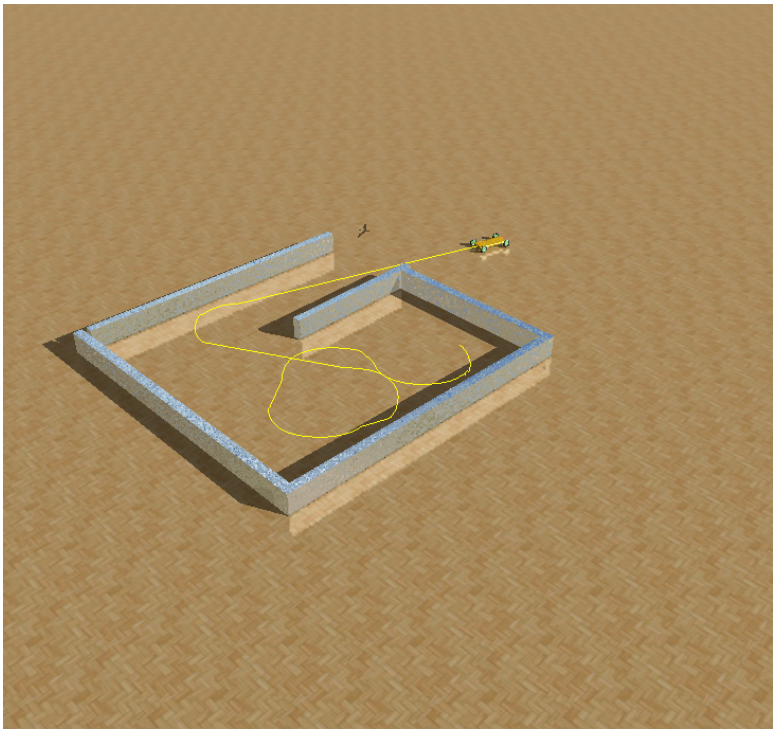


Figure 4.7: Recorded path taken by the semi-autonomous mobile ground vehicle to exit the maze with GCM-AES-128.

The trace-line of the semi-autonomous mobile ground vehicle with GCM-AES-128 security measure applied shows that the impact of the additional delay incurred has an impact on the path taken by the device; whilst TinyAEAD-AES-128 at three rounds and CCM-

AES-128 followed a similar trace-line as no security. The reason why the trace-line does not follow the same patterns as the aforementioned test is because the additional latency incurred at each command causes the vehicle to travel further before a response to the next task is performed; this is as a result of the first in first out scheduler used to compute the tasks as all tasks are undertaken in a sequential order; therefore, this raises the question of how different real-time schedulers would impact on the situation analysed.

4.5.2 Section Summary

The findings presented from the semi-autonomous unmanned ground vehicle tests is that the additional processing delay of security services contributes to the additional distance travelled by the mobile platform before responding to the commands sent. The traces presented in the aforementioned analysis undertaken demonstrates the impact of the security services on the semi-autonomous mobile end-points as the delay impacts on the correct process being complete as the programme follows a deterministic set of instructions to leave a maze; but, the latency between each command begin executed results in the UGV travelling too far before the next action is taken; therefore, the UGV does not perform the correct task of leaving the maze or requires a longer period of time to complete the operation as shown with standardised constructs CCM-AES-128 and GCM-AES-128.

In the context of the research undertaken in this thesis, this reinforces the findings obtained with the mathematical modelling presented in section 4.2; this is because the latency incurred contributes to the distance travelled by the mobile end-point before responding to the command; as the problem focuses on the real-time communications, this further exemplifies the impact of latency with the inclusion of a mobile end-point and consequently, this could result in the mobile actuator falling outside the communication range before the next teleoperation message is transmitted and cause the mobile end-point to become unresponsive.

Knowledge obtained from this analysis is that the alternative hypothesis that the secure communication link will have the same impact on the responsiveness between the command sent and the action undertaken based on the command sent to the mobile ground vehicle is true for this instance of the analysis; however, this analysis has identified that the selection of the task scheduler for real-time communications may influence the latency incurred by the real-time application and therefore requires further investigation to ascertain its impact to the context examined in this thesis.

4.6 Discussion

The mobile end-point adds additional complexity to the multi-faceted research problem presented as the speed that the mobile end-point is travelling impacts on the time available to communicate data between the devices as presented in section 4.4; this is further exemplified with the inclusion of the cryptographic service selected for secure communications reduces the packet rate with the size of the communication time window results in a reduction in the number of real-time teleoperation and telemetry messages transmitted.

The impact of the relationship between the speed of the mobile actuator and the cryptographic service selected on real-time teleoperation and telemetry applications is the maximum communication distance available before a specified packet threshold is no longer met as cryptographic services that have a lower impact on the additional latency have an increased maximum distance in comparison to cryptographic service with a higher impact on the additional latency. The speed of the mobile end-point further contributes to this problem as the speed of the mobile end-point in combination with the cryptographic service selected interplays with the maximum communication distance and the number of packets transmitted per intermediate node on a multiple hop network as presented in section 4.4.2.

Mitigation of the additional distance travelled by the mobile end-point can be achieved by reducing the speed of the mobile device to reduce the additional distance travelled before responding to a teleoperation command; however, this could be problematic in situations where a mobile end-point has limited resources to complete its tactical mission. Alternative measures to overcome the problem identified is to reduced the time required by the cryptographic service to process data as the reduction in latency contributes to the distance travelled by the mobile end-point as presented in section 4.5.

AEAD paradigms investigated throughout this problem analysis have identified that the additional latency incurred has impacted on the real-time communications for static and mobile environments. The current paradigms of security and energy conservation have demonstrated a significant impact on the real-time teleoperation and telemetry context investigated as the security service selected influence the maximum communication distance before the packet threshold is no longer met, this is because the AEAD methods investigated influence the packet rate and the duration of the communication time window. Designs that prioritise security have a greater significant impact in comparison to designs that prioritised energy.

Examination of the findings obtained from the problem analysis conducted in this chapter

shows that the security services investigated influence the real-time teleoperation and telemetry application with a mobile end-point; this is because the processing and communication latency to send packetised data over a secure communication link impacts on the real-time operation of the mobile device as a result of the real-time constraints associated with the system.

An instance of this problem is the human operator piloting the mobile end-point as the corrections to the mobile end-point during operation is manually controlled; as a result of the communication latency incurred using a secure communications link for the real-time teleoperation commands; the human operator would either under-compensate or over-compensate for the delayed between the command initiated at the base station and the actuator acting upon the commands. This links to control theory where delay induced into the system influences the time required by the actuator to reach a steady state; this holds true for the analysis conducted in this Chapter as the real-time applications scenarios can be classified as either an open loop control system (teleoperation of the mobile end-point only) and a closed loop system (human operator makes corrective actions based on real-time telemetry feedback).

This issue is further exemplified with the inclusion of the real-time telemetry link as the communication and processing latency would distort the pilots reaction to an event (i.e. live video stream from the mobile end-point) and consequently impact on the teleoperation of the mobile end-point to conduct a specified task. The findings observed link to existing theory of the Doppler effect and phase lag where the signal is affected by the shift in time; in this case, the processing and communication latency incurred from cryptographic services, the speed of the mobile end-point and the propagation method selected.

The findings obtained indicates that the real-time nature of the application contributes towards the problem examined as the additional time incurred from the cryptographic process has a significant impact on the communication latency incurred for the real-time applications investigated; however, the current analysis of the cryptographic services has been under the assumption that a FIFO task scheduler is selected for all of the test conducted and raises the question of how different real-time schedulers would impact the latency recorded by the real-time applications is identified as an area that requires examination.

4.7 Chapter Summary

This chapter presented the problem analysis from the prospective of the real-time teleoperation and telemetry with the application of contemporary security services identified

in Chapter 2. The questions investigated in this problem analysis examined the impact of contemporary security services on the latency incurred by devices (transmitter and receiver) used in mobile real-time teleoperation and telemetry applications and how contemporary security services influence the maximum communication range between the transmitter and receiver devices used for mobile real-time teleoperation and telemetry applications.

Knowledge obtained from the preliminary tests undertaken in this section of the problem analysis demonstrates that the latency incurred from the transmitter and receiver processing the contemporary cryptographic approaches impacts real-time teleoperation and telemetry and that the speed of the mobile-end point further contributes towards the multi-faceted, non-trivial problem investigated in this thesis by reducing the communication time period between the transmitter and receiver to communicate data.

The findings collated from the in-depth analysis undertaken demonstrates that the core problems identified throughout this problem analysis is the impact of the security services and the speed of the mobile end-point on the instantaneous packet throughput recorded. The impact of this findings to the context investigated in this thesis is that the number of real-time teleoperation and telemetry messages transmitted in a given period of time is reduced dependent on the speed of the mobile end-point, the security service selected and the propagation methods between the transmitter and receiver as all three variables are interlinked by the underlying cause of the problem identified; which is time.

Outcomes from the analysis conducted in this chapter are the mathematical models to ascertain the communication time window and the maximum communication distance for a specified packet threshold for static and mobile end-points. In addition, a visual representation of the impact of security services has been conducted to identify its impact to the real-time application. Application of the findings presented throughout the analysis has assisted with the clarification of the relationship between variables investigated in this analysis. Dissemination of the mathematical models and the analysis undertaken through this chapter has been presented at the following conferences:

- Balancing Throughput and Latency for an Aerial Robot over a Wireless Secure Communication Link - IEEE 2nd International Conference on Cybernetics CYBCONF 2015, Gdynia, Poland - 25th June 2015
- The Affect of Two Cryptographic Constructs on QoS and QoE for Unmanned Control Vehicles - IEEE 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, United Kingdom - 25th June 2015

Copies of the disseminated conference papers are located in Appendix sections U and V.

Analysis conducted in Chapter 3 and Chapter 4 has been undertaken from the perspective of the transmitter and receiver devices for real-time teleoperation communications without the consideration of the communication link as it has been assumed that the communication link is error free and not susceptible to errors when the reality is that the communication link is susceptible to non-ideal channel characteristics. In addition, the task schedulers investigated in this thesis focused on a FIFO scheduler under the assumption that tasks are conducted sequentially in order, whilst real-time applications may use different methodologies dependent on the context of the real-time application.

The next section of the problem analysis will investigate the impact of security services on real-time schedulers used for real-time teleoperation and telemetry application, its focus on how a non-ideal communication link impact on the real-time teleoperation and telemetry communication and factors associated with communication link influences the real-time application scenarios.

5 Investigation of The Communication Link and Real-Time Task Scheduler

5.1 Introduction

The additional communication latency generated by cryptographic constructs has an impact in static and mobile applications, this impact reduces the number of packets transmitted within a given time-frame and the maximum communication distance obtainable by mobile end-points. These findings are presented in Chapter 3 and Chapter 4. Scenario investigated in this chapter focused on the non-ideal nature of the communication link and the real-time task scheduler. In this chapter, the problem analysis undertaken is based on the following questions:

- What is the impact of real-time teleoperation and telemetry on instantaneous packet throughput under non-ideal communication links?
- How does the antenna placement and receiver sensitivity influence the operational range of the real-time teleoperation and telemetry application?
- How does the selection of real-time task schedulers impact on the latency measurements recorded?

The structure of this chapter is as follows. The impact of non-ideal communication links on specified aspects of the real-time teleoperation and telemetry is investigated in section 5.2. Analysis of the impact of additional inter-message arrival latency on UAV teleoperations with secure communications is presented in section 5.3. A discussion of the findings is then presented in section 5.4. A chapter summary concludes in section 5.5.

5.2 Analysis of Non-Ideal Communication Characteristics on Real-Time Communications

This section of the problem analysis investigates the non-ideal communication characteristic sand their impact on real-time teleoperation and telemetry communications. Investigations conducted in this thesis has focused on the real-time teleoperation and telemetry applications scenarios that considered the impact of latency and cryptographic services utilised from the perspective idea communications. This view-point in realistic as real communication links are unpredictable by nature.

Due to varying delays the time from when a packet is generated at the source until it is received at the receiver can fluctuate from packet to packet; this phenomena is called jitter. Presentation of the analysis undertaken is segmented into two sections with the analysis of

the non-ideal communication channel characteristics on the instantaneous packet throughput and the impact of the maximum communication range for real-time teleoperation and telemetry communications at various antenna placements and sensitivities.

5.2.1 The Impact of Non-Ideal Channel Characteristics on Instantaneous Packet Throughput

Real-time applications may required the use of single-hop or multiple-hop communication links to propagate real-time teleoperation and telemetry data between the transmitter and receiver, the utilisation of these links in a real-world situation exposes the communication signal to a variety of unpredictable factors (i.e. crosstalk, interference) that could corrupt the packet as it propagates between communicating nodes. Figure 5.1 presents an illustrative concept of the the non-ideal communication link scenario investigated in this analysis.

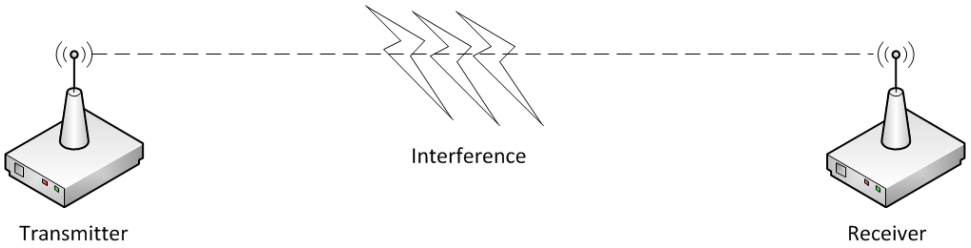


Figure 5.1: Illustrative concept of the non-ideal communication link scenario.

The null hypothesis proposed in this analysis is that the non-ideal channel characteristics will not reduce the number of packets received by the receiver over the same sample time analysed in comparison to the number of packets recorded under ideal channel conditions. The alternative hypothesis is that the non-ideal channel characteristics will reduce the number of packets received by the receiver over the same sample time analysed in comparison to the number of packets recorded under ideal channel conditions.

The test investigated the number of successful packet deliveries from the transmitter to the receiver with various probabilities of packet loss during propagation across the communication link. Measurement based analysis undertaken using Proteus ISIS 8 tallied the number of successful instantaneous packets received over a specified period of time; each node incremented a counter each time a message had been successfully decrypted and authenticated. The instantaneous packet throughput recorded was taken from a sixty second observation based on simulation time.

The communication link between the transmitter and receiver was simulated with the Serial Peripheral Interface (SPI) to mimic an ideal wireless communication channel with

synchronous data transmission rate. An intermediate microcontroller was placed between the transmitter and receiver to intercept the message and mimic the impact of a non-ideal communication link to the message. The interference level was analysed as the non-ideal channel characteristic as it is known that interference contributes towards packet corruption and error as it propagates over the communication medium. The non-ideal channel characteristics of the communication link were derived from a binomial distribution with values of thirty-four per cent, fourteen per cent and two per cent. A random number generator was selected to generate a random number within a byte value of 0 to 255; if the number was within or under the percentage value set for the non-ideal communication link, the packet was modified to reflect packet corruption; otherwise the message was unaffected.

The second variable analysed was jitter; similar to the packet corruption test, the same probability percentages are chosen; however, this test varies the inter-arrival time of the message by delaying the packet at the intermediate hop before propagating to the receiver device. The initial delay sampled in this test was seven milliseconds for thirty-four per cent probability, nine milliseconds for fourteen per cent probability and ten milliseconds for two per cent probability. All timings are taken from the simulator used. It is assumed for this test that the non-ideal channel characteristics on the communication link is a random event and the packet impacted by error is based on probability, therefore, the average of a hundred tests was taken.

The test platform, test plan and details of the test methodology are specified in Appendix I. Table 5.1 and Table 5.2 tabulates the results of the total number of successful packets received from a total of eight hundred packets transmitted for various non-ideal channel characteristics.

Table 5.1: The average impact of a non-ideal communication link on packet throughput for a thirty-six byte packet size for a total of eight-hundred packets transmitted with TinyAEAD-AES-128 at three rounds. (4 MHz processing frequency (2 MIPS), 250 Kbps transmission rate)

Independent Variable	**Dependent Variable**
Probability of packet error	**Packets received (out of 800 packets)**
34%	272
14%	688
2%	784

Table 5.2: The average impact of jitter on packet throughput for a thirty-six byte packet size for a total of eight-hundred packets transmitted with TinyAEAD-AES-128 at three rounds. (4 MHz processing frequency (2 MIPS), 250 Kbps transmission rate)

Independent Variable	**Dependent Variable**
Probability of packet delay	**Packets received (out of 800 packets)**
34% (7 ms jitter)	280
14% (9 ms jitter)	698
2% (10 ms jitter)	784

Results presented in Table 5.1 and 5.2 shows that packet loss and jitter influences the instantaneous packet throughput recorded with the highest number of packet loss recorded for the communication link of thirty-four per cent, whilst the communication link with two per cent interference had the least number of packets dropped and the difference in the packets lost are the percentage difference of the total number of messages transmitted to the receiver device (e.g. fifty per cent interference on the link is equivalent to fifty per cent drop in instantaneous packet throughput).

To analyse how non-ideal communications links would impact real-time teleoperation and telemetry, the results from the aforementioned test are applied to the static to mobile real-time teleoperation and telemetry application as presented in 5.4. As a mobile end-point undertakes commands whilst travelling at a fixed speed; if a packet is not received or is corrupt during transit; the mobile end-point would continue to travel until the next telecommand is received. It is assumed that the mobile end-point is travelling at a fixed speed of fifty-nine miles per hour (twenty-six metres per second). Figure 5.2 illustrates the additional distance travelled by the mobile end-point using TinyAEAD-AES-128 over various interference levels on the communication link

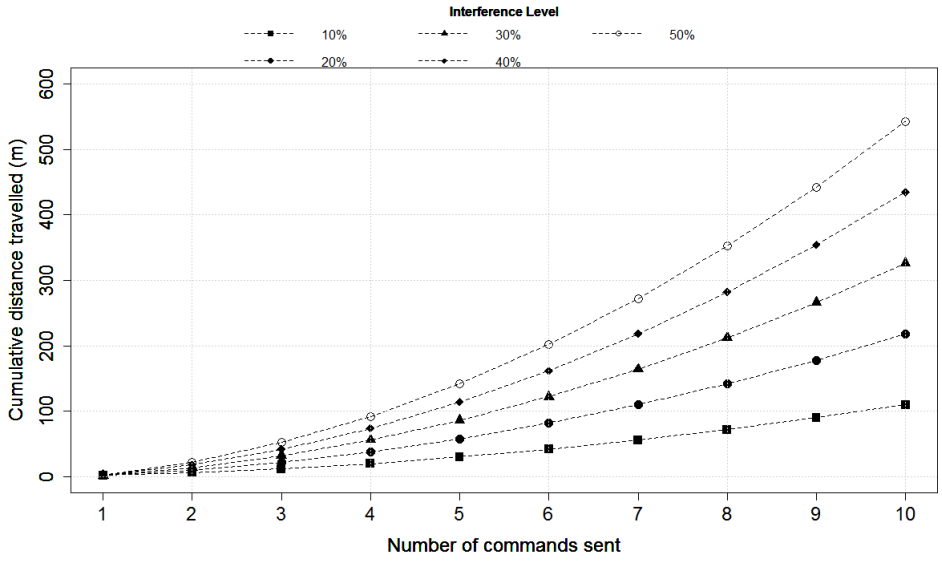


Figure 5.2: Additional distance travelled by static to mobile real-time platform with TinyAEAD-AES-128 on average non-ideal channel characteristics at a speed of twenty-six metres per second.

The data presented in Figure 5.2 shows that the highest probability of packet corruption has the biggest impact on the distance travelled by the mobile end-point and the smallest probability of packet error on the communication channel has the least impact on the additional distance travelled by the mobile end-point.

Analysis of the graph presented in Figure 5.2 shows that there is an exponential growth relationship identified between the number of additional commands transmitted and the cumulative distance travelled by the mobile end-point; this is because the time required to send an additional number of commands impacts on the processing and communication latency incurred. In addition, the probability of a successful packet delivery further adds to the problem as a higher probability of packer error results in an increased number of attempts required to successfully delivery the message to the end-point.

To draw comparison of the influence of CCM-AES-128 and TinyAEAD-AES-128 on the mobile end-point. Figure 5.3 illustrates the additional distance travelled by mobile end-point utilising no security, TinyAEAD-AES-128 and CCM-AES-128 on a non-ideal communication link with a fifty per cent probability of packet error.

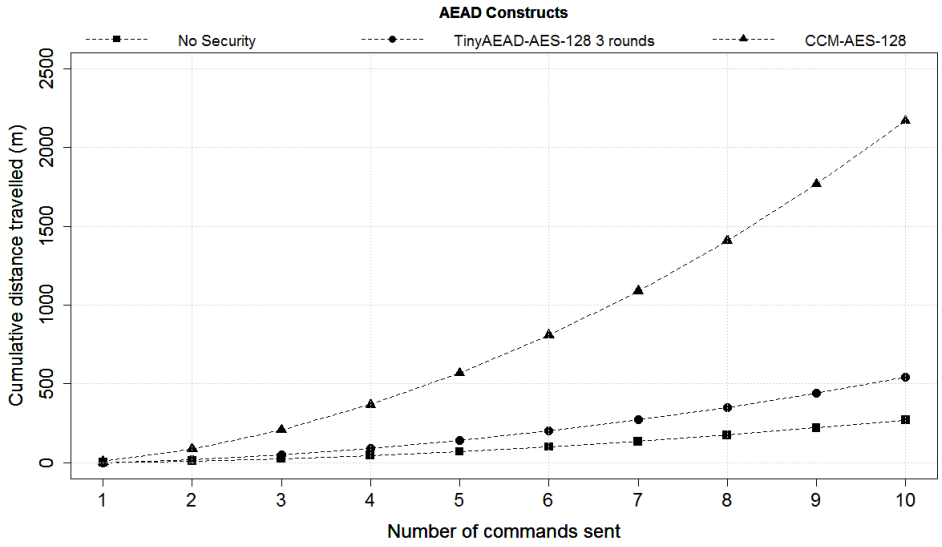


Figure 5.3: Comparison of the additional distance travelled with two AEAD security constructs for a fifty per cent interference level on the communication link at a speed of twenty-six metres per second.

Results presented in Figure 5.3 shows the additional distance travelled by the mobile end-point accumulates for each additional message transmitted; furthermore, the security measure selected contributes to the distance travelled with CCM-AES-128 having an increase on the distance travelled in comparison to TinyAEAD-AES-128 at three rounds. The additional distance travelled by mobile platforms with TinyAEAD-AES-128 was twice as far as no security, whilst the distance travelled using CCM-AES-128 was eight times further in comparison to no security; this shows that the security service selected impacts on the additional distance travelled as a result of an increase in the communication latency recorded (i.e retransmission of packets with security services).

5.2.2 Section Summary

Analysis of the findings presented from the investigation undertaken demonstrates that the alternative hypothesis is true. The non-ideal channel characteristics does reduce the number of packets received by the receiver over the same sample time analysed in comparison to the number of packets recorded under ideal channel conditions. This is because the real-time teleoperation and telemetry packet is unintentionally corrupted as it propagates to the receiver node and is consequently disregarded as the packet would not be decrypted correctly and would fail the integrity check; this is under the assumption that no error correction is undertaken at the receiver nodes.

The impact of this findings in the context of this thesis is the reduction in the number of instantaneous packets recorded in a given period of time: This impacts the static and mobile real-time applications by either reducing the quantity of messages received or the

additional distance travelled before a real-time teleoperation and telemetry message is successfully received.

Mitigation of the additional distance travelled is achievable by reducing the speed of the mobile end-point; however, this would impact the real-time application as the maximum distance attainable for a mobile end-point with constrained energy supply would be significantly reduced and consequently influence the operational range of the mobile device; this raises the question of the impact of a secure communication link on the operational performance of the real-time application.

Analysis conducted in this section examined the non-ideal element of the communication link and not additional variables (i.e transmission power or received sensitivity) that contribute towards the communication channel characteristics; therefore, the next section investigates how variables associated with the communication link interplay with the real-time application scenarios.

5.2.3 Real-World Validation of The Maximum Communication Range for Real-Time Teleoperation and Telemetry Communications at Various Antenna Placements and Sensitivities

Investigation conducted in this section of this problem analysis is to understand the variable of the individual communication components and the maximum communication range attainable. Examination of the real-time problem scenarios specified in Chapter 3 and Chapter 4 shows that the communication range is an important aspect to consider as the static dust explosion scenario may require a specified range to operate the application for safety purpose (i.e. human casualties); whilst mobile real-time application where an end-point is continuously moving may require a specific communication range in order to complete its mission.

Communication range interlinks with the real-time application scenarios as this determines the distance between the base-station and the end-point; however, existing literature presented in Chapter 2 focused on elements of the communication (i.e single and multiple hop propagation of data) but has not taken into consideration how the antenna placement interlinks with the maximum communication range attainable; therefore, this analysis investigates the relationship between the two variables. The problem scenarios presented in this section continues from the analysis conducted in Chapter 4 with an examination of the static to mobile and mobile to mobile scenarios using an Unmanned Ground Vehicle (UGV). Figure 5.4 illustrates the scenario investigated in this chapter.

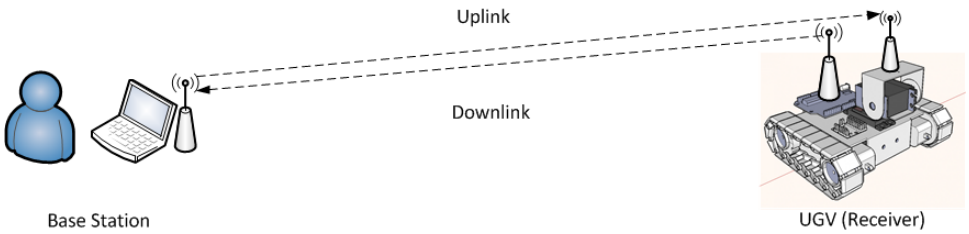


Figure 5.4: Illustrative concept of a single hop line of sight static to mobile communication link with an unmanned ground vehicle (UGV).

The scenario presented in Figure 5.4 is one where the UGV manually controlled in real-time via a point to point communication link by a human operator at base-station. In this scenario, it is assumed that the aerial of the UGV has a maximum vertical height of two metres; this is because in this thesis vertical antenna heights above two metres are considered unsuitable for tactical missions.

The null hypothesis presented in this investigation is that the higher the vertical placement of the antenna; the further the communication range between the transmitter and receiver would be. The alternative hypothesis is that higher the vertical placement of the antenna; the closer the communication range between the transmitter and receiver would be.

The test was conducted using two Raspberry Pi single board computers. One was configured as the transmitter and the other as the receiver device. The TP-Link TL-WN722N 3 dBi omni-directional high gain antenna transceiver dongles were selected for line of sight communication between the Pis; the IEEE standard 802.11g was chosen as the communication protocol. The frequency selected for the communication channel was 2.4 GHz to replicate conventional short range wireless communication systems.

One Raspberry Pi is configured as a wireless access point and the other Raspberry Pi is a client that associated with the wireless access point in order to transfer messages over the same communication link. Vertical placement of the antenna was set at ten centimetres, one metre, and two metres above ground level. One hundred ping commands were sent from the transmitter to the receiver; the average of five tests was taken for the results. The packet size selected for the ping test was fifty-six bytes. The percentage of successfully ping command between the transmitter and receiver was recorded.

The test was conducted as follows: The antenna was placed at the specified height and a transmission power of 0 dBm was used. At intervals of ten metres, the received signal strength and number of packets received ping packets was recorded using appropriate software. The real-world environment test platform is described in Appendix J. Figure 5.5 illustrates the results of the wireless broadcast range at different vertical height placement

of the antenna at a transmission power of 0 dBm.

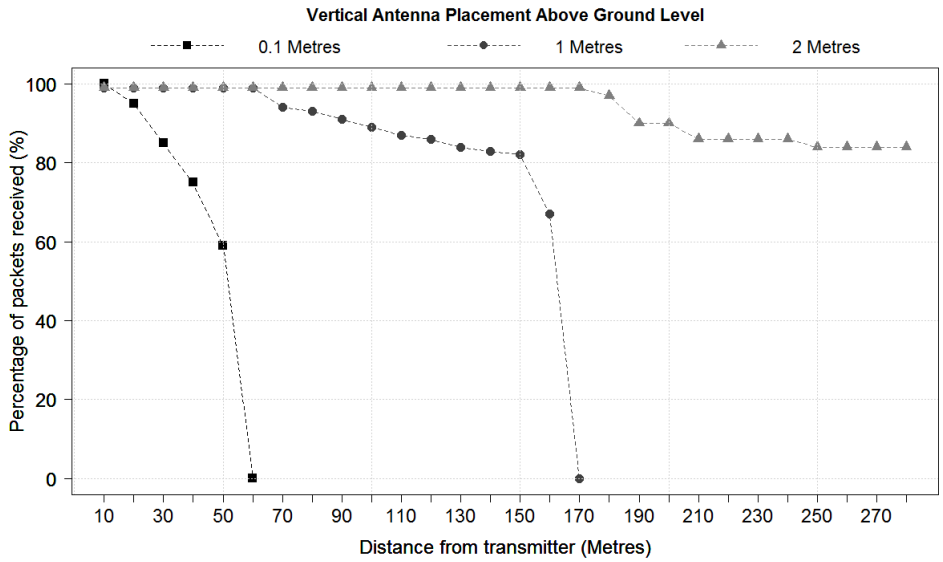


Figure 5.5: Percentage of packets received at ten metre intervals for various antenna height placements at a 2.4 GHz frequency and 0 dBm transmission power.

Data presented in Figure 5.5 shows that the placement of the antenna has an impact on the maximum range of the communication link with antenna placement at the lowest level above ground having the smallest broadcast range; whilst antenna placement at the highest placement had the furthest broadcast range. The statistical comparison of the results obtained for the three antenna height shows that the two metre vertical antenna placement can receive a signal up to thirty-nine per cent further than the one metre vertical antenna placement and seventy-eight per cent for a ten centimetre vertical antenna placement.

The data obtained for the signal strength test shows that the signal strength decreases the further the receiver is away from the transmitter; this is because the placement (in height) of the antenna i interferes with the propagation of the signal, the closer it is placed to ground level, the sooner the signal is absorbed and refracted; furthermore, the application of the inverse square law reduced the intensity of the signal level as the distance increased, causing the signal level to degrade at an earlier distance whilst placements at a higher height had a reduced probability of the signal being refracted or absorbed during propagation; this supports the null hypothesis that the higher the vertical placement of the antenna; the further the communication range between the transmitter and receiver would be.

Additional factors that contribute towards the findings is the influence of the weather conditions as the results presented were taken under rain conditions; this impacts the signal level recorded as the water molecules absorb frequencies of 2.4 GHz band; therefore,

the distance the signal could travel under these conditions is reduced; furthermore, the analysis conducted in this section primarily focused on the height placement of the communicating devices; therefore, an extension of the analysis is conducted to ascertain how the antenna gain contributes towards the multi-faceted problem investigated.

A test was conducted to determine the signal strength obtained using the zero gain Wi-Pi omni-directional antennas and the 3 dBi high-gain omni-directional antenna (TP-Link TL-WN722N) for a simplex communication link. The null hypothesis presented in this test is that the omni-directional antenna with gain will not have an increased communication range than the omni-directional antenna with no gain. The alternative hypothesis is that the omni-directional antenna with gain will have an increased communication range than the omni-directional antenna with no gain.

The height of the antenna placements were sets to one metre above the ground with a transmission power of 0 dBm used. At intervals of ten metres, the received signal strength was was recorded using an appropriate software package. The test plan, assumptions and methodology followed in this analysis are taken from the aforementioned test in this section. Figure 5.6 presents the received signal levels recorded with the two antennas selected.

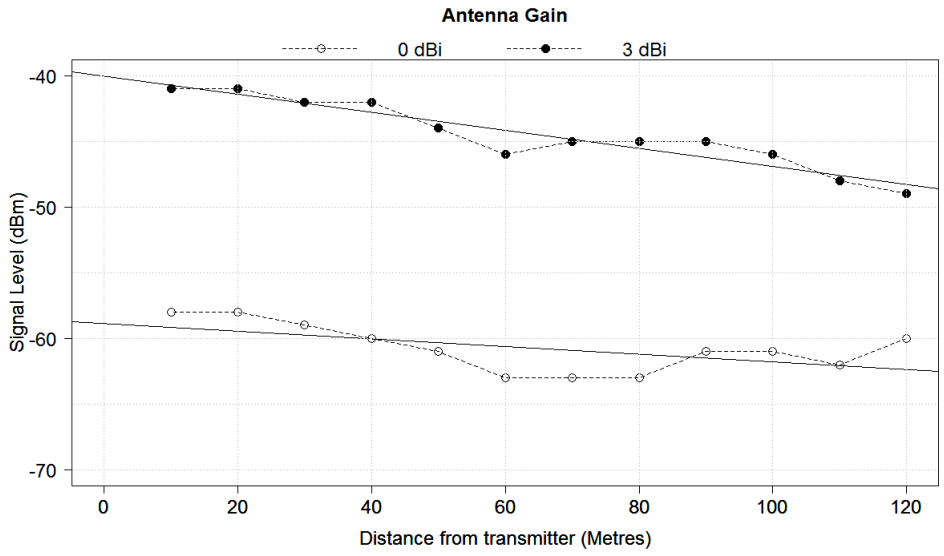


Figure 5.6: Recorded signal strength for streamed data over a simplex communication with a zero gain omni-directional antenna and three dBi omni-directional antenna (transmitter and receiver 1 metre above ground level).

The results presented in Figure 5.6 shows that the 3 dBi gain omni-directional antenna has higher signal strength in comparison to the 0 dBi gain omni-directional antenna; however, the linear regression trend line for both antenna types shows that there is a relationship between the distance between the transmitter and receiver device and the signal level

recorded with a negative correlation recorded; this demonstrates that both 0 dBi and 3 dBi antennas signal level reduces as the distance between communicating nodes is increased. The gain of the antenna contributes towards the received signal and therefore supports the alternative hypothesis that the omni-directional antenna with gain will have an increased communication range than the omni-directional antenna with no gain.

5.2.4 Section Summary

Analysis of the findings collated from the real-world communication range tests undertaken demonstrates that the number of successful packets received is influenced by the vertical height placement of the transmitter and receiver node. Initial analysis of the communication link categorised the state of the communication link as ideal and non ideal; however, further examination of the results shows that there are three categories for the number of successful packet deliveries at a particular range. Figure 5.7 illustrates the classification of the communication link based on the number of successful packet deliveries.

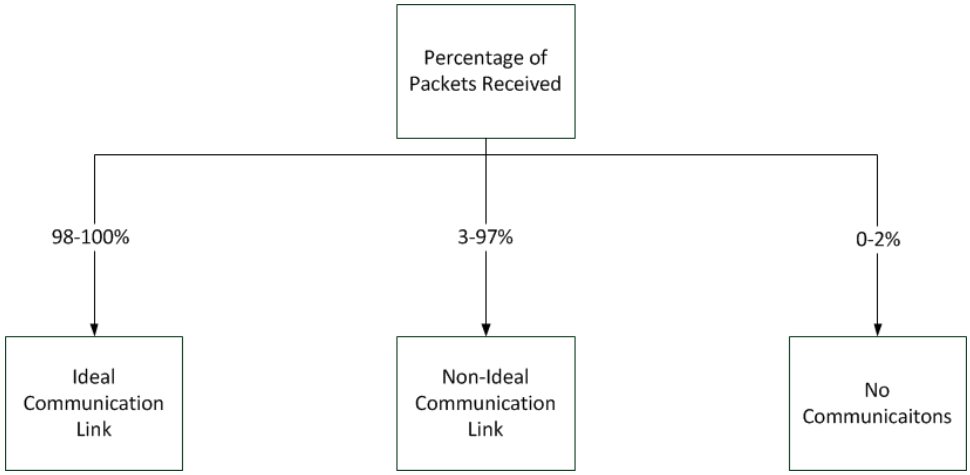


Figure 5.7: Classification of the communication link in relation to the number of successful packet deliveries in reference to Figure 5.5

Findings obtained from the analysis of the communication link demonstrates that the channel has a significant impact on the real-time application and the communication range achievable. Analysis of the communication range was undertaken in this analysis; however, the findings obtained from this analysis does not identify the impact of the cryptographic service on the real-time nature of the applications examined; therefore, the next section of the problem analysis investigated the impact of additional inter-message arrival latency on the real-time application.

5.3 Analysis of Real-Time Task Schedulers on Teleoperation and Telemetry Applications

This section of the problem analysis introduces the impact of the additional latency generated by the cryptographic services on the behaviour of real-time teleoperation and telemetry system. The purpose of this investigation is to determine what the influence of the additional inter-message arrival latency caused by the cryptographic service has on the problem scenarios in relation to periodic and aperiodic tasks and what significance this has on the behaviour of the real-time teleoperation and telemetry.

Analysis undertaken up to this point assumed that the embedded microcontroller devices processed the real-time application tasks in a sequential manner using a first in first out (FIFO) scheduler system as most microcontroller programmes are coded using a continuous "while true loop" to complete repetitive tasks in a sequential order. Reflection of the real-time applications investigated in this thesis may require the use of alternative real-time schedulers in order to prioritise certain tasks within the system; literature presented (Tan & Anh 2009) indicates that the majority of real-time task schedulers used in small microcontrollers are priority based schedulers, where certain tasks are prioritised in the real-time scheduler to be computed over other tasks; therefore, in this instance of the analysis, a comparison of the FIFO and priority based real-time task schedulers is undertaken.

5.3.1 The Impact of Additional Inter-Message Arrival Latency on the UAV Teleoperation with Secure Communications

Analysis of the task schedulers used in real-time teleoperation and telemetry applications is investigated in this section of the problem analysis. Examination of the problem scenarios presented in Chapter 3 and Chapter 4 demonstrates that each scenario has a different set of tasks to compute (i.e. from initialising of dust suppressant for a static actuator, to manual control of an UAV). Real-time task schedulers identified in Chapter 2 are selected dependent on the real-time application; however, as identified in Chapter 3 and Chapter 4, the communication latency generated could be influenced by the ordering of the tasks. Literature presented in Chapter 2 has identified that the task analysis for real-time teleoperation and telemetry applications with security services included is limited, especially for mobile end-points; therefore; this analysis investigated how variants of task schedulers can impact the operational flight characteristics of a mobile UAV application.

The analysis conducted uses mathematical modelling to derive the impact of the AEAD constructs on the operation of the real-time teleoperation and telemetry applications. The model selected derived from queueing theory with an M/M/1 single queue model selec-

ted in this instance of the analysis to model the behaviour of the real-time application (Laplante 2004). Analysis of the mean response time was undertaken using the M/M/1 queue and the inter-arrival rate was acquired from the number of instantaneous packets transmitted per second as specified in Chapter 3, section 3.4.5, Figure 3.15. Calculation of the mean response time is presented in Formula 12.

$$T = \frac{1/\mu}{1-(\lambda/\mu)} \tag{12}$$

Formula 12: Mean response time calculation for a real-time system (Laplante 2004).

Calculation of the mean response time (t) is achieved as follows, the mean process time for the interrupt $(1/\mu)$ is divided by the sub-total of the inter-arrival time by the mean process interrupt time $1-(\lambda/\mu)$. The two sub-totals are divided as presented in Formula 12 to derive the mean response time.

The null hypothesis presented for this investigation is that the cryptographic services with the highest additional latency recorded will not have the lowest inter-message arrival rate recorded. The alternative hypothesis is that the cryptographic services with the highest additional latency recorded will have the lowest inter-message arrival rate recorded. Table 5.3 tabulates the comparison of the mean response time of the real-time application with and without AEAD security services.

Table 5.3: Comparison of mean response times with and without AEAD security services through a M/M/1 queue (8 MHz processing frequency (2 MIPS)).

Independent Variables	**Dependent Variables**	
Security Service	**Inter-message arrival rate (Packets per second)**	**Average times between arrivals (Seconds)**
No Security	1.7	0.58
TinyAEAD-AES-128 3 rounds	1.4	0.71
CCM-AES-128	1.1	0.90

Results presented in Table 5.3 demonstrate that the mean response time of the real-time operation is influenced by the selection of the security service as the average wait times for each task that passed through the AEAD cryptographic services is increased in comparison to no security; this is because of the additional latency incurred from the cryptographic process and results in a longer time duration on the real-time teleoperation or

telemetry task for the same given processing frequency and computational device selected.

Further analysis of the results presented in Table 5.3 demonstrates that there is a negative relationship between the inter-message arrival rate and the average time between arrivals; this is because the additional processing delay of the selected security services influences the rate that the number of packets can be transmitted as identified in analysis conducted in Chapter 3 and Chapter 4 and the consequence of the additional latency incurred is the increase in the average arrival times of the messages; therefore, this further consolidates the findings presented in the aforementioned analysis undertaken throughout this thesis.

Analysis of how the average times between inter-message arrivals influences the problem scenarios is conducted with the total duration of all the tasks in the system to be computed with the inclusion of the longer processing times for the encryption and decryption of the AEAD security services. This is based on the assumption that each task is conducted periodicity and in a sequential manner with a FIFO task scheduler; therefore, the next part of the analysis compares the impact of periodic tasks that use a FIFO scheduler and aperiodic tasks that use a priority based scheduler to process important tasks on the sensitivity of the flight behaviour for a mobile real-time teleoperation and telemetry system.

The impact of the additional latency incurred by the AEAD cryptographic services on the operation of the real-time teleoperation and telemetry systems for a system with aperiodic tasks is examined using the static to mobile scenario as the system could have task priorities in order to process teleoperation command transmitted by the human operator. Analysis of the impact of the additional latency on a mobile real-time teleoperation and telemetry system is achieved by applying the mean response times of the real-time teleoperation and telemetry application with the inclusion of AEAD construct for a packet size of thirty-six bytes at a processing frequency of 8 MHz.

It is assumed for this analysis that the FIFO queue is selected to represent a periodic task system and a priority queue is selected to represent an aperiodic task system that prioritises incoming teleoperation command packet from the base-station; it is also assumed that the periodic FIFO queue requires all aforementioned task to be computed before the command is acted upon with the worst case execution time analysis in section 4.3 used as the total delay before computing the task; whilst the priority queue computes the priority task immediately.

Table 5.4 tabulates the worst case execution time analysis for the static to mobile and mobile to static real-time teleoperation and telemetry system with a FIFO and priority

based queueing system.

Table 5.4: Worst case execution times of periodic and aperiodic queueing systems to process a single teleoperation command at a processing frequency of 8 MHz (2 MIPS).

Independent Variables	**Dependent Variables**	
Security Service	**Periodic task system latency (ms)**	**Aperiodic task system latency (ms)**
No Security	120.4	0.4
TinyAEAD-AES-128 3 rounds	141.0	21.0
CCM-AES-128	194.0	74.0

Results presented in Table 5.4 shows that the task scheduler selected for the real-time teleoperation and telemetry system has a noticeable impact on the additional latency incurred by the system, with differences between the periodic and aperiodic methods up to three hundred times greater for with no security service, up to seven times greater with the TinyAEAD-AES-128 security construct and up to two and a half times increase for CCM-AES-128; this is because a FIFO scheduler has to process the command as the real-time application has to process the current tasks in its queue before it can decrypt the message and act upon the command whilst the priority based queueing system latency would only require the time to process the decryption function as the task is prioritised and processed by the system before the periodic tasks in the system. To showcase the impact the type of queueing has on the operational control of the UAV during flight; Figure 5.8 illustrates the additional distance travelled by the UAV travelling at twenty metres per second with a number of teleoperation commands transmitted using TinyAEAD-AES-128 at three rounds.

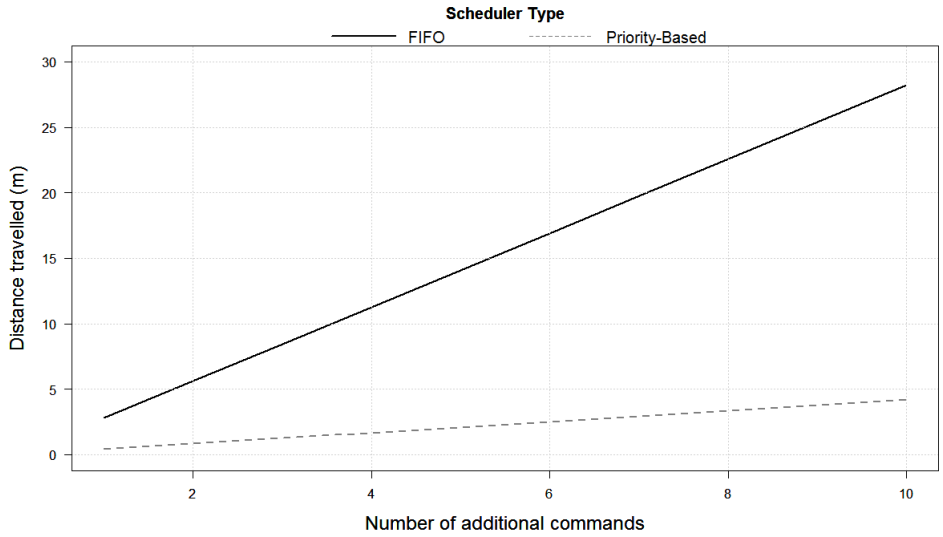


Figure 5.8: Additional distance travelled by a mobile UAV travelling 20 m/s with multiple teleoperation commands transmitted with first in first out and priority queues using TinyAEAD-AES-128 at three rounds.

Data presented in Figure 5.8 demonstrates that the additional latency incurred per teleoperation command processed by the UAV has an impact on the operational control of the mobile end-point; the latency contributes to the additional distance travelled by the UAV before it acts upon the commands sent; this results in the mobile end-point travelling further before acting upon the teleoperation command with the FIFO scheduler whilst the priority based would have a reduced impact on the additional distance travelled.

5.3.2 Section Summary

Findings obtained from the investigation of the inter-arrival rates of messages with the inclusion of AEAD security constructs applied shows that the selection of the AEAD construct has an impact on the average arrival rate of the messages; this is because the rate at which the message arrives is dependent on the rate that the cryptographic service can be processed by the device before the next message is processed. The AEAD constructs selected influences the number of real-time teleoperation and telemetry commands that are computed in a given period of time and supports the findings that the cryptographic services with the highest additional latency recorded will have the lowest inter-message arrival rate recorded; however, the real-time scheduler selected further contributes towards the problem as this varies the time required for the cryptographic service to be computed.

The periodic and aperiodic tasks in the application of real-time system schedulers contribute towards the problem analysed as the time to complete the task varies dependent on the scheduler selected; in the instance analysed, the treatment of all tasks within the system using a periodic process would result in the worst case execution time of the real-

time application ; this is because all previous tasks in the FIFO scheduler would have to be processed in sequential order before it can compute the received message. Instances where a priority driven scheduler system is implemented for specific tasks, the latency to process the cryptographic service on the real-time teleoperation or telemetry message would be limited to the time of the cryptographic task at a specified processing frequency as the task is prioritised over periodic tasks in the system; therefore, this partially supports the alternative hypothesis as the cryptographic service takes a finite amount to time to complete but the order that it is processed is dependent on the task scheduler selected.

Alternative real-time scheduler approaches identified in the preliminary review in Chapter 2, section 2.12.1 could be implemented with the application of a priority driven scheduler that would give precedence to the incoming real-time teleoperation and telemetry packets to be a priority for encryption or decryption to ensure that the aperiodic tasks are computed as close to instantaneous as possible; however, alternative schedulers such as rate-monotonic scheduling would not be best suited in the context of real-time teleoperation and telemetry problem scenarios as the cryptographic process of encryption and decryption can not be interrupted to accommodate for incoming aperiodic tasks in the system: This could corrupt the original message that is processed by the cryptographic service as the new message received would overwrite the buffer that was occupied by the previous teleoperation or telemetry packet that was interrupted during the cryptographic process; therefore, the computation of a periodic or aperiodic task would have to wait until the aforementioned process is complete before it can process the specific task in the system.

5.4 Discussion

Analysis of the real-time teleoperation and telemetry communication propagated over a non-ideal communication link demonstrates that the transmitted packets could be susceptible to unintentional packet loss as a result of the non-ideal channel characteristics; this would impact the problem scenarios identified as the real-time teleoperation and telemetry message would not be received by the actuator to act upon the teleoperation or telemetry messages and therefore not complete the initial tasks transmitted across the communication link; this is problematic in mobile situations where the mobile end-point could travel outside the communication range and therefore unable to respond to any new commands as demonstrated in section 5.2.1.

The behaviour of the non-ideal channel characteristics in the context of real-time teleoperation and telemetry demonstrates that the higher the probability of error or corruption to the transmitted packet through channel interference and jitter as presented in section

5.2.1, the greater the reduction in the number of successfully received packets. This behaviour impacts the real-time teleoperation and telemetry from two different prospectives; the teleoperation and would require an increased number of packet retransmissions to overcome the probability of packet loss and results in an additional distance travelled before responding to the next telecommand.

Analysis undertaken in section 5.2.1 identified that the problem of propagating real-time teleoperation and telemetry packets over a non-ideal communication link is the probability of packet corruption; this is problematic in the context of real-time communications as the retransmission of packets adds additional processing and communication latency to the real-time application. The consequence of packet retransmission on the real-time application is that the real-time constraints specified for the application are not met; this results in the safety, reliability and availability of the real-time application becoming affected as a result of unreliable communications (i.e. unresponsive application).

The real-time telemetry is impacted by the behavioural characteristics of a non-ideal communication link as the delay in the acquisition of the data feedback to the human operator dictates the response chosen by the human operator and the appropriate action to complete based on the information presented in section 5.2.3; this has a direct influence on the safety, reliability and availability of systems as the manual operation of the actuator is controlled by the human and could be at risk if the telemetry data is not acquired in the real-time constants for both static to static and static to mobile scenarios and would require reconsideration of the operational flight parameters of the mobile end-point.

Operational placement of the antenna, transmission power and antenna gain presented in 5.2.3 further reinforces the trade-offs required; the transmission power selected affects the operational range for communications; also an increased transmission power would have an increased energy consumption. Application of the knowledge in the context of real-time teleoperation and telemetry demonstrates that the transmission power of the wireless communication module directly influences the maximum range available for the wireless broadcast medium to propagate to a static or mobile end-point to travel; in addition, the height placement and sensitivity of the antenna contributes towards the maximum distance the wireless broadcast range with higher placement and receiver sensitivities increasing the maximum range attainable.

Application of the findings to the research undertaken in this thesis is that the non-ideal channel characteristics can be segmented into three areas, ideal communications where there is no packet loss between the transmitter and receiver; non-ideal communications where packet loss of a propagating message occurs at a probability between five to ninety-

five percent and no communications where all messages transmitted are corrupted during propagation. The impact of this findings on the research area investigated in this thesis is that the number of real-time teleoperation and telemetry packets received is varied on a probabilistic scale dependent on the configuration of the communication link.

Findings obtained from the real-time task scheduler analysis demonstrated that the cost of the cryptographic operation using variants of task schedulers determines the latency incurred by the real-time application; this is because the task scheduler selected determines order and priority that a process should be conducted. In the context of the research undertaken, the impact of the findings on the real-time teleoperation and telemetry applications investigated is the reduction in the packet rate, this is particularly influential on the real-time telemetry messages as the quantity of messages relayed from the end-point to the base station. The real-time teleoperation is influenced by the delay from the inter-packet arrival latency.

Selection of the cryptographic service has an impact on the inter-message arrival latency for the real-time teleoperation and telemetry application; this is because the time required to process the cryptographic service impacts on the number of messages transmitted in a given period of time; in addition, the selection of the real-time scheduler used by the embedded microcontroller impacts on this finding as the different schedulers process tasks in different order; therefore, the selection of the real-time scheduler is an auxiliary factor to consider but is not the focus of the research undertaken in this thesis as presented in section 5.3: This raises further questions to the impact of the cryptographic services on the real-time applications.

5.5 Chapter Summary

This chapter presented the analysis undertaken of the communication link and the real-time task schedulers used to facilitate real-time teleoperation and telemetry communications. The questions investigated in this problem analysis are: (1) the behaviour of real-time teleoperation and telemetry under non-ideal channel characteristics; (2) how the antenna placement, transmission power and receiver sensitivity influence the operational range of a mobile controlled real-time teleoperation and telemetry device and (3) how the real time task scheduler selected impacts on the latency measurements recorded.

The findings obtained from the investigations conducted reinforce the multi-faceted research problem presented as the characteristics of the communication link and the configuration of the communication components dictates the maximum operational communication range possible. Examination of the real-time scheduler used to process tasks for the

application contributes towards the problem as the scheduler type dictates the worst case execution time to complete the cryptographic task; consequently, influencing the latency measurements recorded.

The cryptographic services and the task scheduler selected contributes to the communication latency incurred as demonstrated with the real-time task scheduler analysis; however, the initial findings form the analysis undertaken indicates that the secure communication link must be integrated with the real-time application and not treated as a segmented component. The next chapter presents the problem analysis of the impact of security services on real-time applications that use real-time teleoperation and telemetry.

6 Investigation of Latency on Real-Time Teleoperation and Telemetry Applications

6.1 Introduction

As discussed in Chapter 5; the non-ideal communication link and the task scheduler selected for the real-time applications have an impact on the communication latency generated as a result of message retransmission or priority of the task ordering in the scheduler. The aforementioned problem analysis conducted did not explicitly investigate the impact of the security services on the operational performance of the stated real-time applications; therefore, in this chapter the investigation of security services and the on the real-time nature of the teleoperation and telemetry applications. In this chapter, the problem analysis undertaken is based on the following questions:

- What is the energy cost of processing and communications on real-time teleoperation and telemetry applications?
- What is the impact of cryptographic services on the energy consumption for real-time teleoperation and telemetry applications?
- How does the implementation method of the cryptographic services impact on real-time teleoperation and telemetry applications?

The structure of this chapter is as follows; analysis of the impact of cryptography on the operational performance of real-time teleoperation and telemetry is examined in section 6.2 with the presentation of the impact on the static end-point; followed by the impact of the additional latency on a scenario with a mobile end-point as presented in section 6.3. A discussion of the findings is then presented in section 6.4. A chapter summary is presented in section 6.5.

6.2 Operational Performance of Cryptography on Real-Time Teleoperation and Telemetry Applications

This section of the problem analysis investigates the impact of cryptography on the real-time teleoperation and telemetry application investigated in this thesis. Items that are examined in this analysis include the energy usage of the communication components as presented in section 6.2.1; followed by the power consumption of the specified cryptographic constructs analysed as presented in section 6.2.3 and the comparison of hardware versus software implementation methods presented in section 6.2.5.

6.2.1 Energy Usage of The Communication Components

The analysis of the cost of processing and the cost of communication on the energy usage was investigated. Analysis conducted in Chapter 3, Chapter 4 and Chapter 5 focused on the impact of the cryptographic service from the perspective of latency and its impact on the case scenarios presented. The findings presented indicated that time is an underlying cause of the problem investigated in this thesis and that this is a t contributing element to a wide range of factors that influence the multi-faced research problem; in this section of the analysis, the focus is on the energy consumption of the components used in real-time teleoperation and telemetry applications.

The test presented examined the power consumption of the components used for wireless communications of real-time teleoperation and telemetry. The null hypothesis presented is that the power consumption for the processing of data is greater than the power consumption for the communication of data. The alternative hypothesis is that the power consumption for the communication of data is greater than the power consumption for the processing of data.

The test platform selected used a real-world PIC18F45K22 microcontroller with a Microchip MRF24WB0MA wireless 802.11g utilising packet sizes of five hundred bytes. Crystal frequencies of 1 MHz, 4 MHz, 8 MHz and 16 MHz were sampled. The crystal frequencies sampled were multiplied by the phase lock loop (PLL) internal to the microcontroller, to multiply the initial crystal frequency selected by four. Current draw of the components was measured in milliamps and converted to power in milliwatts (mW).The test platform, methodology and assumptions are specified in Appendix K. Table 6.1 tabulates the data obtained used for the power consumption of the components.

Table 6.1: Comparison of power consumption for the individual component for real-time wireless communication.

Independent Variable		**Dependent Variables**	
Crystal Frequency (MHz)	**Processing Frequency (MHz)**	**Microcontroller Power Consumption (mW)**	**Communication Power Consumption (mW)**
1	4	0.1	5.4
4	16	0.2	5.4
8	32	0.4	5.7
16	64	0.6	6.0
20	80	0.8	6.1
Mean		0.40	5.78
Standard Deviation		0.27	0.32

Data presented in Table 6.1 shows that the power consumption of the transceiver when communicating has the highest cost in comparison to the processing of the microcontroller for the same number of instruction cycles used; this shows that the cost of the transceiver sending packets over the communication medium has the greatest impact on power consumption in comparison to the transceiver with no communications and the processing undertaken by the microcontroller only.

Results of the statistical analysis shows that on average the microcontroller has a lower impact on the power consumed in comparison to the cost of communications; this shows that on average the power consumed by the communications is greater than the cost of processing. Further statistical analysis of the results presented in Table 6.1 was undertaken to compare the difference of the cost of processing against the cost of communication; statistical method selected for this analysis was the linear regression and the correlation to determine the relationship between the selection of the crystal frequency and the power consumed by the individual component. Figure 6.1 illustrates the linear regression of the cost of processing against the cost of communication.

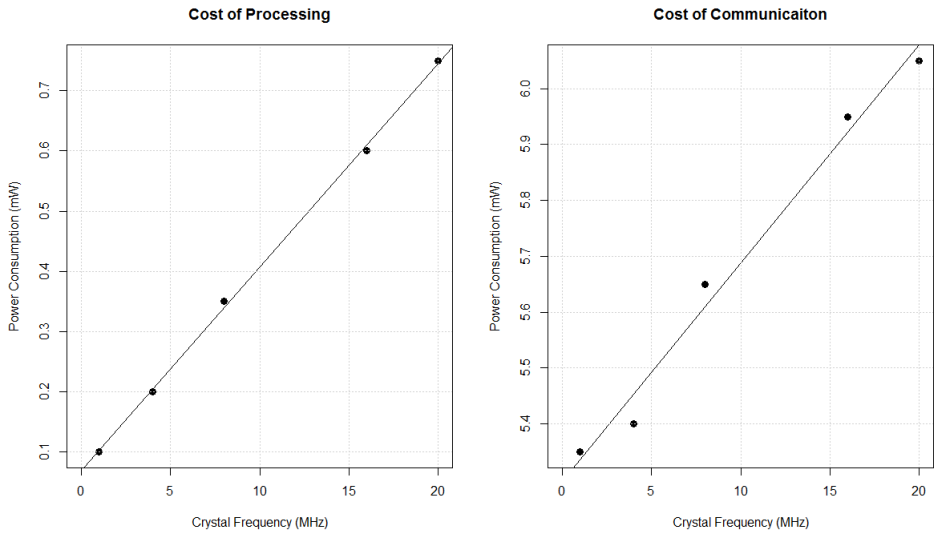


Figure 6.1: Linear regression analysis of the cost of processing (left) and cost of communication (right).

Analysis of the results presented shows a relationship between the power consumption in relation to the crystal frequency selected with a positive linear relationship identified between the crystal frequency and the power consumed and the crystal frequency to cost of communications; this shows a positive linear relationship between the variables analysed.

6.2.2 Section Summary

Findings presented from the analysis undertaken demonstrates that the cost of processing and the cost of communications impact on the energy consumption of the application are correlated; however, further investigation shows that the cost of communications has a higher power consumption (at least fourteen times greater) on average ; this reinforce the alternative hypothesis that the power consumption for the communication of data is greater than the power consumption for the processing of data.

Application of the findings to the context investigated in this thesis shows that the energy cost to communicate real-time teleoperation and telemetry packets is a significant factor that influences the operational performance characteristics of the real-time application, this is prominent for real-time telemetry links that continuously stream data from the end-point to the base station; this is because the quantity of real-time data that is communicated (i.e size of the packets) and the frequency that the data is transmitted and received (i.e size of the packet) will influence how many packets are required to be processed and transmitted across the communication link.

Examination of the cost of communicating real-time teleoperation and telemetry data relates to the problem of the non-ideal communication channel and the security service selected as the reliability of packet delivery is influenced by the non-ideal channel characteristics of the link that may cause packet error as it propagates over the communication link. This findings further contributes to the problem identified as the cost of packet retransmission would impact on the real-time application with an increase in the energy consumption.

The investigation of the individual components required to facilitate secure communications has identified that the cost of communication is greater than the cost of processing. Observation of the analysis conducted primary focused on the processing and communications; however, consideration for the cryptographic services investigated in this problem analysis was not undertaken; therefore, the question raised from this analysis is how the AEAD cryptographic constructs impact on the power consumption of a real-time application device.

6.2.3 Power Consumption of Specified Cryptographic Constructs

The analysis of the configuration of the cryptographic constructs on the power consumption of the system was examined. Observation of the power consumption of the processing device and the communication of data between the transmitter and receiver shows the importance of reducing the energy consumption of the device in situation where energy

conservation is of importance; this includes remote static or mobile end-point that are used in real-time teleoperation and telemetry applications. In this section of the thesis, the examination of the relationship between AEAD constructs power consumption and the processing frequency is investigated.

The null hypothesis presented in this investigation is that AEAD constructs that have the lowest processing latency will also have the lowest impact on the power consumption. The alternative hypothesis is that the AEAD constructs that have the highest processing latency will have the highest impact on the power consumption.

The investigation conducted used a test board designed by the author of this thesis, the specification and the schematic are in Appendix K. The test measured the current drawn by the microcontroller to process the AEAD constructs. The AEAD security constructs selected are CCM-AES-128 and TinyAEAD-AES-128 with the AES-128 selected as the block cipher used by the AEAD constructs specified.

The crystal frequencies selected for this test were 4 MHz, 8 MHz,16 MHz and 20 MHz to represent low, medium and high speed processing frequencies. Packet size of thirty-six bytes was selected. A voltage input of five volts was selected to power the microcontroller with an external power supply. The average measurement of the current draw over ten tests is presented. All measurements obtained in this test were for a single microcontroller with sequential processing. Figure 6.2 presents the result of the power consumed by AEAD constructs with a thirty-six byte packet size selected.

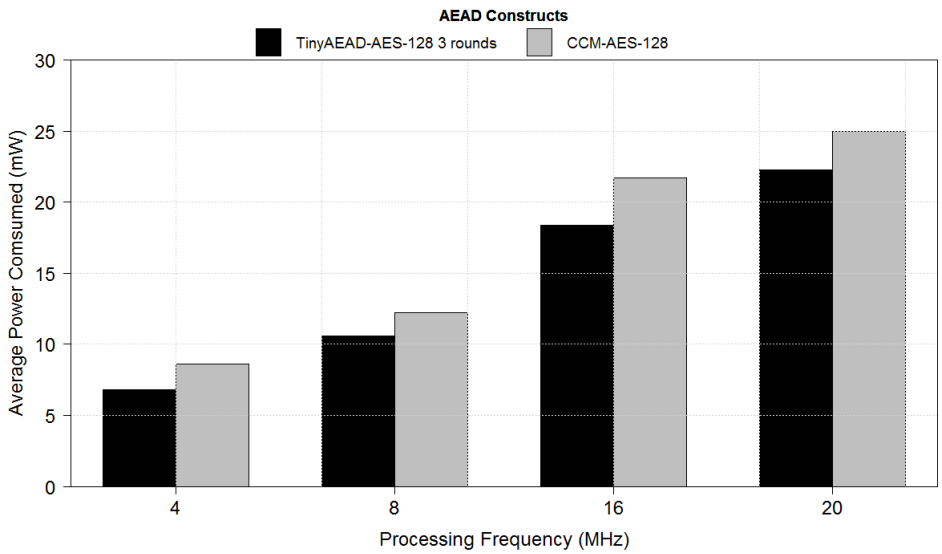


Figure 6.2: Power consumption of AEAD constructs for a thirty-six byte packet at various crystal frequencies.

The results presented in Figure 6.2 shows that CCM-AES-128 has the highest power consumed for the crystal frequencies sampled in comparison to TinyAEAD-AES-128 at three rounds. The relationship between the processing frequency and security measure selected shows a strong positive correlation as the power consumption increased with the higher crystal frequency selected. Results of the tests shows that TinyAEAD-AES-128 at three rounds construct had a mean power consumption of twelve milliwatts whilst CCM-AES-128 had a mean power consumption of fourteen milliwatts, this correlates with the findings that the reduction of iteration (rounds) used by the block cipher reduces the power consumption.

6.2.4 Section Summary

Selection of a higher processing frequency and smaller packet sizes as a method of reducing the processing latency incurred is a feasible approach as smaller packet sizes reduce the number of calls required to the block cipher utilised by the AEAD constructs, also and the higher the processing rate the quicker tasks are completed; however, the higher the crystal frequency selected, the higher increase in the power consumption measured

This could be a problem in real-time teleoperation and telemetry mobile applications as the mobile end-point may have a limited energy supply for the mission duration, the impact of the power consumption for a 20 MHz crystal frequency is five times greater than a 4 MHz crystal frequency with the same configuration applied as demonstrated in Figure 6.2; therefore, it can be expected that the mission time would be reduced by a factor of five times for a 20 MHz crystal frequency in comparison to a 4 MHz crystal frequency and supports the null hypothesis presented in this investigation that AEAD constructs that have the lowest processing latency will also have the lowest impact on the power consumption.

Applying the results obtained from this investigation to the context of the real-time application shows that the increased processing speed of the microcontroller does reduce the latency incurred by the real-time application; however, this does not overcome the bottleneck created by the selected security constructs as is utilising five percent of the available processing frequency as presented in Chapter 3, Table 3.13. This demonstrates that the underlying block cipher has a significant impact on the latency recorded but it is unknown if this is as a result of the software implementation method and therefore, this raises the question of how the implementation of cryptographic services in hardware and software impact the real-time applications.

6.2.5 Hardware versus Software Implementation Methods

Investigation conducted in this analysis has focused on the impact of software cryptographic services on real-time teleoperation and telemetry systems. Real-time application scenarios described in Chapter 3 and Chapter 4 may use a combination of hardware and software implementation methods to deploy secure communication for real-time teleoperation and telemetry applications; this could be for dedicated hardware resources for specific operations or tasks for the real-time application. The following analysis investigated the impact of hardware and software implementation methods of AEAD constructs on real-time teleoperation and telemetry applications.

The null hypothesis for this investigation is that hardware implementation methods will have a reduced impact on the operational performance of the real-time application in comparison to software variants. The alternative hypothesis is that hardware implementation methods will have a greater impact on the operational performance of the real-time application in comparison to software variants.

The test investigated what the impact of hardware and software implementations of cryptographic constructs on real-time teleoperation and telemetry as the aforementioned analysis conducted is focused on the impact of software implementations of cryptographic service. The test analysed the time taken for the microcontroller to process a message through the specified security algorithms using hardware methodologies in order to ascertain how the implementation of the security service contributes towards the latency generated.

Further analysis was undertaken with reference to the Atmel AT86RF212B microcontroller with integrated hardware AES-128 accelerator (Atmel 2015). The data sheet for the Atmel AT86RF212B microcontroller specifies that the standardised AES-128 hardware accelerator requires 234 microseconds (μs) to process ten rounds of AES-128 at a crystal frequency of 16 MHz. This frequency equates to 62.5 nanoseconds (ns) per instruction cycle. The software approach using a PIC18F45K22 microcontroller at the same crystal frequency of 16 MHz would require $975\mu s$ to process ten rounds of software AES-128, which equates to 250 ns per instruction; to demonstrate the significance of this finding, Figure 6.3 illustrates the additional distance travelled per teleoperation command by a mobile end-point travelling at 30 metres per second with hardware and software implementation of the AES-128 block cipher.

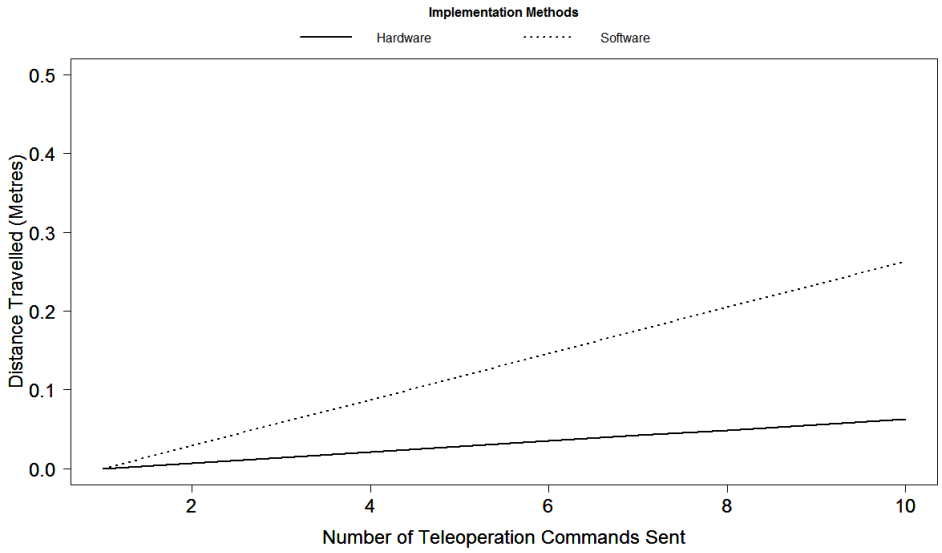


Figure 6.3: Additional distance travelled per real-time teleoperation command by a mobile end-point travelling at 30 metres per second with hardware and software implementations of AES-128 block cipher.

Information presented in Figure 6.3 demonstrate that the the impact of hardware implementations of the security services on the operational performance of a real-time teleoperation and telemetry application as the distance travelled by the mobile end-point is reduced in comparison to software implementation approaches.

6.2.6 Section Summary

Findings presented from the analysis undertaken demonstrates that the implementation does have a significant impact on the latency incurred by the real-time teleoperation and telemetry application and supports the null hypothesis that hardware implementation methods will have a reduced impact on the operational performance of the real-time application in comparison to software variants. There are limitations to using hardware such as: (1) the lack of flexibility of the cryptographic service in real-time as the hardware device is not reconfigurable during the mission; (2) can be expensive to mass produce and (3) the requirement for extra space when employing a hardware module could be problematic from a mobile end-point prospective as the additional weight could impact the operational characteristics and requirements of the device.

The analysis of the findings presented in this investigation further reinforces the section summary presented in section 6.2.3 as the cryptographic construct operates with a reduced latency when implemented in hardware; however, the processing is still restricted to the operation of the security construct as this is the bottleneck for the time required to compute the operation.

Questions raised from the analysis conducted in this section are how cryptographic services impact on the real-time teleoperation and telemetry application and what the consequence of the additional latency is on the operational performance of the real-time application.

6.3 Analysis of The Impact of Cryptography on The Operational Performance of Real-Time Teleoperation and Telemetry Communication Links

This section of the problem analysis investigates how the implementation of a secure communication link impacts a mobile end-point throughout the duration of the mission, because the aforementioned analysis conducted in this chapter has focused on the performance characteristics of the application (i.e. energy consumption).

6.3.1 The Impact of Secure Communication Link on the Operational Performance of a Manual Controlled Mobile End-Point

Investigation conducted in this thesis has examined the impact on the latency, instantaneous packet throughput and energy consumption of the real-time teleoperation and telemetry application but has not investigated the consequence of applying cryptographic services on the operational performance of the real-time application.

The null hypothesis presented in this investigation is that the application of secure communication links will not have an impact on the operational performance characteristics of a mobile end-point. The alternative hypothesis is that the application of secure communication links will have an impact on the operational performance characteristics of a mobile end-point.

Manoeuvres examined in this test investigated the descent of the mobile platform from a fixed height over a fixed period of time and recover back to the original start height. The second manoeuvre examines distance travelled from a continuous transmission of a turn command over a fixed period of time and back to its original flight position. Rules and regulations specified by the UK's CAA does not allow the flying of an UAV within a fifty metre proximity of residential areas and the University of Greenwich health and safety requirements does not permit the flying of an UAV on-site for a real-world validation, therefore, the analysis of the validation is undertaken through emulation and simulation.

The test platform selected for this experiment was a computer simulator called FlightGear, the fixed wing Piper J3 cub selected as the test aircraft. The user interface chosen for this

test was a generic two axis joystick to control the operation of the simulated aircraft; an Arduino Uno development board with an ATMega328p microcontroller was used to read the analogue input from the joystick through the analogue to digital converter and pass the reading to the simulation software over the USB interface. A 16 MHz crystal frequency was selected as the processing frequency of the Arduino microcontroller. Figure 6.4 illustrates the pilots view whilst operating the plane in the FlightGear Simulator.

Figure 6.4: Pilots view of the operation of the plane in the FlightGear simulator.

Additional details of the the test platform, test plan and methodology are specified in Appendix L. Figure 6.5 illustrates the comparison of the additional distance travelled by the mobile platform descending from a height of fifty metres with and without security services applied.

Results presented in Figure 6.5 shows that the delay incurred by the security constructs has an influence on the response time of the UAV to react to the command to descent and to ascend back to the original start flight altitude with TinyAEAD-AES-128 at three rounds requiring an additional seventy-five metres when compared against no security, whilst CCM-AES-128 required an additional one hundred and fifty metres when compared against no security. The trend-line presented for TinyAEAD-AES-128 at three rounds and CCM-AES-128 demonstrates the initial impact of the security construct when manual control of the UAV is implemented as additional latency incurred from processing the security service resulted in a delayed action on the operation of the UAV. Figure 6.6 graphs the response time to perform descent and ascent flight action of the UAV at a height of one hundred metres.

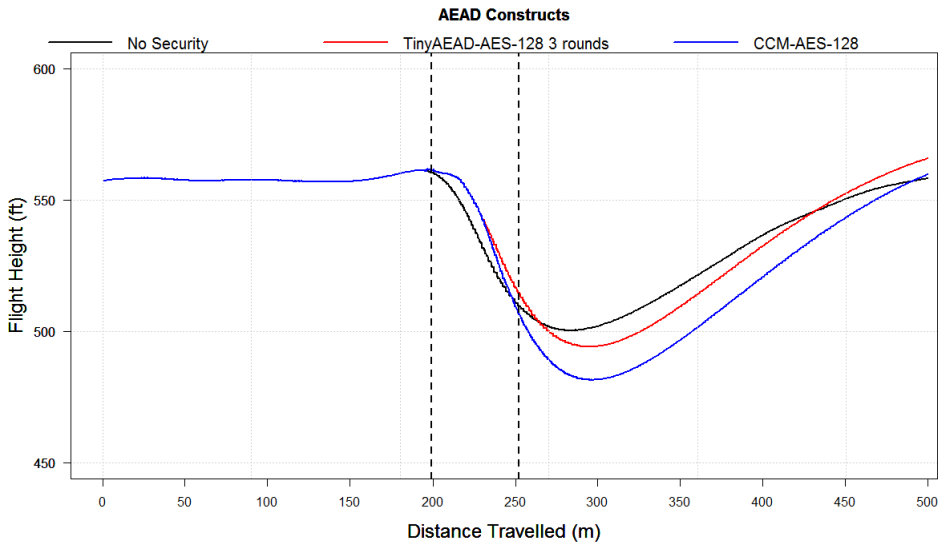


Figure 6.5: Response time to perform descent flight action of the UAV at a height of fifty metres and speed of eighty miles per hour (thirty-six metres per second) with the joystick held for one second in the dive. The first dashed black line represents the change from auto-pilot to manual control; the second dashed black line represents the change from manual control to auto-pilot.

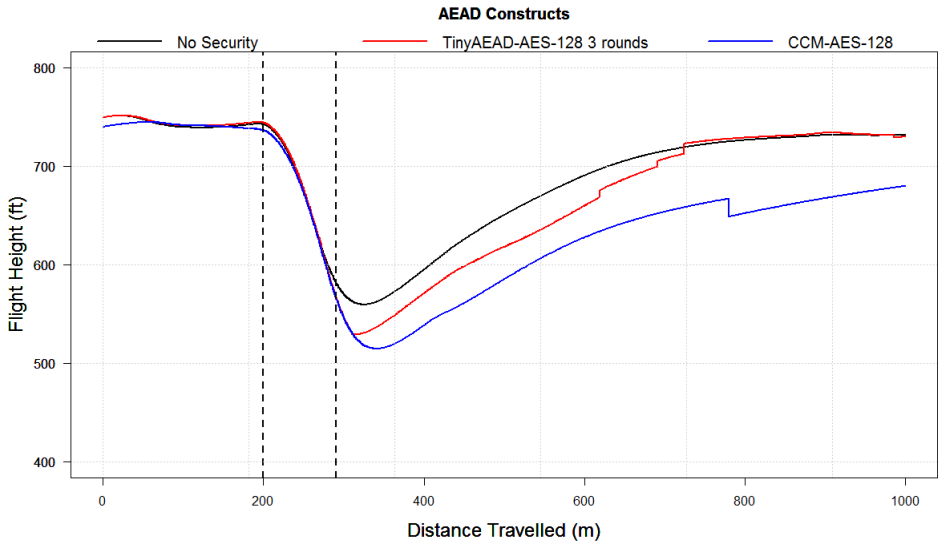


Figure 6.6: Response time to perform descent flight action of the UAV at a height of one hundred metres and speed of eighty miles per hour (thirty six metres per second) with the joystick held for two seconds. The first dashed black line represents the change from auto-pilot to manual control; the second dashed black line represents the change from manual control to auto-pilot.

Data presented in Figure 6.6 shows that the intersect in response time for TinyAEAD-AES-128 at three rounds and no security was achieved after an additional three hundred meters whilst CCM did not intersect in the time-frame analysed; this shows that the selection of the cryptographic construct influences the response time of the UAV to act upon

the command depending on the security construct selected as the additional time incurred to process CCM-AES-128 has a greater impact on the time required by the UAV to return to its original flight height in comparison to TinyAEAD-AES-128 at three rounds.

Analysis of the impact of the security constructs on the heading and roll of the UAV was examined. The test platform selected was the same as the aforementioned test undertaken. The test measured the additional distance travelled by the UAV when conducting a right turn and return to its starting heading with TinyAEAD-AES-128 at three rounds and no security applied.

The height of the UAV was set to one hundred metres and the duration of the joystick held to control the direction of the UAV was two seconds. The roll and the heading of the plane was sampled. Figure 6.7 illustrates the comparison of the flight turn with no security and TinyAEAD-AES-128 at three rounds and Figure 6.8 graphs the comparison of the UAV heading for the flight turn with no security and TinyAEAD-AES-128 at three rounds.

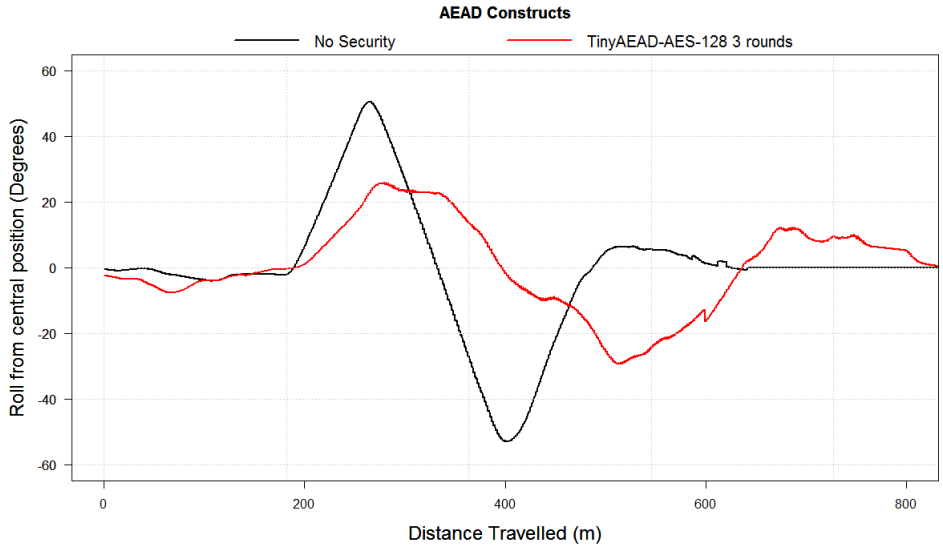


Figure 6.7: Average time required by no security and TinyAEAD-AES-128 at three rounds to perform a horizontal flight turn and return to original flight position with the UAV (Roll of the UAV during a turn horizontal bank around a directional 360 degree axis).

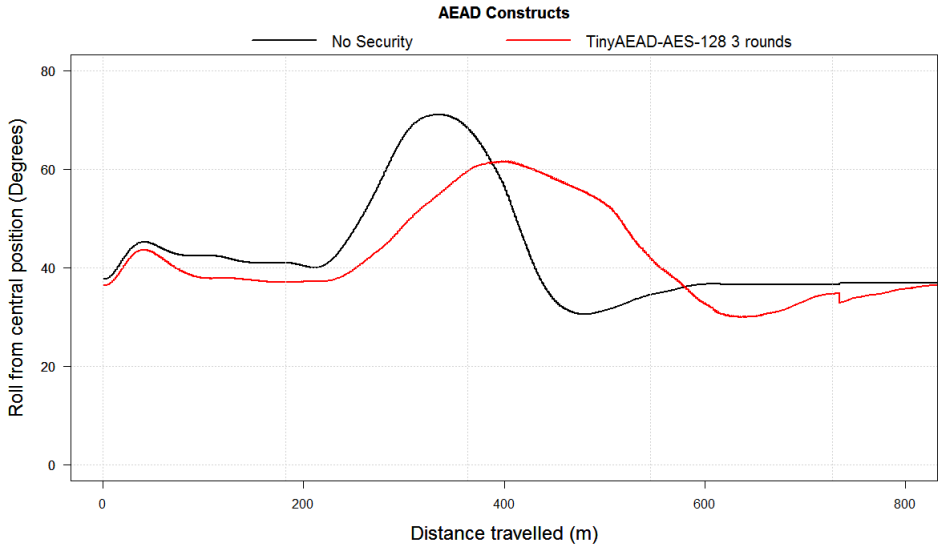


Figure 6.8: Average time required by no security and TinyAEAD-AES-128 at three rounds to perform a horizontal flight turn and return to original flight position with the UAV (heading of the UAV around a directional 360 degree axis).

Data presented in Figure 6.7 shows the roll angle of the UAV changed direction faster with no security service applied in comparison to TinyAEAD-AES-128 at three rounds. The roll undertaken by the UAV shows that the response with no security followed a smooth, responsive action based on the commands sent as reflected by the trace presented; whilst the control of the UAV with TinyAEAD-AES-128 at three rounds applied attempts to follow the same trace as no security, however, the additional delay to the commands sent impacts the response between the change in direction and the settling time to the original flight position.

Results presented in Figure 6.8 show the heading trace for the UAV with no security and TinyAEAD-AES-128 at three rounds follows the same trend; however, the comparison of the two approaches shows the turning circle for no security requires less distance than TinyAEAD-AES-128 at three rounds. The roll profile of TinyAEAD-AES-128 at three rounds is shallower than no security, it can be inferred that the additional latency incurred from the security service impacts the additional distance travelled by the UAV and the time required to complete the action and return to its original start position; this is because the latency incurred from the processing of the security construct contributes to the real-world actions, resulting in a delay in the task completion.

The trend presented in Figure 6.8 correlates with the phenomenon of phase difference in analogue signals as the findings from the tests undertaken in the FlightGear simulator demonstrates that the latency incurred by the processing of the security constructs offsets the response time required to execute the signal; this interlinks with the latency incurred

from the processing of the security constructs as the additional delay in the response to the teleoperation; this delay contributes to the additional distance travelled by the UAV before acting upon the command, consequently, this results in an increase in energy usage to complete the same operation.

6.3.2 Section Summary

Examination of the findings presented establishes a correlation between the human operator transmitting the real-time teleoperation and the response of the UAV aircraft to the teleoperation as the control of the UAV is determined by the additional latency incurred by the security construct as discussed previously. From the prospective of the human operator, the manoeuvres performed are not as responsive for the same period of time the command was undertaken as graphed in Figures 6.7 and 6.8; this influences the safety, reliability and availability of the mobile system as the delay in the processing of the teleoperation could result in damage to the UAV if it does not respond to the command in time; in addition, the human operator has to compensate for the impacts identified in the tests by slowing the speed of the UAV as a result of the delay between the teleoperation command and response of the actuator and therefore supports the alternative hypothesis in that the application of secure communication links will have an impact on the operational performance characteristics of a mobile end-point.

The analysis conducted demonstrates that the cryptographic service selected does have an impact on a manual real-time application. Comparison of the fixed wing aerial mobile device and the mobile ground vehicle analysis conducted in Chapter 5, section 5.3.1, shows that the delay only impacts the ground vehicle in terms of the time required to complete the task or process; whilst the aerial vehicle is impacted by the additional distance travelled by the aircraft before completing the action; this is because the ground vehicle was able to pause in between each command before starting the next task whilst the aerial vehicle is constantly in motion and is unable to stop in-between commands.

6.3.3 The Relationship Between the Vertical Height of the Mobile Device and the Number of Picture Samples Over a Telemetry Link

The purpose of this analysis is to ascertain the coverage area of the image taken by an optical camera at various heights; in addition the resolutions obtained from the image capture and the file size of the telemetry file. Examination of the aforementioned analysis conducted indicates that the cryptographic services would impact on the real-time teleoperation for the applications examined; mitigation of the effects of a secure communication link could be to adjust the operational height of the real-time application; however, the impact on the real-time telemetry link between the transmitter and receiver node could be

impacted as a result of the adjustment of the end-points.

In this section of the analysis, the impact of the secure communications on the real-time telemetry link is investigated. Three areas are analysed in this section, the relationship between the end-points in relation to the resolution and aspect ratio of the surface area captured by the optical camera; the relationship between the aperture of the optical camera lens to the surface area captured and the impact of cryptographic services on the real-time telemetry link.

The null hypothesis proposed in this investigation is that the higher the vertical placement of the optical camera; the greater the coverage area is at the cost of a reduced resolution of the picture details (i.e. buildings, scenery, people, etcetera). The alternative hypothesis is that the higher the vertical placement of the optical camera; the greater the coverage with no cost in resolution of the picture detail. The test platform and assumptions are specified in Appendix M.

The test investigated the picture quality obtained from the two cameras at varying specified heights to determine how the vertical height of the mobile platforms influences the picture quality. Two cameras were selected for this test, the Raspberry Pi colour (RGB) camera and the Raspberry Pi infra-red (IR) camera; both cameras had a picture quality of five megapixels and a viewing angle of sixty degrees and image resolution of 2,592×1,944 pixels. The model scene selected was a 1:148 ratio with three heights scaled to reflect a mobile real-time application flying at heights of eighty metres, one hundred metres and one hundred and twenty metres. No post processing was undertaken on the pictures. No compression techniques were used for the image file. Table 6.2 illustrates the results of the streamed picture quality at the varying vertical heights.

Table 6.2: Telemetry picture file size for a mobile end-point over varying vertical heights.

Independent Variable	**Dependent Variable**		
Camera	**80 Metres**	**100 Metres**	**120 Metres**
RGB Picture File Size (bits)	3,053,051	3,089,833	3,089,523
IR Picture File Size (bits	3,094,598	3,103,703	3,061,551

Data presented in Table 6.2 shows that the largest picture size was obtained at the lowest

vertical height with the infrared camera recording a larger file size in comparison to the RGB for eighty metres and one hundred metres vertical heights, whilst the RGB camera recorded a higher number of pixels for the one hundred and twenty metres height. Figure 6.9 and Figure 6.10 illustrates the difference of the pictures taken with a Raspberry Pi RGB five megapixel camera at the equivalent vertical height of eighty metres and one hundred metres.

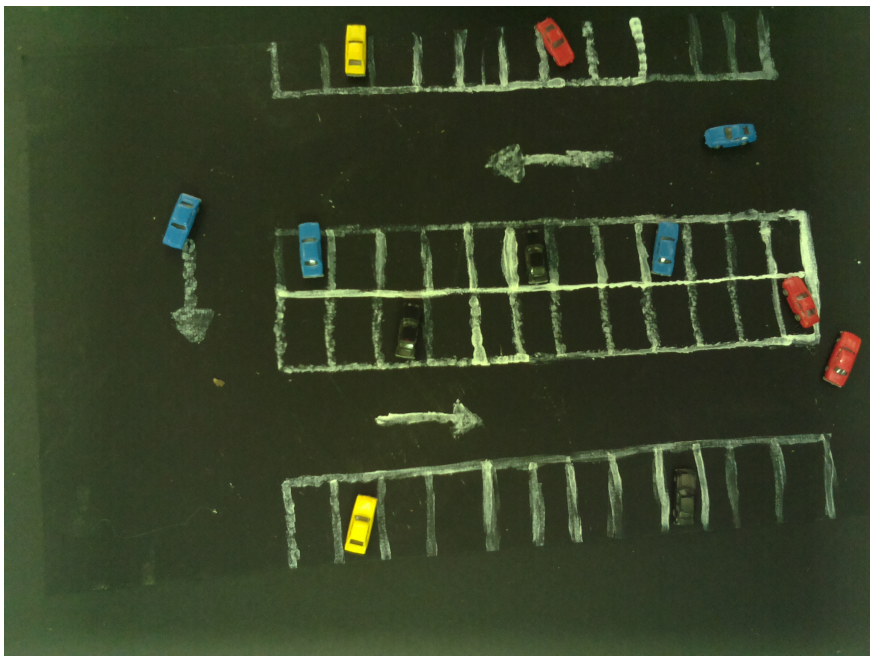


Figure 6.9: Sample picture obtained for an equivalent vertical heights of eighty metres.

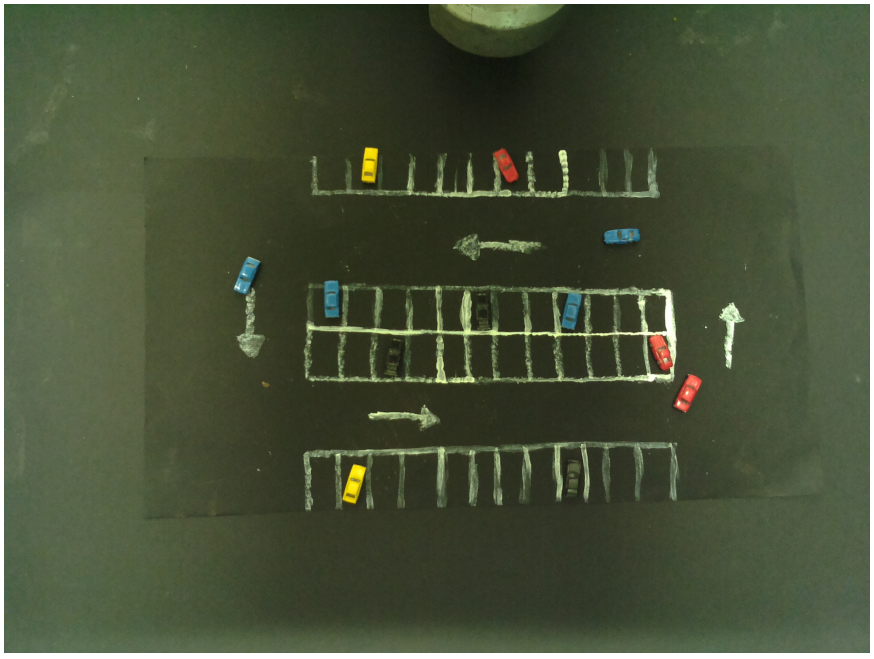


Figure 6.10: Sample picture obtained for an equivalent vertical heights of one hundred metres.

The images obtained in Figure 6.9 and Figure 6.10 shows that the vertical height of the UAV has a significant difference on the scale of the image sampled as the one hundred metres vertical height picture sample has a greater surface area covered in comparison to the eighty metres picture sample.

Calculation of the base area covered by the photograph taken by the UAV was undertaken to showcase the impact of the vertical height on the area of the image taken; as the pixels resolution of the Raspberry Pi camera image is 2,592 pixels in width and 1,944 pixels in length, it is calculated that the ratio between the pixel width and height is a 4:3 aspect ratio. Calculation of the image area was modelled through the use of the Raspberry Pi pixel aspect ratio to determine the relationship between the base width of the image and the area covered within the aspect ratio of the photo. Table 6.3 tabulates the base area covered by the image taken by the UAV at varying vertical heights for a 4:3 aspect ratio.

Table 6.3: Base area covered by the image taken by the simulated UAV at varying vertical heights for a 4:3 pixel aspect ratio.

Independent Variable	**Dependent Variables**	
Vertical Height (m)	**Base Width (m)**	**Area of image captured (m^2)**
10	13.3	133
20	26.6	532
30	40.0	1,200
40	53.3	2,132
50	66.6	3,330
60	80.0	4,800
70	93.3	6,531
80	106.6	8,528
90	120.0	10,800
100	133.3	13,330

Results presented in Table 6.3 show the relationship between the height and the area of the image captured follows a positive correlation pattern as with the distance captured increased with the height of the simulated UAV.

Further analysis identifies the area of the image captured differs in relation to the vertical height and base width; this is because the increased height of the simulated UAV has an increased impact on the base width of the sampled object as the ratio between the height and width is constant; however, the area covered based on the multiplication of the height and width follows an exponential growth.

This correlates with the positive correlation with the increased vertical height to base width as the area also increased as the vertical height increases. Figure 6.11 illustrates the relationship between the vertical height and the base width and the area covered.

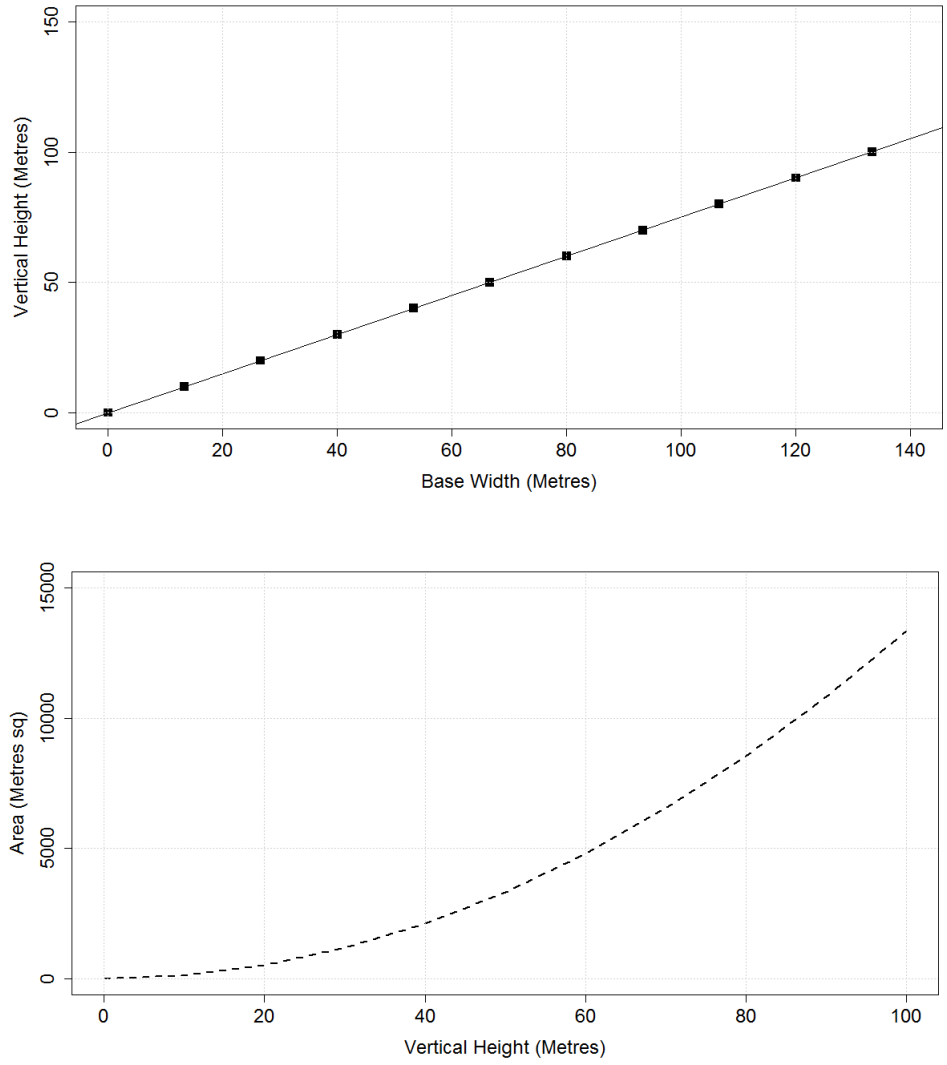


Figure 6.11: Relationship between vertical height and base width of the image (top) and the area covered (bottom).

Further analysis was undertaken on the number of pixels per metre at varying heights. The calculation of the field of view was achieved by dividing the total horizontal resolution in pixels by the height of the camera. Three horizontal pixel sizes were used with 1,296 pixels, 2,592 pixels and 5,182 pixels chosen. Figure 6.12 graphs the number of pixels per metre at varying camera heights for a sixty degree viewing angle.

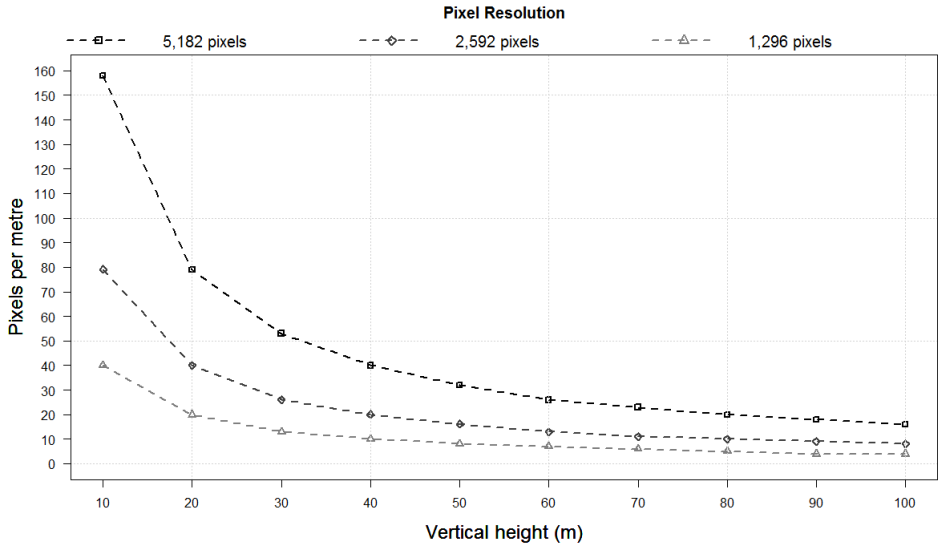


Figure 6.12: Pixels per metre over varying vertical camera heights based on 1,296 pixels, 2,592 pixels and 5,182 pixels.

Information presented in Figure 6.12 demonstrates that the number of pixels per metre follows an exponential decay profile as the height of the camera is increased; this is because the area of the picture size is greater at a higher height, this results in the number of pixels per metre reducing as the pixels are more spread and consequently, this reduces the resolution of the image.

The horizontal pixel size of the image contributes towards the problem as the least number of horizontal pixels has a reduced pixel per resolution; this impacts the context of real-time telemetry as the reduction of the image resolutions impact the quality of the sampled image taken; however, this also reduces the processing time required by the device to compute and transmit the data back to the base-station.

The results presented in Figure 6.12 are in relation to the pixel aspect ratio and resolution to calculate the total area covered by the image at various vertical heights; however, the consideration of the viewing angle of the camera is required to determine the distance covered in the picture. The viewing distance was achieved through mathematical modelling. It is assumed that the camera used by the UAV is fixed focused. Figure 6.13 illustrates the viewing distance of a camera with a viewing angle of sixty-five degrees, thirty-two degrees and sixteen degrees.

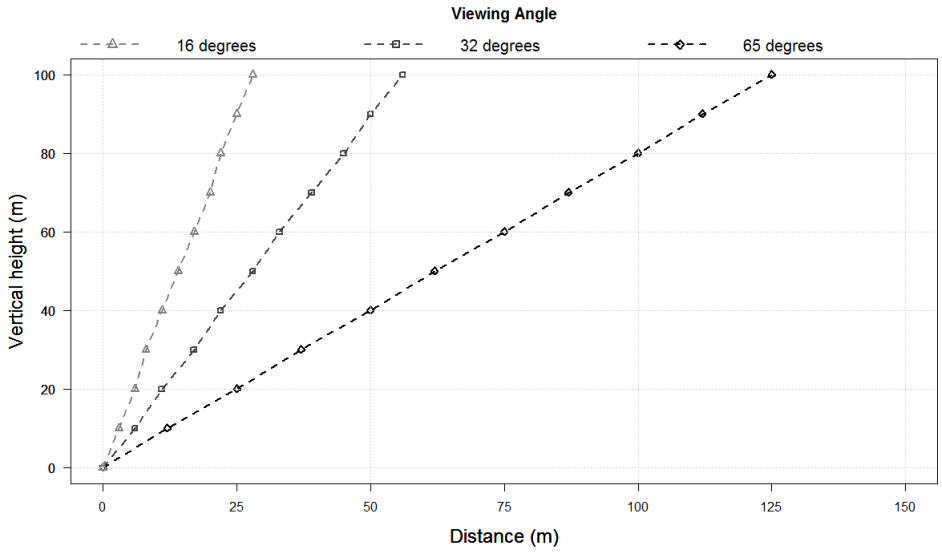


Figure 6.13: Calculated viewing distance of a fixed focused camera on an UAV with a fixed viewing angle of sixteen degrees, thirty-two degrees and sixty-five degrees.

The findings presented in Figure 6.13 shows that the trend between the distance covered by the camera viewing angle based on the vertical placement of the camera is a linear increase as the distance covered by the camera increases at a fixed rate; this correlates with the linear trend identified in the aspect ratio test between the vertical height and base width; however, the selection of the viewing angle significantly influences the distance viewed as a higher degree viewing angle has the greatest distance covered in comparison to lower degree viewing angles. This is because the angle dictates the field of vision for the fixed focused camera to capture the photo (i.e. the maximum distance it can view).

Analysis of the relationship between the distances travelled by the mobile device before a picture is taken at varying speeds of the mobile device is investigated. The security constructs investigated in this scenario are TinyAEAD-AES-128 at three rounds, CCM-AES-128 and GCM-AES-128. The impact was modelled based on the time, distance and speed formula. Figure 6.14 illustrates the relationship between the speed of the UAV and the distance travelled before the command to capture a picture was initiated.

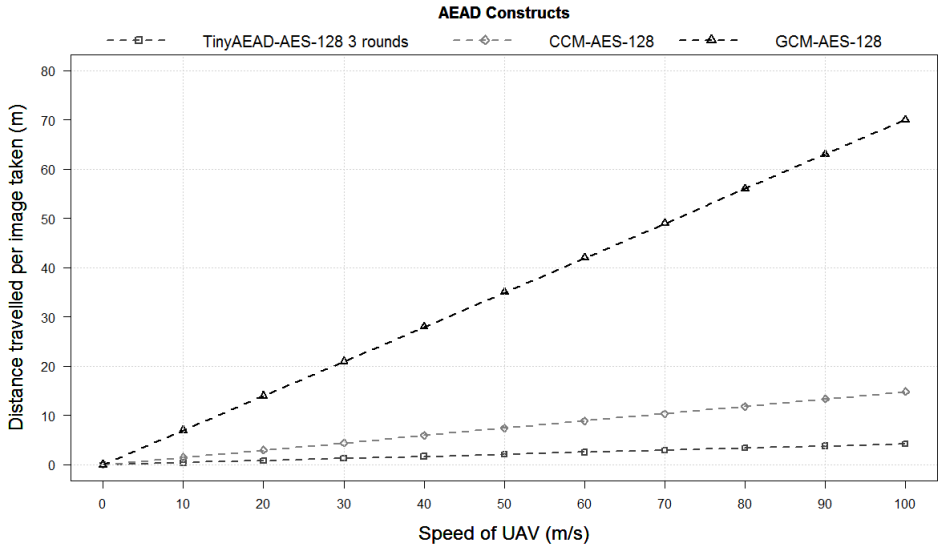


Figure 6.14: Distance travelled by an UAV with various security constructs applied before the real-time telemetry for a picture capture was complete at a processing frequency of 4 MHz (1 MIPS).

Data presented in Figure 6.14 shows that the security construct selected has an impact on the distance travelled by the UAV before the command for an image is complete, the standardised GCM-AES-128 construct had the most significant impact on the distance travelled before the image was captured, whilst TinyAEAD-AES-128 at three rounds had the least significant impact; this is because the time required to process the cryptographic construct contributes to additional distance travelled by the UAV.

The trend identified for the constructs examined follows a positive linear correlation; this shows that as the speed of the mobile device increases, the additional distance travelled before the picture is sampled also increases; this is further exemplifies with the selection of the security construct with fixed standardised constructs having a greater impact on the additional distance travelled.

Analysis of the speed reduction of the UAV with CCM-AES-128 and CCM-AES-128 in reference to obtained the same number of image samples as TinyAEAD-AES-128 at three rounds is investigated. Table 6.4 tabulates speed of the UAV with CCM-AES-128 and GCM-AES-128 constructs to obtain the same number of image samples over the same distance travelled.

Table 6.4: Speed of the UAV to obtain the same number of image samples as TinyAEAD-AES-128 at three rounds at varying speeds at a crystal frequency of 4 MHz (1 MIPS).

Independent Variables	**Dependent Variables**	
Speed of UAV (m/s)	**Speed of UAV with CCM-AES-128 (m/s)**	**Speed of UAV with GCM-AES-128 (m/s)**
10	2.5	0.6
20	5.0	1.2
30	7.5	1.8
40	10.0	2.4
50	12.5	3.2

Results presented in Table 6.4 show that the speed of the UAV speed with CCM-AES-128 is up to four times slower and GCM-AES-128 is up to sixteen times slower to achieve the same image sample rate as TinyAEAD-AES-128 at three rounds; this reduction in speed would influence the total flight time of the UAV as the amount of energy and time required to travel the same distance would increase and impact on the maximum duration of the mission.

The size of the telemetry payload transmitted between the UAV and base-station contributes to the time needed to compute the number of cryptographic calls required to encrypt an image to the base-station. As the aforementioned tests examined a picture size of three megapixels, the calculation undertaken for the total number of encryption calls required for a 128-bit block cipher to process a three megapixel file-size was 187,500 calls to the cryptographic construct. Figure 6.15 graphs the total time required to process a three megapixel image with TinyAEAD-AES-128 at three rounds CCM-AES-128 and GCM-AES-128.

Data presented in Figure 6.15 shows that the time required to encrypt the image with standardised cryptographic construct GCM-AES-128 and CCM-AES-128 are longer than TinyAEAD-AES-128 at three rounds, this correlates with the time require to process each three megapixel image taken as the time required to process the 187,500 encryption calls accumulates and follows a linear trend.

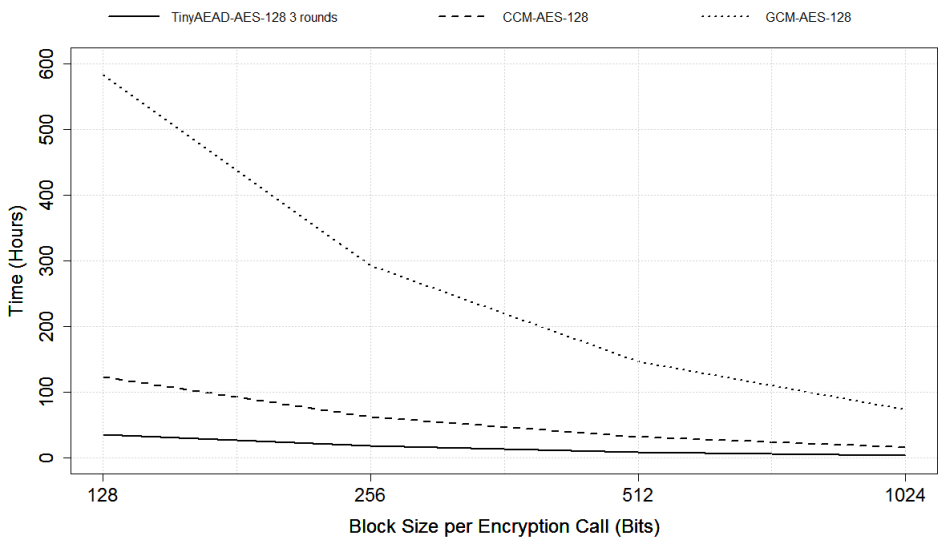


Figure 6.15: Number of hours required to encrypt a three megapixel image with varying block cipher sizes at a processing frequency of 4 MHz (1 MIPS).

Analysis of the block size used for encryption demonstrates that the time required for larger block sizes to encrypt the three megapixel image is reduced in comparison to smaller block sizes; this is because the block size dictates the number of bytes that can be encrypted per encryption call; inadvertently, this also reduces the number of encryption calls required to complete the operation; however, limitations of larger block sizes are the requirement of an increased number of bytes to process the operation and an increased probability of packet error during propagation between the transmitter and receiver.

6.3.4 Section Summary

Findings presented from the analysis undertaken is that the vertical height of the end-point does not impact on the picture resolution as the optical camera captures images at the same resolution for the IR and RGB camera; however, upon further investigation, the placement of the end-points and the viewing angle of the camera lens contributes towards the surface area captured and the detail of the image; this is because of the sampling of the area that is captured in relation to the vertical height with a higher placement of the end-point recording a greater coverage area at the reduction of image resolution (i.e. details in the picture capture); therefore, neither the null or alternative hypothesis are validated in this instance of the analysis.

Applying the findings to the real-time application scenarios investigated in this thesis shows that the security construct contributes towards the reduction in the number of real-time telemetry packets received by the base-station. This is because of the time required by the underlying block cipher to process the number of bytes required for live telemetry

streamlining as this increases the number of block calls to the block cipher.

Mitigation of the impact of security constructs on the real-time telemetry is to increase the height of the mobile end-point to overcome the communication latency on the sampling of the picture as the mobile end-point is travelling; however, a consequence of this is the reduction in the resolution of the image (i.e. the detail of the captured item). This indicates that the security services need to be integrated into the real-time application and not considered as a stand-alone module that is considered after the design of the real-time application.

6.4 Discussion

The findings presented throughout this section of the problem analysis demonstrates that the impact of the additional latency incurred from the implementation of the AEAD constructs examined in Chapter 3 demonstrates the transferable impact on the operational performance from the logical characteristics of latency and throughput measurement to the physical characteristics of the node in both static and mobile situations presented in sections 6.2 and 6.3.

The reduction of the number of iterations used by the underlying block cipher results in the reduction of the energy consumed by the cryptographic service; a by-product is the reduction in the reduction in the latency generated by the cryptographic service. This indicates that there is a relationship between the security, speed and energy in relation to the design of the block cipher; therefore this indicates that the block cipher selected contributes towards the impact on the operational performance of the real-time application and may require further analysis to ascertain the underlying cause of this finding as presented in 6.2.3 and 6.3.1.

Initial knowledge presented in Chapter 3, Chapter 4 and Chapter 5 as the indication is that the speed of the cryptographic service is paramount; however, this problem can not be simply overcome by switching to hardware implementation strategies or by reconfiguring the mobile-end point to compensate for the impact for reasons identified in sections 6.2.5, 6.3.1and 6.3.3. Additional questions formulated from the current problem analysis are focused on the influence of the channel characteristics of the communication link; this includes the operational performance of the real-time teleoperation and telemetry application under non-ideal communication channels; the maximum communication range for a real-time application transmitter and receiver and how this contributes towards the problem scenarios examined in this thesis.

The file size of the real-time telemetry data contributes towards the problem context as the file size of one image using the Raspberry Pi camera equated to 3 megapixels; as discussed in section 6.15, the time to process one image at a set frequency requires a significant amount of time before it is received at the transmitter and viewed by the human operator. The packet size selected to propagate the real-time telemetry data between the transmitter and receiver influences the problem because larger sized packets can propagate an increased volume of data at an increased probability of being impacted by non-ideal channel characteristics and the requirement of more block cipher encryption calls to encrypt the message. Conversely, smaller size packets reduced the number of bytes processed by the encryption call per packet and decreases probability of packer corruption during propagation as the probability is reduced as a result of a reduced number of bytes transmitted. The trade-off of using smaller sized packets is the increased cost in the communications to propagate the increase quantity of packets; which has a more significant impact on the limited energy constraints of portable and mobile situations.

Examination of the real-time telemetry link demonstrated the multi-faceted nature of the research problem investigated as the vertical placement of the end-points, viewing angle of the optical camera lens and the cryptographic service selected all impact on the problem investigated as presented in section 6.3.3. Attempts to mitigate the impact of a secure communication link on the mobile end-point by adjusting the placement of the device or the speed of the mobile actuator have consequences on the number of images sampled and the energy consumption in situation where remote energy constrained real-time applications are selected.

Analysis of the findings obtained in this chapter indicates that the underlying block cipher used for the cryptography could be a possible cause to the problems identified as the time required to process the cryptographic tasks significantly impacts on the latency and operational performance metrics recorded. This indicates that the current approach for the inclusion of security services in this context needs to be reconsidered as security services have been viewed as a separated internal function; whilst the findings presented indicate that there is a requirement for security services to be integrated with the real-time application and be applicable to the real-time constraints without impacting the application instead of a standalone module considered after the design of the real-time application.

The privacy of real-time teleoperation and telemetry messages is a feasible alternative as the duration of the communication time-window to transmit and receive data between the end-points is a finite period of time that the message is required to be intact (i.e. for the specified real-time deadline as presented in Chapter 4, section 4.2); this is applicable in the context investigated in this chapter as real-time applications using telemetry data may

incur increased processing latency for typical message sizes transmitted back to the base-station; this indicates that the security and energy paradigms are not suited to meet the specified real-time constraints and an alternative measure that suits the real-time nature of the applications investigated is required.

The knowledge presented in Chapter 3, Chapter 4, Chapter 5 and Chapter 6 indicates that that the underlying speed of the block cipher used for the cryptographic process dictates the real-time characteristics of the application as the additional latency generated from the cryptographic process selected impacts on the different areas of the multi-faced problems in a similar manner.

6.5 Chapter Summary

This chapter presented the impact of the additional latency incurred by AEAD constructs on the operational performance of real-time teleoperation and telemetry applications from a variety of perspectives. The questions investigated in this section of the thesis examined was how do cryptographic construct impact on the operational performance of real-time applications. Knowledge collated from the analysis showed that the energy usage and communication latency incurred from the cryptographic process increased as a result of the cryptographic method selected; consequently, impacting the real-time teleoperation of the real-time applications examined and the data samples obtained from the real-time telemetry link. Hardware implementation methods overcome the issue of the latency on real-time teleoperation and telemetry but are not an adaptive or flexible approach to secure communications as the configuration is fixed throughout the mission duration.

Examination of the findings obtained from the analysis conducted in this chapter indicate that the current view of security and energy AEAD designs are not best suited to overcome the problem of real-time teleoperation and telemetry communications of real-time applications; instead, the findings indicate that there is a requirement to ensure the privacy of communicated data is maintained between the transmitter and receiver to prevent adversaries from ascertaining the information propagated across the communication link.

The findings obtained from this problem analysis in this section demonstrate that security constructs do have a significant impact on the operational performance of real-time teleoperation and telemetry applications. Analysis of the findings indicate that the root cause of the impact on the operational performance is from the underlying block cipher used for the security construct. The next chapter conducts an in-depth investigation and analysis on the cryptography used for secure communications.

7 Analysis and Profiling of Cryptography

7.1 Introduction

This chapter undertakes a problem analysis of the fundamental areas associated with the cryptography used for secure communications and presents a specification required for the synthesis of the solution in Chapter 8 based on the aforementioned problem analysis undertaken.

In this chapter, the problem analysis undertaken is based on the following questions:

- What is the operational performance profile of the standardised AES-128 block cipher?
- What key implementation methods are used by the AES-128 block cipher and how does each approach frustrate an attacker from compromising the cryptographic key?

The structure of this chapter is as follows; first, the profile of the standardised AES-128 bit block cipher is investigated in section 7.2, followed by the analysis of the key management implementation approaches in section 7.3; followed by a discussion of the findings with the specifications derived from the synthesis of the problem analysis conducted in section 7.4. A chapter summary concludes.

7.2 Profiling of AES-128 Block Cipher

The profiling of the AES-128 block cipher analysed the operational performance of the block cipher in terms of latency, instruction cycles used, relationship of plain-text inputs with cipher-text outputs, the impact of the message size on the cipher-text output and the energy usage of the AES-128 block cipher.

7.2.1 Instruction Cycles used by AES-128 Block Cipher

Analysis of the number of instruction cycles required to process each cryptographic function of the AES-128 block cipher was undertaken to determine the total number of instruction cycles required to compute one round of the AES-128 block cipher. The null hypothesis presented for this investigation is that the MixColums component will have highest number of instruction cycles in comparison to the other components required by the AES-128 block cipher. The alternative hypothesis is that the MixColums component will not have highest number of instruction cycles in comparison to the other components required by the AES-128 block cipher.

The test platform selected was an emulated environment with the Mikroelektronika C integrated development environment (IDE); variables measured in this test were the number of instruction cycles required to compute each cryptographic operation and the time require to complete this process. All measurements were taken from the IDE. Table 7.1 tabulates the time required to process the number of instruction cycles required by AES-128 with a PIC18F45K22 microcontroller at a processing frequency of 1 MHz (0.25 million instruction cycles per second).

Table 7.1: Latency and number of instruction cycles required by each cryptographic function of AES-128 block cipher at one round on a PIC18F45K22 microcontroller with a processing frequency of 1 MHz.

Independent Variable	**Dependent Variables**		
Function	**Time (ms)**	**Number of Instruction cycles**	**Percentage of total process (%)**
SubBytes	0.60	605	22
ShiftRows	0.19	192	8
MixColumns	0.92	922	32
AddRoundKey	1.10	1,103	38
Total	**2.81**	**2,882**	**100**

Results of the test presented in Table 7.1 shows that the AES-128 block cipher has three functions that require the most instruction cycles, the addroundkey function has the highest number of instruction cycles, followed by the mixcolumns and subbytes. The combination of these three functions consumed ninety-two percent of the total number of instructions required to compute the block cipher operation.

Information obtained from the analysis of the time to process the AES-128 block cipher on a microcontroller device with a low processing frequency demonstrates that the AES-128 block cipher was designed to process cryptographic operations with the consideration of the time to process the block cipher whilst maintaining a adequate level for the security service; this supports the findings obtained from the NIST AES competition presented in the preliminary literature review in Chapter 2, section 2.6 that the AES-128 block cipher required a reduced number of instruction cycles and less time to process in comparison to Serpent and Twofish ciphers.

Interpretation of the knowledge obtained from the analysis of the AES-128 block cipher indicates that there is a relationship between the latency incurred by the block cipher and the number of instruction cycles required to compute the service as the data presented in Table 7.1 demonstrates the components with the highest percentage of processing cost have the highest number of instruction cycles to compute; this reinforces the alternative

hypothesis is that the MixColums component will not have highest number of instruction cycles in comparison to the other components required by the AES-128 block cipher in this form of the analysis undertaken.

An investigation of the components used to construct the AES-128 block cipher is an area that requires further consideration in order to meet the time constraints associated with real-time teleoperation and telemetry systems; however, before this relationship is examined; an analysis of the performance metrics of the cipher-text output of the AES-128 block cipher is presented to profile the operational characteristics of the block cipher.

7.2.2 Performance Metrics of the Cipher-Text Output of the AES-128 block cipher

Analysis of the number of rounds (iterations) used by the AES-128 block cipher was investigated to determine the relationship between the cipher-text output characteristics of entropy, arithmetic mean and serial correlation in relation to the number of iterations conducted. The null hypothesis presented in this investigation is that the higher the number of iterations used by the AES-128 block cipher improves the cipher-text output metrics recorded. The alternative hypothesis to this is that higher the number of iterations used by the AES-128 block cipher will not have better cipher-text output metrics recorded. The test platform, configuration, methodology and assumptions are stated in Appendix N.

The application of the strict avalanche test method was selected to analyse the change in the known plain-text input and cipher-text output of the block ciphers investigated; this is to determine if there is any correlation that a change in a particular bit position of the known plain-text is more or less than a fifty percent change in the cipher-text output (Webster & Tavares 1986). The strict avalanche criterion test has been applied to determine the strength of a cipher by measuring the amount of non-linearity of the substitution boxes or alternative non-linear operators (Castro et al. 2005).

Cipher designs that do not ascertain the specified requirement of the strict avalanche criterion are not best suited as a cipher design; this is because the lack of change in the could result in vulnerabilities to known cryptanalysis methods such as differential or linear cryptanalysis as the randomness of the cipher is weak. Formula 13 demonstrates the mathematical notion to determine if a function has a good avalanche effect.

$$V_i = f(X) \oplus f(X_i) \tag{13}$$

Formula 13: Strict avalanche effect mathematical notion derived by (Webster & Tavares 1986)

Presentation of the strict avalanche test by Webster et al.; states that the criterion of an avalanche effect is fulfilled if on average half of the output bits are changed whenever a single bit input is complemented (Webster & Tavares 1986); in the context of block cipher analysis, a single bit change in the plain-text input should effect half of the bit value of the cipher-text output. Further elaboration by Webster et al.; states that in order to determine whether a given m x n (m input bits and n output bits) function (f) satisfies this requirement, the 2^m plain-text vectors must be divided into 2^{m-1} pairs, X and X_i, such that X and X_i differ only in bit i. Then the 2^{m-1} exclusive-or sums must be calculated. These exclusive-or sums will be referred to as avalanche vectors, each of which contains n bits, or avalanche variables (Webster & Tavares 1986).

To quantify if the AES-128 block cipher meets the criterion specified for the strict avalanche test; statistical analysis of the cipher-text output of the block cipher was conducted. Statistical analysis chosen for this test used entropy as the measure of predictability (zero-bits the most predictable and seven-bits the least predictable) arithmetic mean to determine the average weighting of binary zeros and ones in the cipher-text output and the serial correlation test was selected to identify if there is a correlated trend in the cipher-text outputs of the AES-128 block cipher. Arithmetic mean and Pearson's serial correlation formulas used are derived from a standard mathematical textbook.

In information theory, entropy is refereed to as disorder or uncertainty of an event and is used as a unit of measurement to determine the average measure of uncertainty or information based on its output (Shannon 1948). In the context of this thesis; entropy is used to measure the quantity of information output from the block cipher; this statistical methods enables a quantitative measure of uncertainty or randomness in a block cipher output and is measured in bits to reflect the expected surprise; as a the number of bits measured in an output is increased, the inference is that there is an increased level of uncertainty in the cipher-text output; therefore, it is more difficult to deduce the relationship between plain-text input and cipher-text output. The formula used to calculate the entropy of the cipher-text output is presented in Formula 14.

$$p_i I(s_i) = \sum_{i=1}^{n} p_i \, log_2(\frac{1}{p_i}) \tag{14}$$

Formula 14: Entropy calculation (Hamming 1980).

The entropy calculation is as follows; the probability(p_i) of getting the units of information $I(s_i)$ is obtained through the observation of an event (i). The number of possible outcomes $(\frac{1}{p_i})$ is first calculated with the answer is multiplied by the total number of pos-

sible event (log_2) and the probability of the event occurring.

The implementation of the AES-128 block cipher was programmed in visual studio with the C programming language; the mode of operation selected for this test was electronic code book (ECB) mode to modify all byte positions of the payload; sixteen bytes of the payload were encrypted per encryption call. Analysis of the cipher-text output was conducted with the entropy number tester programme to derive the statistical output of the cipher-text. Message size selected for this test was two hundred and fifty six bytes to replicate a maximum packet size of the MAVlink communication protocol. The number of rounds selected for the AES-128 block cipher ranged from one to ten rounds.

The test undertaken in this analysis changed one byte of a zero payload message, encrypted the message through AES-128 block cipher and stored the output into a text file. The byte positions are reset back to their default set values before the next byte position is changed; therefore, a change of one byte position at a time that propagates throughout the payload. The inverse of this test was undertaken where all bytes in the payload were set to an integer value of two-hundred-and-fifty-five with the selected byte changing to a zero. Details of the experimentation are located in Appendix N. Table 7.2 tabulates the metrics recorded for the AES-128 block cipher at a varying number of rounds.

Table 7.2: Metrics recorded for the cipher-text output of the AES-128 block cipher over a varying number of rounds for a two hundred and fifty six byte packet size.

Independent Variable	**Dependent Variables**		
Number of Rounds	**Entropy (bits)**	**Arithmetic Mean (bits)**	**Serial Correlation**
1	1.3	14.3	-0.14
2	4.0	144.0	0.06
3	7.1	124.9	0.05
4	7.1	123.3	0.03
5	7.3	133.1	0.02
6	7.2	129.0	0.09
7	7.1	119.9	0.03
8	7.2	126.6	-0.02
9	7.1	131.2	0.00
10	7.1	123.9	-0.02

Data presented in Table 7.2 shows the entropy score of the cipher-text output was below seven bits at one and two rounds with two-bit and sixteen-bit entropy recorded; whilst the entropy value obtained from three rounds to ten rounds is on average a 128-bit entropy; this correlates with the size of the block cipher used for this test as a 128-bit version of

AES-128 was selected, therefore, the maximum entropy output had been reached after three rounds for 128-bit block cipher.

The arithmetic mean measures the average frequency of zero and ones in a given cipher-text output; in an ideal case, an equal weighting of both values would be present and this is reflected as 127.5 bits (i.e. equally distributed number of zeros and ones per byte (255-bits)). Analysis of the arithmetic mean test shows that the measurements recorded for one and two rounds had the biggest difference from the ideal arithmetic mean of 127.5 bits with a difference of one hundred and fifty nine percent for one round and twelve percent for two rounds. The average percentage difference for three rounds and above was no greater than six percent; this shows that the cipher-text output is closer to the ideal arithmetic mean of 127.5-bits with AES-128 configure at three rounds and above whilst configurations less than three rounds have a greater deviation from the ideal arithmetic mean; resulting in a less even distribution of binary zeros and ones in the cipher-text outputs under two rounds.

Comparison of the serial correlation measurements shows that the biggest discrepancy in the results was recorded under three rounds; this correlates with the relationship with the number of rounds conducted by the block cipher as the more iterations that are undertaken, the more uncorrelated the cipher-text output is from the original plain-text input. Information obtained from this test correlates with the aforementioned tests conducted with entropy and arithmetic mean of the cipher-text outputs following the same trend with the minimum number of rounds required to maintain the cryptographic strength of the AES-128 block cipher is three rounds in order to have uncorrelated cipher-text outputs.

Knowledge obtained from the entropy test correlates with literature presented by Adekunle and Woodhead; who specify the minimum number of round required to maintain adequate strength of the AES-128 block cipher is a minimum of three rounds. Further analysis of the AES-128 block cipher was undertaken with the investigation of the relationship between the number iterations selected to process the AES-128 block cipher and the latency incurred.

The test platform selected for this investigation was the emulated Mikroelektronika C compiler integrated development environment with the PIC18F45K22 selected as the microcontroller. Variables examined in this test were the latency of processing the AES-128 block cipher and the total number of instruction cycles required to complete the operation. Crystal frequency of 4 MHz was selected; message size of the plain-text input was set to sixteen bytes to measure the outcome of one block function call of the AES-128 block cipher; all measurements recorded was taken from the emulation. Figure 7.1 illustrates

the latency of the AES-128 block cipher with varying number of rounds configuration.

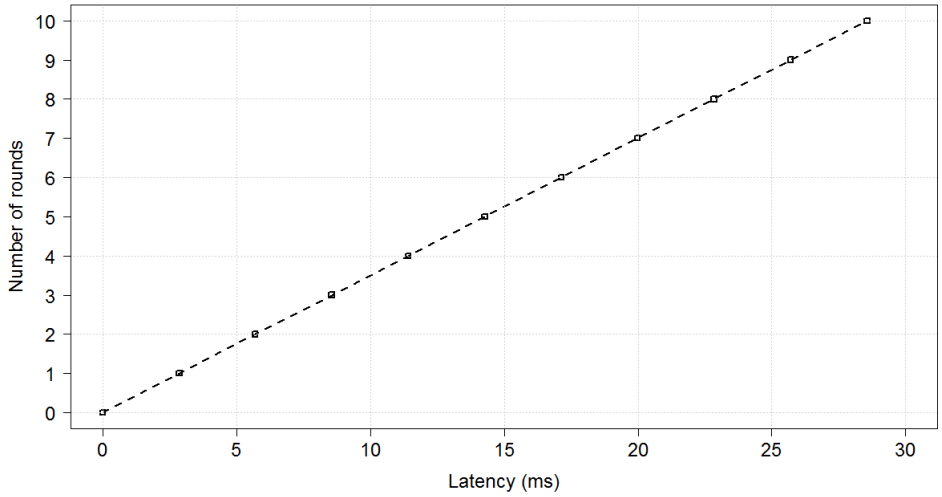


Figure 7.1: Relationship between the number of rounds used and the latency induced by the AES-128 block cipher.

Results presented in Figure 7.1 show that the increased number of rounds configured for the AES-128 block cipher has a positive correlation with the latency recorded with the highest number of rounds showing the biggest increase in latency recorded; this demonstrates that there is a cost of improving the statistical cipher-text output presented in Table 7.2 as the latency increases at a linear rate as the number of iterations selected is increased; therefore, the cost of improved cipher-text output in the context of real-time teleoperation and telemetry is increased latency.

Application of the findings to the problem scenarios specified in Chapter 3, Chapter 4, Chapter 5 and Chapter 6 indicates that the number of iterations configured for the underlying block cipher has a significant impact on all of the specified problem scenarios; this is because the general trend observed from the analysis conducted shows there is that the latency incurred by the block cipher at a higher number of iterations is increased; however, the increased number of rounds contributes towards improved metric for the cipher-text output in terms of entropy, arithmetic mean and serial correlation scores; this further reinforces the notion that there is a trade-off between the time required to process the cryptographic primitive and the metrics of the cipher-text output.

As the real-time nature of the research problem is a contributing factor towards the problem; the consequence of the findings would influence the formulated problem scenarios differently; in a static to static scenario, the impact is the additional processing overhead required to compute the message for a greater number of rounds used by the underlying

block cipher; the result of this additional latency is the increase in the worse case execution time as the actuator would require a longer duration of time to compute the real-time teleoperation and telemetry command and the reduction of the number of the instantaneous packet received in a given time period.

Findings presented in this section of the analysis supports the null hypothesis presented in this investigation is that the higher the number of iterations used by the AES-128 block cipher improves the cipher-text output metrics recorded as the number of iterations has improved the cipher-text metrics recorded; however, in this instance of the analysis, the real-time teleoperation and telemetry message size was fixed and it is unknown how the message size would influence the results identified; therefore, the next section examines the relationship of the entropy measurement of the cipher-text in relation to the message size selected for encryption.

7.2.3 Cipher-text Entropy of the Message Size

The test investigated the impact of the message size on the entropy of the cipher-text output. The test platform selected is the same as the aforementioned test scenario presented in section 7.2.1 and 7.2.2. The null hypothesis presented in this test is that the size of the message does influence the entropy measured for the cipher-text output. The alternative hypothesis presented in this test is that the size of the message does not influence the entropy measured for the cipher-text output.

Message sizes of sixteen, thirty-two, forty-eight, sixty-four, eighty, ninety-six, one hundred and twelve and one hundred and twenty eight bytes was selected with the number of iterations for the AES-128 block cipher was three and ten rounds. ECB mode was selected as the block cipher mode of operation. Metrics measured in this test were the entropy of the cipher-text output in relation to the message size. Figure 7.2 illustrates the results of the entropy record for varying messages sizes with AES-128 block cipher configured at three and ten rounds.

Results presented in Figure 7.2 show the rate of entropy gained in the cipher-text output for a message size under thirty-two bytes is greater with AES-128 at three rounds in comparison to AES-128 at ten rounds; sizes over sixteen bytes shows AES-128 at ten round configuration has a higher entropy score and continues to increase as the message size increases; this reinforces that the number of rounds influences the statistical characteristics of the cipher-text output. The relationship between the message size and the entropy score follows a logarithmic curve with a gradual increase as the message size increases for both AES-128 configurations of three and ten rounds; this shows the more bytes that are input into the block cipher the more entropy is obtained as there is a larger amount of

data to encrypt based on the observational analysis conducted.

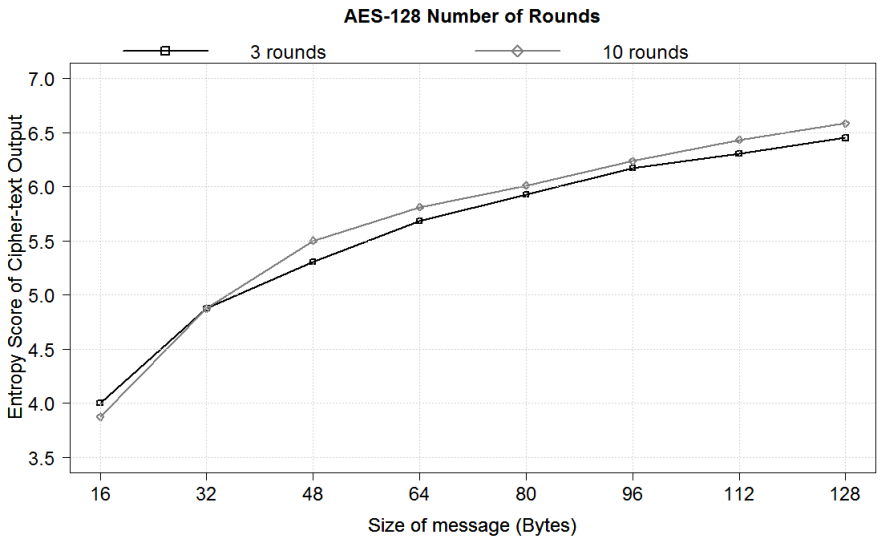


Figure 7.2: Entropy measurements recorded for the cipher-text output of different message sizes with three and ten round configuration of AES-128 block cipher

Examination of the relationship between the message size and the cipher-text entropy demonstrates that the increase in the message size does have an influence on the entropy measured for the same block size configuration; this is because the increased number of bytes in the message creates further uncertainty in the output as there is more information to process in order to ascertain if there is a distinct pattern in the cipher-text output; therefore, this supports the null hypothesis presented in this section.

Analysis conducted in this chapter has primarily focused on the components associated with the data path of the symmetric block cipher; however, the cryptographic key approaches applicable for symmetric block ciphers is required to be investigated as this provides the communicating entities with a shared secret in order to participate in secure communications.

7.3 Analysis of Cryptographic Key Approaches

The analysis of the key management stream investigated the strength of the cryptographic secret over the duration of the mission time and its resilience against a distributed online and offline brute force attack.

7.3.1 Analysis of Key Size against Brute Force Attacks

This section analysed the cryptographic secret of the block cipher; in this thesis, the secret is the cryptographic key selected to encrypt and decrypt communicated data between the

transmitter and the receiver. The null hypothesis presented in this investigation is that the longer length cryptographic key would increase the time required for attackers to locate the correct cryptographic key used for secure communications. The alternative hypothesis is that the longer length cryptographic key would not increase the time required for attackers to locate the correct cryptographic key used for secure communications. Mathematical analysis of the cryptographic key size was undertaken to analyse the relationship between the number of attacker required to brute force the cryptographic key search space using depreciation theory. Figure 7.3 graphs a depreciation of a 2^8 key space.

The data presented in Figure 7.3 shows the rate of depreciation for the cryptographic service is at its highest at the earliest point of time, with the depreciation following an exponential decay trend as the number of attackers is increased; this demonstrates that the linear increase in the number of attackers used, the search space of the cryptographic key follows an exponential decay as the number of searches are divided equally amongst the attackers; this is problematic as the attackers can conduct the brute force attack in parallel, therefore, the time required by a number of attackers to search all the possible cryptographic key candidates follows the exponential trend with a linear increase to the number of attackers.

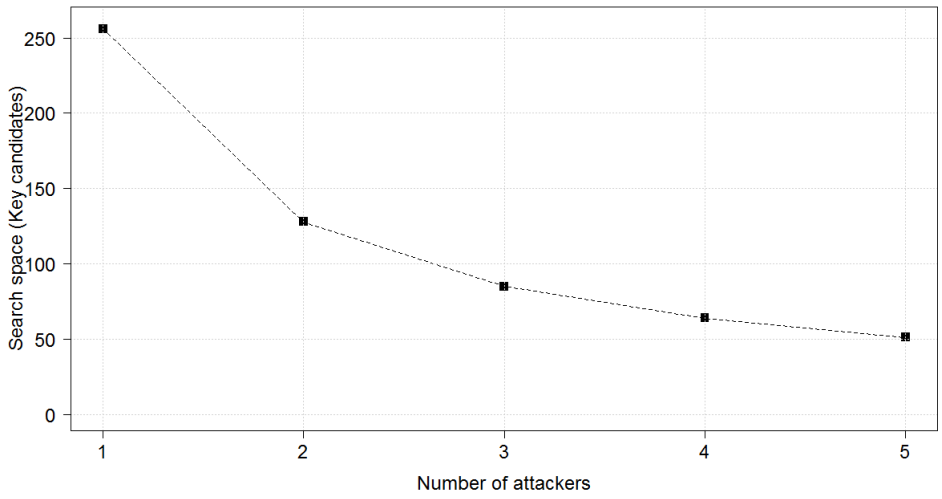


Figure 7.3: Depreciation of a 2^8 key search space in relation to the number of attackers used for a brute force attack.

The attackers could conduct on-site and off-site processing to conduct a brute force attack against the cryptographic key. With the quantity of resources available to the attacker remaining unknown to the defender, the probability of a successful attack is based on realistic resources is analysed. Analysis of the number of pre-computed searches conducted by the attacker before brute forcing the key space is conducted under the assumptions that the attacker has not undertaken any pre-computation, the attacker has conducted a

pre-computation of half of the key search space and that an attacker has pre-computed three quarters of the key search space; it is also assumed that the final key in the search space is the correct key value used for secure communications.

Accumulative probability and risk calculations are selected as the statistical methods to analyse the likelihood of the attacker finding the correct secret cryptographic key for a given search space. It is assumed that the attacker would locate the correct cryptographic key used within half of the known key search space and the search process is conducted using conditional probability. Figure 7.4 illustrates the number of attempts required by an attacker to brute force a 2^8 search space at different probabilities of the attacker knowing the search space.

The results presented in Figure 7.4 shows the number of known searches has an impact on the probability of an attacker successfully obtaining the shared secret with a brute force attack as the number of known attempts conducted by an attacker impacts the accumulative probability of the key being found. All trends presented in Figure 7.4 display characteristics of a polynomial trend which demonstrates that the probability of an attacker finding the cryptographic key fluctuates based on the key space known by the attacker as the more search space that is known to the attacker requires less attempts in comparison to an attacker who does not know a portion of the search space.

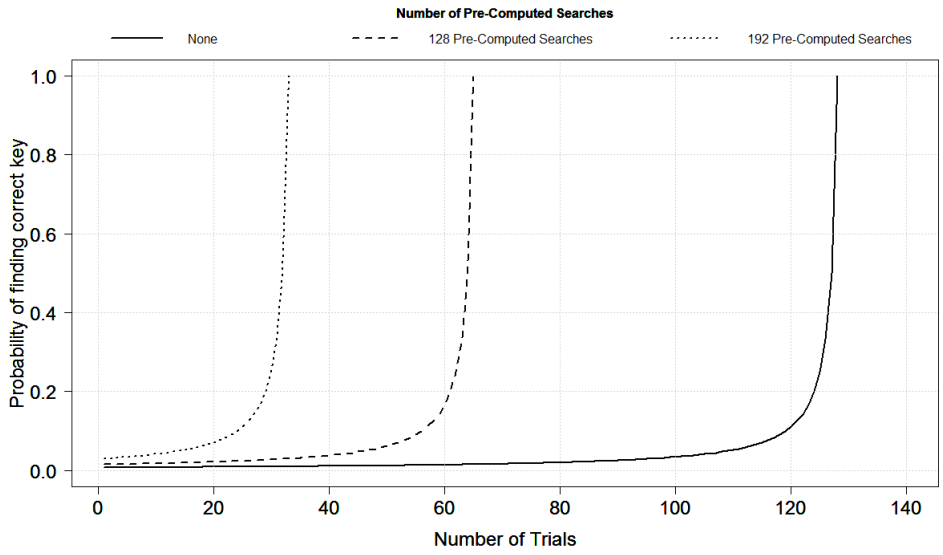


Figure 7.4: Number of linear searches required by an attacker to brute force all possible cryptographic keys for a 2^8 search space with accumulative probability.

A risk analysis was undertaken to quantify the risk of a perceived threat based on the threats, vulnerabilities and impact of a successful attack. The analysis of the risk was achieved with the NIST common vulnerability scoring system (CVSS); a quantitative

model that ensures repeatable accurate measurements while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. The information input into the CVSS is compared against the national vulnerability database that has scores for almost all known vulnerabilities. The formula used for the CVSS risk analysis calculation is presented in Formula 15.

$$R = T \cdot V \cdot I \tag{15}$$

Formula 15: The common vulnerability scoring system calculation (NIST 2017)

The categorisation of the risk has been scaled between zero, the risk of the attack is at its lowest and one, the risk of the attack is at its highest. Risk (R) is calculated by multiplying the likelihood of the threat (T) by the vulnerabilities (V) being exploited and the possible impact of the attack against the system (I). The results for this test assumed that the impact on the system is set to one as the system would be compromised. To ascertain the risk of an online and offline brute force attack on the cryptographic key space; Table 7.3 tabulates the risk analysis of a brute force attack for online and offline attack for a 2^8 search space.

Table 7.3: Risk analysis of an online and offline brute force attack against a 2^8 key search space

Independent Variable	**Dependent Variable**	
Attack type	**Online**	**Offline**
Risk Score	0.4	0.8

The data displayed in Table 7.3 shows the offline brute force attack has a higher risk probability than the online brute force attack; this is because the number of dedicated machines used to search a key space in an online attack in the same vicinity as the system is reduced in comparison to an offline, off-site cluster; in addition, the computational power of an offline attack enables the attacker to pre-compute searches in a paralleled operation; whilst online attacks are constrained to limited resources and sequential operation. To showcase how the online and offline attack impacts the cryptographic key space, Formula 16 integrates the search time required to find the key by the number of resources in a given time period.

$$T = \frac{K_s}{(A_s \cdot A_m)} \tag{16}$$

Formula 16: Calculation of time required to obtain all possible cryptographic keys searches based on attackers resources and search space.

The time required to search the total key search space (T) is calculated by multiplication of the number of searches the attacker can perform in a given time period (A_s) by the number of computational devices that the attacker has access to conduct the attack (A_m). The total search space of the key size (K_s) is divided by the sub-total of $A_s \cdot A_m$ to derive T. Table 7.4 tabulates the time required for an attacker to search through a 2^{32} key space at a processing frequency of 1 GHz, 2 GHz and 3 GHz with varying quantity of attacking machines.

Table 7.4: Time to conduct an online and offline brute force attack against a 2^{32} key search space at 1 GHz, 2 GHz and 3 GHz processing frequencies.

Independent Variable	**Dependent Variables**		
Number of Machines	**1 GHz**	**2 GHz**	**3 GHz**
1	33.88	16.94	11.30
10	3.38	1.7	1.11
100	0.33	0.17	0.11
1000	0.03	0.01	0.01

Findings presented from the analysis of the key size in relation to a brute force attacks shows that the number of resources and the processing frequency of the resource are contributing factors towards the time required to attempt all particular searches in a given space; this problem is further exemplified in situations where an attacker conducts an offline brute force attack against the system in order to compromise the cryptographic services; this therefore supports the null hypothesis presented in this investigation that the longer length cryptographic key would increase the time required for attackers to locate the correct cryptographic key used for secure communications.

Real-time teleoperation and telemetry systems using a secure communication link are susceptible to brute force attacks and require consideration in terms of the crypto-period the key is used; what key management methodology is suitable for the context and how the key management method would impact on the real-time nature of the systems presented in the problem scenarios.

Research identified in the preliminary Literature review in Chapter 2 presents two symmetric key management methods that have been deployed in cryptographic system; methods include the static key, where the cryptographic key value is fixed for the entirety of its operation and the pre-computed key method which rotates between cryptographic keys in fixed period intervals. The next part of the problem analysis investigates the suitability of the identified approaches and if the contemporary cryptographic key methods are applicable to provide a component to the secure communication link of real-time teleoperation and telemetry.

7.3.2 Approaches to Cryptographic Key Implementation

The investigation of the different key implementations used for secured communication links and how the approach chosen impacts the privacy of the secret between the communicating devices on the link was analysed. The two key implementations methods analysed in this section are a single key and pre-computed keys. The null hypothesis presented in this investigation is that the single cryptographic key will be located by the attacker in a shorter period of time in comparison to the pre-computed key method. The alternative hypothesis is that the single cryptographic key will not be located by the attacker in a shorter period of time in comparison to the pre-computed key method.

Mathematical analysis of the two approaches was conducted to determine the privacy of the shared cryptographic secret over a period of time. It is assumed for this test that the cryptographic key length is set to 2^8 bits in length with the probability of an attacker brute forcing the key in half the search space. It is also assumed that the pre-computed keys selected use a maximum of four pre-stored keys for the mission duration. The measurement recorded the number of searches conducted by the attacker. Figure 7.5 illustrates the comparison of the attacker profile for the number of searches required to brute force a static cryptographic key and a pre-computed rotated cryptographic key method.

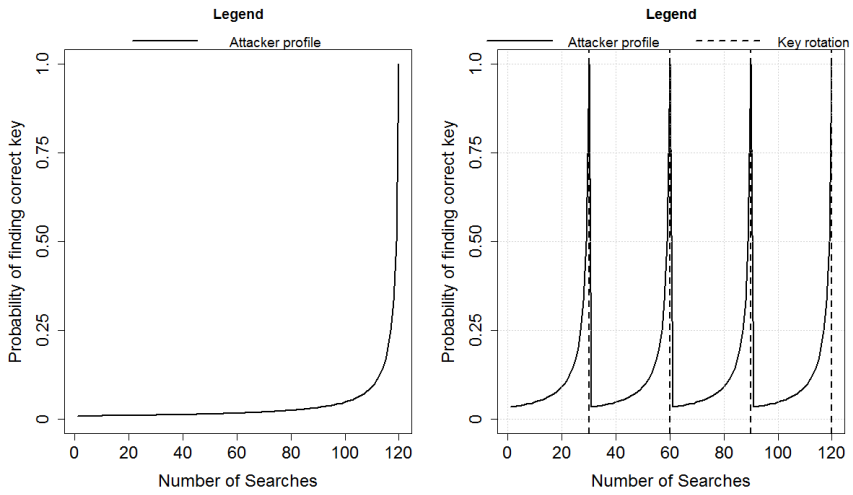


Figure 7.5: Number of searches available to an attacker with static key implementation (left) and pre-computed key implementation (right) on a 2^8 search space over a two hours mission duration.

Information obtained from the findings presented show that the pre-computation and rotation of the cryptographic key has a beneficial impact on the privacy of the shared secret of the secure communication link as the rotation of the pre-computed key resets the attacker to try all possible keys whilst a static implementation of the cryptographic key validates all of the attackers attempts as the cryptographic secret does not change. A limitation of

this approach is that the attacker could conduct a parallel attack against all pre-computed keys used for the secure link in combination with frequency analysis as the rotation of the keys are periodical.

Analysis of the number of key regenerations required to maintain the cryptographic strength of the shared secret was analysed through mathematical modelling with focus on the examination of the number of new cryptographic keys required over a mission duration. Formula 17 presents a mathematical formula has been derived to calculate the number of key regenerations that are required for the mission time specified.

$$K_g = \frac{(M_d \cdot T)}{P} \tag{17}$$

Formula 17: Calculation of the number of key regenerations required over a mission duration

Notation of the key regeneration calculation is as follows; first the number of key regenerations (K_g) is calculated by finding the sub-total of the time to search the key space (T) derived from Formula 16 in section 7.3.1 and is multiplied by the specified duration of the mission duration that the cryptographic service is used (M_d). The sub-total is divided by the probability of the attacker finding the correct cryptographic key in the search space (P).

The mathematical formula presented in Formula 17 was used to calculate the number of key regenerations required to mitigate an attacker obtaining the cryptographic secret over a specified mission time. Cryptographic key sizes of 64-bit, 128-bit and 256-bit lengths were selected to reflect instances of key lengths used by the standardised block ciphers. Preliminary test undertaken on a real-world test platform demonstrated that the number of cryptographic key searches undertaken by a PIC18F45K22 microcontroller at a crystal frequency of 1 MHz was 2,112 searches per minute; therefore, it is assumed that an attacker conducting a distributed offline brute force attack against the cryptographic key with machines operating at 3 GHz crystal frequency would conduct 6,336,000 key searches per minute as the relationship between the processing frequency and the time required to compute the same number of instruction cycles follows a linear profile as identified by aforementioned tests undertaken throughout the problem analysis undertaken of this thesis.

It is also assumed that the probability that the key is found in half of the cryptographic key search space is true. Table 7.5 tabulates the number of attacking machines required

to search half the cryptographic key space under a distributed offline brute force attack at 3 GHz crystal frequency and a search rate of 6,336,000 searches per minute.

Table 7.5: Number of modelled computational resources required by an attacker to search half the cryptographic key space for a two hour mission time at a 3 GHz crystal frequency.

Independent Variable	**Dependent Variable**
Cryptographic key-size (bits)	**Number of attacking machines required**
64	6
96	370,205
128	2.4×10^{10}
192	1.0×10^{20}
256	4.4×10^{29}

Results presented show that the size of the cryptographic key has an influence on the number of attacking machines required to search through the required search space in a mission time of two hours as the 64-bit key size has the least computational nodes required in comparison to 128-bit and 256-bit key sizes. To determine the number of key regeneration required by a 64-bit key to match the equivalent searches required by a 128-bit and 256-bit key; Table 7.6 tabulates the number of key regenerations required to match the same number of searches required for a 128-bit key and 256-bit key.

Table 7.6: Number of key regenerations required by a 64-bit key to have an equivalent search space of a 128-bit and 256-bit cryptographic key for a two hour mission time.

Independent Variable	**Dependent Variable**
Equivalent key size search space (bits)	**Number of key regenerations**
128	1.8×10^{19}
256	6.1×10^{57}

Data presented in Table 7.6 shows the number of key regenerations required for a 64-bit key to match the equivalent resilience for the same brute force attack follows an exponential growth pattern; this is because the number of key regenerations required to replicate the total search space of 128-bit and 256-bit key size is increased by a factorial amount. Analysis of the results presented show a correlation between the number of times a key is regenerated in order to achieve the same number of searches as a longer key size; however; with the increasing prevalence of supercomputers many security agencies may have the computational ability of three million central processing units operating at a frequency of 2 GHz (Cray 2017); the time required to search all possible key spaces would be reduced. Figure 7.6 illustrates the time required to search the half of a 64-bit key search space with varying quantities of supercomputers.

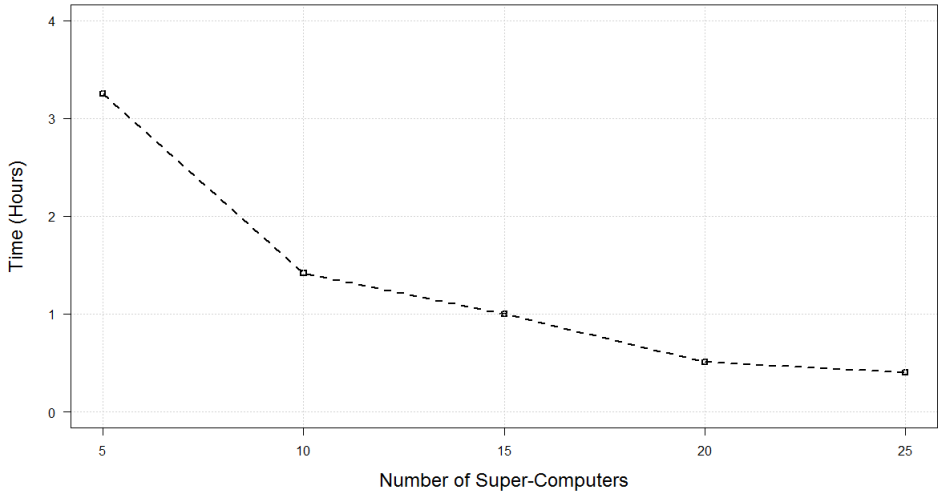


Figure 7.6: Time required to search half of a 2^{64} key space with a varying number of supercomputers.

Results of the calculation undertaken show that the minimal number of super-computers required to brute force half of a 2^{64} key search space is equivalent to ten super-computers in a two hour mission time; this infers that an offline brute force attack against the cryptographic key is possible with the probability of the attacker findings half of a 128-bit key within the mission time of two hours with the increasing number of super-computers operating in parallel.

Information acquired from the analysis of the brute force attack against a 2^{64}search space demonstrates that it is feasible for the attacker to search half of the possible cryptographic keys used for the secure communication link in the specified mission time with commercial computational resources as stated in 7.5 based on the assumption that an attacker is likely to locate the correct cryptographic key within half of the maximum key; this shows that a key size of 2^{64} is not best suited for the context examined as it would be feasible for the attacker to acquire the key in the specified period of time under a distributed offline brute force attack if static or pre-computed key management techniques are deployed as demonstrated in Figure 7.5.

In the context of the static to static, static to mobile and mobile to static case scenarios throughout the problem analysis chapters; the 2^{64} with the current key implementation techniques would not be suited for the scenarios specified; this is because it is possible to locate the cryptographic key used in a feasible period of time; however, this key size could be applicable if a new key implementation method is deployed to maintain the strength of the symmetric cryptographic key used by the transmitter and receiver device and increase the time required by an attacker to search and attempt all possible cryptographic key com-

binations.

A key length of 128-bits is recommended to fully mitigate a brute force attack as the attacker would require an extensive number of commercial resources to attempt half of the possible key values of the key length; this scenario is exemplified in the following scenario where every person on the planet owns ten computers; there are seven billion people on the planet, each of these computers can test one billion key combinations per second. On average, you can crack the key after testing 50% of the possibilities; then the earth's population can crack one encryption key in 77,000,000,000,000,000,000,000,000 years (Arora 2012). In addition to the time required to compute all possibilities for a 128-bit key, the probability of an attacker gaining access to a number super-computer resources is remotely limited as the cost of the resource and ease of access reduces the probability that an attacker could implement this attack strategy.

Application of the findings presented for the analysis of the cryptographic key size used for the block cipher shows that a static key implementation depreciates at a exponential rate as the crypto-period of the key increases; from an attackers prospective, this improves the probability of a successful brute force attack against the key search space the longer it is used. Pre-computed approaches reduced the time required by the attacker to search the key space before the cryptographic secret is rotated and limits the depreciation of the key over the cryptographic period; however, the memory constraints associated with the devices used for real-time teleoperation and telemetry impacts on the feasibility of using this approach (e.g. ten pre-computed 128-bit keys requires 160 bytes of memory).

Consideration of asymmetric key management methodologies specified in Chapter 2, section 2.9 are not best suited in the context of real-time teleoperation and telemetry as existing literature presented in section 2.15 by Kounev et al and Mundhenk et al; have identified that the latency measurements recorded for asymmetric key management schemes can vary up to the seconds range; in the context of the real-time application, the additional latency would have a significant impact between the acquisition of the telemetry and the initiation of the teleoperational commands; furthermore, the computational and memory constraints of a microcontroller device would make it unfeasible to deploy a asymmetric key management approach.

The relationship between the number of attackers searching the cryptographic key spaces and the perceived strength of the cryptographic key follow two different relationships with a linear trend for the number of attackers required to perform the operation; whilst the number of searches required by each attacker decreases at an exponential rate as the portion of the number of searches required by each individual attacker is reduced as the

quantity of attackers increases. This is further exemplified with the implementation of offline parallel attacks against the key search space as a search space of 64-bits can be searched in a two hour mission time; therefore, it is feasible to compromise the shared secret between the transmitter and receiver device and manipulate the real-time teleoperation and telemetry data. Repercussions of this can result in the operation and monitoring of the static or mobile platform to be unresponsive or misused to the attackers desires.

7.4 Discussion

The relationship between the number of rounds selected by the AES-128 block cipher and the metrics measured for the cipher-text output contributes to the statistical metrics of entropy, arithmetic mean and serial correlation scores of the cipher-text. The knowledge obtained from the analysis undertaken of the standardised cryptographic primitive AES-128 shows that the entropy value of the cipher-text output reaches its maximum value at five rounds; however, the AES-128 block cipher with under three rounds shows that the metric of the cipher-text output is significantly reduced in terms of entropy, arithmetic mean and serial correlation.

Increasing the number of rounds for the AES-128 block cipher, results in an increased latency and energy usage; consequently, the limited energy supply of transmitter and receiver devices used for real-time teleoperation and telemetry would deplete quicker in comparison to an AES-128 variant using a reduced number of rounds; therefore, the operational lifetime of the device is reduced as a result of the higher number of rounds selected. The impact of the configuration of the cryptographic service impacts the operational performance of the mobile-end point as the increased latency results in additional distance travelled by the mobile platform; therefore, the mobile platform travels further before responding to the teleoperation command, this has an increased energy usage for the additional distance travelled and has a less sensitive and responsive control.

The findings impact real-time telemetry as the number of samples obtained with cryptographic services is reduced as the time required to process the message increases; this is particularly noticeable for the real-time telemetry capture of sensed data as the additional latency resulted in the observed pronominal not being measured. The quantity of real-time telemetry data contributed to the problem with the size of the real-time telemetry data sent between the transmitter and receiver impacts the time required by the cryptographic service to encrypt and decrypt the data as the number of calls required by the block cipher increases; therefore, instruction cycles need to be processed quicker.

Knowledge obtained from the literature review and the problem analysis demonstrated

that contemporary cryptographic services are not best suited for the application of real-time teleoperation and telemetry. Lightweight block cipher designs identified in the literature review were designed with the priority of providing communication security whilst reducing the energy consumption and hardware area consumed as demonstrated with the NIST standardised lightweight block cipher PRESENT. The PRESENT block cipher scheme and alternative lightweight block ciphers designed with these constraints are benchmarked in term of there performance in terms of latency and throughput by the National Institute of Standard and Technology (NIST) (NIST 2017); however, the concentration of these block cipher designs is directly related to the hardware characteristics of the design; benefits of the outcome implementation have been specified in Chapter 6, section 6.2.5 and are outside the scope of this research as the focus is on software implementation approaches.

Examination of contemporary lightweight software AEAD ciphers designs and their impact on the performance metrics of systems has been disseminated throughout Chapter 3, Chapter 4 Chapter 5 and Chapter 6. Knowledge obtained from the preliminary analysis shows that the processing cost of the AEAD design contributes in the increased latency, reduction in instantaneous packet throughput recorded and greater energy consumption as presented in Chapter 3 section 3.4 and Chapter 6, section 6.2.3; this correlated with findings presented in the literature review that contemporary block cipher designs that were designed with energy conservation as priority have a reduced impact in comparison to design that prioritised the security service; consequently, a by-product is the reduced number of instruction cycles and latency as demonstrated in section 7.2.1. The result of this impact influences the teleoperation in terms of its response as presented in Chapter 4, section 4.5.1, Chapter 6, section 6.3.1 and telemetry as presented in Chapter 6, section 6.3.3; therefore, the findings indicate that it is possible to provide a secure communication link whilst adhering to the the real-time nature of the context examined; however, the requirement to prioritise the speed of the block cipher is of importance in order to achieve a reduced impact on the operational performance of real-time teleoperation and telemetry systems.

The length of the cryptographic key used for the block cipher has a correlation with the time required by an attacker to brute force the search space of the cryptographic key; however, the current method of key management is to select a static, fixed sized cryptographic key or to add a pre-computed fixed quantity of keys that are rotated to frustrate the attacker. The analysis presented shows that the depreciation of the cryptographic strength of the key occurs as the duration of the mission increases; in addition, the probability of an attacker finding the correct key is half the size of the cryptographic key size. As the attacker can conduct both online and offline attacks to brute force the cryptographic key

used by the block cipher, the static and fixed nature of the cryptographic key implementation would increase the probability of a successful brute force attack as demonstrated in sections 7.3.

Implementation of a pseudo-random key rotation method could be applied to this context to variate the selection of the pre-computed keys; however, the limitation of this method is that the keys themselves do not change, only the selection of the keys; this is problematic as the secret between the communicating entities is not renewal but is reused; this could enable an attacker to resume a brute force attack against when the key selection is changed; in addition, the ability to increase the number of keys stored on the microcontroller device for selection is not viable as the limited computational processing would impact on the operational performance of the system as identified from the aforementioned analysis of the contemporary cryptography in real-time teleoperation and telemetry and the limited memory of microcontroller devices makes this method infeasible as each key would require sixteen bytes of storage. A requirement obtained from the examination of the cryptography is for an random like behaviour of the key scheduler and the regeneration of the cryptographic key in order to to renewal the shared secret between the communicating entities without impacting on limited computational constraints and obfuscate the attacker from deriving deterministic patterns in the key scheduler.

7.5 Knowledge Derived from the Problem Analysis

Knowledge obtained from the problem analysis conducted demonstrate that the multi-faceted problems investigated lead to the question of how to reduce the latency incurred by the cryptographic service whilst maintaining secure communication for the crypto-period of the real-time teleoperation and telemetry messages.

The profiling of the AES-128 block cipher disseminated knowledge about the relationship between the number of rounds used by the block cipher and the entropy metric of the cipher-text output, this reinforced that the number of rounds selected for the block cipher determines how random looking the cipher-text output is as a measure of security and the reduction of the number of iterations selected has a reduced impact on the latency recorded at the cost of the reduction in the entropy score given for the same length cipher-text output.

Examination of the number of instruction cycles required by each component of the AES-128 block cipher identified that certain cryptographic function incur a considerable large proportion of the total number of instruction cycles required in order to process the cryptographic operation and consequently constitute to the largest proportion of time required

to process; examination of the impact of secure communications on the mobile actuator demonstrates that there is a considerable impact the sensitivity and responsiveness of the mobile vehicle as the additional distance travelled is dependent on the latency incurred by the cryptographic service and the fixed speed of the mobile actuator.

A method of mitigation is to increase the operational flight height of an aerial UAV or reduce the speed of an mobile actuator to compensate for this latency; however, this may not be feasible in situations where stringent regulations (e.g. CAA) do not permit operation of an mobile actuator outside certain parameters; therefore,this infers that there is scope for further research to reduced the number of instruction cycles required by the cryptographic operators in order to meet the constraints associated with real-time teleoperation and telemetry communications.

The analysis of the AES-128 block cipher cryptographic key lengths differed from the first requirement to enhance the speed of the cryptographic service but instead ascertain how the cryptographic key contributes towards the block cipher operation and its role in the block cipher mechanism.

Knowledge obtained from the investigation of the cryptographic key lengths in relation to its resilience to brute force attacks demonstrates that the role of the cryptographic key can be viewed as the shared secret for the transmitter and receiver device that participate in communications using a symmetric block cipher; this is because both communicating entities require the same cryptographic key in order to successfully act upon communicated messages; therefore, if an attacker had prior knowledge or was able to obtain the cryptographic key in the crypto-period, the attacker would be able to conduct passive and active attacks on the systems; an instance in the problem scenarios derived is the interception of telemetry feeds for reconnaissance and retransmit falsified data to the receiver node or conduct a similar man-in-the-middle attack on real-time teleoperation data to manipulate control of the static or mobile actuator.

The investigation cryptographic key lengths used by the underlying block cipher showed that reduced cryptographic key lengths is susceptible to a brute force attack for the duration for a tactical real-time application dependent on the number of resources at the attackers disposal.

Mitigation of the brute force attack can be achieved by utilising a specific portion of the key length for secure communication; however, this approach is still susceptible to the brute force attacks undertaken in this analysis; therefore, a feasible solution for the context investigated in this thesis is the regeneration of the cryptographic key used by

communicating entities to maintain the privacy of the shared secret and force the attacker to attempt all possibilities.

7.6 Specification for Proposed Philosophy

Based on the knowledge obtained from the problem analysis undertaken; a proposed philosophy to solve the problem brief must consider the following:

- To propose a novel philosophy that prioritises the speed to process the block cipher operation in order to reduce the impact of latency on real-time teleoperation and telemetry applications.
- Derive a novel approach to block cipher design based on the new novel philosophy proposed with an exemplar instance.
- To propose a novel philosophy that prioritises the maintenance of the ephemeral secret between the transmitter and receiver device to frustrate an attacker from successfully brute forcing the shared secret used for secure communications.
- Derive a novel approach to key management schemes that creates unpredictability in the behaviour of the key rotation and key regeneration mechanism in order to prevent adversaries obtaining the shared secret between the communicating entities.

7.7 Chapter Summary

The chapter presented the analysis undertaken of the contemporary standardised cryptographic block cipher AES-128 with profiling of the instruction cycles required to process the operation, statistical analysis of the relationship between the number of rounds configured for the block cipher and the metrics of the cipher-text output and the energy usage of the block cipher. Findings presented demonstrate that three of the four cryptographic functions used by AES-128 contribute a third of the overall number of instruction cycles.

The increased number of rounds configured for the AES-128 block cipher contributed to the statistical improvement of the cipher-text output; however, the energy usage and latency incurred from the process also increased as a result of increased number of rounds used; consequently, impacting the real-time teleoperation of the mobile device and the data samples obtained from the real-time telemetry. Hardware implementation methods overcome the issue of the latency on real-time teleoperation and telemetry but are not an adaptive or flexible approach to secure communications as the configuration is fixed throughout the mission duration.

Analysis of the symmetric key management approaches used for block cipher cryptosystems demonstrates that the current approaches of a static or pre-computation of cryptographic keys are susceptible to a brute force attack as the probability of achieving a successful parallel brute force attack is high and depends on the number of resources available. The specification for the proposed new philosophy was derived to overcome the limitations of contemporary approaches in relation to the problem context. The next chapter introduces the proposed philosophy based on the specifications derived from the problem analysis with the presentation of the cryptographic synergy philosophy.

8 Proposed Novel Philosophy: Cryptographic Synergy (Intrinsic)

8.1 Introduction

This chapter introduces the cryptographic synergy philosophy to address the real-time constraints associated with real-time teleoperation and telemetry and secure data communications between the transmitter and receiver and derives two novel approaches as instance to address the problem investigated. The problem identified from the problem analysis conducted in Chapter 3 Chapter 4, Chapter 5, Chapter 6 and Chapter 7 demonstrates that contemporary software security approaches are not best suited for this context as it has an impact on the operational performance on a real-time teleportation and telemetry device; therefore, the question proposed in this section of the thesis investigates how to prioritise the speed of the block cipher whilst maintaining privacy of the shared secret for secure data communications.

The structure of this chapter is as follows; first, synthesis of the cryptographic synergy philosophy is presented in section 8.2; followed by the proposed speed-centric concept derived from the cryptographic synergy philosophy in section 8.3. Discussion of the composite concept is presented in section 8.4.2; followed by an instance of the intrinsic cryptographic synergy philosophy methodology with the Lightweight Entropy Operations Permutation Addition Rotational Dispersion (LEOPARD) block cipher presented in section 8.4.3. A cryptanalysis of the LEOPARD block cipher derived from the proposed s philosophy is presented in section 8.5. A discussion of the findings are presented in section 8.6. A chapter summary concludes in section 8.7.

8.2 Synthesis of the Novel Cryptographic Synergy Philosophy

The knowledge obtained from the problem analysis Chapter 3, Chapter 4. Chapter 5, Chapter 6 and Chapter 7 demonstrates that real-time teleoperation and telemetry are influenced by a number of variables that impact the operational performance of the system. In this thesis the multi-faceted research problem is divided into four sections which are presented in Figure 8.1.

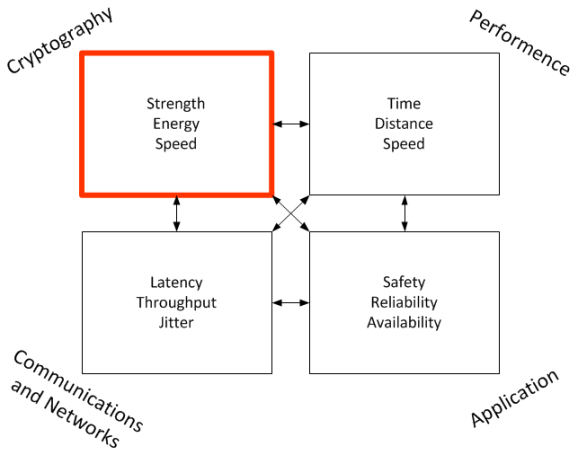


Figure 8.1: Overview of the multi-faceted research problem, the bold square is the emphasis of the solution.

The four sections presented in Figure 8.1 contribute to the problem domain as examined throughout Chapter 3, Chapter 4, Chapter 5, Chapter 6 and Chapter 7. The cryptography category considers the characteristics of the block cipher; the communication and network section prioritises factors linked to packet throughput and packet arrival. The performance category analyses the problem from the prospective of the physical actuator and how it operates (i.e. UAV); finally, the application section considers the impact of the configuration of the aforementioned sections on the context dependent scenario.

The focus of the problem investigated in this chapter examines the cryptography used for secured communications in real-time teleoperation and telemetry as the impact of the additional latency incurred from the contemporary security services examined influenced the other three categories in terms of reduced instantaneous packet throughput, operation of the actuator and the consequences in static and mobile scenarios; therefore, the proposition of the cryptographic synergy philosophy is presented to prioritise the speed of the block cipher to process the operation in the data path of the block cipher whilst maintaining the privacy of the shared secret utilised for secure data communication between the transmitter and receiver.

The cryptographic synergy philosophy is derived from the Greek philosopher Aristotle who stated "*the whole is greater than the sum of its parts*". The interpretation of this philosophy is the individual parts that are connected together to form one entity are worth more than if the parts were in silos; in this instance, the interlinking of security services (i.e. services that mutually support each other).

The novelty of the proposed cryptographic synergy philosophy presented in this thesis is the interlink between the underlying block cipher and the privacy of the shared secret used

for secure communication. This is because the time required to process the underlying block cipher can be reduced without the drawback of unsecure communications as the privacy of the shared secret (i.e. cryptographic key) can be regenerated accordingly to maintain the privacy of data communications whilst meeting real-time constraints.

In the context investigated in this thesis, this philosophy is presented in two parts to address the problem statement specified. An overview of the cryptographic synergy philosophy is shown in Figure 8.2.

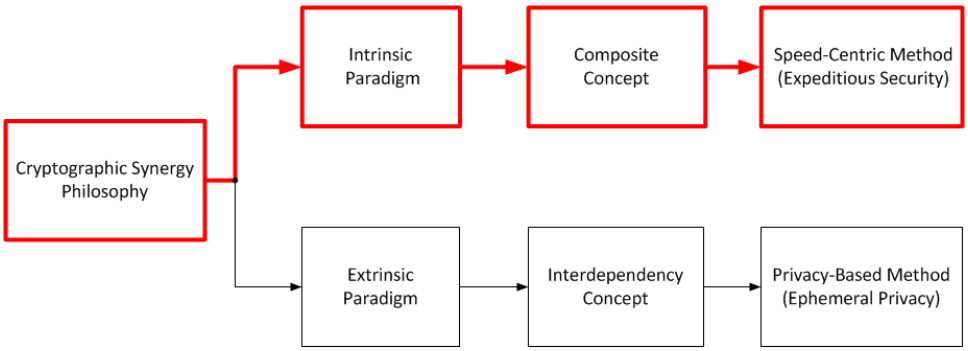


Figure 8.2: Overview of the proposed philosophy (emphasis on the intrinsic paradigm in this chapter in red)

Presentation of the cryptographic synergy philosophy is achieved with the presentation of intrinsic and extrinsic paradigm; in this section of the philosophy, the intrinsic paradigm is discussed as highlighted in Figure 8.2. Details of the extrinsic paradigm are located in Chapter 9.

The intrinsic paradigm is derived for the internal operation of the security services with the focus of reducing the processing overhead of the security service required for a given scenario. In this thesis, the intrinsic paradigm has been utilised reduce the processing latency of the underlying block cipher providing confidentiality and integrity services for real-time communication. The concept derived to achieve the intrinsic paradigm is the composite concept.

The composite concept presented in this thesis is the combination of two or more specialist cryptographic primitives into a generic cryptographic primitive. Output from the composite concept facilitates the design and implementation of cipher designs that prioritise the speed of the security service (a.k.a speed-centric method) to facilitate expeditious security services. Explanation and rationale of the speed-centric concept derived from the intrinsic section of the cryptographic synergy philosophy is discussed in the next section of this chapter.

8.3 Synthesis of the Speed-Centric Method

8.3.1 Conceptual Paradigms of Contemporary Philosophies for Cipher Designs

The classifications of contemporary paradigms relevant towards the research scope are classified into three sub-categories of strength, energy and speed. The strength paradigm prioritises the perceived strength of the cryptographic primitives and is established as a practised philosophy in current research (McGrew & Viega 2007, Ferguson 2005, Rogaway et al. 2001). Strength is defined as the capacity of an object or substance to withstand great force or pressure, whilst the definition of security is the state of being free from danger or threat; in the context of cryptography, this is transferred to the design, configuration and selection of the block cipher used. Current standardised approaches investigated in the literature review and problem analysis place emphasis on the importance of the cryptographic strength of the cryptographic construct with the NIST 800-57 standard specifies a hundred-and-twelve-bit key length as acceptable strength to provide the required security level (Barker 2016*a*); however, in the context of a real-time teleoperation and telemetry, the time to transmit, propagate and receive a message over a communication link requires a specific amount of time to complete.

The energy philosophy prioritises the energy conservation of the operating device to extend its operational life. This philosophy has links to philosopher such as Jones' law of conservation of energy theory which states that the energy of a system can not be created or destroyed but can be converted from one form to another (Lehninger 1971). The energy paradigm has been introduced for AEAD constructs with Adekunle and Woodhead who presented the Joint Cypher Mode (JCM) framework and an instance of the framework with the TinyAEAD construct. The philosophy presented by Adekunle and Woodhead with the JCM framework concentrates on the time required to undertake the cryptography and not on the application.

From the two paradigms presented the strength philosophy priorities the strength of the cryptographic primitive with a low priority given to the speed and energy consumption; whilst the energy philosophy gives low priority to the strength of the cryptographic primitive by reducing the number of iterations (i.e. rounds) used by the cryptographic primitive, this decreases the energy consumption of the device as a lesser number of instruction cycles are processed and a by-product of this philosophy is the increased speed of the cryptography.

Analysis of the two philosophies in the context of real-time teleoperation and telemetry demonstrates that the strength and energy paradigms were not considered for real-time teleoperation and telemetry as speed was not explicitly prioritised; therefore, the pro-

posed paradigm in this thesis prioritises speed at the prominent factor; speed has been classified as the most important factor because; firstly, the time constrained nature of real-time teleoperation and telemetry must be met to ensure safety, reliability and availability of the system; secondly, to limit the impact on the operational performance of the real-time teleoperation and telemetry between the human controller and the actuator.

An element of strength must be present to mitigate attack vectors whilst having a minimal impact on the latency and limited energy resources. The strength and energy philosophies have shown that there is a trade-off between these three variables as changing the priority of the system has a direct influence on the priority of the variables. A quote derived by Paul Virilio, a philosopher of speed states that "Today, everything is about speed and real time. We are no longer concerned with real space" (Borjian 2017). As the requirements for real-time teleoperation and telemetry has been specified with the proposed speed-centric paradigm, the current thinking of the way the three variables are fulfilled must be changed to overcome the research problem presented.

To achieve the specified requirements outlined in the proposed philosophy, the categorisation of the variables have been categorised into two sections, service and security. The variables that are categorised into service are speed and energy as these requirements must meet the quantitative requirements of the research problem; cryptographic strength has been associated with security as the perceived strength of the security measured is based on the application of the real-time teleoperation and telemetry; this is because the constraints of the real-time teleoperation and telemetry is context dependent.

The common link between the variables identified is time; as the measurement of energy consumption or speed to complete a task is measured over a duration of time; the strength of the security measure is linked to time as the cryptographic design must be durable for the duration of the operation, known as the crypto-period. Consideration of time in the existing philosophies does not explicitly account for the requirement of time with the instances of the strength paradigm considering the performance metrics of the cryptographic primitive; whist the energy philosophy implicitly accounted for time through reduced iteration of the cryptographic primitive; therefore, in this thesis, the speed-centric method explicitly incorporates the time paradigm as the main cornerstone between the three areas to balance human reaction and machine operation.

Approaches to implement the speed-centric method can be achieved using two methods; the first method is to reduce the number of iterations used by the block cipher in order to increase the speed of the cryptographic service as demonstrated by Adekunle and Woodhead with the reduction of iterations used by AES-128 in the TinyAEAD construct; how-

ever, knowledge obtained in the problem analysis demonstrates that further improvement is required to reduce the impact of the cryptographic service on the real-time teleoperation and telemetry communications. The alternative method is to reduce the number of instruction cycles required by the block cipher components to process the cryptographic operation as tests conducted in Chapter 7, section 7.2.1 demonstrate that some components require a significantly greater number of instruction cycles to process the operation and consequently increases the latency to compute; therefore, the speed-centric method proposed in this thesis examines how to reduce the processing time of the individual components used by the block cipher whilst providing a secure service.

The consideration of the proposed philosophy derived from the specification presented in the problem analysis undertaken in Chapter 3, Chapter 4. Chapter 5, Chapter 6 and Chapter 7 states that the constants associated in real-time teleoperation and telemetry with consideration for security services to mitigate attack vectors for the specified period of operation. An instance of fulfilling this criterion is derived into two sections; (1) the structural arrangement of a contemporary block cipher (i.e. AES-128) and (2) the composite concept.

8.4 Instance of the Speed-Centric Method

This section of the philosophy chapter introduces the instances of the methods selected to fulfil the speed-centric method. This section is divided into three sections; the first section introduces the structural arrangement of contemporary block cipher with the presentation of two new structural designs with the presentation of the permutation substitution network (PSN) and the permutation substitution permutation network (PSPN). The second section presents the synergy paradigm derived to reduce the number of instruction cycles required by the block cipher to process the cryptographic operation whilst maintaining the security of the cipher-text output. The final section presents an instance of the speed-centric method using the novel approaches with the introduction of the Lightweight Entropy Operations Permutation Addition Rotational Dispersion (LEOPARD) block cipher that was designed with the consideration for speed as the main priority.

8.4.1 Structural Arrangement of Contemporary Block Ciphers

This section of the philosophy investigates if the speed-centric method is achieved by changing the structural arrangement of the block cipher. The substitution permutation network (SPN) structure is used by the standardised NIST AES-128 block cipher; alternative cryptographic structures identified in the literature review were the permutation substitution network (PSN) (Sugita et al. 2000); however, no knowledge of its performance as a cryptographic approach is specified.

The first part of the novel approach rearranges the order of the cryptographic functions to ascertain if the ordering of the functions has an impact on the cipher-text output of the block cipher. The current methods examined in this instance are the SPN structure used by AES-128 as it is the current NIST standard and is the de-facto world standard. The SPN design paradigm consists of functions based on Shannon's confusion and diffusion theory (Shannon 1949) which is substitution and permutation. The substitution box creates confusion by replacing the original plain-text character with a random character and diffusion is achieved through dispersion of the plain-text. As the AES block cipher uses modular cryptographic functions, the structure of the block cipher can be rearranged; the AES-128 block cipher can be implemented in different arrangements as presented in Table 8.1.

Table 8.1: Possible arrangement of the AES-128 block cipher structural components.

	SubBytes	**ShiftRows**	**MixColumns**
Combination 1	1	2	3
Combination 2	1	3	2
Combination 3	2	1	3
Combination 4	2	3	1
Combination 5	3	1	2
Combination 6	3	2	1

Table 8.1 presents six variations of the AES block cipher. The combinations listed in Table 8.1 are further categorised into three sub groups which are SPN, PSN and PSPN (permutation substitution permutation network). Combinations 1 and 2 fall under the SPN design paradigm as the order follows substitution before permutation; combination 3 and 4 comprise the PSPN design paradigm as permutation happens before and after the substitution. Combinations 5 and 6 are categorised under the PSN design paradigm as the permutation operations are undertaken before the substitution. The pseudo code for PSN and PSPN structures for AES-128 is presented in Figure 8.3.

PSN paradigm

```
Round(State, RKey)
{
MixColumn(State);
ShiftRows(State);
SubByte(State);
AddRKey(State, RKey);
}
MixColumn(State);
ShiftRows(State);
SubByte(State);
AddRKey(State, RKey);
```

PSPN paradigm

```
Round(State, RKey)
{
MixColumn(State);
SubByte(State);
ShiftRows(State);
AddRKey(State, RKey);
}
MixColumn(State);
SubByte(State);
ShiftRows(State);
AddRKey(State, RKey);
```

Figure 8.3: Pseudo code of the PSN paradigm (Left) and the PSPN paradigm (Right).

The PSN and PSPN structures specified in Figure 8.3 are analysed against the SPN structure to identify if the order of the functions determine the operational characteristics of the cryptographic primitive. A test was conducted to evaluate the statistical output of the three approaches with a focus on the entropy, arithmetic mean and serial correlation of the cipher-text output.

The test was programmed in visual studio with the C programming language selected to implement the three structures; a message size of two-hundred-and-sixty bytes was selected with the number of iterations for the cryptographic primitives varied between one to ten rounds. Electronic Code Book (ECB) was selected as the block cipher mode of operation. The entropy number tester was selected as the method of analysing the cipher-text output. Figure 8.4 draws the results of the accumulative entropy of the cipher-text output obtained from the three structures specified.

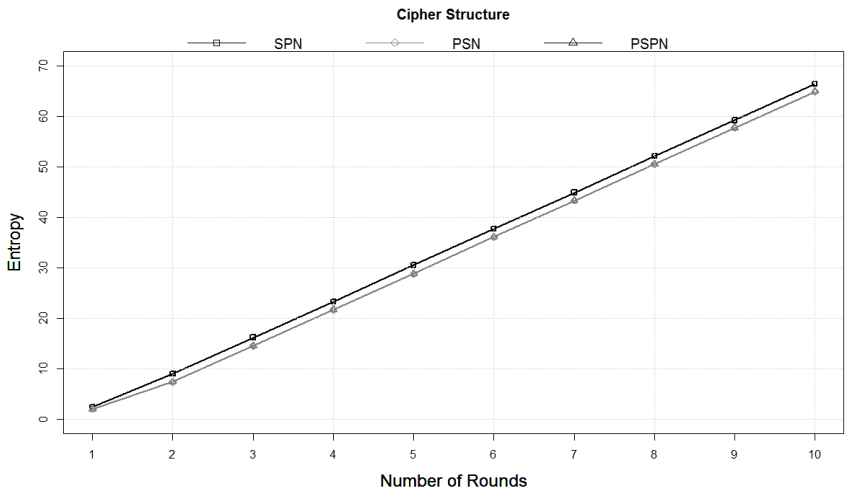


Figure 8.4: Comparison of the accumulative entropy scores for the cipher-text output for SPN, PSN and PSPN structure for a two-hundred-and-fifty-six byte message. PSN and PSPN overlay.

The results presented in Figure 8.4 shows that the order of the functions used by the cryptographic primitive has a minimal difference on the entropy scored of the cipher-text output as the entropy output for SPN, PSN and PSPN are within one standard deviation for the entropy scores recorded for all structures examined. Table 8.2 tabulates the data obtained for the arithmetic mean score for the three cryptographic structures analysed.

Table 8.2: Arithmetic mean of the cipher-text output for SPN, PSN and PSPN structures for a two-hundred-and-fifty-six byte message size.

Independent Variable	**Dependent Variables**		
Number of Rounds	**SPN Arithmetic Mean**	**PSN Arithmetic Mean**	**PSPN Arithmetic Mean**
1	67.3	40.2	40.2
2	134.6	136.1	136.1
3	127.4	129.3	129.3
4	120.8	121.5	121.5
5	125.5	130.1	130.1
6	125.9	124.8	124.8
7	126.0	127.0	127.0
8	123.7	127.8	127.8
9	118.6	128.1	128.1
10	129.1	125.3	125.3
Mean of Results (127.5 ideal mean)	119.8	119.0	119.0

The results presented in Table 8.2 shows that the mean results of the arithmetic mean analysis for SPN, PSN and PSPN strictures are within one standard deviation of the ideal arithmetic mean score of 127.5; this indicates that the structural configuration of the block cipher does not have a significant impact on the weighting of binary zeros and ones in the cipher-text output. Table 8.3 tabulates the results of the serial-correlation test between the SPN, PSN and PSPN design paradigm for a two-hundred-and-fifty-six message size over a various number of rounds.

Table 8.3: Serial correlation results for SPN, PSN and PSPN design paradigms with a two-hundred-and-fifty-six byte message size over a varying number of rounds.

Independent Variable	**Dependent Variables**		
Number of Rounds	**Serial-Correlation SPN**	**Serial-Correlation PSN**	**Serial-Correlation PSPN**
1	0.56	-0.16	-0.16
2	0.01	0.08	0.08
3	-0.09	-0.05	-0.05
4	-0.04	0.21	0.21
5	-0.07	-0.01	-0.01
6	-0.01	-0.04	-0.04
7	0.02	-0.04	-0.04
8	-0.02	0.05	0.05
9	0.07	0.05	0.05
10	0.10	0.04	0.04

Analysis of the serial correlation tests for the SPN design paradigm shows that the mean correlation score was 0.05 whilst the PSN and PSPN design paradigms had a mean correlation score of 0.01. The standard deviation of the results indicates that SPN has a value of 0.18 whilst PSN and PSPN structures have a value of 0.09. This shows that the variation in the cipher-text output was greater with SPN in comparison to PSN and PSPN.

Analysis of the difference between the PSN and SPN structures was undertaken to determine if there is a significant difference between the behaviour of the block cipher with different structures applied. PSPN was not selected for this test as the behaviour of PSN and PSPN. Comparison of the SPN and PSN structures was conducted with a normalised t-test of the arithmetic mean. Variables measures in this analysis was the t-value to determine if there is a significant difference between a population of means and the P-value to derive the probability of finding the observed results when the hypothesis of the study holds true. The test conducted changed the value of an individual byte position of a sixteen byte plain text message with the same value before each encryption call. The data from the cipher-text outputs were normalised against the random mean average for a byte of data (127.5 bits) before statistical analysis was conducted. Table 8.4 tabulates the output of the paired t-test.

Table 8.4: Normalised paired-t-test comparison of SPN and PSN paradigms at a ninety-five percent confidence interval.

Independent Variable	Dependent Variable
T-value	1.05
Degrees of freedom	9
P-value	0.32
Mean of differences	6.8

Results from the normalised paired t-test shows that the variance between the SPN and PSN structures are not significantly different as the t-value represents that a difference between the two arithmetic mean data sets in relation to the hypothesis that both data sets are different does not hold; this is justified as the cryptographic operators used for the SPN and PSN ciphers are the same. The outcome of the P-value statistic demonstrates that as the probability of a difference between SPN and PSN outputs are not likely to fulfil the null hypothesis as there is a 68 per cent probability that that there is no significant difference between the two results, therefore, it can be inferred that the PSN design paradigm is a suitable method for block cipher designs in comparison to SPN approaches.

A test is derived to investigate the affect of the cryptographic structures SPN and PSN on the instantaneous packet throughput for a static tactical UAV transmitting real-time tele-operation and telemetry using a point to point communication link. The simulator Proteus ISIS8 is selected for benchmarking the two structures. The Microchip PIC18F45K22 is selected as the microcontroller used for the transmitter and receiver. The Serial Peripheral Interface (SPI) is selected as the physical layer (i.e. OSI model) to transmit and receive messages between each microcontroller. The TinyAEAD construct is the selected AEAD construct due to its flexibility and adaptability of operations.

The metrics selected for the test procedure are seconds for the sampling time of the test, packet count to measure how many packets arrived in the sample time of ten seconds. It is assumed that an ideal communication channel is operating (i.e. no interference). All timings are taken from the simulator used. Configuration of the components selected are as follows, the crystal frequency selected is 4 MHz with packet payload sizes of sixteen, sixty-four and ninety-six bytes chosen. Table 8.5 graphs the comparison between SPN and PSN design paradigms at ten rounds with various byte sized messages.

Table 8.5: Instantaneous Packet throughput measurements recorded for SPN and PSN design paradigms in a ten second time sample.

Independent Variable	**Dependent Variables**		
Number of Bytes in Payload	**Number of Packets (No Security)**	**Number of Packets (SPN)**	**Number of Packets (PSN)**
16 bytes	3,992	150	150
64 bytes	735	16	16
96 bytes	549	11	11

Results obtained show that the PSN design paradigm and the SPN design paradigm are correlated with the same number of packets generated; it can be inferred that the PSN design paradigm is suited for the application of tactical UAV as the SPN design paradigm as it takes the same time to process through the cryptographic construct; this is because both paradigms utilised the same substitution and permutation functions. Based on the findings obtained from the test undertaken, the structural arrangement of the cryptographic primitive does not have a significant difference on the cipher-text output as all three approaches are correlated for entropy and serial correlation test.

The impact on the operational and performance characteristics of the real-time teleoperation and telemetry using the selected approaches demonstrates that both PSN and SPN design paradigms have an impact on the total number of packets received by real-time teleoperation and telemetry with a percentage difference between the test without security and using security of ninety-five percent for sixteen bytes, ninety-seven percent difference for sixty-four bytes and ninety-eight percent difference for ninety-six bytes.

From the analysis of the test conducted, the structure of the cryptographic primitive can be assorted into various combinations to achieve an output which is not significantly different in terms of cryptographic strength and impact on real-time teleoperation and telemetry; therefore, the ordering of the cryptographic functions can be rearranged to derive new cryptographic primitives; however, it is noted that the rearrangement of the structures does not adjust the amount of time required to process through the cryptographic functions as the functions called are the same as the original AES-128 block cipher functions; therefore, further investigation is needed to find an approach to obtain lightweight cryptographic primitives that maintain required cryptographic strength.

Examination of the cryptographic profile presented in Chapter 7 section 7.2 demonstrated that the cryptographic functions used by the standardised AES-128 block cipher contribute towards the total latency and number of instruction cycles used for the cryptographic

process. As the proposed speed-centric method prioritises the speed as the priority of the cryptographic operation; the configuration of the cryptographic functions is examined to determine how the operation can be optimised to meet the speed-centric method presented.

The cryptographic operation examined in this instance is the substitution-box as this function had the second largest per cent of the overall time and number of instruction cycle to process; in addition, the memory requirement of a pre-computed substitution table is significantly greater than the rest of the cryptographic functions examined in Chapter 7 section 7.2.

The purpose of the investigation analyses how the configuration of the substitution-box impacts the metrics of the cipher-text output. The aforementioned test platform and metrics used to analyse entropy, arithmetic mean and serial correlation for the comparison of SPN and PSN structures is selected; the configuration of the substitution-box uses five modes; the standardised AES-128 configuration, linear configuration, linear configuration with one byte shift to the left and a linear configuration with one byte shift to the right. All configuration methods are applied using SPN and PSN generic constructs.

Figure 8.5 and 8.6 illustrates the entropy score comparison of the SPN and PSN structures with varying substitution box configurations.

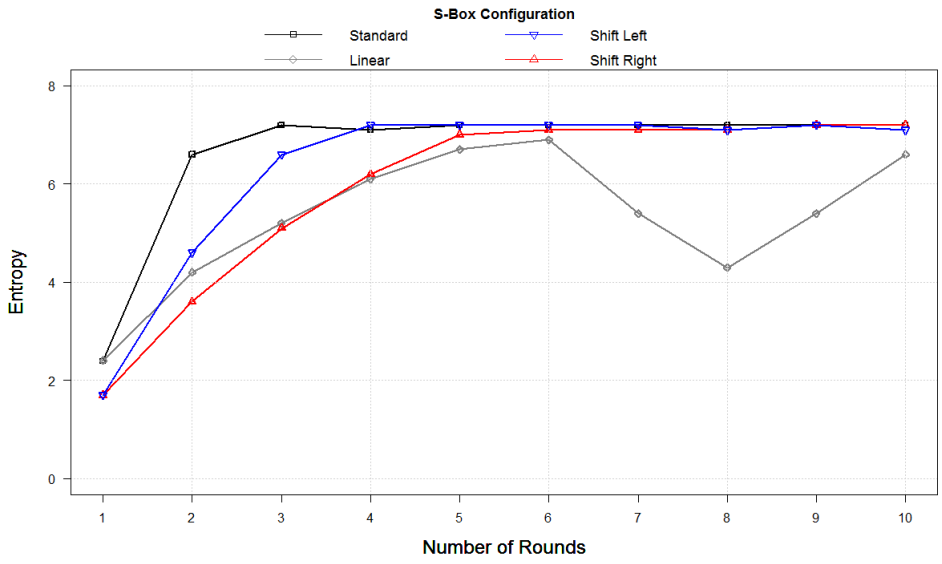


Figure 8.5: Entropy profile SPN with various substitution-box configurations for a two-hundred and fifty-six byte message size.

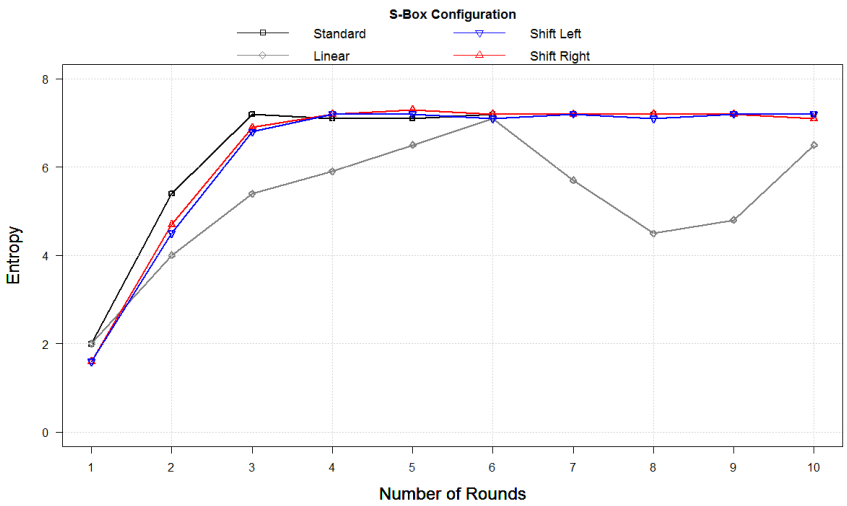


Figure 8.6: Entropy profile of PSN with various substitution-box configurations for a two-hundred and fifty-six byte message size.

Results in Figure 8.5 and 8.6 shows that the entropy profile for the standard configuration of the substitution box reaches its maximum entropy value after three rounds for both SPN and PSN generic structures. Findings presented from the analysis demonstrates that the modification of the substitution box used by AES-128 block cipher has a greater impact when the SPN structure is selected as the spread between the entropy obtained in comparison to the PSN structure for all configurations selected; therefore, it is easier to distinguish what cryptographic structure is selected based on the entropy profile of the cipher-text output.

Based on this knowledge obtained, the use of a PSN or PSPN structure for a block cipher design is applicable; however, the latency, instruction cycles used and memory required by the security service has still not been reduced to improve the operational performance of real-time teleoperation and telemetry; in addition, the current cryptographic functions used by AES-128 with the structural rearrangement design paradigm shows that the spread of entropy between substitution box configurations are better suited for the SPN design paradigm.

As the structural arrangement of the block cipher does not fulfil the speed-centric method, further investigation is undertaken to achieve to meet the requirements of the philosophy specified. The reason why there was not a significant difference in the cipher-text output with the SPN and PSN structures is because the same cryptographic functions were used to complete the process; therefore, the next question asks if the speed-centric method can be achieved by modifying the cryptographic functions used whilst maintaining an element of cryptographic strength.

8.4.2 Composite Concept

This section introduces the composite concept, the composite concept combines cryptographic processes to reduce the time and number of instruction cycles required to process the cryptographic operation and is used in this instance on the standardised AES-128 block cipher to showcase how the method is transferable to any block cipher. Achievement of the speed-centric method through the composite concept originated from the profiling of the AES-128 block cipher in Chapter 7, section 7.2.1 of the problem analysis as the total number of instruction cycles required by AES-128 block cipher to process the cryptographic operation was the main source of the problem.

Investigation of the reason to the cause of the larger quantity of instruction cycles required by the AES-128 block cipher to compute the cryptographic operation was segmented by component with a profile analysis of the number of instruction cycles required by each components of the block cipher with the substitution box, shiftrows, mixcoloms and XOR round key examined. Findings obtained from the analysis of the individual components demonstrated that the most significant percentage of the overall process in terms of instruction cycles required was the substitution box and the XOR round key with a combined total of up to 60% of the overall block cipher operation. Modification of the shiftrows and the mixcolumns were discounted in this instance of the composite concept as both components are essential in order to fulfil Shannon's theory of confusion and diffusion; therefore, the requirement to reduce the total number of instruction cycles required by these components was prioritised in order to fulfil the speed-centric method and improve the speed of the underlying block cipher.

The purpose of the composite concept as stated earlier in this section is to reduce the number of instruction cycles required to process the cryptographic operation in order to increase the speed of the block cipher operation; in this instance, the composite concept replaced the specialist substitution box and XOR round key components with a integer addition component; this is because the integer addition acts as a substitution function as the combination of two values together replace the initial input with a different output value; furthermore, the propagation of the carry adds additional complexity as each bit position has a $\frac{1}{4}$ probability of a bit flip as a result of the integer carry; therefore, adding further entropy to the behaviour of the non-linear component through the use of a novel composite concept approach to derive generalise instance of a component that acts in a similar manner to the specialist substitution box and XOR round key.

Application of the structural arrangement of the block cipher was also factored into the instance of the composite concept as the new component derived from the composite

concept was placed in-between the mixcolumns and shiftrows components; this is because the mixcolumns creates diffusion with the collision of individual byte positions colliding together before the output is passed into the composite component of the integer addition. The output of the integer addition is passed to the shiftrows component in order to cause permutation of the byte positions in order to prevent clumping of the carry bit as it propagates to the most significant bit position and thus further fulfilling Shannon's theory on confusion and diffusion. Figure 8.7 illustrates the application of the composite concept to achieve a block cipher that fulfils the speed-centric method.

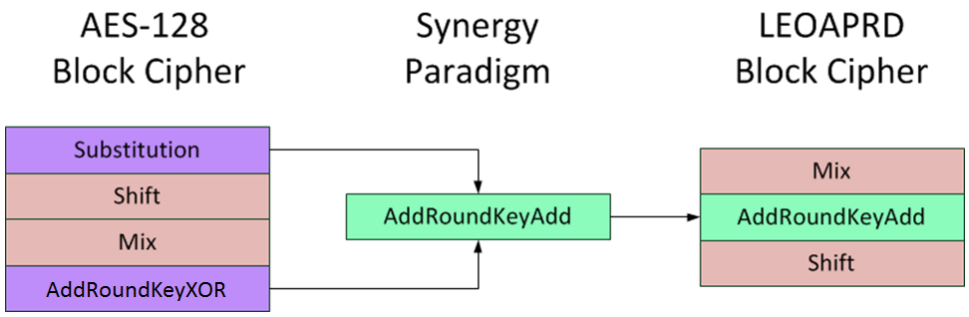


Figure 8.7: Application of the composite concept on the AES-128 block cipher to combine cryptographic operation in order to fulfil the speed-centric method

As depicted in Figure 8.7 the concept of the AES-128 block cipher is comprised into four sections, the substitution bytes, shiftrows, mixcolumns and the XOR of the round key. The composite concept combines two cryptographic operations into one to reduce the time required to process the cryptographic operation and fulfil the proposed speed-centric method. In this instance, the combination of the substitution function and the XOR of the round key was selected as these two operations were the most time consuming as identified from the profile of the AES-128 block cipher in Chapter 7, section 7.2.

The function that has been selected to fulfil the composite concept is the use of an addition function; this is because the addition operator has comparable with the substitution function for the entropy output of the block cipher over various number of rounds. Application of the addition function with the round key used substitutes the plain-text input with the addition of the key value to derive a cipher-text output; furthermore, a result of the addition could create a possible permutation with the carry of the bit values across byte positions; thus, this fulfils Shannon's confusion and diffusion principles in one operation.

The structural arrangement of the AES-128 block cipher has been modified to accommodate for the linearity of the addition function as this could be susceptible to linear and differential cryptanalysis techniques as the mixcolumns and shiftrows positioning before and after the composite function permutates the input and the output of the operation;

therefore, this prevents an attacker from conducting known cryptanalysis techniques to identify linearity in the block cipher operation. Proof of theorem is presented in section 8.5 that analyses the instance of the block cipher designed through the speed-centric method, the lightweight encryption operation permutation addition rotation and diffusion (LEOPARD).

Investigation into the feasibility of the proposed composite concept is undertaken with a test to profile the behaviour of combining cryptographic functions. It is hypothesised that the composites of cryptographic functions would not have a significant impact on the cipher-text output as the fundamental principles of confusion and diffusion have been maintained. A real-world test platform is selected to test the presented hypothesis. The test examined the number of changes recorded in each byte position of the cipher-text output for the standardised AES function and the composite function.

The test analysed the entropy of the cipher-text output with the application of the composite function using the addition operator and benchmarked the results against the substitution box and the XOR operator. The test conducted used the Microsoft Visual Studio IDE; the SPN structure with a zero value cryptographic key. The mode of operation selected for this test was ECB mode to modify all byte positions of the payload; sixteen bytes of the payload were encrypted per encryption call; the cipher-text output was stored into a text file. The entropy of the cipher-text output was analysed for the three complementation approaches specified. Figure 8.8 illustrates the entropy value of AES with a standardised substitution function, additional function and XOR function over a varying number of rounds.

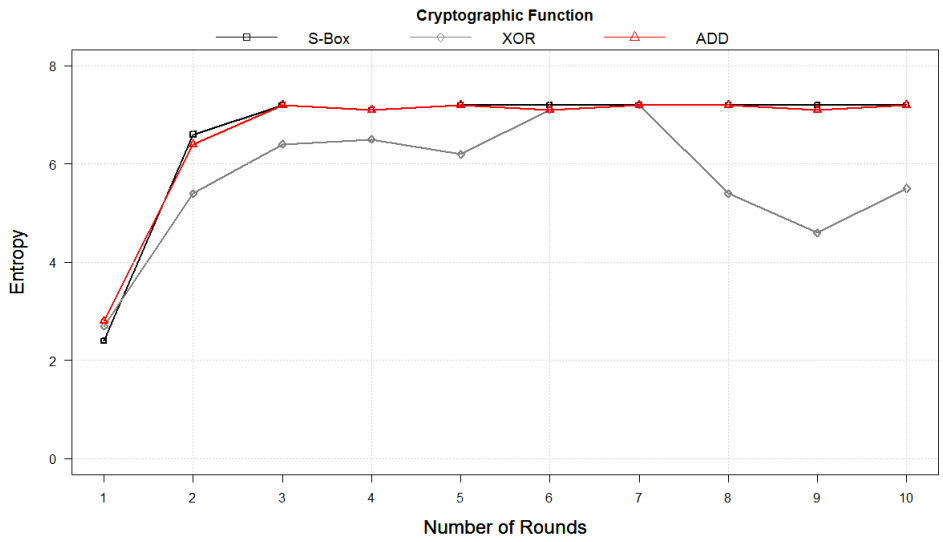


Figure 8.8: Comparison of AES substitution function, addition function and XOR function over varying number of rounds for a two hundred and fifty-six byte message.

Results presented in Figure 8.8 shows that the substitution and addition function follow a similar profile for the entropy gained over a various number of rounds; whilst the XOR operator has a significant difference on the entropy score obtained after five and six rounds. The reason for this profile is because the XOR operator conducts a linear substitution through bit logic; however, as the operation was called twice during the main block call of AES-128 for this test, the two XOR operators cancelled each other out and returned the message back to its original state. This finding correlates with the linear substitution box profile presented in Figure 8.5 in section 8.4.1 as both trends display similar characteristics towards in their entropy value recorded over a varying number of rounds; this demonstrates that the XOR operator is linear and the use of two XOR operators inverts the impact of the original bit logic change.

Further analysis of the XOR operator was conducted to identify whether the profile represented in Figure 8.8 was a characteristic of the XOR operator or an influence of a particular value selected for the key input into the block cipher. The aforementioned test was conducted on the block cipher with XOR operators selected; four randomly generated key input values was selected which were generated based on the value of pi. Table 8.6 tabulates the variation of the PI keys and their associated valued used in this instance of the analysis

Table 8.6: Values set for the Pi Keys

Independent Variable	**Dependent Variable**
Pi Key	**Value in Hexadecimal**
1	243F6A8885A308D313198A2E03707344
2	A4093822299F31D0082EFA98EC4E6C89
3	452821E638D01377BE5466CF34E90C6C
4	C0AC29B7C97C50DD3F84D5B5B5470917

The variants of the Pi keys were passed through the same test to identify if the phenomena observed was as a result of the cryptographic key chosen or a characteristic of the XOR component. Figure 8.9 illustrates the comparison of the entropy score obtained for the XOR operations with random input keys.

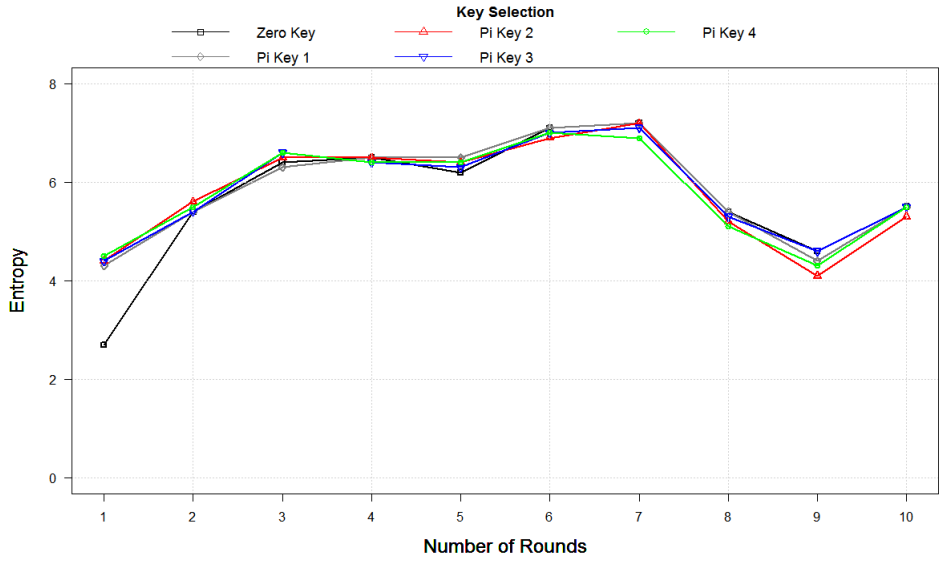


Figure 8.9: Comparison of entropy scores for the XOR operator with random input keys

Results presented in Figure 8.9 demonstrates that the entropy scores recorded for all of the random key input values correlate with the initial result of the XOR operator with a zero key presented in Figure 8.5 with a similar profile identified between all of the entropy measurements obtained; this demonstrates that this finding is the characteristic of the XOR operator in this application; therefore, the reasoning presented in the aforementioned test is supported by these findings. Additional analysis of the relationship of the key value selected and its impact on the block cipher operation was not conducted as this is not the focus of the research conducted in this thesis and is and is classified as a future area of research.

Advantages of the selection of the addition function as an alternative approach to the replacement of the substitution-box is the reduction in the memory requirements as the substitution-box requires two-hundred and fifty-six bytes of memory; whilst the composite function required two sixteen byte variables to compute the output. Additional benefits of the addition function is that the data input into the block cipher is added to the cryptographic key; this is beneficial in situations where pre-commutated keys are used as the key value is changed in order to prevent an attacker conducting a brute force on a single key value. The final benefit is the profile of the addition function follows a similar profile to the substitution-box for the entropy value obtained.

Analysis of the cipher-text was conducted with the entropy number tester to identify the metrics of the cipher-text output with the AES subbytes and XOR functions and the composite function. Message size of two-hundred-and-fifty-six bytes was sampled with a key value of the first sixteen digits of pi selected. Metrics recorded for this test were the entropy, arithmetic mean and serial correlation of the cipher-text output. The mode of

operation selected for this test was ECB mode to modify all byte positions of the payload; sixteen bytes of the payload were encrypted per encryption call; the cipher-text output was stored into a text file. Table 8.7 tabulates the comparison of the cipher-text output for the AES and composite functions.

Table 8.7: Profile of the cipher-text output for AES and composite functions with a two-hundred-and-fifty-six byte packet at ten rounds.

Independent Variable	**Dependent Variables**	
Configuration	**Arithmetic Mean**	**Serial Correlation**
AES-128 function	155.87	0.14
Composite function	121.28	0.48

Results presented in Table 8.7 demonstrate that the composite concept and AES-128 function are correlated for the arithmetic mean of the cipher-text output, the composite concept is closer to the ideal mean of 127.5 bits; however, the serial correlation results show that the composite function has a more correlated output in comparison to AES-128. Further analysis was undertaken of the arithmetic mean with the normalised paired t-test between the composite function and AES-128 function over one to ten rounds. Table 8.8 tabulates the results of the normalised paired t-test.

Table 8.8: Normalised paired t-test comparison of the composite function and AES functions at a ninety-five percent confidence interval.

Independent Variable	**Dependent Variable**
T-value	-0.65
Degrees of freedom	10
P-value	0.53
Mean of differences	-6.2

Results from the normalised paired t-test shows that the variance between the substitution-box and addition functions are not significantly difference as the t-value represents a small difference between the two arithmetic mean data sets; this is because the functions perform the same principle of Shannon with confusion. The outcome of the P-value obtained reinforces that the difference between the two approaches are not significantly different as the P-value recorded demonstrates that the substitution-box and addition functions results are more likely to meet the null hypothesis that there is no significant difference between the two results; this demonstrates that the composite concept is a suitable method for the design of cryptographic operations as the comparison of the entropy, arithmetic mean and serial correlation metrics for the standardised AES-128 cryptographic functions and the composite functions are correlated based on the observational analysis undertaken.

Findings from the analysis of the composite concept demonstrates that the combination of cryptographic functions appears to have a profile that is similar to the operation of the substitution-box based on the basic cryptographic profiling of the two functions; however, the question that is presented as a result of this investigation is if the combination of the structural rearrangement of the block cipher and the composite concept can fulfil the requirement of the speed-centric method.

8.4.3 Design and Implementation of the LEOPARD Block Cipher

The synergy of the cryptographic functions is combined with the structural arrangement of the cryptographic primitive to derive a new suite of block cipher cryptographic primitives; this is referred to as the Big Cat Block Cipher Suite. There are a number of combinations applicable to the Big Cat Block Cipher Suite based on the design considerations and the structural arrangement of the cryptographic primitive; Table 8.9 tabulates the combinations that fulfil the criteria of the Big Cat family derived by the author.

Table 8.9: Big Cat Block Cipher Suite cryptographic primitives for real-time teleoperation and telemetry. (Derived by the author)

Name of primitive	Cryptographic Structure
LEOPARD	PSPN
LION	SPN
JAGEUAR	PSN
TIGER	SPN
LIGER	PSN
TIGON	PSPN

The construction of the new cryptographic primitives for real-time teleoperation and telemetry has considered the proposed philosophy of the trade-off between the strength, energy and speed of the cryptographic method; each approach listed in Table 8.9 was designed to meet the specifications dependent on the context of the scenario. As the philosophy presented in this section of this thesis is biased for the speed of real-time teleoperation and telemetry, a new block cipher is presented to fulfil this requirement using the structural rearrangement and composite concept presented with the Lightweight Entropy Operations Permutation Addition Rotational Dispersion (LEOPARD) cryptographic primitive as an instance of a method designed for speed.

As the LEOPARD block cipher is adopting cryptographic operations used by the AES-128 block cipher and the permutation substitution network (PSN) structure; it is assumed that the cryptanalysis undertaken for AES in previous research is applicable for this application (Fouque et al. 2013, Piret & Quisquater 2003, Bogdanov et al. 2011, Gilbert & Peyrin 2010). As the main consideration of the speed-centric method is to reduce

the impact on the operational performance of real-time teleoperation and telemetry; the validation of the instance of the speed-centric method is focused towards its impact in comparison to contemporary approaches. Figure 8.10 presents the pseudo-code for the LEOPARD cryptographic primitive.

LEOPARD paradigm

```
Round(State, RKey)
{
MixColumn(State);
AddRKeyAdd(State, RKey);
ShiftRows(State);
}
SubByte(State);
ShiftRows(State);
AddRKey(State, RKey);
```

Figure 8.10: Pseudo-code of the LEOPARD cryptographic primitive.

The configuration of the LEOPARD block cipher presented in Figure 8.10 follows a PSN structure in combination with the composite concept with the addition function used as a replacement substitution-box function by adding the input data and the cryptographic key used by the block cipher. The final round uses the same ending as the standardised AES block cipher as a method of screening the internal concept of the LEOPARD block cipher as presented in the following research dissemination (Sparrow, Adekunle, Berry & Farnish 2016, Sparrow, Adekunle & Berry 2016).

The composite function used in this instance of the block cipher design is the addroundkey-add cryptographic function which uses an addition operator to combine the round key used by the block cipher with the state of the input in order to meet Shannon confusion and diffusion principles. The structural arrangement of the LEOPARD block cipher uses a PSPN structure, this arrangement order the permutation function before and after the composite function in order to disperse the linearity of the addition operator; consequently, this causes difficulty for an attacker to conduct attacks such as linear and differential cryptanalysis as the linearity of the operator is disguised through the permutations. Analysis of the resilience of the LEOPARD block cipher against cryptanalysis techniques is presented in the next section.

Expansion of the pseudo-code presented in Figure 8.10 is presented with the explanation of the individual components used by the LEOPARD block cipher scheme.The LEOPARD block cipher uses cryptographic functions that are used by the standardised AES-128 block cipher, however, the inclusion of the composite function derived from the composite concept in order to meet the speed-centric method is included into the LEOPARD block cipher design. Figure 8.11 illustrates the LEOPARD block cipher diagram.

Figure 8.11: Block diagram of the LEOPARD block cipher

The operation of the LEOPARD block cipher depicted in Figure 8.11 illustrates the process of the block cipher; first, the plain-text input is passed to the addroundkey function, this derives an XOR sum of the plain-text and the pre-shared key. The output of the state is passed into the mixcolums which permutates the byte positions of the input sate before the round key is added to the state to substitute the original input values; the shiftrows offsets the byte positions of the state to create permutation. The operation is undertaken over a specified number of iteration before the the state is passed to the final round operation. The final round of the LEOPARD block cipher uses the same configuration as the standardised AES-128 block cipher with the subbytes, shiftrows and the XOR of the round key; this is to obfuscate the attacker from viewing the internal mechanism of the block cipher by masking the final round output. Additional detail of the individual components used by the LEOPARD block cipher is presented in the next section, the cryptanalysis of the proposed LEOPARD block cipher.

Benefits of the proposed cipher scheme presented in comparison to cipher schemes disseminated in the literature review and the problem analysis is that the proposed cipher

scheme was designed with the consideration of the speed of the cipher as the main priority as specified in the requirements of the synthesised requirements to overcome the identified problem as stated in Chapter 7, section 7.4 of the discussion and presented in the presentation and instance of the speed-centric method; whilst existing cipher schemes either prioritised the security service or the energy consumption of the cipher. Software implementation of the LEOPARD block cipher is beneficial in the context of real-time teleoperation and telemetry systems as there is not a requirement for additional hardware area and space for the cryptographic module; whilst the majority of identified lightweight schemes presented in the literature review are hardware implementations that prioritise energy conservation or hardware area consumed for the cipher.

Examination of an existing lightweight cipher scheme identified in the Chapter 2, section 2.7 of the literature review was conducted against the derived proposed solution, the LEOPARD block cipher to differentiate the benefits of the proposed scheme. The lightweight cipher selected for comparison is the SPECK lightweight block cipher scheme published by the national security agency (NSA) as the researchers claim the scheme to be flexible for software implementation whilst having a minimal impact on the performance on constraint devices through the use of simplistic components (Beaulieu et al. 2015). SPECK is a feistel structure cipher that uses addition, rotation and XOR (ARX) operators to create confusion and diffusion of the plain-text input and transpose into the cipher-text output; variants of the SPECK cipher have been proposed by the authors with variable block lengths and key sizes.

Benefits of the LEOPARD block cipher scheme over the SPECK cipher are the operators used for the SPECK cipher are intense on the computational over the LEOPARD block cipher operators as the result of using a software rotation as demonstrated in the cost per byte to process the data in comparison to the de facto standard AES-128 block cipher (Beaulieu et al. 2015); this indicates that SPECK may not be suited for real-time situations as the additional latency would impact on the real-time nature of the context in terms of its behaviour as identified in Chapter 3, Chapter 4. Chapter 5, Chapter 6 and Chapter 7; this is further exemplified as the number of rounds specified by the authors for the SPECK cipher for a block length of 128-bits is thirty two rounds; whilst the number of rounds specified for the LEOPARD block cipher is variable dependent on the security level required for the real-time teleoperation and telemetry context; resulting in the proposed scheme flexible in comparison to the SPECK cipher.

The implementation of the proposed instance of the speed-centric method; the LEOPARD block cipher has advantages in comparison to the existing ciphers identified throughout this research as the structure of the LEOPARD block cipher utilises a PSPN arrange-

ment that has been validated to be just a suitable as PSN schemes used by existing cipher schemes; however, the benefit of this methods has facilitated the composite concept that combines cryptographic functions to improve the speed of the block cipher and maintain an acceptable level for the security and as a by-product, reduce the energy consumption of the cipher as a result of less instruction cycles to process. Validation of the cryptographic resilience of the LEOPARD block cipher is presented in the next section of this chapter with cryptanalysis of the LEOPARD block cipher to ascertain if the instance of the proposed philosophy shows sufficient resistance against a known cryptanalysis method and if it is comparable to contemporary cipher schemes.

8.5 Cryptanalysis of LEOPARD Block Cipher

This section introduces the cryptanalysis of the LEOPARD block cipher. This investigation examines whether the proposed instance of the speed-centric method using the new taxonomy of block cipher structures and the composite concept is resilient against known cryptanalysis techniques.

Cryptanalysis methods selected in the analysis undertaken in this thesis is linear cryptanalysis; this is because the composite component derived uses an integer addition that is known to have linear characteristics in its operation and the linear cryptanalysis technique is an established methods of identifying linearities in the block cipher operation; therfore, the linear cryptanalysis will demonstrate the resilliance of the LEOPARD block cipher against this method.

An in-depth cryptanalysis can take up to two years to fully ascertain the cryptographic weaknesses associated with a cipher design; therefore, the cryptanalysis undertaken in this thesis is conducted on a scaled down variant of the LEOPARD block cipher with the presentation of the LEOPARD Cub block cipher.

Presentation of the cryptanalysis is presented in three sections, first, an introduction to the cryptanalysis technique used to analyse the LEOPARD block cipher is discussed; followed by a formal analysis of the proposed block cipher scheme based on the speed-centric method and composite concept. The final section discusses the findings in relation to the research context of real-time teleoperation and telemetry.

8.5.1 Linear Cryptanalysis of the LEOPARD Cub Block Cipher

The hypothesis examined in this section of the thesis is that the resilience of the LEOPARD block cipher against established contemporary cryptanalysis methods can be represented through a scaled 4-bit variant, named the LEOPARD Cub block cipher as the

components and structure used by both ciphers are the same. The form of proof selected to prove or disprove the stated hypothesis stated is constrictive proof with the presentation of logical sequential steps to derive at a conclusion.

Cryptanalysis has been selected to benchmark block cipher designs as described in Chapter 2, section 2.8, the two most common techniques are linear and differential cryptanalysis. The justification of the selection of the linear cryptanalysis method over differential cryptanalysis is because propriety block cipher designs such as the Data Encryption Standard (DES) were designed with the consideration of differential cryptanalysis as this method was widely known to the cryptographic community with a total of 2^{47} chosen cipher-text pairs required to successfully break the DES block cipher, however, the application of the more recent linear cryptanalysis by Matsui et al; exposed the vulnerabilities with the DES bock cipher with less number of plain-text pairs required (2^{43}) (Matsui 1994); therefore, in this thesis; the linear cryptanalysis method has been selected to validate the resilience of the proposed cipher scheme against an established cryptanalysis method and determine if there is linearities between the plain-text input and cipher-text output as a result of the structural configuration of the 4-bit variant of the LEOPARD block cipher, the LEOPARD Cub block cipher and if the linear cryptanalysis would reduce the average number of attempts required to identify the correct cryptographic key in comparison to brute force methods of obtaining cryptographic key selected.

Linear cryptanalysis attempts to approximate the behaviour of the non-linear components of a cipher scheme, this is achieved with the application of linear approximations to linearise the process of the plain-text input and the cipher-text output of the non-linear component for each iteration of the block cipher. The purpose of this analysis is to determine if the structural arrangement of the proposed cipher scheme and the cryptographic components derived from the application of the composite concept are sufficient resilient against this technique in the context of real-time teleoperation and telemetry.

The number of bits examined for the linear cryptanalysis was a 4-bit variant of the 128-bit LEOPARD block cipher; this is because the time required to generate all known plain-text cipher-text pairs and analyse all possible linear approximations for a 128-bit block cipher would not be feasible in the time-frame of this research; this is further reinforced by research conducted by (Kokes & Lorencz 2015, Swenson 2008) that conduct linear cryptanalysis on small or reduced scale variants of the block ciphers; therefore, the linear cryptanalysis is conducted on a 4-bit variant of the LEOPARD block cipher named the LEOPARD Cub block cipher. The LEOPARD Cub block cipher components are derived from the 128-bit variant of the LEOPARD block cipher; therefore, the explanation of the components are transferable to the full scale 128-bit LEOPARD block cipher.

The components of the LEOPARD Cub block cipher are the mixcolums, addition of the round key, shiftrows, substitution box and the key whitening of the block cipher input and output. Configuration of the LEOPARD Cub block cipher follows the PSPN structure to reflect the same structure as the LEOPARD block cipher. The substitution box replaces an input value with a corresponding value in its table in order to create confusion by obscuring the relationship between the key and the cipher-text output. The shiftrows permutates the byte positions of each row of the message by a fixed byte number to create transposition of the byte position of the message and the mixcolumns creates diffusion; this function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column; resulting in another new matrix consisting of sixteen new bytes.

The integer addition function is an instance of the proposed composite concept used within the internal number of iterations of the LEOPARD Cub block cipher; the reason to the selection of the integer addition is because this operation conducts substitution of the input with the addition of the round key per iteration of the block cipher to create confusion with injection of entropy from the key scheduler into the data path of the block cipher; in addition, a carry as a result of the addition of the input and subkey value; consequently, this creates diffusion across the most significant byte positions with a probability of occurrence being $\frac{1}{4}$ of the time; resulting in a fulfilment of the composite concept as multiple operations are combined into one operation.

The key whitening is applied to the input of the LEOPARD Cub block cipher to prevent the attacker knowing the master key used to initialise the key scheduler and the output of the LEOPARD Cub block cipher to screen the cipher-text output at the last round. Examination of the components chosen for the LEOPARD Cub block cipher shows that there are two non-linear components used; the integer addition and the substitution box and both components are analysed for the linear cryptanalysis as the subsequent components conduct a linear operation.

The configuration of the specified cryptographic functions used for the LEOPARD 128-bit block cipher and the LEOPARD Cub 4-bit block cipher are as specified in the standardised AES-128 standard for the substitution box, shiftrows, mixcolumn and the key whitening; however, the 4-bit LEOPARD Cub cipher has slight modifications to the functions in order to operate on a 4-bit block cipher; this has been applied to the shiftrows and mixcolumns operator in order to conduct the analysis on a small scale variant of LEOPARD. Table 8.10 tabulates the shiftrow configuration of the LEOPARD Cub block cipher.

Table 8.10: Shiftrow mapping of the input and output bits for the LEOPARD Cub block cipher

0	2	4	6
8	10	12	14
1	3	5	7
9	11	13	15

Configuration of the mixcolum used for the LEOPARD Cub block cipher follows the same principle as the standardised AES-128 block cipher; however, in this instance of its implementation, the collision of the bit positions are presented in a simplistic configuration as the focus is on the linear cryptanalysis of the non-linear component of LEOPARD Cub block cipher, the integer addition. Formula 18 illustrates the mixcolums configuration for the LEOPARD Cub block cipher.

$$B_1 \leftarrow b_1 \oplus b_4$$

$$B_2 \leftarrow B_1 \oplus b_2$$

$$B_3 \leftarrow B_2 \oplus b_3$$

$$B_4 \leftarrow (b_4 \oplus rc) \oplus B_3 \tag{18}$$

Formula 18: Mathematical representation of the MixColumn configuration for the LEOPARD Cub block cipher

The value of each bit position is directly influenced as a result of the cascade across all bit positions as bit positions are tracked to certain tracks as demonstrated in Formula 18 and as a result, can be performed in reverse to return to the original input state; however, the application of the round constant at bit column position four creates additional uncertainty for the an attacker attempting to reverse back through the operation as they would require prior knowledge of the round constant as this can be configured at the practitioners discretion, the value of each auxiliary input and the relationship between each mixcolumn track. The final component of the LEOPARD Cub block cipher is the key scheduler that has been designed for demonstration purposes to frustrate attackers that may conduct a sliding attack against the cipher. Figure 8.12 illustrate the key scheduler used for the LEOPARD Cub block cipher

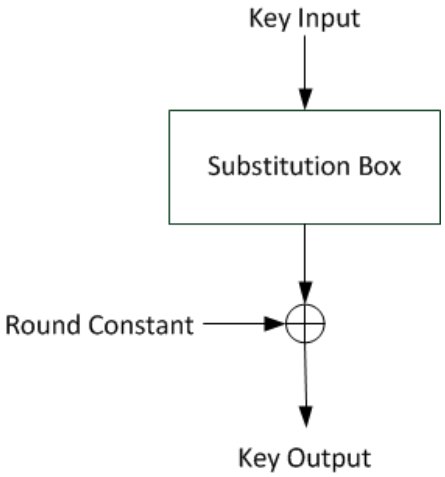


Figure 8.12: Visual representation of the LEOPARD Cub key scheduler

Implementation of the linear cryptanalysis is achieved using a Linux Ubuntu 16.04, 64-bit operating system operating at 2 GHz quad-core processor with the linear cryptanalysis conducted in Microsoft Excel Spreadsheet and validated against a computerised implementation of the attack (King 2017); the computerised linear cryptanalysis was computed in the C programme language in the code blocks integrated development environment. Integration of the composite concept presented in section 8.4.2 has been applied in this instance of the cryptanalysis by tabulating the shiftrow and mixcolum process in order to increase the time required to complete the linear cryptanalysis at the increased cost of memory usage. The number of plain-text and cipher-text pairs used for the experiments was set to sixteen to reflect all possible permutation of input and output pairs. It is assumed that the substitution box is a fixed configuration and is known by the attacker.

In this analysis, it is assumed that the substitution box at the final round of the LEOPARD Cub block cipher is known to the attacker in addition to the mixcolumns, shiftrows and XOR screen at the input and output of the block cipher and the attack is focused on the components used for the iterative number of rounds, the internal substitution box and the integer addition function (i.e. the linear cryptanalysis undertaken was performed on the internal iterative rounds of the cipher structure). It is also assumed that the attacker would have prior knowledge of the structural arrangement of the block cipher and the input and output mask generated would be applicable throughout the number of iterations used by the LEOPARD Cub block cipher as the configuration of the integer addition function is fixed. Figure 8.13 illustrates an overview of the procedure undertaken for this analysis.

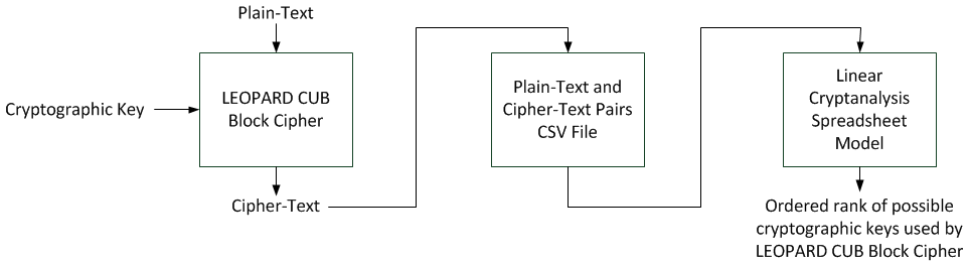


Figure 8.13: Overview of the linear cryptanalysis methodology derived in this thesis

The linear cryptanalysis of the LEOAPRD Cub block cipher is conducted in three phases; the first stage of the process automates the generation of the plain-text and cipher-text pairs with the LEOPARD Cub block cipher; the generated pairs are stored into a CSV file as a record. The final step of the process takes the plain-text input and the cipher-text output of the final round of the LEOPARD Cub block cipher as the values used in the derived linear cryptanalysis model created using mathematical modelling in a spreadsheet.

The methodology for the creation of the linear cryptanalysis mathematical model is as follows; the plain-text input and cipher-text output of the last round generated from the automated programme is copied into the mathematical model spreadsheet. The first process generates the cipher-text of the first iteration of the block cipher by passing the plain-text input through each components of the LEOPARD Cub block cipher (mixcolumns, addroundkeyadd and shiftrows) with a selected key by the attacker.

The cipher-text output of the first iteration of the block cipher obtained from the mathematical model is used in a parity check with the cipher-text output of the next iteration of the LEOPARD Cub block cipher; in this analysis, the number of iterations selected is restricted to two rounds. The parity check of the cipher-text for the first iteration and the second iteration of the LEOPARD Cub block cipher is achieved by examining the individual bit values of the cipher-text outputs of the first and second iteration of the block cipher by using bit wise AND logic to compare the individual bits from the least significant to the most significant bit of the cipher-text. The parity bits of the cipher-text obtained from the first iteration and the second iteration are compared to determine how many bits are the same; the process is repeated for all possible keys values in the search space based on the block size of the block cipher; in this analysis, this is 2^4 instances.

Once the parity score for all possible key values have been obtained, the bias score for the key values are obtained; this is achieved by dividing the parity bit score by the maximum total score for the parity bit check. The bias values are ranked in highest vale according to the key values with the greatest bias from $\frac{1}{2}$; values that are closest or equal to $\frac{1}{2}$ bias are ranked at the lowest key values as there is minimal indication that this key has charac-

teristics that align with both cipher-text outputs. In the event that two or more key values have the same bias score, the key value with the lowest numerical value is prioritised as the higher ranked value in this analysis. Appendix O and P tabulates the linear approximation table for all linear approximations for the integer addition and the substitution box functions.

Data collated from the analysis of the linear approximations for the integer addition and the substitution box demonstrates that there are a variety of linear approximations that are applicable towards the profiling of the integer addition and substitution functions; in this instance of the analysis, one of the linear approximations with the highest bias percentage was selected as an instance of the likely probability of a successful linear cryptanalysis attack against the LEOPARD Cub block cipher.

The linear approximations selected for the analysis of the integer addition functions is an input and output mask value of nine; whilst the substitution function a input and output mask of eleven was selected; this is because both linear approximations scored a bias score of 88% of holding true of linearising the non-linear components. Application of the linear approximations are applied at the input and output of the non-linear component in order to calculate the probability of a particular key used for the LEOPARD Cub cipher. The final element of the mathematical analysis derives the cryptography key used by the second round iteration through a meet in the middle attack method by either subtracting the cipher text from iteration one and two to obtain the possible key value for a integer addition function or a XOR operator for instances that use a substitution box as presented in the next section.

8.5.2 Derivation of The Cryptographic Key

The next section of the linear cryptanalysis attempts to derive the cryptographic key used at each iteration of the block cipher by checking the parity of the plain-text input bits and the cipher-text output bits using the input and output masks derived from the aforementioned analysis of the linear approximations of the non-linear components.

The test conducted examined the probability of the cryptographic key holding true based on the bias calculation of the linear approximation. Calculation of the bias is achieved by conducting a frequency analysis of the parity check between the plain-text input masked with the input mask and the cipher-text masked with the output mask. Ranking of the keys was ordered on the bias scores of the key values that have the greatest difference from 50%; in this instance, this is represented by the value eight as it is half of the total number of bits examined.

The implementation of the linear cryptanalysis was conducted using Microsoft Excel spreadsheet with validation of the process conducted on a computerised linear cryptanalysis using the C programme language. Calculation of the parity bit check was conducted for all possible key values ranging from zero to sixteen with the selected input and output masks of nine for the integer addition and eleven for the substitution box. The number of plain-text and cipher-text pairs generated for this test was sixteen to reflect all possible combinations of the sixteen bit space; all plain-text inputs were generated using a pseudo random number generator.

Analysis of the non-linear components was confuted over two iterations of the LEOPARD Cub block cipher. The probability score for the key ranking is derived from the deviation of the frequency of the parity bit check holding true against the ideal probability of 50%. It is assumed that key values with the same probability score are attempted in ascending order. Key values of two for the first round key and twelve for the second round key was selected for the substitution box and key values of two for the first round key and twelve for the second round key for the integer addition was selected. Table 8.11 tabulates the order of the possible cryptographic keys used for the substitution box based on the outcome of the parity bit check

Table 8.11: Comparison of the key ranking of the parity bit check for the substitution box over one round configuration using the LEOPARD Cub block cipher

Rank	**Spreadsheet Key Value**	**Bias Score (%)**
1	2	81
2	13	81
3	6	75
4	9	75
5	3	56
6	4	56
7	5	56
8	6	56
9	7	56
10	10	56
11	11	56
12	12	56
13	0	50
14	1	50
15	14	50
16	15	50

Results presented in Table 8.11 demonstrates that the ranking of the key values using the mathematical analysis obtained from the spreadsheet and the computerised version

of the analysis are correlated as both methods sort the possible key value in the same order; furthermore, the actual key used for the first round is presented as the first possible cryptographic key; resulting in a successful application of the linear approximation to derive the first round key using the substitution table. Table 8.12 tabulates the key ranking based on the linear cryptanalysis of the integer addition scheme.

Table 8.12: Comparison of the key ranking of the parity bit check for the integer addition over a one round configuration using the LEOPARD Cub block cipher

Rank	**Spreadsheet Key Value**	**Bias Score (%)**
1	2	100
2	3	100
3	10	100
4	11	100
5	4	88
6	12	88
7	1	75
8	5	75
9	6	75
10	9	75
11	13	75
12	14	75
13	0	63
14	8	63
15	7	56
16	15	56

Data presented in Table 8.12 demonstrates that the linear cryptanalysis of the integer addition function correctly selects the correct key used for the first round of the integer addition operation with the key value of two ranked as the highest score out of the possible sixteen key values.

Analysis of the one round linear cryptanalysis of the integer addition and the substitution box components indicates that the substitution box and integer addition components are susceptible to linear cryptanalysis over one iteration of the block cipher; this is because it is easy to trace the bits through one iteration of the block cipher (Swenson 2008); however, most modern block cipher designs use multiple iteration to transform the plain-text input into a cipher-text output as a mitigation strategy to overcome this known cryptanalysis techniques; therefore, linear analysis of the non-linear functions in the LEOPARD Cub block cipher is conducted over two rounds.

The linear cryptanalysis undertaken in this section of the analysis uses the plain-text and

cipher-text pairings generated from the LEOPARD Cub block cipher to derive the second round key used by the block cipher. The attack used in this instance is to derive the second round key by using the cipher-text output obtained from the first round and compare if the value obtained from the one round decryption of the cipher-text output of the second round; this is achieved with an XOR for the substitution function and a subtraction for the integer addition function. It is assumed in this analysis that the attacker has obtained the correct key value from the application of the linear cryptanalysis applied on the first round of the LEOPARD Cub block cipher with a substitution box and an integer addition operators. Table 8.13 tabulates the comparison of the key value obtained for the substitution box and the integer addition function.

Table 8.13: Comparison of the second round key value for the integer addition and substitution functions with the application of linear cryptanalysis

Non-linear Component	**Linear Cryptanalysis Key Value**	**Correct Key Value**
Integer Addition	12	12
Substitution Box	12	12

Information presented in Table 8.13 shows that the linear cryptanalysis is applicable to the substitution box as the second round key was derived successfully; the reason why the substitution box was susceptible to a linear cryptanalysis attack is because the configuration of the substitution box is fixed throughout the whole block cipher implementation; this results in the same input and output masks derived from the linear approximation table of the substitution box holding true for the same probability throughout each round of the LEOPARD Cub block cipher.

Analysis of the linear cryptanalysis undertaken demonstrates that the LEOPARD Cub block cipher is susceptible to linear cryptanalysis techniques based on the internal iterations used by the block cipher; this is because the components follow a deterministic process on the data and can be traced throughout the block cipher mechanism to derive the cryptographic key used per round; however, the linear cryptanalysis conducted in this thesis did not take into consideration the unknown configuration of the substitution box and the XOR whitening screen at the input and output of the block cipher.

8.5.3 Time Comparison of Linear Cryptanalysis vs Brute Force Attacks against LEOPARD Cub Block Cipher

The final section of the analysis undertaken on the LEOPARD Cub block cipher investigates the feasibility of a linear cryptanalysis in comparison to a brute force attack. The hypothesis presented in this analysis is that the linear cryptanalysis method should on av-

erage locate the correct cryptographic key used by the LEOPARD Cub block cipher in a reduced number of attempts in comparison to brute force methods. It is assumed in this analysis that the probability of an attacker locating the correct cryptographic key used by the LEOPARD Cub block cipher is half of the key size selected.

Analysis of the linear cryptanalysis key ranking was conducted to determine what the average ranking of the correct cryptographic key using the linear cryptanalysis methodology. The test method derived to validate this hypothesis used the linear cryptanalysis process as described in section 8.5.1, Figure 8.13. The number of trials conducted was five trails with a different plain-text, cipher-text pair and cryptographic key selected for each trial. The analysis was conducted on two rounds of the LEOPARD Cub block cipher. It is assumed that the attacker has the cryptographic key used for the first iteration of the block cipher. Table 8.17 tabulates the average ranking of the correct cryptographic key over the five trials conducted.

Table 8.14: Average mode of the key ranking order using the linear cryptanalysis parity check methodology

	Key Rank Test 1	**Key Rank Test 2**	**Key Value Test 3**	**Key Value Test 4**	**Key Value Test 5**
Trial 1	6	5	4	8	2
Trial 2	11	2	12	10	5
Trial 3	15	5	5	3	15
Trial 4	5	10	7	14	3
Trial 5	9	13	14	7	10
Average Mode	9	7	8	8	7

Results presented in Table 8.14 demonstrate that on average the correct key value is found within half of the total key possibilities; this demonstrates that on average, the linear cryptanalysis methodology would require the same unit of time to locate the correct key as a brute force attacks based; therefore, this reinforces that the resilience of the LEOPARD Cub block cipher against linear cryptanalysis is the same resilience as a brute force attack against the block cipher; this is because on average; the correct cryptographic key is located in $\frac{8}{16}$ attempts, this equates to $\frac{1}{2}$ attempts on average to derive the correct cryptographic key used by the LEOPARD Cub block cipher.

Information obtained from the linear cryptanalysis key ranking test demonstrates that on average the cryptographic key is obtained in half of the total search space; as this reflects the average duration for a brute force attack to obtain the correct cryptographic key, the final part of this analysis examines the time required to brute force for various sized search

spaces. The test was conducted on a Linux Ubuntu 2.4 GHz, Intel i7 quad core laptop and was implemented in the code blocks integrated development environment with the C programming language.

The number of searches required was coded using nested for loops in order for the machine to attempt all possible values. Search spaces examined in this test investigated the total searches required to search half and all possible value for the LEOPARD Cub block cipher over one to ten iterations as presented in Table 8.17. It is assumed in this test that the attacker is conducting the search in a sequential manner starting from the lowest value to the highest value in the list. Table 8.15 tabulates the time to conduct a brute force attack with and without LEOPARD Cub block cipher for all possible attempts over a various number of iterations.

Table 8.15: Time required to conduct a brute force attack on all number of attempts over multiple iterations with and without LEOPARD Cub block cipher

Number of Iterations	**Number of Attempts**	**No security time (Seconds)**	**LEOPARD Cub time (Seconds)**
1	2^4	0.001	0.001
2	2^8	0.001	0.001
3	2^{12}	0.002	0.003
4	2^{16}	0.004	0.005
5	2^{20}	0.007	0.012
6	2^{24}	0.031	0.116
7	2^{28}	0.358	1.595
8	2^{32}	5.416	24.892
9	2^{36}	86.196	397.264
10	2^{40}	1395.169	6397.079

Data presented in Table 8.15 demonstrates that the time to conduct a brute force attack against an increased number of iteration used by the block cipher results in a greater duration of time required in order to attempt all possible cryptographic key values, the reason for this is because the number of attempts per iteration increases the number of attempts exponentially; consequently, this reflects in the time required to compute the operation with both no security and LEOPARD Cub displaying an exponential growth trend as the number of attempts is increased per iteration.

Comparison of the no security and LEOPARD Cub times recorded to conduct the brute force attack shows that the additional latency recorded from the LEOPARD Cub block cipher grows up to five times greater than no security time recorded above six iterations; however, the times recorded in this analysis assumes the worst case scenario that the

attacker would locate the correct cryptographic key on the last attempt; therefore, further analysis is conducted to determine the average time required by an attacker to conduct a successful brute force attack, in this instance of the analysis this is half of the search space based on the concept of probability theory. Table 8.16 tabulates the time required to conduct a brute force attack over multiple iterations with and without LEOPARD Cub block cipher.

Table 8.16: Time required to conduct a brute force attack on half of the number of attempts over multiple iterations with and without LEOPARD Cub block cipher

Number of Iterations	**Number of Attempts**	**No security time (Seconds)**	**LEOPARD Cub time (Seconds)**
1	2^2	0.001	0.001
2	2^4	0.001	0.001
3	2^6	0.002	0.003
4	2^8	0.004	0.005
5	2^{10}	0.004	0.007
6	2^{12}	0.006	0.009
7	2^{14}	0.007	0.025
8	2^{16}	0.034	0.121
9	2^{18}	0.172	0.945
10	2^{20}	1.360	6.889

Results presented in Table 8.16 shows that the time required to conduct a brute force attack on half of the search space reduces the total time for an attacker to compute; this is because the number of attempts is significantly reduced and enables the attack to be computed in a reduced period of time; therefore, this enables the attacker to find the correct cryptography key in a shorter period of time.

8.5.4 Translation of Findings from LEOPARD Cub Block Cipher to LEOPARD Block Cipher

Analysis conducted in the aforementioned section of the linear cryptanalysis of the LEOPARD Cub block cipher demonstrated that the internal iterations of the block cipher were susceptible on the two rounds conducted; however, the increased number of iterations configured for the block cipher reduces the probability of a successful linear cryptanalysis on the cipher, this is because the attack would require the state at each round to be correct in order to derive the cryptographic key; therefore, the probability of deriving the correct cryptographic key over an increased number of rounds is reduced (Swenson 2008). Validation of this method is presented to demonstrate the significance of this argument.

The number of iterations used by the LEOPARD block cipher further contributes to the complexity of performing a linear cryptanalysis as the number of possible key candidates generated per round increases; this is because at each iteration of the LEOPARD block cipher, the key used by the addition function changes as a result of a direct injection from the key scheduler; the consequence of this operation is that a new key value is selected at each round of the LEOPARD and LEOPARD Cub block cipher operation and requires the attacker to attempt all possible key values at each round of the cipher. The mathematical notation to the calculate the total number of searches required to attempt all possible key values for the linear cryptanalysis over a set number of block cipher iterations is represented in Formula 19.

$$2^{(n \cdot r)} \tag{19}$$

Formula 19: Number of searches required to be undertaken by an attacker over a number of block cipher iterations

The number of attempts required by the attacker can be expressed as the number of key values obtained for one iteration (n) multiplied by the number of iterations (r) to derive the maximum number of possibilities required for the linear cryptanalysis of the non-linear component examined. Table 8.17 tabulates the number of searches required to attempt all possible key values at each round of the LEOPARD Cub block cipher.

Table 8.17: Number of searches required by an attacker to attempt all possible key searches for a set number of iteration of the LEOPARD Cub block cipher

Number of Iterations	**Number of Attempts**
1	2^4
2	2^8
3	2^{12}
4	2^{16}
5	2^{20}
6	2^{24}
7	2^{28}
8	2^{32}
9	2^{36}
10	2^{40}

Analysis of the data presented in Table 8.17 of the LEOPARD Cub block cipher demonstrates that the number of iterations selected for the block cipher configuration increases the number of key attempts for the attacker to conduct in order to analyse all possible key values at a linear rate; this is because the relationship between the number of iterations used by the block cipher and the new key value at each round injected by the key

scheduler results in an accumulation of the number of searches required by the attacker to conduct using known cryptanalysis techniques.

The consequence of the increased number of rounds on contemporary cryptanalysis techniques such as linear cryptanalysis is the time required to conduct the process for all possible key values at each iteration of the block cipher, this is demonstrated with the LEOPARD Cub block cipher as the number of iterations for one round is sixteen possible key values; whilst LEOPARD Cub configured at ten iterations requires 1,099,511,627,776 searches to compute. This value is still feasible to calculate on a computational device; however, the full scale variant of the LEOPARD block cipher uses 2^{128} bit key lengths that would require a greater period of time to conduct the liner cryptanalysis.

Justification of the significance of an unknown substitution box contributes to the outcome of the linear cryptanalysis technique as the maximum number of possible configuration that the attacker would have to attempt in order to perform a full linear cryptanalysis on the full scale variant of LEOPARD block cipher is 256!; this is because this is the maximum number of possible configuration the substitution box could be set to based on the practitioners implementation.

This is further exemplified if the substitution box is randomly generated each time a call to the block cipher is initiated; the consequence of this is that a mask generated for the linear cryptanalysis to analyse this component of the LEOPARD block cipher would not be feasible as the time required to compute each possibility would not be within the crypto-period for the specified research problem of real-time teleoperation and telemetry system as the maximum number of configuration would equate to $8.5782 * 10^{506}$.

The application of the exclusive or (XOR) at the input and output of the block cipher forces the attacker to try all possible combinations before they could conduct the linear cryptanalysis using he plain-text and cipher-text pairs; this results in further delay to the attacker and would therefore reduce the probability of an attacker deriving the correct cryptographic key used by the block cipher for the crypto-period examined for real-time teleoperation and telemetry applications.

The integer addition operation has further resilience against the linear cryptanalysis technique as the addition of two numbers creates a probability of a carry to propagate across to the most significant bits of the input message. The probability of the carry operator occurring in this instance is a $\frac{1}{4}$ probability of occurrence as the condition is only met if the bit value of one and one are added together in the same position; however, the propagation of the carry across the bit positions varies depending on the neighbouring bit values and

could vary the bit position the carry across the 128-bits; therefore, it is difficult to trace the carry operator throughout each round of the block cipher.

8.5.5 Section Summary

The findings presented from the analysis undertaken in this section demonstrates that the LEOPARD block cipher is susceptible to linear cryptanalysis as a result of the linear characteristics of the integer addition; however, in the context of the research problem investigated, the LEOPARD block cipher is suitable as the cryptographic period that the block cipher has to be resilient for is limited to tactical real-time scenarios (i.e. less than 2 hours).

Further findings collated from the analysis undertaken shows that the linear cryptanalysis attack would be effective against the LEOPARD block cipher under the assumption that the same randomly generated substitution box is used throughout each round of the LEOPARD block cipher as the same masks would hold true with a high bias percentage; however, if the substitution box is randomly generated per round, the linear cryptanalysis method would be less feasible as the time required to calculate all possible substitution boxes per rounds is 256 factorial.

In addition to the randomly generated substitution boxes at each round, the cryptographic key generated is directly influenced by the different substitution boxes selected; this is because the key scheduler used by LEOPARD uses the substitution box to derive the cryptographic key used for the session and therefore increasing the time required to undertake the linear cryptanalysis. The final findings presented is that the time required to conduct a linear cryptanalysis on a 128-bit key length that changes per round is not feasible in the context of real-time teleoperation and telemetry as the real-time requirements and mission duration would reduced the probability of an attacker obtaining the correct key value and could experience time that are similar to the time required to conduct a brute force attack against the key search space.

8.6 Discussion

Knowledge obtained from the analysis of the brute force attack against is that the total time required to conduct the attack on a scaled down version of the LEOPARD block cipher is dependent on the number of iterations configured by the underlying block cipher, this is because the total search space that an attacker has to attempt follows an exponential growth; this is consequently reflected in the times recorded for the brute force of the entire search space and half of the search space as the exponential trend has been identified in the analysis of both of the experiments; therefore, this requires an increased period of

time for the attacker to attempt all possible cryptographic keys.

Conclusion of the linear cryptanalysis conducted on the scaled down variant of the LEOPARD block cipher demonstrates that the internal iterations of the LEOPARD Cub block cipher is susceptible to a linear cryptanalysis is applicable towards the non-linear functions used by the cipher; however, the time required to attempt all possible linear approximations and derive the correct key values at each iteration would not be feasible in the context of this research which is the real-time teleoperation and telemetry; this is because the increased number of iterations used by the LEOPARD block cipher would reduce the bias in the probability of deriving the correct key as a result of the entropy injected from the key scheduler; furthermore, the time required to conduct such attacks would not be feasible as the crypto-period examined in this thesis is within the millisecond range; therefore, the LEOPARD block cipher is resilient against linear cryptanalysis methods for the crypto-period of the message in the context of real-time teleoperation and telemetry.

Application of the knowledge acquired from the analysis of the LEOPARD Cub block cipher is transferable to the full scale variant of the LEOPARD block cipher as the block cipher structure and components used by both variants are identical; this demonstrates that the LEOPARD block cipher has a greater resilience to linear cryptanalysis as the number of iteration selected is increased, this is because the attacker has to correctly guess the correct data and key that was added at each round of the cipher, furthermore, the mixcolumns and shiftrows obfuscate linear and differential cryptanalysis as the bit positions for the mixcolumn have an injection of a bit entropy on one of the columns that the attacker has no prior knowledge of and the shift of the byte position prevents differential attacks because the difference in the plain-text input and cipher-text output is masked as a result of the data being rearranged.

The 128-bit full scale variant of the LEOPARD block cipher indicates that a linear cryptanalysis or brute force attack would not be feasible on a 128-bit cryptographic key for the context of real-time teleoperation and telemetry systems, this is because the time required to attempt all possible key values using the linear cryptanalysis technique would equate to times recorded for a brute force attack; this is further exemplified with the increased number of iterations configured by the block cipher as the number of attempts increases at an exponential rate; therefore, for the context of real-time teleoperation and telemetry applications, this method of the speed-centric method applicable based on the crypto-period of the communications during propagation over the communications link.

As the context of this research is focused on real-time teleoperation and telemetry applications; the length of the crypto-period is constrained to the real-time requirements of the

system as the validity of the teleoperation or telemetry message is limited to the milliseconds domain; this further reinforces that the feasibility of a contemporary cryptanalysis methodologies and brute force attacks are not best suited as the LEOPARD block cipher would have sufficient resilience for the crypto-period examined; however, as a result of the analysis conducted; the problem of maintaining the privacy of the shared secret between the transmitter and receiver nodes for secure communication has been identified as a component of the system that requires attention as a possible limitation of the LEOPARD block cipher is the period that the cryptographic key is used.

Contemporary approaches identified in the literature review in Chapter 2 and in the problem analysis of the cryptography in Chapter 7 are configured to either be static, where the same key is used throughout the duration of the mission or pre-computed keys that rotate at fixed intervals and requires memory to store the cryptographic key of the system; therefore, a new philosophy is required as known cryptanalysis methodologies target the cryptographic key in order to infiltrate the secure communications link; therefore, a philosophy that focuses on maintaining the privacy of the shared secret between the transmitter and receiver device is required to mitigate known cryptanalysis methodologies.

8.7 Chapter Summary

The chapter presented the derivation of the cryptographic synergy philosophy with the presentation of intrinsic paradigm and composite concept to derive the speed-centric method presented in this chapter. The speed-centric method presented alternative structural arrangements of the cryptographic primitive has been presented with the PSN and PSPN structures. Derivation of the composite concept was formalised based on the structural arrangement of the block cipher to combine the operation of cryptographic function in order to reduce the number of instruction cycles required to compute the cryptography. Initial analysis demonstrates that the composite concept is a feasible concept with comparable metrics to AES functions; furthermore, the application of the structural rearrangement of the AES-128 block cipher facilitated an instance of the speed-centric method with the presentation of the LEOPARD and the Big Cat Block Cipher Suite.

Dissemination of the intrinsic paradigm using the composite concept and speed-centric method at the following conferences:

- Novel Block Cipher Design Paradigm for Secured Communication - IEEE 10th International Systems Conference, Orlando, Florida, United States - 17-24th April 2016.
- LEOPARD: Lightweight Encryption Operation Permutation Addition Rotation and

Diffusion - IEEE 10th International Conferences on Signal Processing and Communication Systems, Brisbane, Australia - 19-21th December 2016.

Copies of the disseminated conference papers are located in Appendix sections W and X.

Presentation of a instance of a block cipher with the inclusion of the structural arrangement and composite concept to fulfil the stated requirements of the speed-centric method and the intrinsic paradigm; however, the philosophy presented focused on the design of the block cipher to prioritise the speed of the cryptographic process; this introduces the question of how to maintain an element of privacy of the shared secret used for secure data communications between the transmitter and receiver. The next section of this thesis introduces the second part of the cryptographic synergy philosophy with the presentation of the extrinsic paradigm.

9 Proposed Novel Philosophy: Cryptographic Synergy (Extrinsic)

9.1 Introduction

This chapter of the thesis investigates the question poised in Chapter 8 of the Cryptographic Synergy Philosophy of how to maintain an element of cryptographic strength between the transmitter and receiver.

The result of designing block cipher with speed as priority is the reduction in the cryptographic strength of the block cipher as the strength is reduced to enhance the speed of the operation which presents issues with the security and the privacy of the data communicated during propagation.

The focus of the extrinsic paradigm examines the cryptographic key that is required by the block cipher to provide a cryptographic service as it is the known shared secret between the transmitter and receiver and how to maintain the privacy of the shared secret between the communicating devices.

Section 9.2 presents the cryptographic synergy philosophy with the extrinsic paradigm. The introduction of the contemporary philosophies used to maintain the cryptographic privacy of the shared secret used by the cryptographic services; the application of the presented philosophies is analysed in the context of real-time teleoperation and telemetry and facilitated the derivation of the privacy-based method using the interdependency concept. Design and implementation of the key regeneration mechanism and expert unit used by the privacy cryptographic unit (PCU) to meet the privacy-based method is presented. A chapter summary concludes.

9.2 Synthesis of the Novel Cryptographic Synergy Philosophy

This section continues from the cryptographic synergy philosophy presented in Chapter 8, section 8.2 with the presentation of the extrinsic paradigm. Preliminary analysis of the instance of the intrinsic paradigm through the composite concept and speed centric method, the LEOPARD block cipher shows that the paradigm appears to reduced the processing latency incurred at the cost of the reduction in the statistical metrics of the cipher-text output; this indicated that there is a trade-off between the security and the speed of the underlying block cipher and a requirement to preserve the privacy of the shared secret (i.e. the cryptographic key) used for secure communication is presented.

To overcome the trade-off identified with the intrinsic paradigm, this chapter introduces the second part of the cryptographic synergy philosophy with the extrinsic paradigm. Figure 9.1 illustrates an overview of the second part of the cryptographic synergy philosophy.

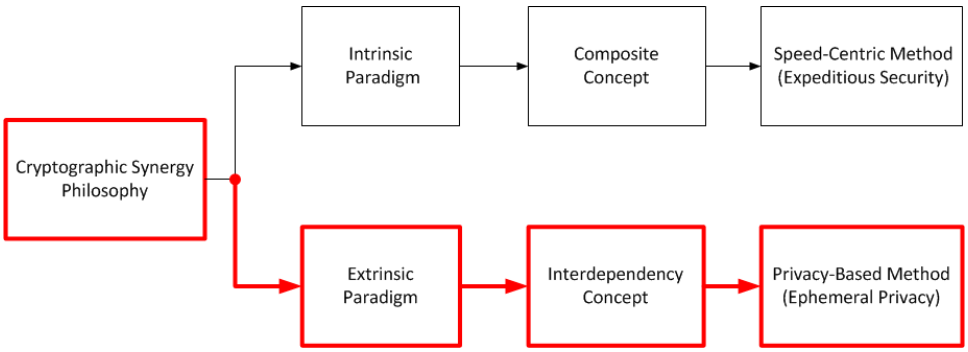


Figure 9.1: Overview of the proposed philosophy (emphasis on the extrinsic paradigm in this chapter in red)

The extrinsic paradigm in this thesis is the external element that is encompassed with the intrinsic paradigm to fulfil the cryptographic synergy philosophy. The purpose of the extrinsic philosophy is to support the intrinsic paradigm by integrating the cryptographic synergy philosophy to the global environment (i.e. the context or scenario it is applied to) instead of the internal security services presented in the intrinsic paradigm.

Application of this paradigm in the context investigated in this thesis is achieved through the interdependency concept where two or more items are dependent on each other to form synergy; this is achieved by combining the sum of whole parts together as stated in the cryptographic synergy philosophy where the intrinsic paradigm is mutually supported and interlinked with the extrinsic paradigm.

In the context of the research undertaken in this thesis, the interdependency concept is achieved through the maintaining the ephemeral privacy of the shared secret through the privacy-based method. The high level overview of the privacy-based method in this thesis is to maintain the privacy of the shared secret utilised by security services (i.e. the cryptographic key) by refreshing or regenerating the ephemeral secret on a variable basis based on internal and external elements. The next section introduced the synthesis of the privacy-based method.

9.2.1 Synthesis of the Privacy-Based Method

The philosophy of security has a broad application in various areas; the generalised definition of security is the state of being free from danger or threat (*Security* 2016). Strength is defined as the capacity of an object or substance to withstand great force or pressure (*Strength* 2016) and is commonly associated with security to define the durability of the

security service. Priority of strength in security is discussed frequently in contemporary philosophies with emphasis on the strength of the security measure; examples identified include the cryptographic key length used by the AES-128 block cipher and the minimum number of rounds required by the block cipher to obtain a cryptographic secure ciphertext output.

An alternative philosophy to overcome the research problem statement specified is the application of privacy to the context of real-time teleoperation and telemetry. The term privacy is the state in which one is not observed or disturbed by other people (*Privacy* 2016). Comparison of security and privacy are often used within the same context as the current view is that privacy is achieved through security; however, in this thesis, the security and privacy are discussed as two separate entities. As the first section of the proposed philosophy focused on maintaining an element of strength whilst increasing the speed of the cryptographic process through the speed-centric method; the second aspect of the privacy-based method prioritises privacy of the transmitted real-time teleoperation and telemetry as the main priority.

The method presented in this chapter is to provide and maintain privacy of the shared secret between the transmitter and receiver nodes with the regeneration of the cryptographic key to increase the duration of time required by an attacker to attempt all possible cryptographic keys. The core of the method interlinks with the speed-centric method with the priority of time as the area of consideration; however, for the privacy-based method, the trade-off is between the number of key regenerations performed to maintain the privacy of secured communications to the time required to brute force the cryptographic secret.

Consideration of a novel key renewal scheme is required for the context of real-time teleoperation and telemetry in order to renew the privacy of the shared secret between the transmitter and receiver device and maintain the secure communication link over the mission duration. Analysis conducted of the LEOPARD and LEOPARD Cub block cipher presented in section 8.5 demonstrates that the entropy of the block cipher was obtained from the entropy injection from the key scheduler into the data path of the block cipher and that the shared secret between the communicating entities is a significant aspect that requires careful consideration in order to have a secure communication link.

Instances where the privacy of the shared secret between the transmitter and receiver node has been documented with the key reinstallation (Krack) attack on Wi-Fi Protected Access version 2 (WPA-2) protocol (NCSC 2017). The analysis of the attack shows that the Krack attack forces the Wi-Fi device to reinstall an already-in-use key by manipulating

and replaying cryptographic handshake messages and force the number only used once (NONCE) and the packet counter to reset to their initial value and enabling an attack on a fixed key (Vanhoef & Piessens 2017). Based on this recent attack, this further reinforces the requirement to maintain the shared secret used between the transmitter and receiver communication node to prevent attackers from conducting passive and active attacks against the communication link.

Investigation conducted in the problem analysis in Chapter 7 showed that the strength and privacy of a block cipher can be segmented into two areas, the data path and the key path. The cryptographic functions used by the block cipher are directly related to its strength; the strength of the cipher-text can be quantified through the metrics of entropy, arithmetic mean and serial correlation; whilst this may show the perceived strength of the output of the block cipher, the concept of privacy is not applicable as the block cipher's algorithm is generally known and is a deterministic function. The privacy between the devices that participate in symmetric secured communication is achieved through the known shared secret between the transmitter and receiver, the cryptographic key; this is because the same cryptographic key is used by the transmitter and receiver to encrypt and decrypt messages.

Cryptographic key management methods used in contemporary applications of block ciphers are applied in two instances, a single static cryptographic key as the secret between the transmitter and receiver device or a fixed number of pre-computed assigned cryptographic keys that are rotated after a set period. Knowledge obtained from the findings of the analysis of the cryptographic key management schemes presented in Chapter 7, section 7.3 showed that the application of a static cryptographic key of 128-bits length is susceptible to a distributed brute force attack; this is transferable to the pre-computed keys that are rotated after a specified period of time.

The contemporary approaches to key renewal are the static key, deterministic key and random generated key rotation mechanisms; limitation with the static key method is that the key does not change throughout the duration of the mission; this could result in the an increased probability of the attacker conducting known cryptanalysis against a block cipher as the shared secret between the communicating entities is fixed.

Deterministic keys attempt to address this issue with the storage of multiple cryptographic key that are rotated periodical to renewal the key used for secure communications; however, limitations of this approach is the fixed periodical time to rotate the keys as this leave a pattern for the attacker to exploit; furthermore, the memory requirements to store multiple 128-bit key values could exceed the memory constraints associated with micro-

controller devices used for real-time teleoperation and telemetry systems.

As part of the novel approach to key renewal, the approach presented is a variable key renewal system that adjust the frequency of the key renewal process throughout the mission duration; however, the requirements stated for this instance of the privacy-based paradigm is for a probabilistic system instead of a deterministic system as this would assist with the obfuscation of attacker profiling the behaviour of the key rotation system that is applicable on static and deterministic approaches; in addition, an element of control must be present in order to adjust the frequency of the key regeneration time in relation to the context and environment it is applied; therefore, in this instance of the privacy-based paradigm, a pseudo-random key rotation mechanism is selected as it fulfils both of the aforementioned requirements specified. Figure 9.2 presents an illustration of the proposed novel key renewal approach against contemporary key renewal methods for an exemplar scenario of a 2^8 search space.

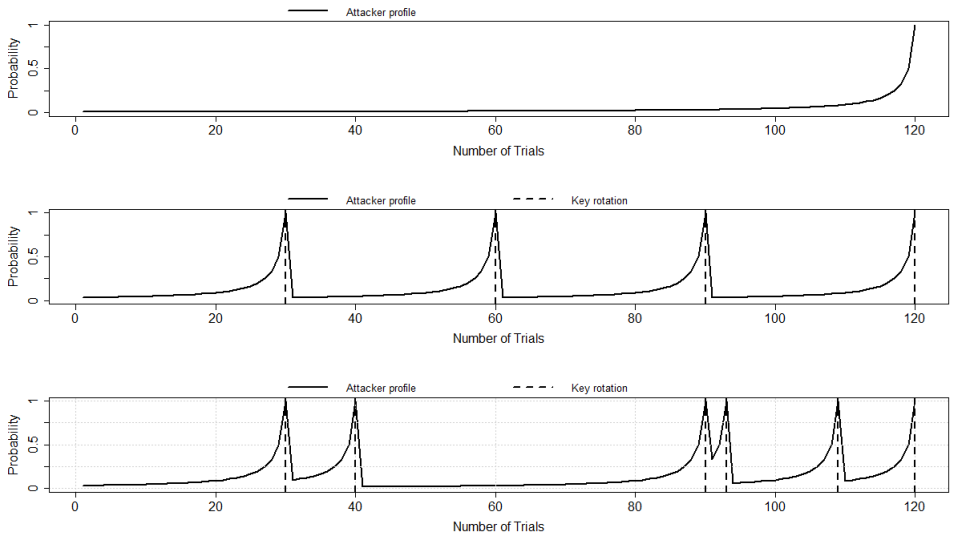


Figure 9.2: Illustration of static (top), deterministic (middle) and the pseudo-random (bottom) key renewal schemes for a 2^8 search space.

The behaviour of the pseudo-random rotation schemes presented in Figure 9.2 differs from the contemporary key management approaches as there is no distinct pattern in the frequency of the key regeneration with the creation of pseudo-random behaviour.

The objective of the variable key renewal scheme is to create a pseudo-random like behaviour of the renewal of the shared secret between the transmitter and receiver in order to obfuscate attackers from profiling the occurrence of the key rotation and force the attacker to reattempt all possible key combination tried in order to ascertain the correct key value used for secure communications. The concept of the variable key renewal scheme stems

from control theory that attempts to regulate systems based on the difference in input and output variables; however, for the context of this research, the method is to create an unstable and chaotic process that impacts on the behaviour of the key renewal process.

The current presentation of the variable key scheme manually varies the frequency of the key renewal; however, this method may not be feasible in real-time teleoperation and telemetry systems as the operator may not have the expert knowledge in the field of security and secure communication; consequently, this could compromise the secure communication link if configured incorrectly; in addition, as memory requirements are constrained in applications that use real-time teleoperation and telemetry systems, the cryptographic key must be generated using on the fly keying in order to reduce the impact on the limited storage of a microcontroller. Application of random key rotations between the transmitter and receiver nodes would fluctuate the number of key rotations conducted; however, the limitations of this approach is the behaviour of the system is unrelated to the context of the situation present and may not best suited for the real-time environment.

Examination of contemporary key rotation approaches suggests that the pseudo-random key rotation methodology with on the fly key renewal scheme is the most suited method for the problem scenario investigated in this thesis as the behaviour of the system can be influenced by a particular action or decision and limits the computational requirements of key storage as the key used for the cryptoperiod is overwritten once the key regeneration process is initiated.

As a result of the initial presentation of the pseudo-random on the fly key renewal scheme; an additional requirement is identified; this is to apply an adaptive system that could adjust the behaviour of the key rotation system based on the perception of the current situation and its environment in an autonomous action. Selection of a pseudo-random on the fly key renewal scheme has been identified as the most suited approach for the context of this research examined in this thesis; however, in order to create a chaotic like output with the key rotation and renewal scheme, the system must have the ability to adapt to the perceived risk based on information that is has received in order to select the most suitable action based on the scenario presented in a computerised manner without the assistance of a human in the system and therefore varies the frequency of key regenerations based on the interpretation of the scenario in an autonomous fashion in real-time.

Contemporary philosophies in the field of classical adaptive control considered the requirement of a system that must adapt to a control system where parameters vary or are uncertain; this is normally achieved through the modification of the control law used to govern the system in real-time in order to achieved the desired behavioural characteris-

tics. Implementation of classical adaptive controller can be achieved using a variety of combinations; Table 9.1 presents the variation of classic adaptive control methodologies applicable towards the context investigated.

Table 9.1: A holistic overview of the methods and components used for classical adaptive control (Derived by Author)

Adaptive Control Type	**Purpose**	**Method Classification**	**Control mechanism**
Iterative Learning Control	Tracking control for repetitive systems	Direct - Over iterations	Feedback
Model Reference Adaptive Control	Stabilised control under uncertain conditions	Indirect - Mathematical reference	Feedback and Feedforward
Self Tuning Regulator	Stabilised control under uncertain conditions	Indirect - Mathematical reference	Feedback

Examination of some classical adaptive control methods presented in Table 9.1 demonstrates that there are a variety of approaches to achieving an adaptive controller; however, the main components that are required for a classical adaptive controller are an controller to configure the set-point of the actuator, an adjustment mechanism to make the necessary changes to the behaviour of the system in order to reduce the error in the expected behaviour and the reference model that is used to benchmark the ideal behavioural characteristics against the output of the system process.

Application of feedforward and feedback control mechanism are integrated into various classical adaptive control approaches dependent on what element of the classical control system behaviour is being adjusted; for example, a feedback control mechanism is prominently used in closed loop systems to conduct a comparison of the input measurement to the output measurement; whilst a feedforward mechanism is used more frequently in open loop control systems as there is no feedback loop to control its action.

Evaluation of the contemporary classic adaptive control methodologies presented in Table 9.1 demonstrates that the design considerations of the methods examined were to stabilise the set-point of the controller in order to regulate an actuator under uncertain conditions; certain fundamental components and methods that are discussed are applicable toward the handling of uncertainty and the unpredictable nature of an attacker in relation to obtaining the shared secret between the transmitter and receiver; however, the application of clas-

sical adaptive control is not best suited for this situation as the specification stated in Chapter 7, section 7.6 is to create a chaotic like behaviour of the duration that the shared secret is used for secure communication between the transmitter and receiver devices.

Implementation method of classical adaptive control systems presented in Table 9.1 are segmented into two approaches, direct and indirect methods; the indirect method is used influence the controller by adjusting the estimated parameters used to influence the control characteristics whilst the direct method to change the rules referenced by the controller directly.

As the proposed privacy-based method is required to adjust its behaviour based on the perceived risk in real-time; a hybrid of direct and indirect methods is chosen, this is because the rules selected to control the behaviour of the system must change in relation to direct or indirect modification of parameters in the system in order to ascertain an perspective of the situation based on internal and external stimuli sense.

The privacy-based method integrates elements of classical adaptive control theory as the requirement to adapt to a situation in real-time is an requirement in order to achieve secure real-time communication for the application; however, the purpose of the privacy-based method is to maintain the shared secret, whilst the classical adaptive control method is to stabilise the operation of the actuator under uncertain conditions.

The concept of the adaptive nature under uncertain conditions is transferred to the privacy-based method with the purpose to variate the frequency of the key regeneration between the transmitter and receiver device by adjusting the process based on the perceived risk of an unpredictable instance in real-time; therefore the classical adaptive control method selected for this instance of the method is the hybrid method based on the requirements specified in the problem analysis and proposed privacy-based method stated. The next section introduces the privacy based paradigm that is derived from the synthesis of the ideas formulated from the privacy-based method.

9.2.2 Privacy-Based Method

The privacy-based method autonomously adapts the privacy of the shared secret between the transmitter and receiver in real-time. The concept of an adaptive system are relevant to meeting the specification and research problem statement as the system needs to dynamically adjust to the situation it is presented with in real-time.

The privacy-based paradigm can be conceptualised based on the concept of maintaining a shared secret between authorised communicating entities; in this instance of the

method, this is maintaining the privacy of the shared secret between the two communication devices by refreshing the shared secret; the symmetric key used by the block cipher.

An analogy of this concept is to prevent unauthorised personnel from listening to the communication between two entities via the use of the known shared secret (e.g the crib sheet or code book); in order to prevent unauthorised personnel profiling the communications through cryptanalysis techniques; the shared secret between the two communicating entities is regenerated by changing the crib sheet or code book used to encode communications; resulting in all previous analysis conducted by the unauthorised personnel being irrelevant as the secret used for secure communication has been renewed. In this instance of the analogy, the secret is the symmetric cryptographic key used for secure communications between the transmitter and receiver nodes.

The privacy-based method requires continuous operation throughout the duration of the mission in order to generate an experience over the course of time; this enables the privacy-based approach to continuously monitor events in real-time with the integration of Giddens' structuration theory as an adaptive system can adjust its operation based on the interpretation of the situation as time processes.

The concept of structuration theory is that a change in a social system has a relationship with two elements, the structure which is the arrangements that limits the choices available and the agent is a group of individuals to act on their own choices with free will; both elements influence change to each other and this pattern is repeated over the course of time to change the structural and agents view of society.

Giddens' structuration theory can be transferred to the context of secure communication links for real-time teleoperation and telemetry as the relationship between human agency and social structure is interlinked with the perceived strength of the shared cryptographic secret and the perceived threat from adversaries over the course of time; this is because both sets of variables are continuously changing over the course of time; however, a computational device alone has no ability to determine when the change is required or if change is necessary.

The human expert may not be able to meet the real-time constraints associated with this context and fail to make the correct decision process in real-time through a manual process; therefore, a requirement for a computerised system is required in order to conduct the human expert tasks without human intervention in real-time. The holistic concept of the proposed privacy-based method is derived into two operations; the privacy and the diagnostic function blocks. Figure9.3 illustrates an overview of the privacy-based method.

As the principle of the privacy unit is to incorporate an adaptive action based on the perceived risk monitored through continuous analysis and undertaking the operations in real-time, The application of the privacy unit is applied to influence the process through a prognosis of the situation and change the output of the system as a result. Figure 9.3 illustrates a block diagram of the incorporation of the privacy unit into a system process model.

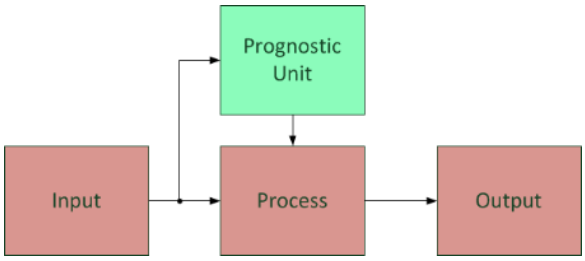


Figure 9.3: Systems model overview with the inclusion of the privacy-based paradigm

The block diagram presented in Figure 9.3 illustrates that the application of the privacy unit is applied between the input and process function blocks in order for the privacy unit to adjust the systems behaviour based on the input process in real-time; this is beneficial in the scope of this thesis because the cryptographic process is modified based on the interpretation of the situation in real-time in order to mitigate possible threats against the communication link.

This instance of the privacy-based paradigm uses a feedforward control loop between the input and the process; this is accuse the frequency of the shared secret between the transmitter and receiver device is driven by the risk of the unpredictable external environment; this would reflect a practitioner selecting the best mitigation strategy to overcome change in the risk level of a perceived security risk and make appropriate adjustments to the security service to remedy the situation.

As the privacy-based paradigm specifies a requirement for a computerised element to adjust the behaviour of the of the system, in this instance the frequency of the key regeneration between the transmitter and receiver nodes; investigation to the contemporary approaches used in classical adaptive control is analysed. Classical adaptive control systems are often used to make appropriate adjustments to a systems behaviour in reference to a decision made or a change in the environment.

Current methods of classical adaptive control systems are conceptualised into two categories; the Proportional-Integral-Derivative (PID) controller and the fuzzy logic controller. The PID controller is commonly associated with closed loop feedback systems to correct

an operation through a mathematical function based on the set-point and the feedback value from the system output in order to stabilise the operation of an actuator.

The advantages of the PID methodology is that the correction mechanism attempts to reduce the error between the set-point and system output through precise calculations; however, the limitations of this approach is the configuration of the PID controller is usually set for a specific context and the time required to calculate the error from the system output may create latency that is not best suited for the context of real-time teleoperation and telemetry.

This method of classical adaptive control does not fulfill the requirements of the proposed privacy-based method as the PID methodology is designed to correct the action of an actuator in order to achieve stable and reliable operation; this would not be best suited in the context of security as a repetitive, consistent behaviour of the regeneration of the shared secret between the communication entities enables the attacker to profile the frequency and conduct timing analysis of the use of the shared secret before it is discarded.

An alternative approach to adaptive control systems is the fuzzy logic controller; the methodology used in this approach classifies the one or many input variables received into a membership categories to create fuzzified values for each input; the values are then passed to the inference engine to determine their associated rule strength or weights based on the inference logic and engine method selected.

The rule strengths derived from the inference engine are then defuzzified through various methods (e.g. weighted average or centre of gravity) to derive the crisp output value used by the system as the new set-point value. Advantages of this method is that its application can be transferred to any context with minimal configuration changes required as the inference engine determines the rule strengths it should use based on the fuzzified inputs; unlike PID controllers that requires reconfiguration of its set-point for each scenario it is applied.

Limitations of the fuzzy logic controller is the additional memory requirements to store the list of membership groups and the rules sets for the inference engine; however, the by-product of this is the reduction in latency to process the operation as a result of the time versus memory trade-off; however, the classification method and inference best reflect the behaviour of a human decision making process as the process does not give a specific outcome like the PID methodology; but instead a probability like scale of the event based on the interpretation and logic configured for the fuzzy logic control method; therefore, this reflects how different expert practitioners would make a decision based on

the scenario that is presented to them.

In the context of this thesis, the adaptive control system selected for this instance of the decision making element of the privacy unit is the fuzzy logic controller as it is best suited to meet the specified requirements identified in Chapter 7, section 7.4; however, modification to the fuzzy logic control is required in order to make this method feasible in the context of security; this is achieved by removing the weighting method to allocate strength to the rule sets specified, this is because the time required to train the weights would not be feasible in tactical security situations such as secure communications between a ground control station to a mobile end-point; therefore, this instance of the privacy-based paradigm uses a fixed rule set for demonstration purposes; however, incorporation of an weighted inference engine for operation and strategic level security is presented as an area of future research.

The data from the stimuli inputs are classified and translated to an expert action by privacy unit and applied to the process block of the system in order to adjust the behaviour of the system. The privacy unit uses a feed forward control system in order to pass the data from the stimuli inputs directly into the privacy unit; this is because the system does not rely on the frequency of the key regeneration to influence the situation; instead, the input stimuli is directly passed into the PCU to adjust the regeneration of the shared secret based on the perceived risk of the external environment.

The utilisation of a feed forward control system with the privacy unit differs in comparison to methods derived in traditional control theory (i.e. a Proportional-Integral-Derivative controller) as the privacy-based method does not attempt to stabilise a system but instead create a chaotic and unpredictable behaviour of a system process in order to prevent an attacker from understanding the mechanism of the system; in combination with the fuzzy-like privacy unit results in a different response to the input stimuli values each time the process is invoked.

As the system adapts to the situation in real-time, the feed-forward mechanism is selected in order to replicate a sensation of feeling that the system uses to adjust the paranoia level; this is because the feed-forward mechanism has no prior knowledge of prior events and is a stateless system that is a more suited representation of a psychological response to a situation; whilst a feedback mechanism is a stateful system that has knowledge of its outcome based on the system output and is more applicable to passing a state back into a system (e.g. a past experience or action). In order to understand how the privacy unit achieves this objective, Figure 9.4 presents a block diagram of the privacy unit mechanism.

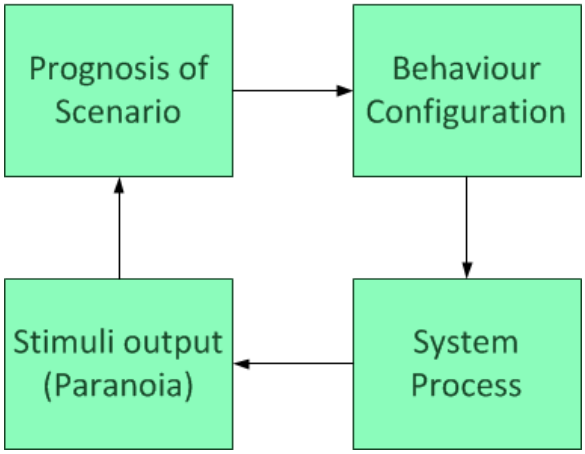


Figure 9.4: Block diagram of the internal mechanism of the privacy unit

The privacy unit is comprised of four function block in order to achieve a chaotic and unpredictable system which are the prognosis of the scenario, behaviour configuration, system process and the stimuli output. An initial prognosis of the situation is conducted first where the privacy unit classifies the data obtained from the input stimuli into information based on the expert interpretation. The outcome of the expert interpretation is used to adjust the behavioural configuration of the system process; in this application of the privacy unit, this will adjust the number of key regenerations undertaken by the transmitter and receiver device.

Once the behaviour configuration of the system has been derived, it is applied to the system process to reflect the prognosis derived by the privacy unit. The final section outputs a stimuli output value named paranoia level which influences the duration between the key regeneration mechanism and the initiation of a new prognosis. The purpose of the paranoia stimuli is to create a pseudo-psychological experience for the system in order to generate an experience or feeling of the situation that will influence the behaviour of the process mechanism to reflect the state of mind of the computerised expert in the system.

Relationship of the paranoia level and the privacy of the shared secret are interlinked in the proposed privacy paradigm as the psychological state of the system reflects how frequent the regeneration of the shared secret based on its perceived level of privacy of the secure communication link. The holistic concept of the proposed privacy-based method is derived into two operations; the privacy and the diagnostic function blocks. Figure 9.5 illustrates an overview of the privacy-based method.

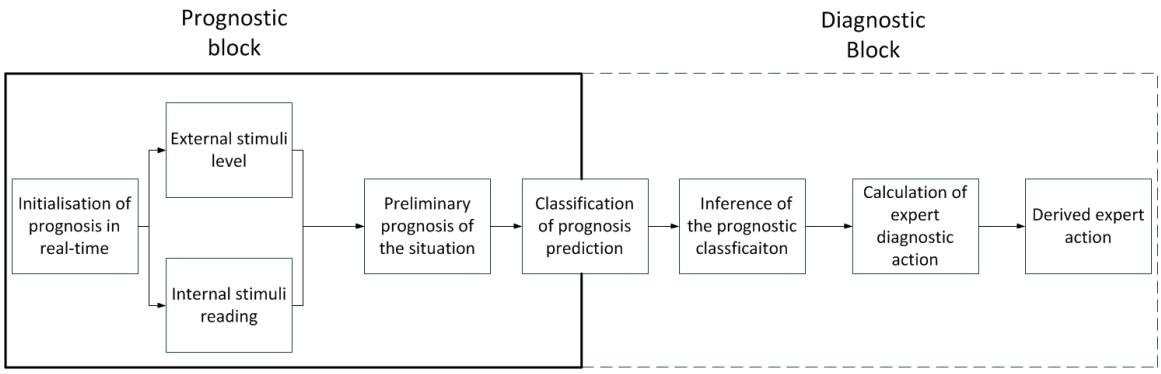


Figure 9.5: Block diagram of privacy based paradigm

Advantages of the proposed privacy-based method is that the system can be adjusted to the scenario analysed; this enables the concept to be transferable to a variety of contexts that require an expert interpretation of the situation without human intervention; examples include the prognosis of time required before component failure of a machine to the prognosis of natural disasters based on environmental changes.

The benefit of the privacy-based method from a general prospective is that the expert knowledge is applied and utilise for the detection and interpretation of the scenario in a given instance of time to determine the likely outcome; this initial understanding based on the analysed phenomena can provide a positive, neutral or negative prognosis of the scenario and conduct relevant action based on the generated prognosis.

Application of the privacy unit in the context of the key regeneration of the shared secret between the transmitter and receiver device meets the specification stated that and the proposed method as the expert interpretation would vary the length of time the shared secret is used before it is regenerated between the communicating devices; this differs from current key management approaches stated in Chapter 2 literature review as symmetric key methods selected either use a static or pre-deterministic key methods to ensure privacy of the shared secret between the communicating entities; whilst the application of the privacy unit adds variability in the duration that the shared secret is used; this enables the shared secret to be used for a minimum crypto-time period before it is changed or use the same key for a longer crypto-period; in addition, the privacy unit varies the crypto-period in real-time based on the real-time prognosis of the scenario; therefore, this concept is versatile and adaptive in comparison to contemporary key management schemes that are static or behave in a deterministic manner.

The design and the implementation of the privacy based paradigm is categorised into two sections; first, the design and implementation of the key regeneration mechanism to preserve the privacy of the shared cryptographic secret between communicating entities is

presented; followed by the design and implementation of the privacy cryptographic unit to select a course of action based on the expert interpretation.

9.2.3 Design and Implementation of the Privacy Cryptographic Unit Key Regeneration Mechanism

This section of the chapter introduces an instance of a novel approach derived from the privacy-based method, known as the privacy cryptographic unit (PCU). The PCU is a variable and adaptable cryptographic system that adjust in real-time and was designed to provide adaptive and autonomous secure communication link for real-time teleoperation and telemetry.

The overview of the method is to forecast the likely outcome of threats through its external interpretation of the sensed external environment; psychological elements of paranoia are used to construct an experience of the likelihood of an attack and is influenced by the external sensing of the environment to determine the paranoia level of the system. The result of the change in the paranoia level impacts the frequency of the key regeneration in real-time to mitigate online and offline brute force attacks. Figure 9.6 illustrates the adaptation of Giddens' structuration theory based on the privacy-based method as a concept for the PCU real-time teleoperation and telemetry security method.

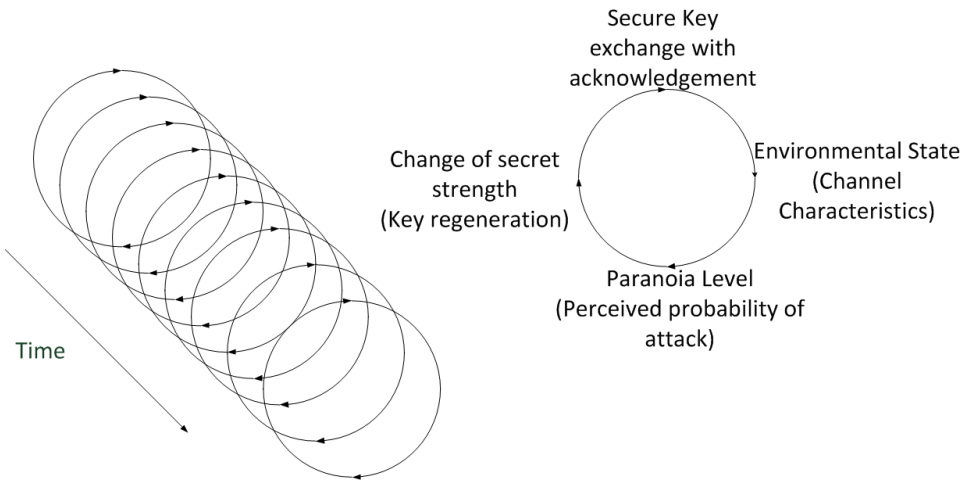


Figure 9.6: Adaptation of Giddens' structuration theory for an approach to real-time teleoperation and telemetry security

As presented in Figure 9.6, the design of the PCU key regeneration mechanism is the reactive element of the system as it initiates the key regeneration based on the conditions of the internal and external environment. The six components that are processed by the PCU are the total size search space of the cryptographic key, the signal level of the communication link, number of packets transmitted to the receiver, the initial paranoia level,

the mission time set by the human operator and the process selection.

The design of the PCU key regeneration mechanism is the reactive element of the system as it initiates the key regeneration based on the conditions of the internal and external environment. The six components that are processed by the PCU are the total size search space of the cryptographic key, the signal level of the communication link, number of packets transmitted to the receiver, the initial paranoia level, the mission time set by the human operator and the process selection. A state diagram of the internal mechanism of the PCU used for the privacy unit is presented in Figure 9.7.

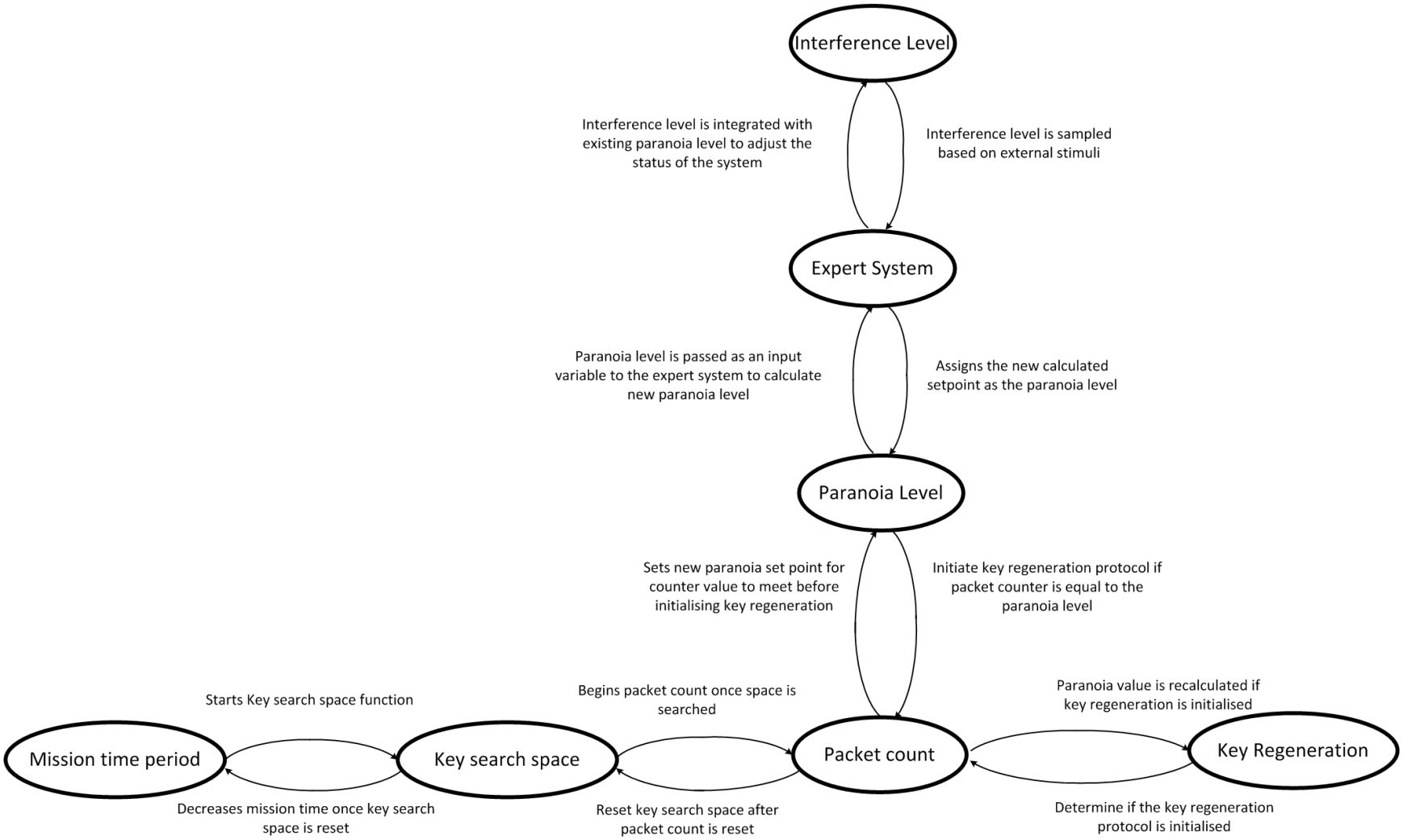


Figure 9.7: State diagram of the privacy cryptographic unit overview

All of the specified variables are inputs into the PCU; the variables are processed by the PCU with two outputs, whether to initialise the key regeneration protocol and the new paranoia level set at a result of the process and is feedback into the PCU for the calculation of future events.

The operation of the PCU is as follows, the PCU has a pre-programmed paranoia level set by a human operator at the beginning of the operation to pre-set the experience for the privacy unit. A mission time is specified by the human operator and is used to determine the period that the PCU is required to predict foreseeable events; the mission time is influenced by the time required to search through the byte positions of the cryptographic key length. The packet counter is benchmarked against the paranoia level set to determine when a key regeneration is required. The signal level of the external sensing through the wireless extensive service set identification (ESSID) is used as a measure to adjust the paranoia level based on the sensed change in the environment to generate a new experience in that particular period of time. This operation is initialised by the transmitter before a message is transmitted.

The initialisation of the key regeneration is achieved through packetised transmission between the transmitter and receiver. The overview of the packet structure used for the PCU key regeneration function is shown in Figure 9.8.

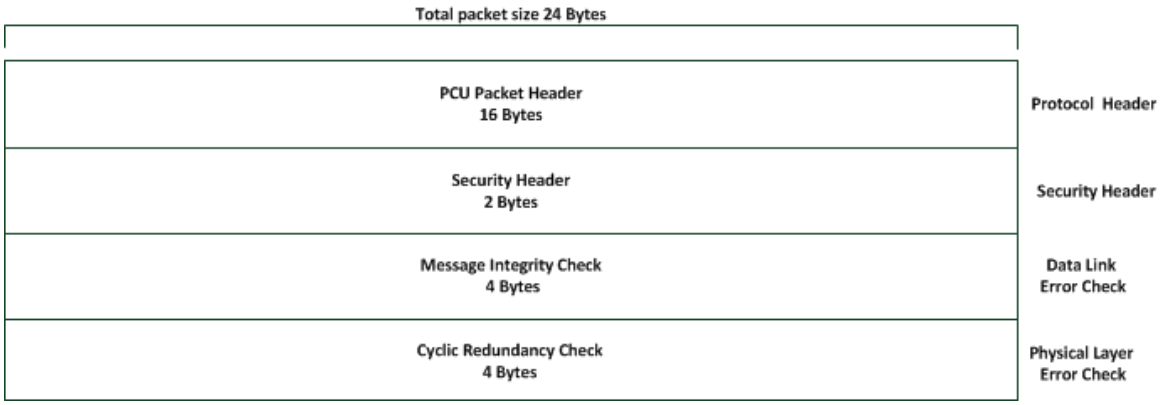


Figure 9.8: Packet structure of the PCU key regeneration protocol

The packet structure of the PCU key regeneration protocol is segmented into four areas; the packet header, security header, message integrity check and the cyclic redundancy check (CRC). The packet header field is assigned to the specified protocol format chosen; the security header contains the initialisation flag byte value for the key regeneration between the transmitter and receiver; the remaining two bytes of the security header is reserved for the counter value used for the random payload generation which is specified in the PCU key regeneration mechanism. The message integrity check appended to check for intentional modification of the packet. The CRC check is applied to check for unin-

tentional errors from the physical layer of the communication link, the CRC is generally calculated using hardware to achieve faster speeds.

To synchronise the transmitter and receiver with the same cryptographic key, the transmitter initiates the key regeneration protocol based on the output of the PCU. The concept selected is a challenge response to instigate and authenticate that the receiver has regenerated a correct cryptographic key through a TCP connection based three way handshake; Figure 9.9 illustrates the schematic operation of the key regeneration protocol between the transmitter and receiver.

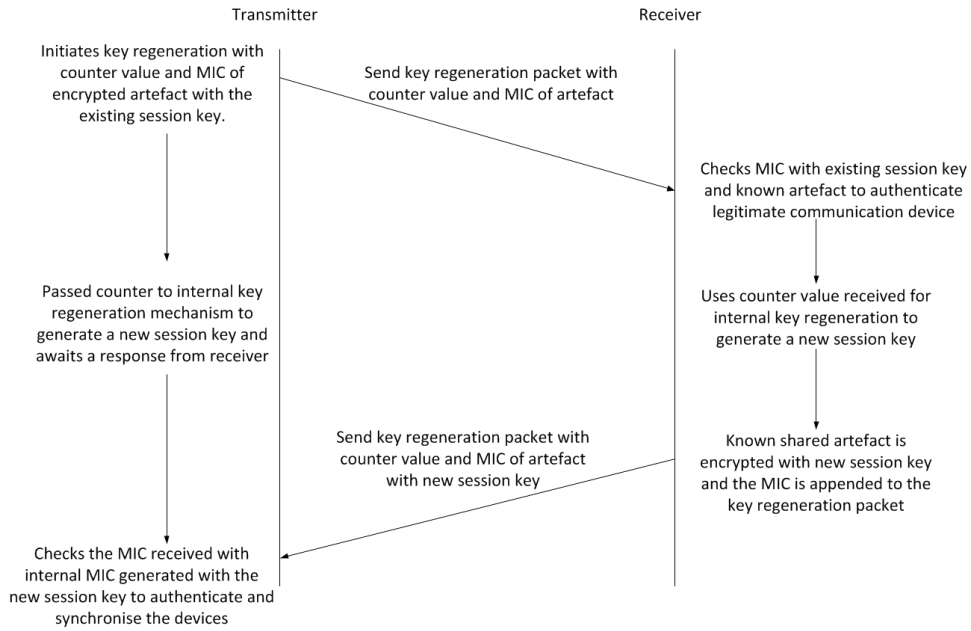


Figure 9.9: Key regeneration protocol process between the transmitter and receiver

Resynchronisation between the transmitter and receiver is required as the non-ideal nature of the communication link may result in packet corruption or loss. To overcome this possibility, the resynchronisation method attempts to resend the message from the transmitter to the receiver for a maximum number of times preset by the human; each attempt will increase the paranoia level of the system as it is assumed that the more retries that are required, the higher the probability that the communication channel between the transmitter and receiver is under attack.

The key regeneration mechanism proposed in this thesis is an adaptation of a challenge response protocol used in protocol such as secure shell (SSH). The operation of the key regeneration mechanism is conducted internally on the transmitter and receiver nodes and the exchange of the symmetric keys are not transmitter over the unsecure communication link as the attacker could conduct passive analysis of the transmitted data over the wireless communication link and obtain the symmetric key during the key exchange process;

instead, a key regeneration protocol is presented to achieve key regeneration without the exchange of keys over the communication. The internal key regeneration mechanism used by the transmitter and receiver is presented in Figure 9.10.

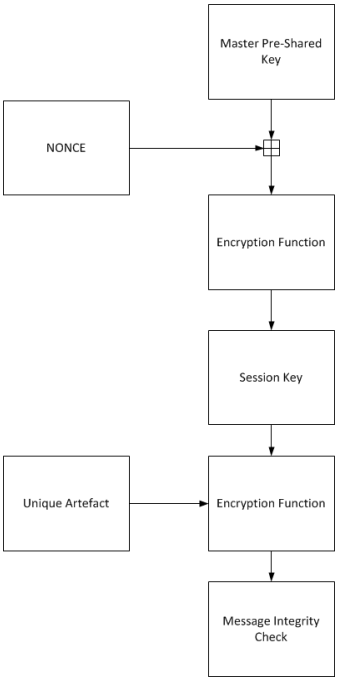


Figure 9.10: Internal key regeneration mechanism of the transmitter and receiver communication devices

A master pre-shared key is configured by the practitioner on the ground control station and the mobile application before the mission is commenced over a direct connection using a wired communication link. The master-key is passed through a function (e.g. block cipher or linear-feedback shift register) to derive the session key used by the ground control station and UAV for that instance of time.

A number only used once is added to the most significant bit of a copy of the master pre-shared key to vary the value of the function output; furthermore, the unique serial number of the ground control station and the UAV are added to the master pre-shared key before it is input into the function to ensure all bytes of the master pre-shared key are masked and synchronize the ground control station and UAV with unique artefacts to facilitate secured symmetric communication links.

The initialisation of the key generation mechanism as depicted in Figure 9.7 is initialised once the packet counter set by the paranoia level has been met; once this conduction has been met, the key regeneration mechanism process is instigated by the ground control station only. The mechanism of the PCU key regeneration protocol is based on the concept of a challenge response between the transmitter and receiver device. When the

PCU initialises the key regeneration protocol, the number only used once value used as the input with the master pre-shared key is set and placed into the security header of the packet. The message integrity check (MIC) is generated based on the encryption of the unique artefact of the ground control station serial number and is appended to the key regeneration protocol message before it is transmitted to the receiver device.

The receiver device stores the key regeneration packet and stores the security counter value (number only used once) and the MIC of the message; the number only used once added to a copy of its own pre-configured master pre-shared key and is passed through the same function as configured on the ground control station to generate a new session key. The new session key is used to encrypt the unique artefact of the serial number of the ground control unit and derives the MIC; if the MIC generated is equal to the MIC received from the key regeneration protocol, an encryption of the UAV serial number is conducted and the MIC is appended to the key generation packet and is sent to the transmitter to conduct a similar operation to determine if the MIC is correct and the same session key is used.

In the event that the key regeneration protocol between the ground control station and UAV was unsuccessful, the current session key used between the ground control station and the UAV is stored into a temporary buffer as a fail-safe method and can be reused to reinitialise the protocol with a new number only used once value stored in the protocol header.

Application of the proposed method would mitigate issues associated with key regeneration; this is because the key regeneration mechanism proposed uses a master pre-shared key configured by the practitioner for the transmitter and receiver device before initialisation and is masked with a number only used once value and a process function in order to generate a new session key; this prevents the attacker knowing the master key used for the key regeneration process and how the number only used once value is applied to the system to derive a new session key.

Additional benefits of this approach is the key exchange process does not transmit the new session key across the communication link as the protocol appends the number only used once value and the MIC from the encryption of the unique artefacts; this is beneficial as the attacker could not derive the session keys that are transmitted over an unsecure communication link or acquire all of the components to replicate the key regeneration mechanism.

The number of key regenerations calculated for the specified mission period is varied de-

pendent on the probability of the attacker successfully conducting a brute force attack against the cryptographic key search space; this variable is directly controlled by the paranoia block of the PCU as the human operator predefines the probability of an successfully attack based on the interpretation of the context; in addition, the paranoia value is constantly changing during the mission period, therefore, the PCU recalculates the initialisation point to perform a key regeneration.

The basic version of the PCU mechanism derives the new paranoia level by the combination of the initial pre-set paranoia level set by the operator with the signal strength obtained from the ESSID through a NOR logic gate to generate a new set-point value for the packet counter; it is assumed for this implementation the operator would input an initial paranoia level between five to ninety-five percent to prevent a lock state condition. Figure 9.11 graphs the impact of the variable set-point when the received signal level is decreased.

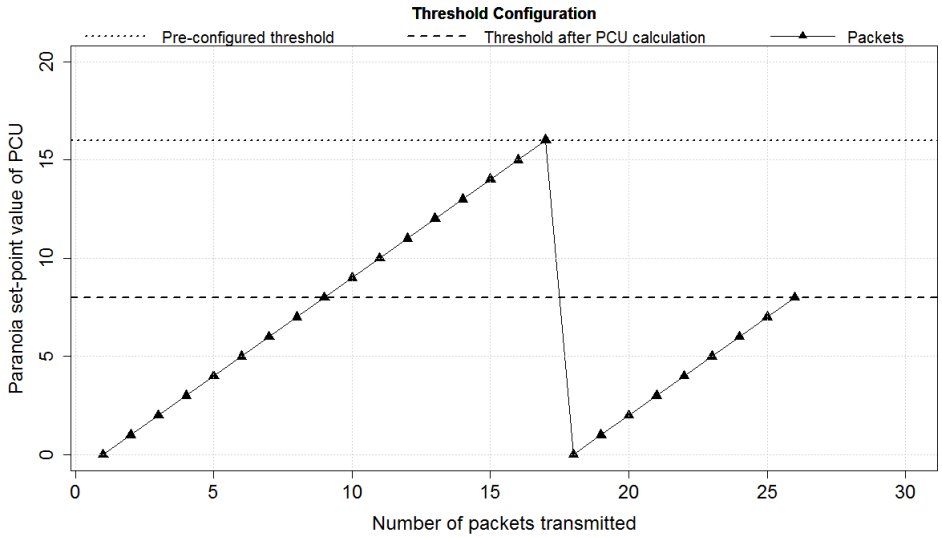


Figure 9.11: Visual representation of the reduction of the paranoia set-point value with a reduced signal level on the communication link.

The packet counter is used as an incrementing counter and is compared against the set-point value to determine when the key regeneration process is initiated. The mechanism is similar to the method used for digital comparators as the key regeneration is not conducted unless the packet counter and the set-point are equal in value; however, as the set-point value is updated after initiation of the key regeneration protocol. The set-point for the packet counter value is dynamic and based on the external environment.

Once the initial paranoia set-point value has been reached by the number of packets transmitted; the paranoia value is recalculated based on the real-time sampling of the internal and external environment; as the external variable measured increases, the number of

packets required to meet the new paranoia set-point is reduced and therefore the key regeneration process is performed more frequently and maintains the privacy of the shared secret between the transmitter and receiver device as the shared secret has been modified. The process is also reversible in situations where the PCU has calculated a low paranoia level based on its input stimuli; this impact causes the threshold to be increased and results in a longer duration that the shared secret is used before a key regeneration between the transmitter and receiver is initiated.

9.2.4 Design and Implementation of the Privacy Cryptographic Unit Adaptive Control Making Security System

The proposed method stated in this chapter discussed the requirement of a system that makes a decision based on the internal and external stimulus to influence the sub-conscious process and derive the correct action for the situation. The basic operation discussed in the design and implementation of the PCU key regeneration does not incorporate expert logic or rules to take a correct action. To achieve this an modified variant of an adaptive control system is required in order to be proactive and select the correct decision based on the information collated.

The implementation of the privacy cryptographic unit system in this thesis is segmented from the main computational device that is activated once the requirement of a key regeneration is initiated by the main processing unit; this is to enable practitioners to reconfigure the PCU in real-time and implement software or hardware variations of the approach. Figure 9.12 illustrates the system diagram of the modified adaptive control system to the processing device.

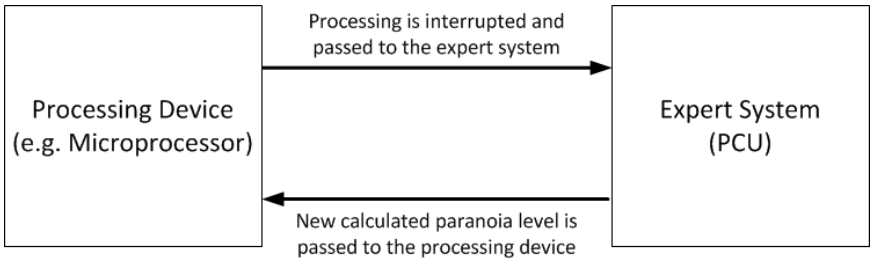


Figure 9.12: Overview of the interaction between the PCU and the main processing unit

The role of the PCU is to influence the operation of the key regeneration mechanism. The modified adaptive control system is segmented into five processes; the input variables, membership classification, inference of rules and the new paranoia output value. A block diagram of the interaction between the components of the PCU is presented in Figure 9.13.

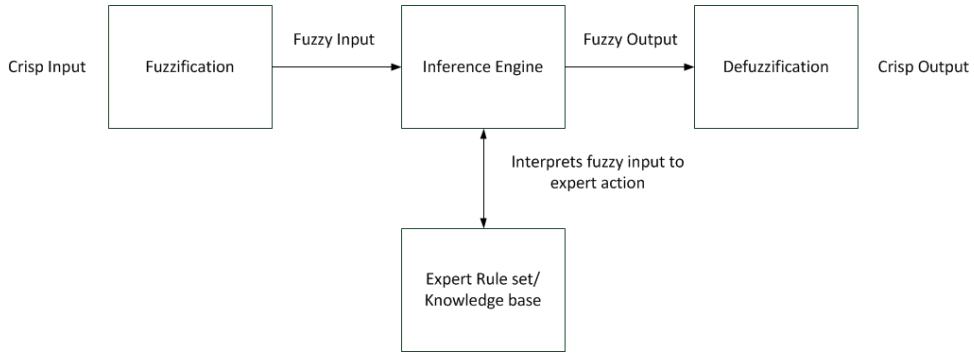


Figure 9.13: Block diagram of the PCU adaptive control system (Botura et al. 2002)

Design and implementation of the expert knowledge base of the modified adaptive control system was the main consideration of the privacy cryptographic unit as the design of the expert rule sets and the behaviour of the modified adaptive control system contributes to the actions selected in relation to the initial prognosis.

The implementation method selected is a mapping system that quantifies level that the paranoia state is adjusted based on the interpretation of the system inputs by the privacy cryptographic unit. In this instance of the privacy cryptographic unit, the relationship between the interference level of the communication link is used as the system input which influences the number of key regenerations undertaken.

The relationship between the interference level and the number of key regenerations performed is justified in this scenario as it is assumed that an attack would require a wireless interface in order to conduct passive and active attacks against the communication link in scenarios where a mobile element is present in the system.

The interference from an intentional or unintentional jamming attack has an impact on the paranoia and consequently increases the number of key regenerations conducted; this acts indiscriminately as the system does not distinguish between known or unknown attack vectors against the communication link and assumes a worst case scenario of a disturbance to the system; in addition, the impact of packet error and packet loss as observed in the Chapter 5, section 5.2.1 demonstrates that increased interference on the communication link contributes towards the problem as real-time teleoperation and telemetry data is either dropped or corrupted whilst in propagation; consequently, the PCU classifies this observation as a characteristic of an unsecure communication link.

Interpretation of the input stimulus for the privacy cryptographic unit was achieved using a fuzzy-like system to classify process the result into a tangible output for the paranoia level. The classification of the input stimuli was achieved by a fuzzification-like process

to transfer the real-world input values into fuzzy-like values through the use of membership functions to enable the privacy unit to interpret the values into tangible classifications.

Two separate membership classifications were derived for this instance of the implementation; the first fuzzification-like process transfers the measured interference level of the communication link and the second membership classification rates the paranoia level to its fuzzified-like value; each membership categorisation consists of five membership groups to represent, very low interference, low interference, medium interference, high interference and very high interference levels; this process is replicated for the paranoia membership groups. Table 9.2 tabulates the classification of two input stimuli values to their associated membership groups.

Table 9.2: Classification of input stimuli values to their associated membership groups

Membership Group	**Very Low**	**Low**	**Medium**	**High**	**Very High**
Input Stimuli value (%)	0-20	20-40	40-60	60-80	80-100

The membership functions presented in Table 9.2 are formed using a triangular membership function; within each membership group, the strength of the input to the associated rule set is scaled between a value of zero to represent zero percent association and one to represent a hundred percent strength; an example of this analogy for a medium membership group would be zero percent weighting for values closest to twenty or forty percent; however, a value that is closes to thirty percent would have a weighting closer to one hundred percent; this is referred to the central point.

Calculation of the membership strengths is achieved by the highest percentage value of the input signal away from central point of the membership classification it is classified into to derive its membership strength; the remainder of the membership strength is associated with the neighbouring membership classification; this is derived dependent on what side of the triangle the percentage value is calculated (e.g. for a low membership rule strength between twenty and thirty percent, the remainder rule strength would be associated with very low membership group, whilst percentage values between thirty and forty percent, the remainder of the rule strength would be associated with the medium category).

The evaluation of the strength of the input to the membership category was achieved using a series of if-else logic statements to classify the signal input into its associated membership group; as stated in Table 9.2, the classifications are set within boundaries; however, in a fuzzy-like system; it is unlikely that a input will be classified in one category but instead in more than one category. As a fuzzy-like system uses associated rule strength

to quantify the input signal; the categorisation of the value could be associated with multiple membership categories; this is calculated by using a Mamdani-like inference system.

The logic used in this method of the Mamdani-like inference system is the bitwise AND operator to compare the strength of each fuzzified input membership classification and select the minimal value as the weight used for the interpretation of the minimal value to the associated rule selected. The outcome of the minimum output classifications of the paranoia and interference level are then inferred by the knowledge rule based to determine the weighting used for the system.

The pre-set rules set in the knowledge base system are categorised into two approaches, linear and non-linear rule based systems. The linear knowledge rule based system applies a fixed increment value between the rule sets in the knowledge base and impacts the calculated crisp value by increasing or decreasing the value in a linear pattern; whilst non-linear approaches to knowledge rule bases adjust the calculation of the strength of the rule set in a non-linear fashion (e.g. exponential or logarithmic). Modification of the knowledge rule based block is undertaken with the application of a hybrid rule base system. Table 9.3 tabulates the values associated with the linear and non-linear expert rules sets for a varying input stimuli classification and a static paranoia classification.

Table 9.3: An example of the Linear and Non-Linear rule sets weights to associated values with a varying interference stimuli levels

Paranoia Stimuli Classification	**Interference Stimuli Classification**	**Linear Value (%)**	**Non-Linear Value (%)**
No Threat	No Threat	0.0%	0.0%
No Threat	Low Threat	1.5%	0.7%
No Threat	Medium Threat	3.0%	3.0%
No Threat	High Threat	4.5%	9.0%
No Threat	Very High Treat	5.0%	27.0%

Table 9.3 presents an instance of the percentage change in the paranoia level according to the classification of the previous paranoia level and the interference level recorded; however, this represents one instance of the expert rule set as the selection of the rule sets used by the privacy unit varies based on the configuration of the paranoia level threshold set by the practitioners; details of the expert rule sets used for the validation of the PCU in Chapter 10, section 10.4 and 10.6 are presented in Appendix Q.

The final stage of the privacy cryptographic unit process is to conduct a defuzzification-like process of the values obtained from the inference of the rule set to obtain the output value. The defuzzification-like method selected in this instance is the weighted average method to derive the average between the two classification values to prevent conflict between two membership classifications of the two input variables and derive an output crisp value used for the paranoia level of the privacy unit.

The crisp value obtained from the defuzzification-like process of the input variables is added to the paranoia value to derive the new paranoia level for the system; this outcome adjusts the set-point level for the counter to reach before re-initiating the key regeneration protocol by increasing or decreasing the set-point threshold before the condition of a key regeneration is met.

The selection of the expert rule sets used by the privacy cryptographic unit is achieved by varying the rule sets chosen based on the paranoia level calculated; this is to reflect the change of opinion of an expert practitioner in relation to the change in the scenario analysed and is influenced by the paranoia level threshold set by the practitioner. Figure 9.14 illustrates the additional modifications undertaken in the knowledge rule base function block of the modified adaptive control system.

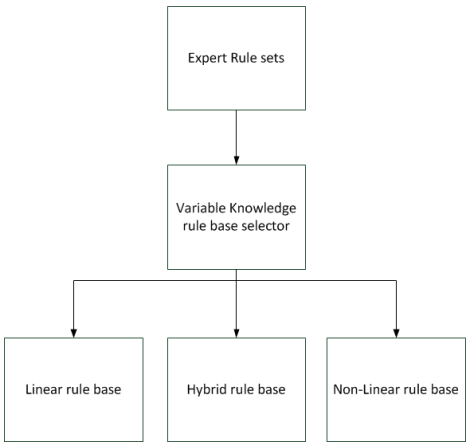


Figure 9.14: Expert modified adaptive control system rule set selection for the privacy cryptographic unit

The variable knowledge rule base block facilitates a hybrid approach between the selection of the strength of the rule sets as the duration of the mission progresses; an example of this instance presented in this thesis is the combination of both linear and non-linear rule sets as this impacts the rate of change between the current paranoia level set and the new paranoia level to be used.

Justification for a hybrid of rule set is to enable flexibility and provide an appearance of a random-like rate of change of the paranoia level used to initiate the key regeneration process as the practitioner can define the boundaries within the variable knowledge rule base block to determine when to change the block rule sets and enables irregularity in the key regeneration mechanism.

Alternative methods such as AI could be applicable to the design of the privacy cryptographic unit in situations that requires complex mapping between unrelated variables in order to derive an action for the system as machine learning could be applied to learn how these relationships interlink to influence the security of a system (i.e. influence the time between key regenerations); however, as the focus of the research is on the secure communication link with real-time constraints; this has been classified as a future area of research that could be applicable to alternative applications that require a prognosis of a situation without any associated constraints in computational or time resources.

9.3 Discussion

The overarching philosophy presented differs from the conventional philosophy of the selection of a single key at a fixed number of bits as the philosophy presents the view of maintaining the privacy of the shared cryptographic secret by adjusting the frequency of key regenerations between the transmitter and receiver over the course of the mission duration.

The benefit of the philosophy is that it is applicable to any cryptographic key length and is transferable to all block cipher lengths as the frequency of the key regeneration obfuscates the attacker by resetting the probability of all previously attempted brute force attacks becoming feasible; this is because the attacker and defender are equated as the PCU forces the attacker to attempt all known items in the search area again once the key regeneration has taken place; therefore, the exponential decay trends associated with contemporary key rotation approaches are transferred to a linear operation which cancels the advantage of additional attacker machines conducting the attack in parallel.

The privacy based paradigm presented proposes the privacy cryptographic that is a combination of two mechanisms, the key regeneration mechanism as a method that initiates the key regeneration between transmitter and receiver and the privacy unit that controls the feedback to control the internal paranoia level set for the key regeneration through an expert decision making system. The application of internal and external stimuli throughout the duration of the mission to make changes in real-time; similar to the operation of the brain where repetitive conscious actions influence the sub-conscious behaviour and

impact the actions undertaken.

The difference with this instance of the proposed privacy-based method is that the PCU does not attempt to think at the conscious level like an AI system and it does not learn about the context of the situation like machine learning systems; the PCU instead follows an expert decision making systems approach; in this instance, it is a risk driven approach to adjust the duration between key regenerations based on the perceived internal and external risks sensed.

This approach enables flexibility and ease for the practitioner to implement expert rule sets for different scenarios and change the frequency of the key regeneration based on the calculated paranoia value based on the internal and variables; facilitating the philosophy of trading the possible searches in a given space for the time required to search all possibilities through the frequency of the key regeneration.

9.4 Chapter Summary

The chapter presented the derivation of the extrinsic paradigm through the interdependency concept. The derivation of the privacy-based method differentiates from contemporary philosophies for secure communication as the emphasis of the philosophy prioritises the privacy of the shared secret between the transmitter and receiver device over the cryptographic strength and security. The application considered for the privacy-based method was targeted for the cryptographic key used to facilitate a secure communication link between the transmitter and receiver.

The method presented to represent an instance of the privacy-based method through the PCU. The integration of the key regeneration mechanism which refreshes the privacy of the shared secret between the transmitter and receiver through the regeneration of the cryptographic key used to mitigate brute force attacks.

The mechanism presented is integrated with an expert decision making system that incorporates expert logic to derive a prognosis of the situation based on the psychological perception and interpretation of the external environment in real-time and adjust the frequency of the number of key regenerations used through the internal paranoia level of the system over the course of the mission duration; therefore, facilitating a variable and adaptive technique that adjust the cryptographic period of the shared secret to maintain the privacy of the shared secret in real-time for time constrained communications.

The next chapter presents the validation of the speed-centric and privacy-based methods

through the validation of the instances derived, LEOPARD and the PCU in the context of real-time teleoperation and telemetry.

10 Validation of The Synthesised Novel Cryptographic Synergy Philosophy

10.1 Introduction

This chapter presents the validation of the proposed cryptographic synergy philosophy in a specified scenario through a series of experiments. The structure of this chapter is as follows; first, the validation scenario is presented, followed by the validation of LEOPARD. The validation of the basic implementation of the PCU is presented; followed by the behavioural characteristics of the privacy unit used by the privacy cryptographic unit (PCU). A chapter summary concludes.

10.2 Validation Scenario

The scenario presented is a manually operated UAV controlled by a human operator from the base-station; the course set out is a rectangle circuit where the UAV captures telemetry data at the straight of the circuit and transmits the images to the base-station over a two hour mission duration. Dual-communication links (uplink and downlink) are used to transmit burst, event-driven messages to teleoperate the UAV and on the downlink obtained telemetry from the UAV.

Rules and regulations specified by the UK's CAA does not allow the flying of an UAV within a fifty metre proximity of residential areas. The university of Greenwich's health and safety requirements does not permit the flying of an UAV on-site for a real-world validation, therefore, the analysis of the validation is undertaken through modelling, simulation and emulation.

10.3 Validation of Derived Instance: LEOPARD

10.3.1 Profile Comparison of LEOPARD and AES-128

The first test compared the statistical output of the cipher-text of LEOPARD against the standardised AES-128 cipher over a varying number of rounds. The message size selected for this test was two-hundred-and-fifty-six bytes, the number of rounds selected ranged from one to ten rounds. The mode of operation was ECB mode to modify all byte positions of the payload; sixteen bytes of the payload were encrypted per encryption call; the cipher-text output was stored into a text file. The cipher-text output was analysed with the entropy number tester (ENT) software using the metrics of the entropy, arithmetic mean and serial correlation analysed. Figure 10.1 and 10.2 illustrates the entropy and arithmetic mean scores of LEOPARD and AES-128 over a varying number of rounds.

10.3.2 Entropy and Arithmetic Mean Test

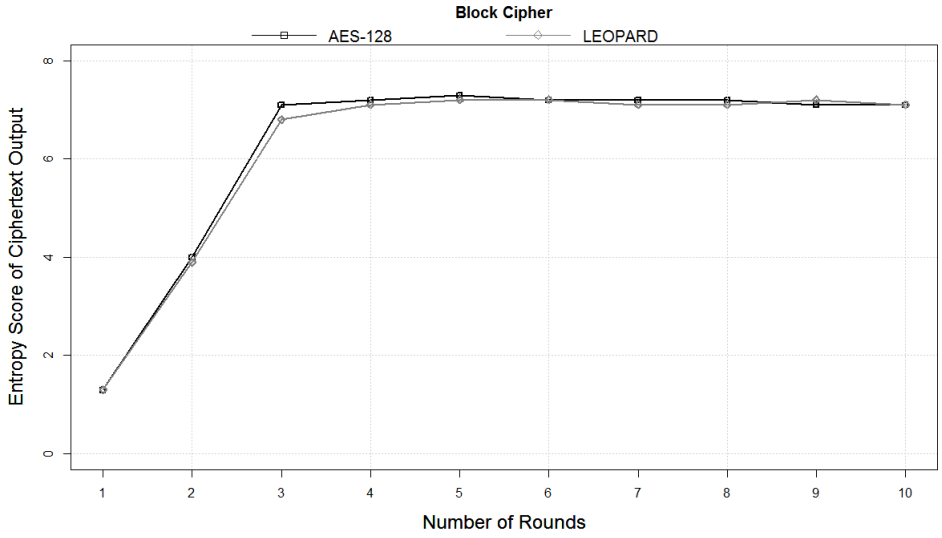


Figure 10.1: Entropy of the cipher-text output for LEOPARD and AES over a varying number of rounds for a two-hundred-and-fifty-six byte message

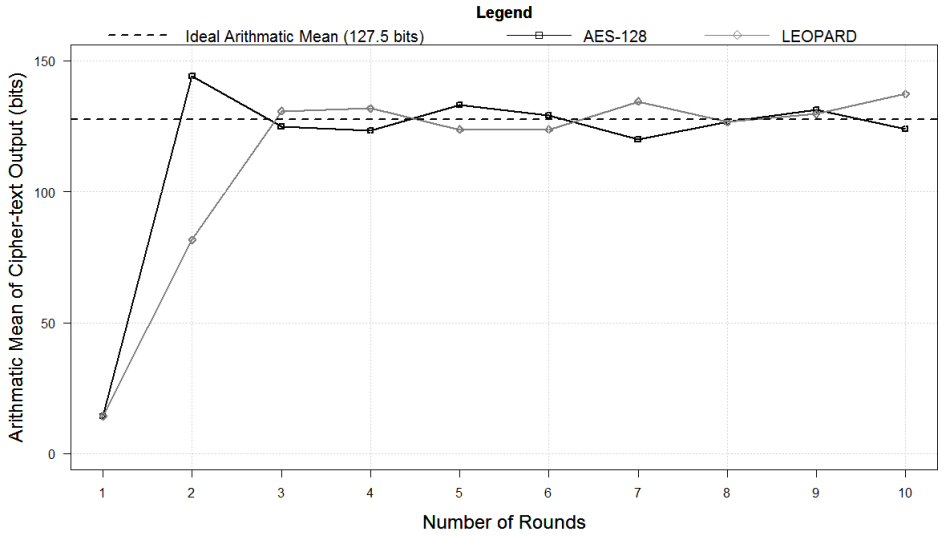


Figure 10.2: Arithmetic mean of the cipher-text output for LEOPARD and AES-128 over a various number of rounds for a two-hundred-and-fifty-six byte message

Results of the entropy test show that AES-128 has an increased entropy score in comparison to LEOPARD. The average percentage difference between the two cipher-text output up to three rounds was three per cent; however, the average percentage difference after three rounds was less than zero per cent; this shows that the entropy of the cipher-text output is not significantly different as the block cipher of both ciphers are based on the concept of Shannon's confusion and diffusion theory.

Data presented in Figure 10.2 shows that the arithmetic mean of the cipher-text output increases up to three rounds for both LEOPARD and AES-128, after three rounds the arithmetic mean fluctuates between the ideal arithmetic mean value of 127.5.

Further comparison between AES-128 and LEOPARD shows that the rate of reaching the ideal arithmetic mean differs with AES-128 overshooting the arithmetic mean up to three rounds whilst LEOPARD has a gradual rise; this shows that AES-128 reaches randomness at two rounds quicker than LEOPARD as the difference from the ideal arithmetic mean for AES-128 at two rounds is twelve per cent whilst LEOPARD has a percentage difference of forty-three per cent difference from the ideal arithmetic mean; however, the average difference across the rounds sampled for AES-128 was eight per cent whilst LEOPARD was eleven per cent.

Analysis of the instance of the speed-centric method concurs with the contemporary block cipher design philosophy of energy conservation as the reduction in the number of rounds showcased a reduction in the cryptographic strength of the cipher-text output; this is also true for the speed-centric method as the combination of cryptographic two or more components into one operation limits the ability for the cipher to produce a comparable cipher-text output for the same number of block cipher rounds selected; this is because the new synergy component was not designed to conduct a specific, specialist operation but instead a more generic operation of the two components.

10.3.3 Instruction Cycles Test

The number of instruction cycles required to process LEOPARD and AES-128 was analysed with comparison to the energy consumption and the time required to process the functions used in the cryptographic process. Table 10.1 tabulates the number of instruction cycles required for LEOPARD and AES-128.

The results presented in Table 10.1 illustrates that the number of instruction cycles used by LEOPARD was 4,562 cycles in comparison to 5,088 cycles used for AES-128; this shows that the combination of cryptographic functions used by LEOPARD has a ten per cent reduction per round over AES-128; this demonstrates that this would translate to a twelve per cent reduction in processing latency and energy consumption as the programme would have less instruction to compute.

Table 10.1: Profile of the number of instruction cycles required for LEOPARD and AES-128 per round.

Independent Variable	**Dependent Variables**	
Cryptographic Function	**Number of instruction cycles**	**Overall percentage of code size (%)**
LEOPARD Shiftrows	192	2.3
LEOPARD Mixcolums	922	20.2
LEOPARD Addroundkeyadd	1,332	29.2
LEOPARD Addroundkey	2,206	48.3
Total	**4,562**	**100**
AES Subbytes	605	12.2
AES Shiftrows	192	3.7
AES Mixcolumns	922	18.1
AES Addroundkey	3,309	65.0
Total	**5,088**	**100**

To show the impact of this reduction on real-time teleoperation and telemetry; Table 10.2 tabulates the time required to process LEOPARD and AES-128 using a PIC18F45K22 microcontroller operating at 4 MHz processing frequency.

Table 10.2: Time required to process LEOPARD and AES-128 cryptographic primitives with a PIC18F45K22 microcontroller operating at a crystal frequency of 4 MHz.

Independent Variable	**Dependent Variables**	
Crystal Frequency (MHz)	**LEOPARD (ms)**	**AES-128 (ms)**
1	31.00	34.08
4	7.75	8.52
8	3.88	4.26
16	1.94	2.13
20	1.55	1.70

Data displayed in Figure 10.2 shows that the time required by LEOPARD to process a block call is reduced in comparison to AES-128 by nine per cent per round; this shows that the accumulative impact of processing the cryptographic process would be reduced if the LEOPARD design method was selected as the time dictates the latency incurred by the real-time teleoperation and telemetry.

Further investigation is undertaken on the analysis of latency recorded for LEOPARD and AES-128 to process longer message lengths. The test was conducted in Mikroelectronika C IDE with message lengths of one hundred and twenty-eight bytes, two-hundred-

and-fifty-six bytes and one-thousand-and-twenty-four bytes selected to represent different length teleoperation and telemetry packets. Metrics used is the latency due to processing the cryptographic operation, all timings are taken from the IDE. Table 10.3 tabulates the impact of LEOPARD and AES-128 cryptographic primitives on the latency to process streamed data.

Table 10.3: Latency induced by LEOPARD and AES-128 at ten rounds for various sized packet lengths at a crystal frequency of 16 MHz.

Independent Variable	**Dependent Variables**	
Number of bytes in payload	**Latency recorded LEOPARD (ms)**	**Latency recorded AES-128 (ms)**
128 bytes	31.8	35.1
256 bytes	59.5	65.8
1024 bytes	261.5	289.4

Data presented in Table 10.3 shows that the latency induced for LEOPARD operating at ten rounds for the one-hundred-and-twenty-eight bytes, two-hundred-and-fifty-six bytes and one-thousand-and-twenty-four bytes packet lengths was reduced by ten per cent in comparison to AES-128. To demonstrate how the reduction in time impacts a static to mobile system, Figure 10.3 illustrates the distance travelled by a mobile device operated in real-time using LEOPARD and AES-128 to secure the communication link.

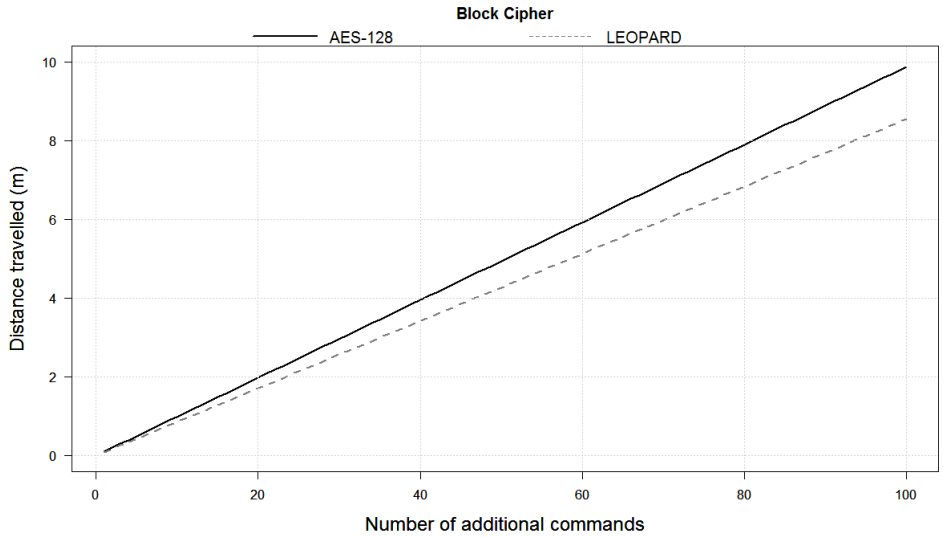


Figure 10.3: Distance travelled by a mobile real-time teleoperation and telemetry using LEOPARD and AES-128 at a fixed speed of seventy metres per second.

The results presented in Figure 10.3 shows that the distance travelled using AES-128 is increased in comparison with LEOPARD. The divergence between the two methods widens as the more additional commands sent. The trend identified in this graph shows

characteristics of a linear growth as both cryptographic methods influence the additional distance travelled at different rates, this demonstrates that there is a relationship between the selection of the cryptographic method and impact on the real-time teleoperation and telemetry as the cryptographic process determines the rate of the distance travelled by the mobile device before acting upon the command sent; therefore, the mobile real-time teleoperation and telemetry would be less responsive to commands sent with AES-128 in comparison to LEOPARD; this signifies the a beneficial outcome from using the speed-centric method.

10.3.4 LEOPARD vs AES-128 with the TinyAEAD Construct

This section of the validation conducts a benchmark comparison of the latency and additional processing incurred by the LEOPARD and standardised AES-128 block cipher with the inclusion of an authentication scheme, this is because the authenticated communication between the transmitter and receiver device is of importance in order to fulfill the confidentiality, integrity and authentication principles associated with a secure channel. Principles associated with the authentication approaches is to ensure a process or action of verifying the identity of a user or process and the act of confirming the truth of an attribute of a single piece of data claimed true by an entity; without authentication, an attacker could conduct a masquerade, replay or spoof attacks against legitimate devices on the communication link.

Incorporation of an authentication scheme with the instance of the synergy paradigm LEOPARD is an essential component in order to prevent the aforementioned attacks against the block cipher; this is because the encryption of the message does not prevent against data modification; therefore, in this analysis, the LEOPARD block cipher has been applied to the conventional method of Authenticated Encryption with Associated Data (AEAD) constructs as the underlying block cipher used in these scheme are transferable (i.e the selection of AES-128 or AES-256); in addition, the TinyAEAD construct has been selected because the problem analysis conducted demonstrates that this method induces the least amount of latency and is flexible in terms of block cipher selection; whilst CCM-AES-128 and GCM-AES-128 are limited to the use of the standardised AES-128 block cipher.

Analysis of the total latency to process a message through an AEAD construct with LEOPARD and AES-128 block ciphers is investigated using the Mikroelektronika integrated development environment to measure the time and number of instruction cycles recorded. The TinyAEAD construct was selected as the AEAD construct. Sixteen bytes of the payload were encrypted per encryption call with a total packet size of thirty-six bytes selected at a processing frequency of 1 MHz.

As the analysis of the components used for AES-128 block cipher have been analysed in Chapter 7; section 7.2.1; Table 7.1; this analysis examines the number of time the underlying block cipher is called by the TinyAEAD construct for one round; in this instance, that is four block cipher calls for the confidentiality of construct and four block cipher calls for the integrity of the construct. It is assumed that authentication is applied implicitly as the communicating entities would require the same correct symmetric key to encrypt and decrypt the message for confidentiality and to check the integrity of the message. Table 10.4 tabulates the Comparison of the latency incurred by LEOPARD and AES-128 block ciphers at ten rounds at a 1 MHz processing frequency with and without the TinyAEAD construct.

Table 10.4: Comparison of the latency incurred by LEOPARD and AES-128 block ciphers at ten rounds at a 1 MHz processing frequency with and without the TinyAEAD construct

Independent Variable	**Dependent Variable**	
Cipher	Without Authentication Latency (ms)	TinyAEAD Latency (ms)
LEOPARD	105	120
AES-128	442	500

Information presented in Table 10.4 demonstrates that the inclusion of the AEAD construct to provide authentication to the secure the communication link has a noticeable impact on the additional latency generated with the difference between LEOPARD with an without the TinyAEAD construct is one hundred and twenty percent and one hundred and twenty two percent for AES-128 with and without the TinyAEAD construct; this shows that the inclusion of an authentication scheme has a significant impact on the additional latency incurred by the real-time teleoperation and telemetry systems. Table 10.5 tabulates the difference in the number of instruction cycles for a cipher scheme with and without authentication schemes at a 1 MHz processing frequency.

Table 10.5: Comparison of the number of instruction cycles required by LEOPARD and AES-128 block ciphers at ten rounds at a 1 MHz processing frequency with and without the TinyAEAD construct

Independent Variable	**Dependent Variable**	
Cipher	**Without Authentication (Instruction cycles)**	**TinyAEAD (Instruction cycles)**
LEOPARD	26,288	110,420
AES-128	29,975	125,243

Data presented in Table 10.5 shows that the additional instruction cycles required by the microcontroller is increased with the inclusion of the TinyAEAD authenticated encryption scheme is up to four times greater in comparison to the operation of the block cipher without an authentication scheme, this demonstrates that there is a significant impact of the inclusion of an authentication scheme on the operation of a real-time teleoperation and telemetry link as the increased number of instruction cycles required to compute the scheme has a correlated impact on the additional latency incurred by the system; therefore, there is a requirement for future research in the design and implementation of authentication schemes to meet the constraints associated with the real-time nature of teleoperation and telemetry systems.

Comparison of the speed-centric and contemporary philosophies to block cipher designs demonstrates that the application of the speed-centric method is beneficial to fulfilling the specified requirements obtained from the problem analysis in Chapter 7, section 7.6 as the synergy paradigm for the cryptographic components has reduced the number of instruction cycles required by the underlying block cipher and therefore reduced the latency recorded to compute the cryptographic operation.

10.3.5 Instantaneous Packet Throughput Test

The downlink communication channel where the data is streamed over intermediate multi-hop communications is selected to identify how the combination of the cryptographic functions influences the instantaneous packet throughput of real-time teleoperation and telemetry. The test is undertaken on an emulated version of the point to point link test based on the multiple-hop platform presented in Chapter 3, section 3.4.1. A crystal frequency of 8 MHz is selected. The results obtained are taken over of a sixty second time frame; all timings are recorded on a real-world stopwatch. Table 10.6 presents the instantaneous throughput obtained over a point to point communication link using LEOPARD and AES-128 cryptographic primitives.

Table 10.6: Instantaneous packet throughput LEOPARD and AES-128 cryptographic primitives for a point to point communication link at a crystal frequency of 8 MHz and a sample time of sixty seconds.

Independent Variable	**Dependent Variables**		
Number of Bytes in payload	**No Security (Packets)**	**LEOPARD (Packets)**	**AES-128 (Packets)**
36 bytes	20,095	1,810	1,639
52 bytes	13,660	1,320	1,230
84 bytes	8,407	861	805

Data presented in Table 10.6 shows that the latency induced for LEOPARD operating at ten rounds had a ten per cent increase in instantaneous throughput recorded in comparison to AES-128 for all three packet sizes sampled. This further reinforces the fact that the LEOPARD cryptographic primitive has an influence on the number of real-time teleoperation and telemetry packets transmitted in a given time period; in addition, this contributes towards the increased sensitivity of the physical operational performance of the mobile platform as the reduced latency of the LEOPARD cryptographic primitive results in actions undertaken in a shorter period of time.

Analysis of the instantaneous packet throughput over a multiple hop propagation of data between the transmitter and receiver over heterogeneous communication links is presented with the comparison of LEOPARD and AES-128 at three rounds using the test platform presented in Chapter 3, section 3.4.5. Figure 10.4 illustrates the instantaneous throughput recorded at each hop with LEOPARD and AES-128 cryptographic approaches.

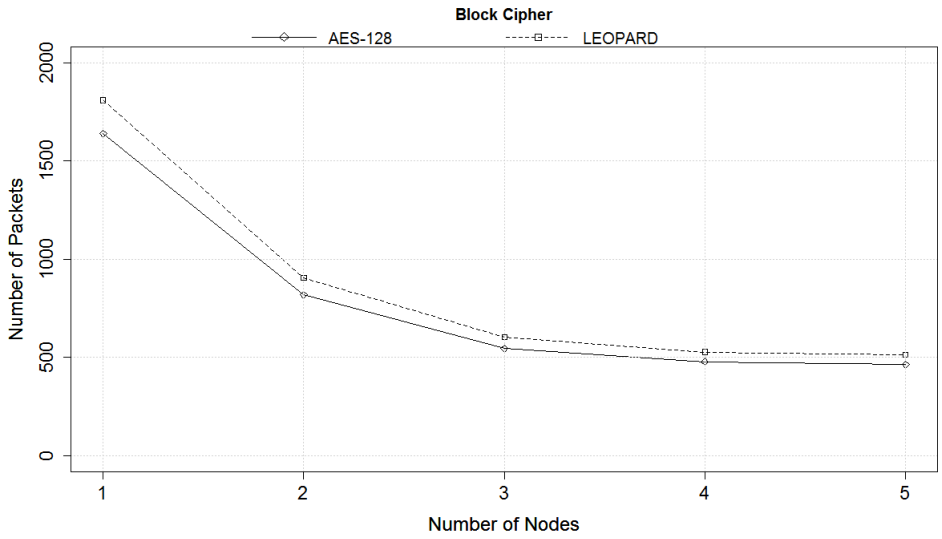


Figure 10.4: Instantaneous packet throughput recorded at intermediate node with LEOPARD and AES-128 cryptographic approaches over a heterogeneous communication link with a thirty-six byte packet size and crystal frequency of 8 MHz.

Results presented in Figure 10.4 demonstrates that the instantaneous throughput obtained with AES-128 was less than LEOPARD for the same number of intermediate hops on the network; this is because the time required to encrypt and decrypt the cryptographic operation is reduced for LEOPARD as there is lesser number of instructions to process due to the combining of cryptographic functions; the results of this is the increased number of packets that are propagated between the base-station and mobile platform.

10.3.6 The Impact on the Operational Performance of Real-Time Teleoperation and Telemetry

Validation of the proposed method on the operation of real-time teleoperation and telemetry in a real-world context is investigated; the experiment examines the number of revolutions obtained in a specified time period with comparison of the proposed philosophy against the contemporary security approaches.

The test platform selected is an emulated environment using two PIC18F45K22 microcontrollers, one device is the transmitter and the other device is a receiver. The crystal frequency selected for the microcontrollers was 4 MHz. The SPI is selected for communications between the transmitter and receiver.

Packet sizes of thirty-six, fifty-two and eighty-four bytes were sampled. Time frame sampled for this test is sixty seconds; the time was recorded with a real world stopwatch. The motor operated is an input voltage of two volts for the propeller actuators and five volts for the wheel actuator. A frequency of 5,000 KHz was used to drive the actuator.

Three individual attachments were sampled on the motor, a twin-blade propeller, a triple-blade propeller and a wheel. The dimensions of the twin blade propeller was seven centimetres from the tip of the blade to the centre point with a width of two centimetres; the three blade dimensions was 6 centimetres from the tip to the centre point and one and a half centimetres wide. The circumference of the wheel was three centimetres. Table 10.7 tabulates the results of the revolutions recorded using LEOPARD and AES-128 security applied over various configurations.

Table 10.7: Average number of revolutions per second recorded with LEOPARD and AES-128 cryptographic primitives over various packet sizes operating at a 5,000 KHz frequency with a wheel actuator, twin blade and triple blade propeller.

Independent Variable	**Dependent Variables**		
Average Number of Revolutions	**Twin Blade**	**Triple Blade**	**Wheel**
LEOPARD 3 rounds (36 bytes)	31.7	80.3	68.5
LEOPARD 3 rounds (52 bytes)	29.5	73.5	68.5
LEOPARD 3 rounds (84 bytes)	26.7	65.9	66.4
AES 3 rounds (36 bytes)	30.8	66.8	67.4
AES 3 rounds (52 bytes)	28.7	71.0	67.4
AES 3 rounds (84 bytes)	26.4	65.8	66.4

Results presented in Table 10.7 shows the number of revolutions obtained per second with LEOPARD was greater for the thirty-six and fifty-two byte packet sizes; over the course of a minute duration, the percentage difference between the average number of revolutions recorded for LEOPARD and AES-128 with a triple-blade propeller was eighteen per cent for a thirty-six byte packet size, four per cent for a fifty-two byte packet size and less than one per cent for an eighty-four byte packet size. The justification to why LEOPARD was outperformed by AES-128 at this packet size was due to the addition function used; this is because the carry operation used requires a set period of time to process and the additional size of the message therefore increased the number of bit carries required to complete the overall process. This trend is consistent across three actuator platforms examined.

In the context of a mobile platform using real-time teleoperation and telemetry operating in a tactical scenario, the results of the test undertaken were extrapolated over the course of a two hour mission duration to determine the impact on the mission. Figure 10.5 illustrates the number of revolutions obtained with LEOPARD and AES-128 over a two hour mission with a two blade and three blade propellers.

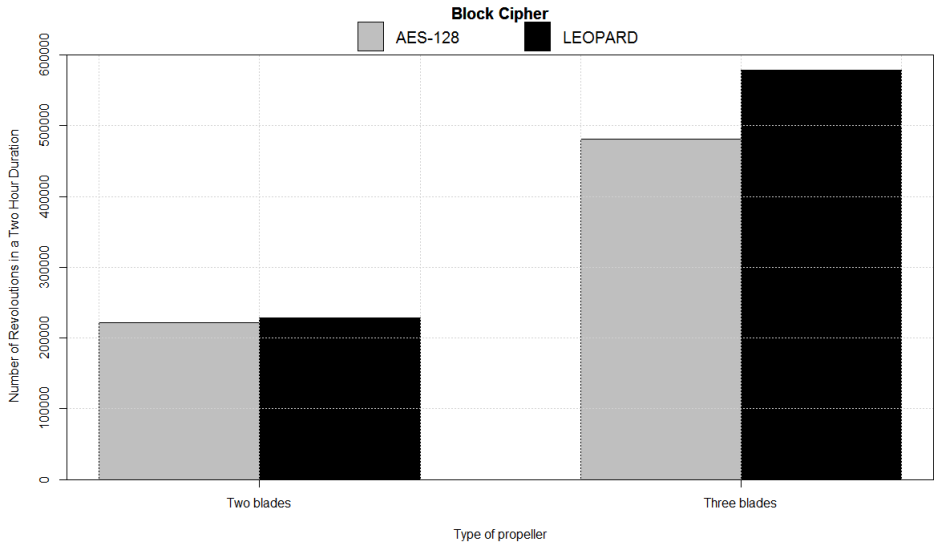


Figure 10.5: Number of revolutions per second with LEOPARD and AES-128 cryptographic primitives for a thirty-six byte packet size over two hours with a 5,000 KHz frequency for the motor.

Results presented in Figure 10.5 shows that the difference in the number of revolutions recorded utilising LEOPARD and AES-128 was six-thousand-four-hundred-and-eighty revolutions over the course of the two hour mission with a two blade propeller; whilst the three blade propeller recorded a difference between LEOPARD and AES-128 of ninety-seven-thousand-and-two-hundred revolutions over the two hour mission; this correlates with the reduced latency by LEOPARD, as a result this has an impact on the physical operational performance of the actuator.

Analysis of the distance travelled by the mobile platform utilising real-time teleoperation and telemetry with LEOPARD and AES-128 is presented. The test investigates the distance that a mobile platform would have to travel before an encrypted picture is transmitted back to the ground station. The validation of the two approaches was undertaken through mathematical modelling using the time, distance and speed formula to calculate the distance travelled by an UAV based on the latency to process the cryptography and the speed that the UAV is travelling.

The parameters used for the validation assumes that the transmission of a three megapixel image on the downlink between the UAV and the ground station; packet size of one-thousand-five-hundred bytes was selected to represent a maximum packet size of the IEEE 802.3 protocol. It is assumed that the communication link has ideal channel characteristics (e.g. no interference). The delay is calculated based on the time required by the difference in latency to encrypt and decrypt the data using LEOPARD and AES-128 at 4 MHz crystal frequency; which was calculated at four seconds difference. Figure

10.6 illustrates the distance travelled by the UAV with LEOPARD and AES at a speed of fifty metres per second.

Figure 10.6: Distance travelled by the UAV before transmission of a three mega-pixel picture is completed at a speed of fifty metre per second with LEOPARD (red) and AES (blue). Image drawn with Google Earth.

Results presented in Figure 10.6 demonstrate that the additional time required by AES-128 to process the image has resulted in a further distance travelled by the UAV in comparison to LEOPARD. The additional three hundred milliseconds incurred by the AES-128 block cipher in comparison to LEOPARD block cipher resulted in the UAV travelling an additional fifteen meters to process a three megapixel image as AES-128 required eighty metres and LEOPARD required sixty-five metres per three megapixel image at the same UAV speed.

Further analysis was undertaken with a reduction of the UAV's speed to fifteen metres per second to determine if the speed of the platform correlates with the distance travelled before the transfer of one image is completed. Figure 10.7 illustrates the distance travelled by the UAV with LEOPARD and AES-128 approaches applied travelling at fifteen metres per second before the image is transferred and received.

The image presented in Figure 10.7 demonstrates that the speed of the UAV has a correlation on the distance travelled before the image is taken as the circumference of the circle is reduced for both LEOPARD and AES-128; however, the comparison in the distance trav-

elled by LEOPARD and AES-128 remains constant as AES-128 recorded a distance of sixty meters difference in comparison to LEOPARD; therefore, the offset between the two approaches is consistent despite the change in the physical speed of the mobile platform; this is because the accumulation of the latency incurred per block cipher call extrapolates based on the same parameters used.

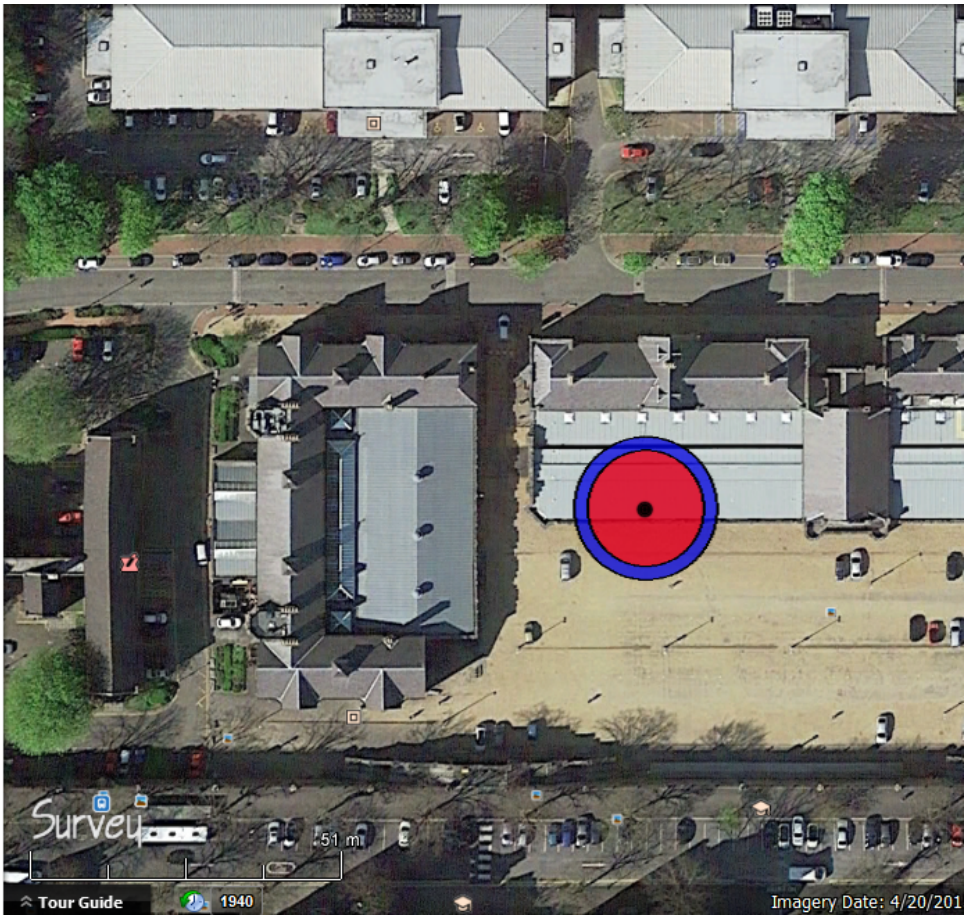


Figure 10.7: Distance travelled by the UAV before transmission of a three mega-pixel picture is complete at a speed of fifteen metres per second with LEOPARD (red) and AES (blue). Image drawn with Google Earth.

Application of the knowledge obtained from the findings presented in Figure 10.6 and Figure 10.7 are investigated from the additional distance travelled by a UAV with the integration of LEOPARD and AES-128 block ciphers for secure communications between the transmitter and receiver. Figure 10.8 graphs modelled the additional distance travelled by a UAV with LEOPARD and AES-128 at various fixed speeds.

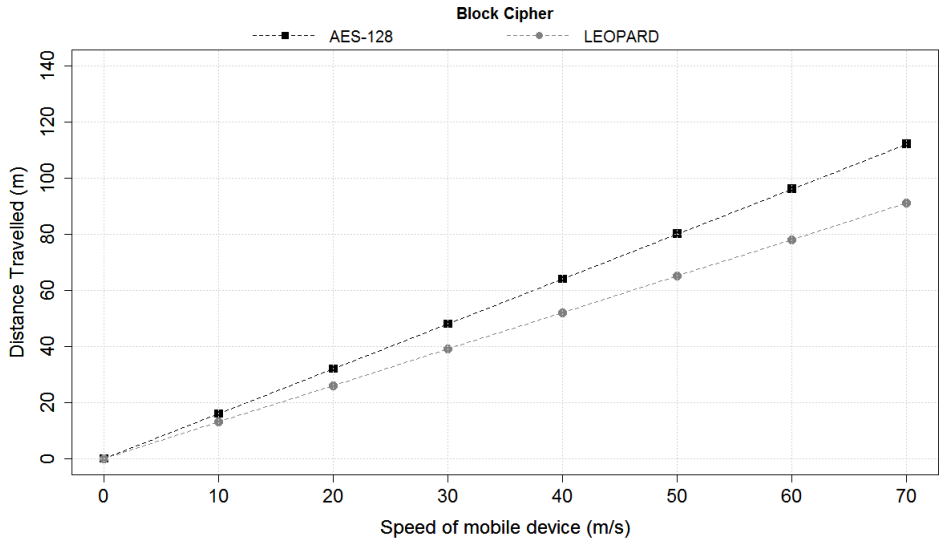


Figure 10.8: The additional distance travelled by the UAV with LEOPARD and AES-128 at various fixed speeds for the UAV.

Data presented in Figure 10.8 shows that the modelled impact of the distance travelled by the UAV with LEOPARD and AES-128 applied at various speeds. Results presented correlate with the analysis of the distance travelled by the UAV during flight as the difference in time required to process the image with the cryptographic approaches is constant per message. Further analysis is undertaken with an investigation into the relationship between the latency recorded for various number of messages transmitted at a fixed speed of fifty metres per second; results are presented in Figure 10.9.

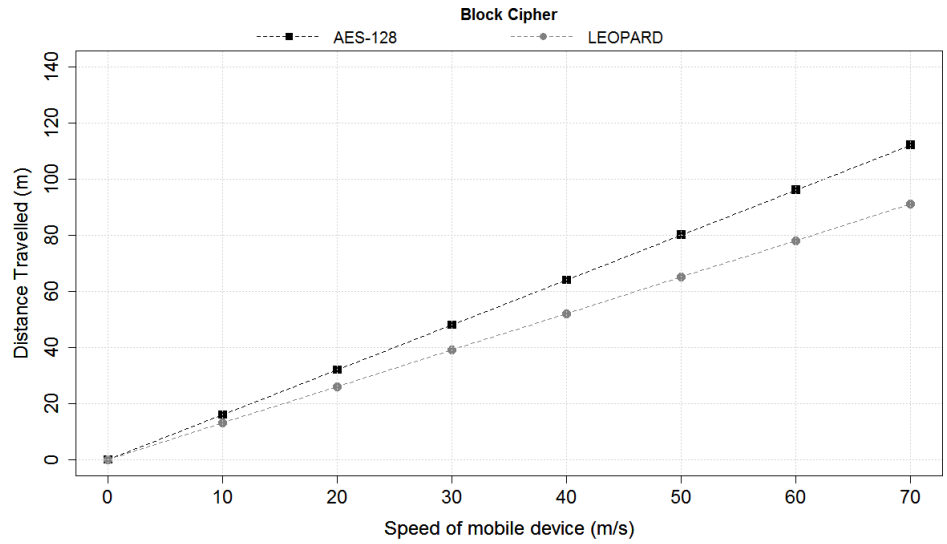


Figure 10.9: The distance travelled by the UAV with LEOPARD and AES-128 at varying number of three mega-pixel images transmitted. (UAV speed of fifty metres per second).

Results illustrated in Figure 10.9 demonstrate that the number of messages influences the

distance travelled by the UAV with LEOPARD and AES-128 cryptographic approaches applied as the accumulation of the latency incurred from the encryption and decryption calls of the block cipher accumulate throughout the duration of the mission and transfers into distance travelled by the UAV before the next image is taken; however, the comparison of the two approaches shows that the difference between the two approaches is a constant offset as AES-128 travels four times further per message in comparison to LEOPARD.

10.3.7 Energy Usage Test

Analysis of the energy consumption of the two cryptographic primitives was undertaken. The proposed test investigated the current draw of a microcontroller to process the cryptographic primitives at different crystal frequencies. The test was conducted on an emulated environment using a PIC18F45K22 microcontroller; crystal frequencies of 4 MHz, 8 MHz, 16 MHz and 20 MHz are chosen. A packet size of thirty-six bytes is selected. The results represent an average of one hundred measurements. A five volt input is selected to power the microcontroller. A multimeter is used to obtain the current draw of the microcontroller. All measurements were recorded in milliwatts. Figure 10.10 graphs the current draw of the microcontroller to process LEOPARD and AES-128 cryptographic primitives.

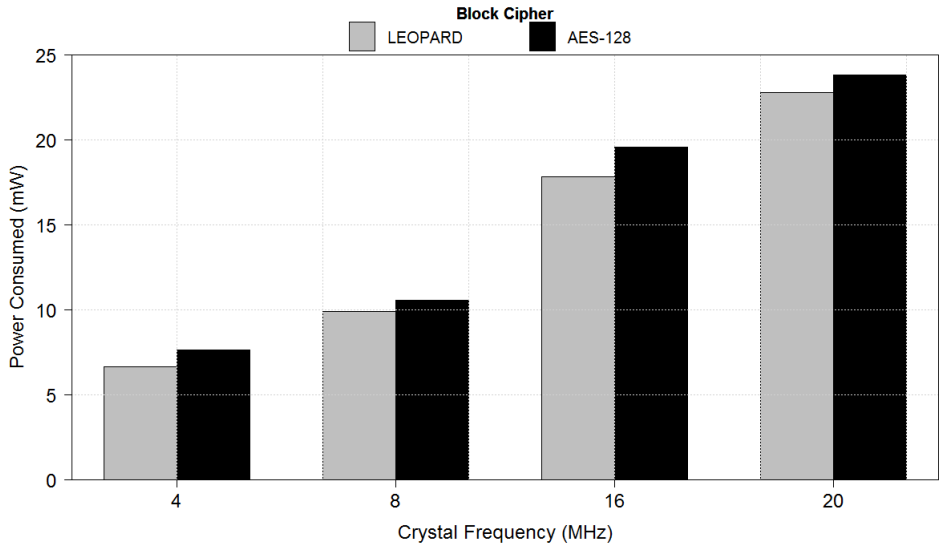


Figure 10.10: Power consumption of LEOPARD and AES-128 cryptographic primitives at various crystal frequencies with a thirty-six byte packet size at three rounds each.

Results presented in Figure 10.10 shows that the power consumption for AES-128 was higher in comparison to LEOPARD for all of the crystal frequencies sampled. The greatest difference in measurements was recorded for a 16 MHz crystal frequency with a difference of 1.75 mW whilst the lowest difference recorded was 0.65 mW for 8 MHz

crystal frequency. The mean difference for the current drawn between AES-128 and LEOPARD for the crystal frequencies sampled was 1.11 mW.

10.4 Validation of Derived Instance: Privacy Cryptographic Unit

10.4.1 Test Scenarios for Privacy Cryptographic Unit

The derived test scenarios presented in this section examine the operation of the PCU at its basic configuration without the adaptive control system applied. Four scenarios are examined to validate the application for the PCU from the prospective of a static-mobile and mobile to static end-point. Scenario one analyses the operation of the PCU under ideal channel characteristics. Scenario two investigates the impact of non-ideal channel characteristics on the PCU. The final scenario studies the behaviour of the PCU under a communication link that is susceptible to random burst error.

10.4.2 Scenario 1: Ideal Communication Channel Conditions Test

The first scenario examined the behaviour of the PCU under ideal communication channel conditions to determine if the novel approach presented operates correctly. An instance presented of this scenario is applied to static to static real-time teleoperation and telemetry where the communication link is unaffected by external factors as the communication medium between the transmitter and receiver is wired cabling protected by shielding.

The test platform selected for this test was an emulated environment with the PIC18F45K22 microcontroller used for the transmitter and receiver device. The Serial Peripheral Interface (SPI) is selected as the physical layer to transmit and receive messages between each microcontroller. The test measured the number of key regenerations undertaken between the transmitter and receiver with different paranoia levels set for the basic configuration of the PCU without the adaptive control system. Paranoia levels selected for the PCU were zero per cent, twenty-five per cent, fifty per cent, seventy-five per cent and one hundred per cent of a byte value. Packet size for the key regeneration protocol was set to twenty-four bytes. A sample time of sixty seconds was selected with all timings taken from a real-world stopwatch. The mean result of a hundred trials is presented.

Calibration of the basic operation of the PCU was tested to examine the mechanism and how this impacts the nature of the real-time teleoperation and telemetry. Figure 10.11 illustrates the average number of key regenerations undertaken at various paranoia levels with no security services applied.

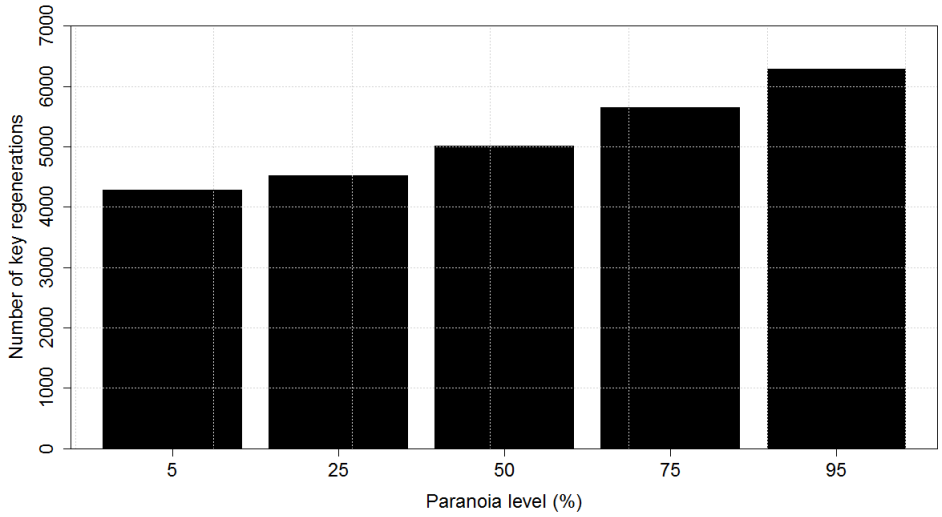


Figure 10.11: Average number of key regenerations performed by the basic implementation of the PCU at various initial paranoia levels in a sixty second time sample under ideal channel conditions at a crystal frequency of 4 MHz.

Data presented in Figure 10.11 shows that the initial paranoia level set by the human operator has an influence on the number of key regenerations processed by the PCU with the lowest paranoia level having the least number of key regeneration whilst the highest paranoia level had the highest number of key regenerations. This demonstrates that the basic implementation of the PCU impacts the number of key regenerations when the paranoia level of the system is increased as the time between regenerations is reduced as the packet counter value is directly influenced by the new calculated paranoia level; therefore, the increased frequency of key regenerations is observed.

Analysis of the key-length variable input used by the PCU is undertaken to see if the size of the cryptographic key used by the block cipher has an impact on the operational performance of the system. The emulated test platform used in the aforementioned test was selected. Key sizes of 64, 128, 192 and 256-bit keys were sampled to reflect key sizes used by block ciphers (e.g. AES and DES). The time required for the key regeneration mechanism to initiate was recorded as the measurement for this test. A sample time of sixty seconds was selected with all timings taken from a real-world stopwatch. Figure 10.12 illustrates the time required by the PCU to process the key regeneration mechanism with different sized cryptographic keys.

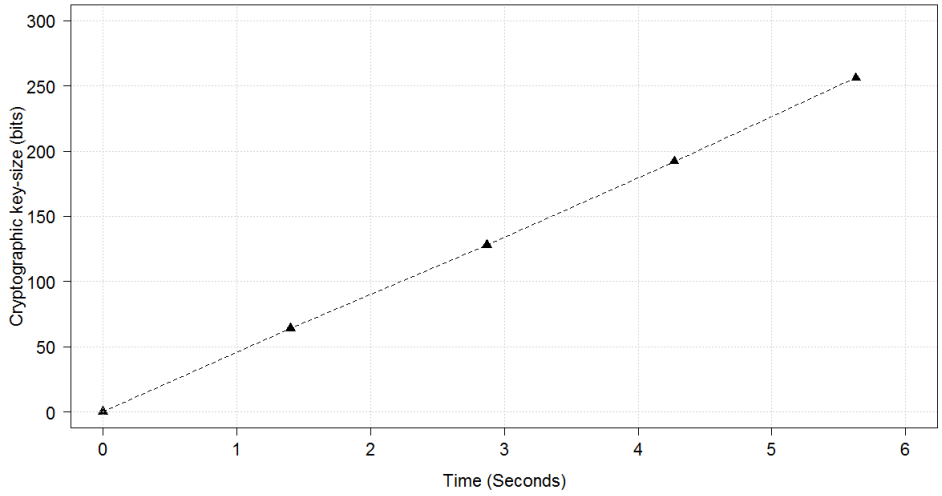


Figure 10.12: Average time taken by the PCU to process various sized cryptographic key length in a sixty second time sample at a crystal frequency of 4 MHz.

Results presented in Figure 10.12 shows that the time required by the PCU to compute the operation based on the cryptographic key length follows a positive linear growth trend as the larger the key size, the longer the time required before the key regeneration is performed; this correlates with the time required by an attacker to search through all possible keys based on the key size selected, the smallest key size would require less time to brute force whilst larger key sizes would require a longer duration to obtain the correct cryptographic key used with the same number of machines available to the attacker.

10.4.3 Scenario 2: Non-ideal Communication Link Test

The second scenario analysed the behaviour of the basic implementation of the PCU under non-ideal channel characteristics between the transmitter whilst the packet is in propagation. The test platform selected for this test was the emulated environment as discussed in Scenario 1 with preset interference levels set to mimic the PCU sensing the external environment through the signal level obtained from the ESSID. The level of interference set of the test range between zero and fifty per cent. The test measured the frequency of key regenerations undertaken between the transmitter and receiver with different interference levels set for the PCU. The paranoia level selected for the PCU was set at zero per cent. A sample time of sixty seconds was selected with all timings taken from a real-world stopwatch. The mean result of ten trials is presented. The results of the number of key regenerations undertaken by the PCU under non-ideal channel characteristics is presented in Table 10.8

Table 10.8: Average number of key regenerations performed by the PCU with a paranoia levels set at various interference levels in a sixty second time frame.

Independent Variable	**Dependent Variable**
Interference Level (%)	**Number of Key Regenerations**
0	3,607
10	3,735
20	3,866
30	3,999
40	4,147
50	4,310

Data presented in Table 10.8 shows that the number of key regenerations performed by the PCU increased as the interference level increased; this correlates with the proposed operation of the PCU mechanism as the set-point of the calculated paranoia level is reduced to account for the increased level of the sensed external interference on the communication link; as a result, the new calculated set-point value is reduced and the number of packets required to be transmitted before the key regeneration process is initiated; as a result more key regenerations occurs in the same period of time.

The trend identified from the result presented in Table 10.8 show a linear increase for the number of key regenerations performed as the interference level increases; this shows a linear correlation of the relationship between the interference level and the number of key regenerations performed; this results in the increased frequency of re-initialising the key regeneration operation between the communicating entities.

10.4.4 Scenario 3: Burst Interference on the Communication Link

The scenario investigates how the PCU behaviour adjusts in the presence of a communication link that is susceptible to burst error; it is assumed in this situation that the attacker attempts to interfere with the communications between the transmitter and receiver sporadically to avoid detection. The test platform selected for this test was the emulated environment as discussed in Scenario 1 and 2. A pseudo random number generator is selected to generate a number within a byte value of 0 to 255. The value is compared against the probability of a burst error causing packet corruption. Probability of errors sampled for this test ranged from zero to fifty per cent.

The test measured the number of key regenerations undertaken between the transmitter and receiver with different probabilities of a successful burst error impacting the packet during the propagation of the key regeneration initialisation packet. Paranoia level selected for the PCU is fifty per cent. A sample time of sixty seconds is selected with all

timings taken from a real-world stopwatch. The mean result of ten trials is presented. TinyAEAD-AES-128 at three rounds was selected as the security service for the transmitter and receiver. Figure 10.13 graphs the results of the number of key regenerations undertaken by the PCU under a burst jamming attack.

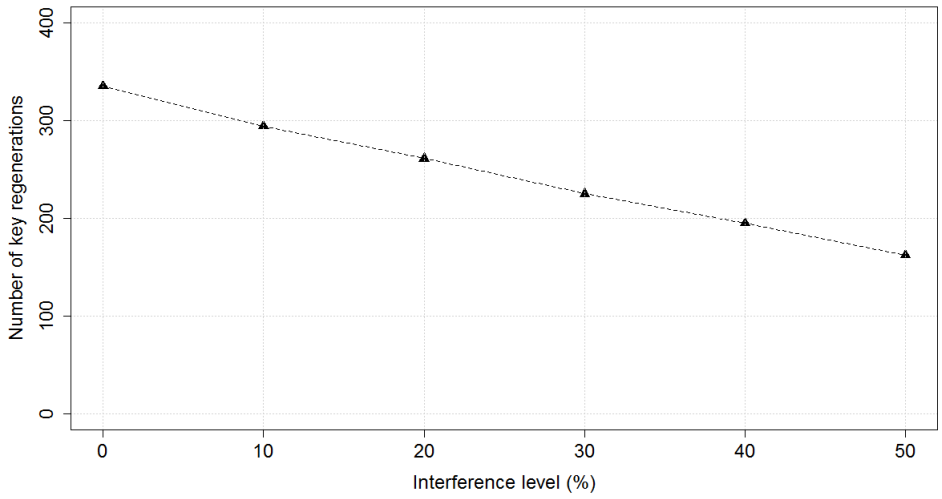


Figure 10.13: Average number of key regenerations undertaken by the PCU under burst jamming attack with TinyAEAD-AES-128 at three rounds at a crystal frequency of 4 MHz.

Data presented in Figure 10.13 shows that the probability of a burst error has an impact on the number of key regenerations that the PCU undertakes with more regenerations performed with the reduction of the probability of a burst error impacting the packet during propagation on the communication link. The trend presented shows a linear decrease as the increase in the frequency of the random burst attack reduces the number of successful key regeneration undertaken. The impact of this in the context of real-time teleoperation and telemetry is that the additional latency generated as a result of re-initiating the protocol would increase in order to complete the process; this results in the initial control message sent to the actuator and the response of the actuator becoming delayed; implications of this action in the context of a static-mobile and mobile to static prospective is the delay in the responsive of piloting the UAV and the quantity of streamed data to the base-station.

10.5 Profiling of the Privacy Cryptographic Unit

Analysis of the energy, latency and number of instruction cycles is examined. The test is conducted on an emulated environment using PIC18F45K22 microcontrollers; crystal frequencies of 4 MHz is chosen. A packet size of twenty-four bytes is selected to represent the PCU challenge-response protocol with an initial paranoia level set to its lowest

setting of zero per cent. TinyAEAD-AES-128 operating with AES-128 at three rounds is selected as the security method. A point to point link between the transmitter and receiver was selected. The results represent an average of one-hundred measurements. A multimeter is selected to obtain the current draw of the microcontroller and a real-world stopwatch to measure the sample time used. An input voltage of 5 volts was selected. All measurements were recorded in milliamp (mA) and converted to milliwatts (mW). Figure 10.14 presents comparison of the power consumption of the PCU to LEOPARD at three rounds, TinyAEAD-AES-128 at three rounds and CCM-AES-128.

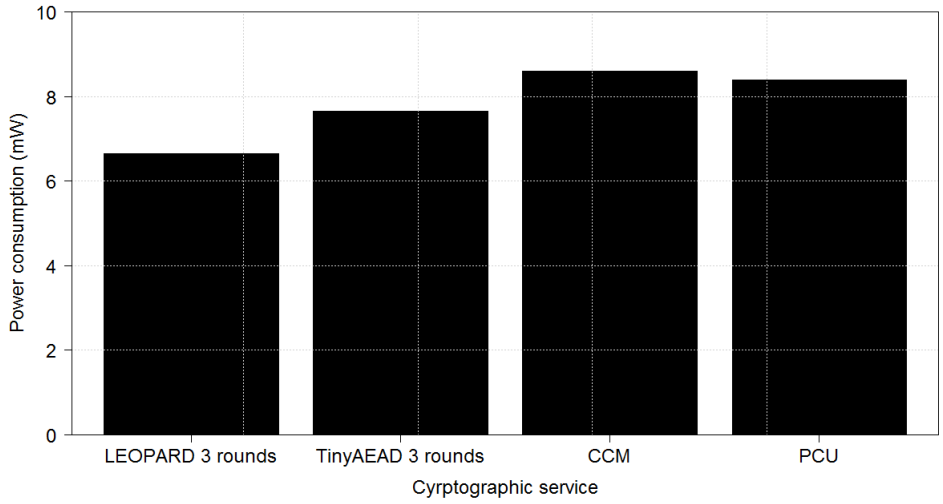


Figure 10.14: Power consumption of the PCU, LEOPARD at three rounds, TinyAEAD-AES-128 at three rounds and CCM-AES-128.

Results presented in Figure 10.14 show that the power consumption of the PCU is reduced in comparison to CCM; however, it is not as efficient as LEOPARD and TinyAEAD-AES-128 at three rounds, this is because the number of instruction cycles required to complete the selected cryptographic process with TinyAEAD-AES-128 is less than CCM and the PCU.

10.5.1 Latency of the PCU Test

To establish the impact on the context of real-time teleoperation and telemetry; analysis of PCU latency is undertaken. A test is conducted on an emulated test platform; the Microchip PIC18F45K22 is selected as the microcontroller for the base-station and tactical UAV. The Serial Peripheral Interface (SPI) is selected as the physical layer (i.e. OSI model) to transmit and receive messages between each microcontroller. The TinyAEAD construct is the selected AEAD construct with a crystal frequency of 4 MHz selected. A packet size for the uplink communication to the UAV is thirty-six byte; the challenge response for the key regeneration protocol is twenty-four bytes in size. It is assumed for this

test that the channel characteristics are ideal as the focus is on the latency generated by processing the PCU function call. All timings are recorded from an oscilloscope trace of a LED turning on and off to indicate the process is completed; the findings are validated in the Mikroelektronika C IDE with the number of instruction cycles measured. Table 10.9 tabulates the latency recorded for the functions of the PCU.

Table 10.9: Number of instruction cycles required by the software implementation of the PCU at a 4 MHz crystal frequency.

Independent Variable	**Dependent Variables**	
Component	**Time (ms)**	**Number of instruction cycles**
Key Regeneration protocol (Transmitter)	85.1	85,091
Key Regeneration protocol (Receiver)	201.6	201,583
Expert decision making System	7.2	7,208

Results presented in Table 10.9 shows that the total number of instruction required by the key regeneration protocol at the receiver induced the longest latency; however, the adaptive control system process in software recorded the smallest impact on latency recorded; this demonstrates that the privacy-based concept of using expert prognosis is an applicable implementation method in software as the process requires minimal instruction cycles to compute.

The key regeneration mechanism is analysed to identify how the number of key regenerations influences the latency recorded to complete the operation of the PCU. The test is undertaken in an emulated test platform with the Mikroelektronika C programming environment selected to measure the latency of the resynchronisation process. Three crystal frequencies were sampled at 4 MHz, 8 MHz and 16 MHz. The time required to complete the number of resynchronisations is examined. All measurements are taken from the integrated development environment. Figure 10.15 graphs the latency of the number of retries selected by the PCU to complete its operation at various processing frequencies.

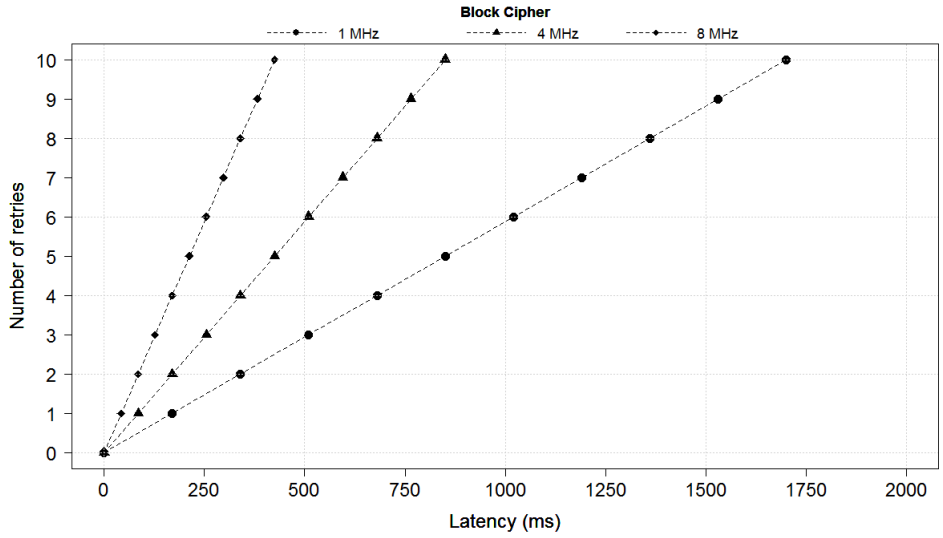


Figure 10.15: The additional latency incurred from the number of resynchronisation retries undertaken by the PCU operating at various crystal frequency.

The data presented in Figure 10.15 shows that the number of retries used by the PCU has an increased growth on the latency induced by the system. The latency for the PCU process follows a linear increase as the number of retires requires additional processing to compute. Additional benefits of the PCU for reliable communications is that the PCU process does not initiate for every message that is transmitted and initiates sporadic at irregular intervals as the PCU system initiates based on the perceived experience of the information sensed after the initialisation of the initial paranoia level set by the user.

10.5.2 The Impact of the Privacy Cryptographic Unit on the Operational Performance of Real-Time Teleoperation and Telemetry

The distance travelled by the UAV is examined with the additional distance travelled by the device before the response to the command to take-off is completed based on the profile of the PCU presented in Table 10.9. It is assumed for this analysis that the UAV is travelling at a ground speed of fifty-two metres per second and the communication link between the UAV and ground station is operating in ideal conditions with no interference or error present on the link. Figure 10.16 illustrates the additional distance travelled by the UAV with the PCU and existing security services.

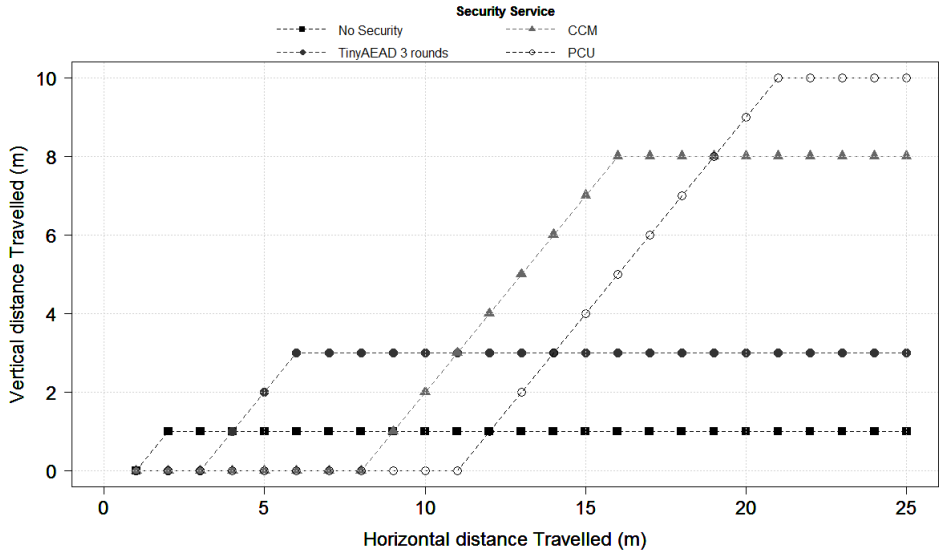


Figure 10.16: Additional distance travelled by an UAV at take-off and after completion of climb with PCU, TinyAEAD at three rounds and CCM at a crystal frequency of 4 MHz

The difference in the additional distance travelled between TinyAEAD at three rounds and the PCU is seven metres and the difference between the PCU and CCM is two metres; this shows that the increased strength gained from the PCU processes impacts on the distance travelled by the UAV as the response time between the initial message transmitted and the action completed results in the distance travelled becoming increased.

10.5.3 Teleoperational Control of the Mobile Platform Test

The impact of the additional distance travelled is analysed with the number of additional commands sent to the UAV over the mission time is examined. Validation of the impact of the operational performance of the UAV with LEOPARD and the PCU approaches is undertaken to quantify the initial findings presented in Figure 10.16. The test analysed the additional distance travelled by the UAV whilst performing a decent from a fixed altitude. The test platform is the Flight-gear simulator software with the test platform is configured as presented in Chapter 6, section 6.3.1. The starting altitude of the UAV before decent is set to one thousand feet (three-hundred-and-four metres) at a fixed speed of eighty miles per hour (thirty-five metres per second). The duration of the decent command is set to three seconds before the auto-pilot is initiated to return the UAV to the original starting altitude. An average of ten test runs is presented with all results obtained from the logging operation from the simulation. All timings are taken from the simulation clock. Figure 10.17 graphs the additional distance travelled by LEOPARD and the PCU to complete a decent and return to the starting altitude.

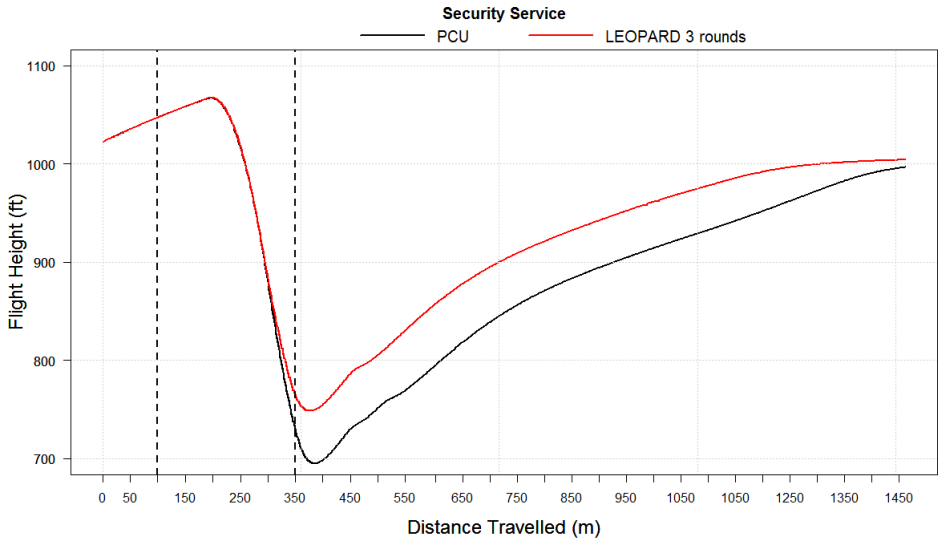


Figure 10.17: Distance travelled by the UAV to complete a three second decent and return to the starting altitude at a speed of thirty-five metres per second utilising LEOPARD and the PCU.

Data presented in Figure 10.17 shows that LEOPARD had a reduced impact on the additional distance travelled by the UAV in comparison to the PCU approach, an additional sixty metres is travelled by the UAV before the response to the teleoperation is undertaken; this demonstrates that LEOPARD is better suited for the real-time teleoperation data; whilst the PCU would be better used for the real-time telemetry data due to the additional latency incurred.

10.6 Validation of the Adaptive Control System

This section continues from the implementation of the PCU presented in the aforementioned section with validation of the adaptive control system integrated into the system. The tests derived in this section investigates the ability of the adaptive control system to conduct the correct action based on the received input variables to influence the set paranoia level of the PCU system before the key regeneration mechanism is activated. The behaviour of the adaptive control system deployed under various scenarios is investigated to derive its characteristics based on the implementation of the logic and the output action.

The test environment used for the validation of the adaptive control system is an emulated environment with the Mikroelektronika C compiler selected to implement the variation of the adaptive control system. Fixed levels are used for the stimuli variables that ranged from zero to one hundred per cent with incremental steps of fifteen per cent for paranoia and interference levels. Five input membership classification functions are selected to represent very low, low, medium, high and very high levels; each membership category is represented by a triangular shape and divided equally into twenty per cent sections with a

overlay of twenty-five per cent between each membership function.

The number of rules set in this instance of the adaptive control system was twenty-five to reflect all possible combinations of the two input functions. Two rule sets values were investigated in this test with linear and non-linear weighted values. The Mamdani inference system (Mamdani & Assilian 1999) was selected as the method of assigning the output rule strength with the logical AND operator to assign the lowest weight for the rule set condition. The defuzzification technique selected for this implementation method was the weighted average approach (Liu & Mendel 2008). Metrics measured was the crisp output measured from the calculation of the adaptive control system and the new paranoia level derived from the adaptive control system. All measurements were taken from the emulation.

10.6.1 Behaviour of Linear and Non-Linear Adaptive Control Systems: Fixed Paranoia Level and a Fixed Interference Level over a Varying Number of Iterations

The first scenario investigated is the comparison of linear and non-linear values used for the logic rule set with the interference level fixed to ten per cent and the paranoia variable fixed to ninety-five per cent. The number of iterations used to calculate the new paranoia level range from one to ten rounds. Figure 10.18 illustrates the comparison of the adaptive control system with linear and non-linear values for the rule set outputs.

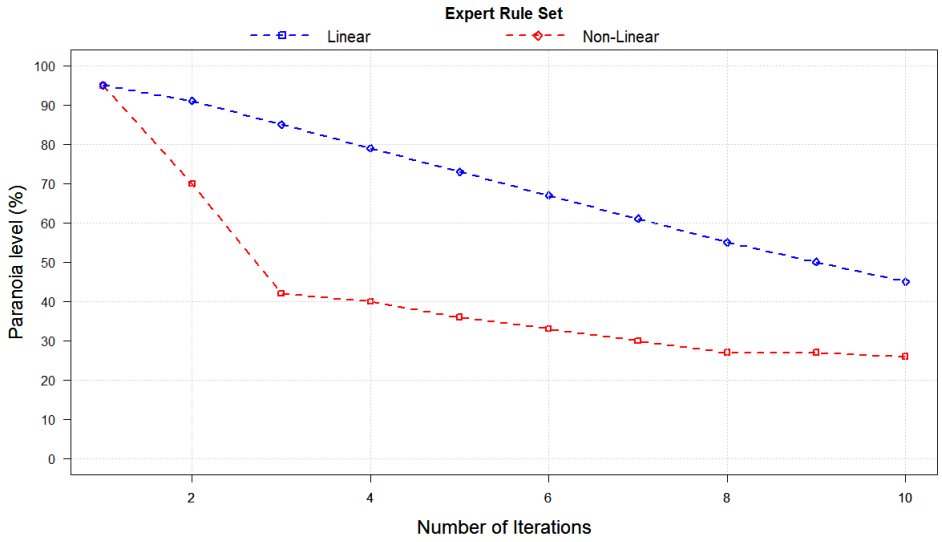


Figure 10.18: Characteristic of the linear and non-linear rule sets over a varying number of iterations. (Initial paranoia start level 95%, Interference level set to 10%)

The trend presented in Figure 10.18 illustrates the rate of change between the linear and non-linear approaches; the linear method increases and decreases the paranoia in fixed

quantities whilst the non-linear method follows an exponential trend; this influences the time required to change to the new state as the linear values would require longer to reach a new state based on extreme inputs (e.g. very high paranoia and very low interference level) which differs from non-linear methods where it is better suited for this change; however, the linear method would be better suited for situations where the expected state of change is minimal as the variation with small adjustment is greater in comparison to the non-linear implementation.

10.6.2 Behaviour of Linear and Non-Linear Adaptive Control Systems: Fixed Paranoia Level and a Variable Interference Level over One Iteration

The second scenario investigated is the comparison of linear and non-linear values used for the logic rule set with the paranoia input level fixed to ninety-five per cent and the interference variable increased in fixed steps of fifteen per cent intervals starting from zero to ninety-five per cent. Figure 10.19 illustrates the results of the interference level fixed to ninety-five per cent and the paranoia level changing from zero to ninety-five per cent with linear and non-linear values selected for the rule sets.

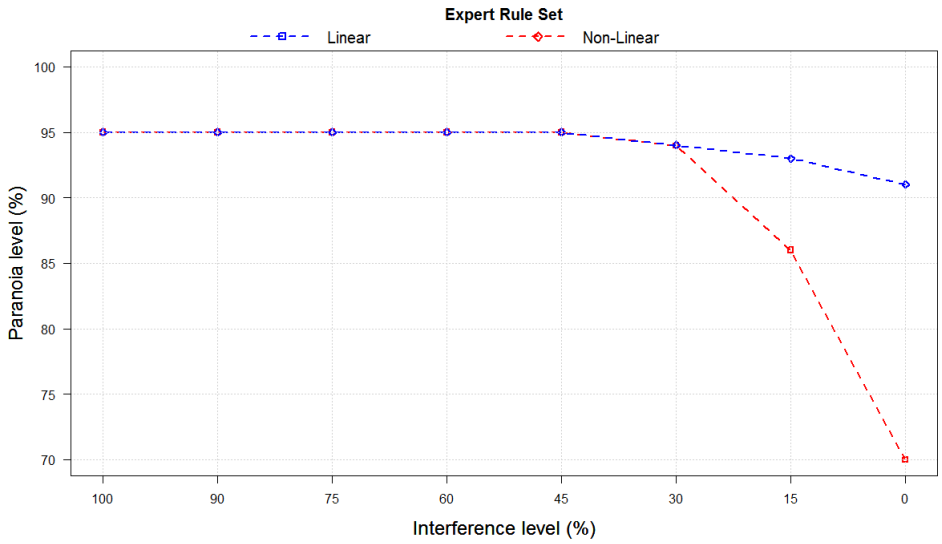


Figure 10.19: Characteristic of the paranoia level with varying interference levels with linear and non-linear values selected for the rule base. (Initial paranoia start level 95%)

Data obtained in Figure 10.19 shows that the trend between the linear and non-linear fuzzy rule sets follows a positive correlation as the increased interference level influenced the rate of the newly calculated paranoia level output. The rate of change between the two approaches differs with the linear approach following fixed decrements as the interference level decreases whilst the non-linear approach follows an exponential decay profile. The trend of both methods after the interference level is set above thirty per cent follows a linear pattern; this is because the maximum threshold bound set for the calculation of the

new paranoia level has been configured to not exceed the maximum value of ninety-five per cent.

10.6.3 Behaviour of the Hybrid Adaptive Control System: Relationship between the Paranoia Level and Number of Iterations Performed

Analysis of the hybrid rule based adaptive control system was undertaken in reference to the linear and non-linear rule set values presented in the aforementioned tests in section 10.6.1 and 10.6.2 to determine the behaviour of the system at various configuration settings for the hybrid rule base; in this instance of the analysis two rule bases are chosen which are linear and non-linear rule sets from the aforementioned validation. The analysis first investigates the impact of varying the point of change between the selection of the two rule sets and how the calculated output is impacted by this approach. Figure 10.20 plots the rate of change of the paranoia level with a varying number of iterations used with an interference level set to ten per cent.

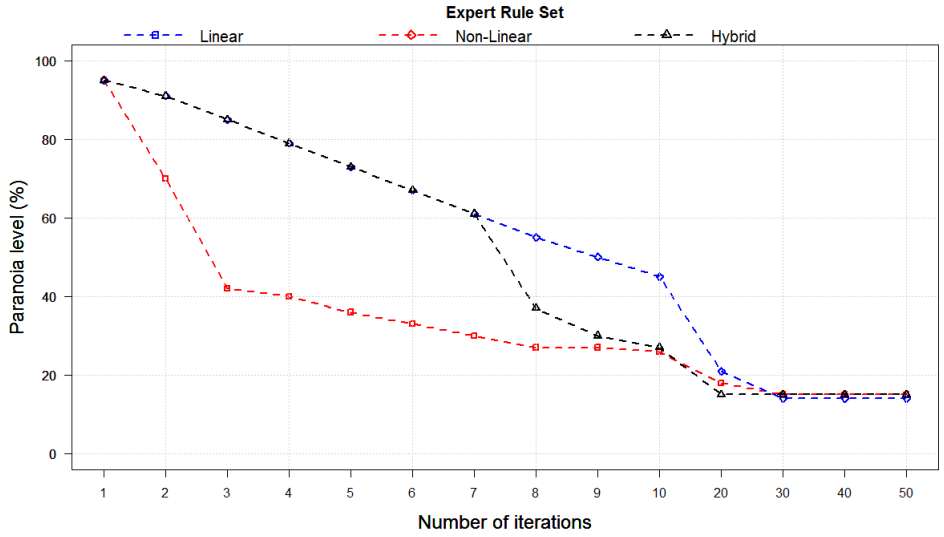


Figure 10.20: Characteristic of linear, non-linear and hybrid rule set values on the paranoia value over a varying number of iterations with an interference level set to ten per cent

Results presented in Figure 10.20 shows that the hybrid rule set follows a linear profile up to seven iterations before the selection of the non-linear rule set was selected; this demonstrates that the hybrid rule set changed after the paranoia value fell below the threshold of fifty per cent; therefore, the behaviour of the adaptive control system change as reflected in the profile of the hybrid approach. To further reinforce this point, Figure 10.21 illustrates the characteristics of linear, non-linear and hybrid rule sets over various number of iterations with an interference level of fifty per cent.

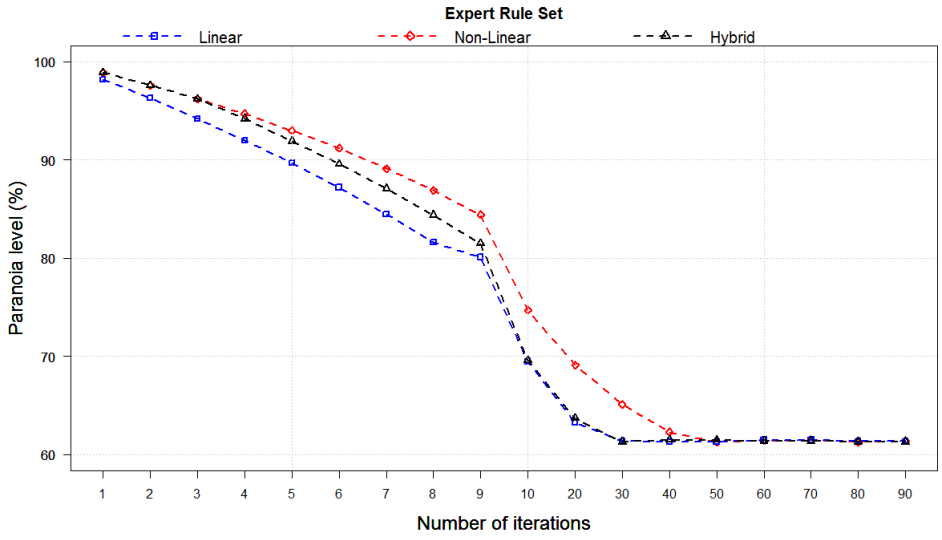


Figure 10.21: Characteristic of linear, non-linear and hybrid rule set values on the paranoia value over various number of iterations with an interference level set to fifty per cent

Results presented in Figure 10.21 demonstrates that the characteristic of the hybrid rule set profile operates in an area in-between the linear and non-linear logic rule sets. The initial trend line presented shows that the hybrid system follows an identical operation to the non-linear approach; however, after three iterations the hybrid rule set changes its operation to a linear rule sets and diverges from the non-linear profile; resulting in the hybrid approach converging with the linear trend-line as the number of iterations increases. The behaviour of the hybrid rule set indicates that rate of change with the hybrid rule set is greater than linear and non-linear approaches because the design of the hybrid rule set combined the greatest values for linear and non-linear approaches in order to change state at the fastest rate.

10.7 Discussion

Validation of the novel approaches against the specification has been achieved. The PCU adjusts as the frequency of the key regenerations to maintain the privacy of the shared cryptographic secret and the LEOPARD block cipher integrates the combination of operation into one function to increase speed of processing whilst maintaining secure communications.

The focus of the speed centric method through the Big Cat Block Cipher Suite and LEOPARD method presented was derived from the viewpoint of increasing the speed of the operation through the data path of the cryptographic primitive. Validation of the method shows an instance of the proposed speed-centric method that proved to process a fixed

block length quicker than the standardised de-facto AES-128 block cipher.

The analysis of the LEOPARD cryptographic primitive based on the test conducted correlate with the idea of combining cryptographic functions to undertake the same task has a reduction on the time required to process the security operation which results in an increase in speed and reduction in energy consumption; however, a disadvantage of this paradigm is the impact on the cipher-text produced, the entropy, arithmetic mean and the serial correlation are reduced but still comparable to the standardised AES-128 configuration.

The comparison of LEOPARD and AES-128 cryptographic primitives in the context of real-time teleoperation and telemetry show differences in the time required to process the cryptographic constructs; however, the method selected to showcase the speed-centric method is based on the current cryptographic functions used by AES-128; an instance of a combination of cryptographic primitive presented with the novel LEOPARD approach shows that the implementation of a cryptographic system that prioritises speed a better approach for the context of real-time teleoperation and telemetry.

A limitation of the Big Cat Block Cipher Suite is the constraint to the existing standardised implementation of the AES-128 cryptographic primitive as the Big Cat family of block ciphers' design suite follows the variations of the structural arrangement that the AES-128 cryptographic primitive can be set.

The privacy based method was achieved with the presentation of the PCU methodology to maintain the privacy of the shared cryptographic secret between communicating entities. The validation of the PCU demonstrates that the incorporation of an adaptive control system to make an initial prognosis based on the analysis of information obtained in real-time to dictate the key regeneration mechanism is a viable concept as the output of the privacy analysis through the expert logic influenced the behaviour of the number of key regenerations required to maintain the cryptographic secret between the transmitter and receiver; therefore, an attacker conducting an offline parallel brute force attack would be forced to re-attempt the search for all possible cryptographic keys as the probability that the regenerated key is located in the previous search area is plausible.

The design and implementation of the expert logic into the PCU enables flexibility in terms of application for various scenarios and contexts as the expert can pre-define the rule-sets, weighting of each rule and the variate between the behaviour patterns through the use of the hybrid rule set approach. Application of the hybrid rule set enables the system to change its behaviour to account for changes in the observations obtained from

the external environment; this is beneficial in situations that are chaotic as the change in the environment results in the expert logic changing its prognosis in that period of time and therefore impacting the diagnostic action to select based on the inference of the expert logic implemented for the mission time. Furthermore, the mechanism of the PCU only initiates once specific criteria has been meet (e.g. packet count has meet the set-point of the previous paranoia level) which aids the privacy of the shared cryptographic secret as the process is aperiodic and contributes towards the mitigation of frequency analysis due to the random like behaviour of the PCU in real-time.

10.8 Chapter Summary

The chapter presented the validation of the two novel approaches based on the derived speed centric and privacy based methods based on the cryptographic synergy philosophy. Validation of the two instances of the methods was undertaken and benchmarked against the current approaches presented in the problem analysis and on the contrived scenarios presented in this chapter.

Findings presented from the validation of the two novel approaches demonstrate that the instance of the speed centric paradigm with the LEOPARD block cipher has a reduced impact on the operational performance of real-time teleoperation and telemetry. The latency, energy consumption and responsiveness of the mobile platform is improved whilst maintaining a comparable cryptographic metrics of the cipher-text output when benchmarked against AES-128. Validation of the privacy based method with the PCU approach demonstrated that the expert logic approach enabled the privacy of the shared secret to be maintained with communicating entities when incorporated into the key regeneration mechanism as the initialisation of the process is determined by the prognosis based on the programmed expert logic. The presentation of a hybrid rule set that included both linear and non-linear approaches was proven to achieve the desired set-point at a faster rate in comparison to linear and non-linear approaches; helps mitigate deterministic behaviour and requires the attacker to attempt all possible cryptographic keys each time the process is undertaken. The next chapter presents the conclusion of the research.

11 Conclusion

11.1 Introduction

This chapter presents the conclusion of the research undertaken and future research areas based on the research findings. The structure of this chapter is as follows; first, the justification of the specified aims and objectives are presented and discussed; followed by the key findings obtained from the research and the dissemination of the research conducted in this thesis. Future research directions are identified and discussed. A chapter summary concludes.

The research undertaken in this thesis investigated the challenge of balancing secure communications, real-time operations and performance as the problem is multi-factoring, non-trivial and an open problem. The justification for undertaking the research presented in this thesis was to mitigate passive and active attackers from impacting the performance and operation of real-time teleoperation and telemetry in various scenarios.

The research sought to clarify how the impact of current contemporary security philosophies and approaches influence the behaviour of real-time teleoperation and telemetry. The literature presented in this field showed that the focus of the current philosophies steamed from enterprise systems that prioritised cryptographic strength with newer philosophies prioritised energy conservation. The consideration for time, privacy and speed has not been explicitly considered for this context; therefore, the research sought to establish a new philosophy that meets the time constraints and computational limitations associated with real-time teleoperation and telemetry whilst maintaining an element of cryptographic privacy of the shared secret required for the secure communication links.

11.2 Justification of Research Aim and Objectives

The application of the cryptographic synergy philosophy has facilitated achieved the aim specified in this thesis to provide a novel approach to symmetric cryptographic secured communication links that will have a reduced impact on the operational performance of real-time teleoperation and telemetry in comparison to contemporary standardised symmetric cryptographic approaches to secured communication links.

The aim of the research project has been fulfilled in this thesis as two novel approaches to symmetric cryptographic secured wireless communication links for real-time teleoperation and telemetry has been proposed and validated. The speed-centric method was presented with consideration of the element of time to prioritise speed of the cryptographic service in relation to the application of the real-time teleoperation and telemetry

and the privacy-based method presented to take expert action based on the prognosis of the situation at real-time to maintain the privacy of the cryptographic secret.

Validation of the proposed methods derived from the cryptographic synergy philosophy has shown the speed-centric method has an up to ten percent reduction on the processing latency of the block cipher whilst maintaining the privacy of the ephemeral shared secret through the privacy-based method.

Combination of the two methods derived achieved the cryptographic synergy philosophy specified as the LEOPARD block cipher is internal security service used by the real-time application to provide confidentiality and integrity services to packetised data; whilst the shared secret (i.e. the cryptographic key) is the external security service that is influenced by the global environment as the privacy cryptographic unit is integrated to operate with the internal real-time teleoperation and telemetry application and the external environment it is applied to.

11.2.1 Research Objectives Achieved

The objectives specified to meet the aim have been met with a comprehensive literature survey and literature review undertaken in Chapter 2. Identification of existing knowledge related to the research problem and the research gaps were presented and areas of original contribution identified.

Examination of current contemporary security philosophies in the context of real-time teleoperation and telemetry was undertaken through a series of preliminary tests in order to ascertain the problems associated with the research area and why existing security philosophies were not suited for this application as presented in Chapter 3, Chapter 4, Chapter 5, Chapter 6 and Chapter 7. The conclusion of the preliminary experiments were then analysed and knowledge obtained as to the variables that contribute to the problem statement where analysed as to how the variables influenced the problem.

Analysis of current contemporary security paradigms on the behaviour of real-time teleoperation and telemetry has been established in Chapter 3, Chapter 4, Chapter 5, Chapter 6 and Chapter 7 and the factors linking secure communication and real-time teleoperation and telemetry have been demonstrated from the problem analysis undertaken with a generalisation of the variables into categories to give a holistic overview of the factors that require consideration for the proposed philosophy. A specification derived to overcome the problem examined for the context of this research has been stated.

The speed-centric and privacy-based methods was proposed in Chapter 8 and Chapter

9 based on the specification of the factors identified in Chapter 7, section 7.6 with two novel instances of the philosophy presented and implemented through the Privacy Cryptographic Unit and the Lightweight Entropy Operations Permutation Addition Rotational Dispersion block cipher in order to provide symmetric secure communication links for real-time teleoperation and telemetry, both implementations are validated against current and relevant methods as presented in Chapter 10.

11.3 Research Outcome

The empirical findings of the research undertaken answer the problem statement specified for this thesis.

- Selection of the security measure for secure communications has an impact on the operation and performance of real-time teleoperation and telemetry; factors such as latency, throughput and energy consumption are impacted. The security measures that follow a strength based philosophy have a larger negative impact in comparison to the energy based philosophy at the same processing frequency as the number of instructions required to process the security measure is increased.
- The asymmetric nature of the communication links (i.e. different transmission rates for uplink and downlink) used for mobile real-time teleoperation and telemetry requires different security methods as the nature of the communicated data between the transmitter is command and control data for the uplink channel and streamed sensor data for the downlink channel.
- A balance between the cryptographic strength, energy consumption and speed required to process the security measure is explicitly linked to time.

11.4 Contributions of Research

The contributions ascertained from the completion of this research are as follows.

- The presentation of the cryptographic synergy philosophy with two novel approaches to achieve the proposed philosophy with the speed-centric method that uses the composite concept and the intrinsic paradigm to reduce the time required to process packetised data and the privacy based method that maintains the ephemeral secret used for secure communications. The significance of the proposed philosophy enables the creation of new block cipher designs that prioritise the speed to process the cryptographic process and the ephemeral shared cryptographic secret is maintained through the application of expert knowledge that directly influences the behaviour of a given system based on its interpretation of the scenario in an autonomous operation.

- A new taxonomy of block cipher designs with the PSN and PSPN cipher structures that can be used to design new block ciphers and can be extended to the redesign of existing block ciphers.
- A novel approach to block cipher design that incorporates the speed-centric method and composite concept with an the instance presented the LEOPARD block cipher and the Big Cat Family of block ciphers that were designed with the consideration for the context of real-time teleoperation and telemetry but are also transferable to alternative scenarios that prioritises the speed of operation.
- A novel approach to key renewal was derived from the privacy-based method that used autonomous expert knowledge to influence the behaviour of the variable key renewal scheme with the instance presented the privacy cryptographic unit. The significance of this contribution is that the privacy of the shared secret between the communicating entities is maintained to obfuscate attack vectors and enable autonomous operation without human intervention.

The areas of contribution derived from the findings presented in this thesis is comprised of two novel approaches with the speed-centric method and the privacy-based method. The proposed speed-centric method prioritises the speed of the cryptographic operation in order to meet the constraints associated with real-time teleoperation and telemetry as contemporary cryptographic services are not best suited for this application as the speed of the cryptographic operation was not prioritised as the main consideration.

Proposed paradigms to meet the criteria of the speed-centric method have been proposed with the a new taxonomy of block cipher design with the PSN and PSPN structures and the synergy paradigm, which combines cryptographic operations to reduce the processing time of the cryptographic process in order to have a reduced impact on the operational performance of the real-time teleoperation and telemetry.

The proposition of the speed-centric method and synergy based paradigm is transferable to any block cipher design that requires the prioritisation of speed and can be generalised to other research area to prioritise the speed of the cryptosystem for a particular application; this contrasts from the existing philosophies of cryptographic strength or energy conservation of the block cipher and introduces a significant change in the design method of block ciphers.

Validation of the speed-centric method and synergy paradigm in Chapter 10 demonstrates that the proposed novel approach has a reduced impact on the processing latency of the block cipher; outcomes of the reduction of the processing latency of the block cipher on the real-time teleoperation and telemetry is the increased quantity of real-time telemetry

messages transmitted between the transmitter and receiver, reduced distance travelled by a mobile real-time teleoperation and telemetry system before processing a command and the implementation of secure communications to mitigate passive and active attack vectors.

A by-product of the reduction in processing latency is the reduction in the energy consumption of the block cipher has a reduced impact on the energy consumption of a real-time teleoperation and telemetry system and increase the operational lifetime and results in a prolonged use of the system for remote data acquisition or control.

The second novel approach proposed in this thesis is the privacy-based method that derives an expert prognosis of a situation based on internal and external experiences that are interpreted by an expert knowledge based in the system in real-time. Contribution of the privacy unit enables variance and adaptiveness of a process in real-time in order to meet the requirements of the situation; in addition, the privacy-based method is transferable of any generalised system processes with a customisable expert rule set to retrofit the application and modify the behaviour of the system in real-time operation.

The significance of this contribution is that the privacy-based method proposes an unstable, chaotic control system; this differs from traditional control systems methods that attempt to stabilise a systems process as the cornerstone of this method is to create unpredictability of the key regeneration of the shared secret between communication devices.

The instance of the proposed philosophy presented in this thesis is the privacy cryptographic unit that prioritises the privacy of the shared secret between the transmitter and receiver device through the key regeneration of the symmetric key used for secure communication and variates the frequency of the key regeneration based on the outcome of the expert prognosis.

The validation of the privacy-based method demonstrates beneficial impacts with the minimal processing latency required to derive prognosis of the scenario that reduces the impact of secured communication on real-time teleoperation and telemetry and the variation of the system dependent on the prognosis of the situation, in this instance the privacy unit is used to enhance the privacy of the shared secret between the transmitter and receiver.

11.5 Dissemination of Research

The findings of the research have been presented at conference proceedings; copies of the paper submissions are located in Appendix R-X. The conference paper titles and date are

formatted in chronological order:

Conference paper 1: Simulating and Modelling the Impact of Security Constructs on Latency for Open Loop Control, IEEE 6th Computer Science and Electronic Engineering Conference (CEEC) 2014, Colchester, Essex, 26th September 2014.

Conference paper 2: Simulating and Modelling the Impact of Secure Communication Latency for Closed Loop Control, IEEE 6th International Conference on Internet Technologies & Applications 2015, Wrexham, Wales, 11th September 2015.

Conference paper 3: Study of Two Security Constructs on Throughput for Wireless Sensor Multi-Hop Networks, IEEE 38th International convention on information and communication technology, electronics and microelectronics, Opatija, Croatia, 27th May 2015.

Conference paper 4: Balancing Throughput and Latency for an Aerial Robot over a Wireless Secure Communication Link, IEEE 2nd International Conference on Cybernetics CYBCONF 2015, Gdynia, Poland, 25th June 2015.

Conference paper 5: The Affect of Two Cryptographic Constructs on QoS and QoE for Unmanned Control Vehicles, IEEE 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, England, 25th June 2015.

Conference paper 6: A Novel Block Cipher Design Paradigm for Secured Communication, IEEE 10th International Systems Conference, Florida, United States of America, 17-24th April 2016.

Conference paper 7: LEOPARD: Lightweight Encryption Operation Permutation Addition Rotation and Diffusion, IEEE 10th International Conference on Signal Processing and Communication Systems, Brisbane, Australia, 19-21st December 2016.

11.6 Future Work

Future research to be undertaken based on the knowledge presented should focus on mobile to mobile systems as the investigation of this thesis was primarily for scenarios that were static to static, static to mobile or mobile to static that were manually controlled. The consideration for secure communication links for a mobile to mobile platform system has different requirements and problems to consider as the continuous movement and the integration of autonomous platforms adds to the complexity of the system and requires

further research.

Semi-autonomous and autonomous systems are areas that are considered future research as the nature of mobile devices are beginning to incorporate partial or full control to the system without human intervention; the application of these approaches would be useful for operational and strategic use of unmanned vehicles as the identified variables that contribute to secure communication for real-time teleoperation and telemetry would be applicable with the adaptation for self regulating security measures.

Avenues of future research in this area include the design and analysis of new fuzzy logic rule and inference systems to modify rules during the course of the mission time and defuzzification approaches to derive an answer through human reasoning; in addition, the incorporation of the human involvement in manual, semi-autonomous and fully autonomous applications with the PCU has been identified as future work to facilitate the flexibility of manually changing the expert logic rule base throughout the duration of the mission through the human in the loop.

Application of artificial intelligence mechanism in the PCU is an area identified as future research as the concept of artificial intelligence could be used with the PCU to be applied if more complex mappings between a number of unrelated input variables (representing threat level) are used to adjust key regeneration time. Benefits of incorporating artificial intelligence paradigms in this context would be advantageous as the PCU would have the ability to learn and create new rule sets that are more suitable based on the real-time analysis of the scenario.

11.7 Chapter Summary

The chapter presented the conclusions based on the research undertaken for this thesis, the aim and objectives of the research have been achieved. Benefits and limitations of the proposed philosophy and novel approaches have been specified with suggestions to future research directions to overcome the current limitations and apply the proposed philosophy in alternative research areas.

References

Adekunle, A. & Woodhead, S. (2012), An aead cryptographic framework and tinyaead construct for secure wsn communication, *in* 'Wireless Advanced (WiAd)'.

Aeroviroment (2017), 'Unmanned aircraft systems: Tactical uas'.
URL: *https://www.avinc.com/uas/smalluas/raven*

Al-Janabi, S. T. F. & s. Rasheed, M. A. (2011), Public-key cryptography enabled kerberos authentication, *in* 'Developments in E-systems Engineering (DeSE), 2011'.

Ali Alheeti, K., Ehsan, S. & McDonald-Maier, K. (2014), An assessment of recent attacks on specific embedded systems, *in* 'Emerging Security Technologies (EST), 2014 Fifth International Conference on', pp. 88–93.

Anderson, R., Biham, E. & Knudsen, L. (1999), 'Serpent: A proposal for the advanced encryption standard', Online.

Arora, M. (2012), 'How secure is aes against brute force attacks?'.
URL: *http://www.eetimes.com/*

Arpaci-Dusseau, R. H. A.-D. A. C. (2015), *Operating Systems: Three Easy Pieces*.

Atmel (2015), Atmel at86rf212b, Technical report, Atmel.

Attie, A., Fadlallah, A. & Raad, M. (2015), Analysis of the tradeoff between compression ratio and security level in real-time voice communication, *in* 'Applied Research in Computer Science and Engineering (ICAR), 2015 International Conference on'.

Audsley, N., Burns, A., Davis, R., Tindell, K. & Wellings, A. (1995), *Real-Time System Scheduling*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 41–52.

Barker, E. (2016*a*), 'Nist special publication 800-57 part 1 revision 4 recommendation for key management part 1: General', Online.

Barker, E. (2016*b*), 'Recommendation for key management part 1: General'.

Beaulieu, R., Treatman-Clark, S., Shors, D., Weeks, B., Smith, J. & Wingers, L. (2015), The simon and speck lightweight block ciphers, *in* '2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)'.

Bellovin, S. M. & Merritt, M. (1990), 'Limitations of the kerberos authentication system'.

Bernstein, D. (2016), 'Caesar: Competition for authenticated encryption: Security, applicability, and robustness', Online.
URL: *https://competitions.cr.yp.to/caesar.html*

Bian, J., Seker, R. & Xie, M. (2013), A secure communication framework for large-scale unmanned aircraft systems, *in* 'Integrated Communications, Navigation and Surveillance Conference (ICNS), 2013'.

Biham, E. & Shamir, A. (1991), 'Differential cryptanalysis of des-like cryptosystems', *Journal of Cryptology* **4**(1), 3–72.

Biryukov, A. & Wagner, D. (1999), *Slide Attacks*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 245–259.

Blomer, J. & May, A. (2004), A generalized wiener attack on rsa, *in* 'International Workshop on Public Key Cryptography'.

Bogdanov, A., Khovratovich, D. & Rechberger, C. (2011), *Advances in Cryptology – ASIACRYPT 2011: 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, Springer Berlin Heidelberg, Berlin, Heidelberg, chapter Biclique Cryptanalysis of the Full AES, pp. 344–371.

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y. & Vikkelsoe, C. (2007), *PRESENT: An Ultra-Lightweight Block Cipher*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 450–466.

Borisov, N., Goldberg, I. & Wagner, D. (2001), Intercepting mobile communications: the insecurity of 802.11, *in* 'Proceedings of the 7th annual international conference on Mobile computing and networking'.

Borjian, M. (2017), *Language and Globalization: An Autoethnographic Approach*.

Botura, C. A., Botura Jr., G., Carvalho Jr., J. A., Mesquita, L. & Ferreira, M. A. (2002), 'Simulation of Active Control Using Fuzzy Logic Applied to a Pulse Combustor', *Journal of the Brazilian Society of Mechanical Sciences* **24**, 134 – 138.

CAA (2015), 'Unmanned aircraft system operations in uk airspace guidance'.

Castro, J. C. H., Sierra, J. M., Seznec, A., Izquierdo, A. & Ribagorda, A. (2005), 'The strict avalanche criterion randomness test', *Mathematics and Computers in Simulation* **68**(1), 1 – 7.

Chand, N., DeLuck, T., Andrew, J. H., Eteson, B. M., Daniel, T. M. & Carlson, R. T. (2010), Compact low-cost non-rf communication solutions for unmanned ground vehicles, *in* 'MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010'.

Choi, J., In, Y., Park, C., Seok, S., Seo, H. & Kim, H. (2016), 'Secure iot framework and 2d architecture for end-to-end security', *The Journal of Supercomputing* pp. 1–15.
URL: *http://dx.doi.org/10.1007/s11227-016-1684-0*

Cisco (1999), 'Token ring/ieee 802.5'.
URL: *https://www.cisco.com/cpress/cc/td/cpress/fund/ith2nd/it2409.htm*

Clayton, N. & Pandya, H. (2016), 'Vpn over ipsec', Online.
URL: *https://www.freebsd.org/doc/handbook/ipsec.html*

Cobham, A. (1954), 'Priority assignment in waiting line problems', *Journal of the Operations Research Society of America* **2**(1), 70–76.

Coffman, Jr, E. G. & Kleinrock, L. (1968), Computer scheduling methods and their countermeasures, *in* 'Proceedings of the April 30–May 2, 1968, Spring Joint Computer Conference'.

Coppersmith, D., Franklin, M., Patarin, J. & Reiter, M. (1996), Low-exponent rsa with related messages, *in* 'Proceedings of the 15th Annual International Conference on Theory and Application of Cryptographic Techniques', Springer-Verlag, pp. 1–9.

Corbellini, A. (2015), 'Elliptic curve cryptography: a gentle introduction'.
URL: *http://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/*

Cray (2017), 'Cray xc series'.
URL: *http://www.cray.com/sites/default/files/Cray-XC-Series-Brochure.pdf*

Cummings, C. E. (2002), Simulation and synthesis techniques for asynchronous fifo design, *in* 'SNUG 2002 (Synopsys Users Group Conference, San Jose, CA, 2002) User Papers'.

Czybik, B., Hausmann, S., Heiss, S. & Jasperneite, J. (2013), Performance evaluation of mac algorithms for real-time ethernet communication systems, *in* 'Industrial Informatics (INDIN), 2013 11th IEEE International Conference on'.

Daemen, J. & Rijmen, V. (2002), *The design of Rijndael: AES the Advanced Encryption Standard*, Springer.

Dallaire, G. (2010), 'Bilocation in the lives of the saints'.
URL: *http://www.miraclesofthesaints.com/2010/09/bilocation-of-st-padre-pio.html*

Dhanalakshmi, K. S., Kannapiran, B. & Divya, A. (2014), Enhancing manet security using hybrid techniques in key generation mechanism, *in* 'Electronics and Communication Systems (ICECS), 2014 International Conference on'.

Dictionary, O. (2018*a*), 'Balance'.
URL: *https://en.oxforddictionaries.com/definition/balance*

Dictionary, O. (2018*b*), 'Optimise'.
URL: *https://en.oxforddictionaries.com/definition/optimize*

Drozhzhin, A. (2016), 'Tesla model s was hacked remotely'.
URL: *https://blog.kaspersky.com/tesla-remote-hack/13027/*

Dunkelman, O., Keller, N. & Shamir, A. (2012), Minimalism in cryptography: The even-mansour scheme revisited, *in* 'Proceedings of the 31st Annual International Conference on Theory and Applications of'.

Dvorsky, G. (2016), 'This robotic tractor looks seriously badarse'.
URL: *http://www.gizmodo.com.au/2016/09/this-robotic-tractor-looks-seriously-badarse/*

Dworkin, M. (2004), 'Recommendation for block cipher modes of operation: The ccm mode for authentication and confidentiality'.

Dworkin, M. (2007), 'Recommendation for block cipher modes of operation: Galois/counter mode (gcm) and gmac'.

Elgamal, T. (1985), 'A public key cryptosystem and a signature scheme based on discrete logarithms', *IEEE Transactions on Information Theory* **31**, 469–472.

Emerson (2014), 'Level and volume measurments of bulk solids', Website.

Ferguson, N. (2005), Authentication weaknesses in gcm, Technical report, National Institute of Standards and Technology (NIST).

Fouque, P.-A., Jean, J. & Peyrin, T. (2013), *Structural Evaluation of AES and Chosen-Key Distinguisher of 9-Round AES-128*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 183–203.

Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A. D., Ritchey, R. W. & Sharma, S. R. (2005), 'Guide to ipsec vpns', *NIST Special Publication* pp. 1–126.
URL: *http://federalcybersecurity.org/CourseFiles/NIST/77IPSecVPNs.pdf*

Gilbert, H. & Peyrin, T. (2010), *Super-Sbox Cryptanalysis: Improved Attacks for AES-Like Permutations*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 365–383.

Glendinning, A. (2015), 'Bosley mill explosion: More human remains found at site', Website.
URL: *http://www.manchestereveningnews.co.uk/news/greater-manchester-news/bosley-mill-explosion-more-human-9739987*

GlobalSecurity (2015), ‘Unmanned aerial vehicles (uavs)’.
URL: *http://www.globalsecurity.org/intell/systems/uavintro.htm*

Gold, S. (2014), ‘Engineering technology’, *Get your head around hacker psychology [Information Technologycyber-Security]* **9**, 76–80.

Gong, Z., Nikova, S. & Law, Y. W. (2012), *KLEIN: A New Family of Lightweight Block Ciphers*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1–18.

Goossens, J., Funk, S. & Baruah, S. (2003), ‘Priority-driven scheduling of periodic task systems on multiprocessors’.

Grez, M. (2015), ‘Drone crashes onto piste, misses champion skier by inches’, Website.
URL: *http://edition.cnn.com/2015/12/23/sport/marcel-hirscher-drone-crash/*

Hamming, R. (1980), *Coding and Information Theory*.

Hartmann, K. & Steup, C. (2013), The vulnerability of uavs to cyber attacks - an approach to the risk assessment, *in* ‘Cyber Conflict (CyCon), 2013 5th International Conference on’.

Hienrich, H. (1988), Ablauf von gas- und staubexplosionen gemeinsamkeiten und unterschiede, *in* ‘Sichere Handhabung brennbare Stäube, Band I, VDI Verlag, W. Germany.’.

Huang, H.-M. (2004), Autonomy levels for unmanned systems (alfus) framework, Technical report, National Institute of Standards and Technology.

Hultman, S. (2015), ‘Monitoring bulk solids inventory’, Website.
URL: *http://www.processingmagazine.com/ext/resources/white-papers/2014/Monitoring-Bulk-Solids-Inventory.pdf*

IEEE (1997), ‘Ieee std 802.11-1997’, *IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* pp. i–445.

IEEE (2006), ‘Media access control (mac) security’.

Inagaki, T. & Stahre, J. (2004), ‘Human supervision and control in engineering and music: similarities, dissimilarities, and their implications’.

Instruments, T. (2014), ‘2.4 ghz ieee 802.15.4 / zigbee-ready rf transceiver’.
URL: *http://www.ti.com/lit/ds/symlink/cc2420.pdf*

ISO (2015), ‘Iso 11898-1:2015:- road vehicles – controller area network (can) – part 1: Data link layer and physical signalling’.

Jarvis (2016), 'Parrot disco review'.
URL: *http://gearopen.com/cameras/parrot-disco-review-42909/*

Jawhar, I., Mohamed, N. & Al-Jaroodi, J. (2014), Unmanned aircraft systems (icuas), 2014 international conference on, *in* 'Data communication in linear wireless sensor networks using Unmanned Aerial Vehicles'.

Jiang, K., Eles, P. & Peng, Z. (2012), Co-design techniques for distributed real-time embedded systems with communication security constraints, *in* 'Design, Automation Test in Europe Conference Exhibition, 2012'.

Jiang, W., Jiang, K., Zhang, X. & Ma, Y. (2015), 'Energy optimization of security-critical real-time applications with guaranteed security protection', *Journal of Systems Architecture* **61**(7), 282 – 292.
URL: *http://www.sciencedirect.com/science/article/pii/S1383762115000570*

Jing, Z. & Xi, C. (2012), A security-enhanced encryption scheme on power system real-time data communication, *in* 'Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on'.

Johnson, D., Menezes, A. & Vanstone, S. (2001), 'The elliptic curve digital signature algorithm (ecdsa)', *International Journal of Information Security* **1**, 36–63.

Jung, Y. & Festijo, E. (2013), Securing rtp packets using per-packet selective encryption scheme for real-time multimedia applications, *in* 'Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on'.

Kasper, J. (2014), 'Rq-11 raven'.
URL: *http://www.fi-aeroweb.com/Defense/RQ-11-Raven.html*

Kaur Grewal, J. (2015), ElGamal:Public-Key Cryptosystem, PhD thesis.

Khomani, N. (2015), 'Bosley mill explosion: fourth body recovered from wreckage', Website.
URL: *http://www.theguardian.com/uk-news/2015/jul/22/bosley-mill-explosion-disaster-waiting-to-happen*

King, J. (2017), 'Linear cryptanalysis tutorial'.
URL: *http://theamazingking.com/crypto-linear.php*

Kokes, J. & Lorencz, R. (2015), Linear cryptanalysis of baby rijndael, *in* '2015 Forth International Conference on e-Technologies and Networks for Development (ICeND)'.

Kounev, V., Tipper, D., Yavuz, A. A., Grainger, B. M. & Reed, G. F. (2015), 'A secure communication architecture for distributed microgrid control', *IEEE Transactions on Smart Grid* **6**, 2484–2492.

Laplante, P. (2004), *REAL-TIME SYSTEMS DESIGN AND ANALYSIS*.

Lehninger, A. (1971), *Bioenergetics: The Molecular Basis of Biological Energy Transformations*, Biological teaching monograph series, W. A. Benjamin.
URL: *https://books.google.co.uk/books?id=ZGadhLuFIRcC*

Liu, F. & Mendel, J. M. (2008), 'Aggregation using the fuzzy weighted average as computed by the karnik-mendel algorithms'.

Maitra, S. & Paul, G. (2008), *Progress in Cryptology - INDOCRYPT 2008: 9th International Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008. Proceedings*, Springer Berlin Heidelberg, Berlin, Heidelberg, chapter Analysis of RC4 and Proposal of Additional Layers for Better Security Margin, pp. 27–39.

Mamdani, E. & Assilian, S. (1999), 'An experiment in linguistic synthesis with a fuzzy logic controller', *International Journal of Human-Computer Studies* **51**(2), 135 – 147.
URL: *http://www.sciencedirect.com/science/article/pii/S1071581973603035*

Matsui, M. (1994), The first experimental cryptanalysis of the data encryption standard, *in* 'Advances in Cryptology'.

Matsui, M. & Yamagishi, A. (1992), A new method for known plaintext attack of feal cipher, *in* 'Advances in Cryptology'.

Mattsson, J. & Westerlund, M. (2015), 'Authentication key recovery on galois/counter mode (gcm)'.

McFadyen, S. (2015), 'Watch champion skier marcel hirscher escape serious injury as drone falls out of sky missing him by inches', Website.
URL: *http://www.mirror.co.uk/news/world-news/watch-champion-skier-marcel-hirscher-7060053*

McGrew, D. (2008), 'An interface and algorithms for authenticated encryption'.

McGrew, D. & Viega, J. (2007), 'The galois/counter mode of operation (gcm)', Online.

Merkle, R. C. & Hellman, M. E. (1981), 'On the security of multiple encryption'.

Minematsu, K., Morita, H. & Iwata, T. (2012), 'Cryptanalysis of eaxprime', Online.

Moise, A., Beroset, E., Phinney, T. & Burns, M. (2011), Eax cipher mode, Technical report, American National Standards Institute.

Mundhenk, P., Steinhorst, S., Lukasiewycz, M., Fahmy, S. A. & Chakraborty, S. (2015), Lightweight authentication for secure automotive networks, *in* 'Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition'.

NCSC (2017), ''krack' wi-fi guidance'.
URL: *https://www.ncsc.gov.uk/krack*

Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J. & Roback, E. (2000), Report on the development of the advanced encryption standard (aes), Technical report, National Institute of Standards and Technology.

Neuman, C., Yu, T., Hartman, A. & Raeburn, K. (2005), 'The kerberos network authentication service (v5)', Online.
URL: *https://www.ietf.org/rfc/rfc4120.txt*

Nguyen, D. Q., Toulgoat, M. & Lamont, L. (2016), 'Impact of trust-based security association and mobility on the delay metric in manet', *Journal of Communications and Networks* **1**, 105–111.

NIST (1999), 'Recommended elliptic curves for federal government use'.
URL: *http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf*

NIST (2007), 'Special publication 800-38d, recommendation for block cipher modes of operation: galois/counter mode (gcm) and gmac', Online.

NIST (2014), 'Cryptographic competitions: Aes: the advanced encryption standard'.
URL: *https://competitions.cr.yp.to/aes.html*

NIST (2017), 'Nvd cvss support'.
URL: *https://nvd.nist.gov/vuln-metrics/cvss*

Nohmi, M. & Bock, T. (2006), Contact task by force feedback teleoperation under communication time delay, *in* '2006 IEEE International Conference on Robotics and Biomimetics'.

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T. & Whitty, M. (2014), Security and privacy workshops (spw), 2014 ieee, *in* 'Understanding Insider Threat: A Framework for Characterising Attacks'.

Oorschot, P. C. V. & Wiener, M. J. (1990), A known-plaintext attack on two-key triple encryption, Springer-Verlag.

Pandey, V. K. & Singh, H. (2015), Enhancing security of mac protocol in manet using trust based engine, *in* 'Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on'.

Papini, I. (2016), 'Robot simulator'.
URL: *http://www.hangsim.com/rbs/*

Parrot (2017), 'Parrot disco fpv'.
URL: *https://www.parrot.com/uk/drones/parrot-disco-fpv*

Pigatto, D., Freire Roberto, G., Gonçalves, L., Rodrigues Filho, J., Roschildt Pinto, A. & Castelo Branco, K. (2014), Hamster - healthy, mobility and security-based data communication architecture for unmanned aircraft systems, *in* 'Unmanned Aircraft Systems (ICUAS), 2014 International Conference on', pp. 52–63.

Piret, G. & Quisquater, J.-J. (2003), *A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 77–88.

Privacy (2016).
URL: *https://en.oxforddictionaries.com/definition/privacy*

Priyadharshini, M. R., Prasanna, S. & Balaji, N. (2014), Energy and mobility based group key management in mobile ad hoc networks, *in* 'Recent Trends in Information Technology (ICRTIT), 2014 International Conference on'.

QGroundControl (2016), 'Mavlink micro air vehicle communication protocol', Online.
URL: *http://qgroundcontrol.org/mavlink/start*

Rajatha, B., Ananda, C. & Nagaraj, S. (2015), Authentication of mav communication using caesar cipher cryptography, *in* 'Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference on', 58-63.

Rescorla, E. (1999), 'Diffie-hellman key agreement method'.
URL: *http://www.rfc-editor.org/info/rfc2631*

Rivest, R. L., Shamir, A. & Adleman, L. (1978), 'A method for obtaining digital signatures and public-key cryptosystems', *Communications of the ACM* **21**, 120–126.

Rogaway, P., Bellare, M., Black, J. & Krovetz, T. (2001), Ocb: A block-cipher mode of operation for efficient authenticated encryption, Technical report.

Rogaway, P. & Wagner, D. (2003), 'A critique of ccm', Online.

Saarinen, M.-J. O. (2012), *Fast Software Encryption: 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, Springer Berlin Heidelberg, Berlin, Heidelberg, chapter Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes, pp. 216–225.

Salla, G., Sartin, A., Floro da Silva, N., Pigatto, D. & Branco, K. (2012), Performance evaluation of security communication in critical embedded systems, *in* 'Critical Embedded Systems (CBSEC), 2012 Second Brazilian Conference on', pp. 54–57.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. & Ferguson, N. (1998), 'Twofish: A 128-bit block cipher', Online.

Security (2016).
URL: *https://en.oxforddictionaries.com/definition/security*

Shannon, C. E. (1948), 'A mathematical theory of communication'.

Shannon, C. E. (1949), 'Communication theory of secrecy systems', *Bell System Technical Journal* **28**, 656–715.

Shaw, A. (2001), *Real-Time Systems and Software*.

Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T. & Shirai, T. (2011), *Piccolo: An Ultra-Lightweight Blockcipher*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 342–357.

Shin, K. G. & Ramanathan, P. (1994), 'Real-time computing: a new discipline of computer science and engineering'.

Shneiderman, B. (1984), 'Response time and display rate in human performance with computers'.

Siemens (2010), 'Using industrial ethernet networks for profinet', Online.

Singhal, N. & Raina, J. (2011), 'Comparative analysis of aes and rc4 algorithms for better utilization', *International Journal of Computer Trends and Technology* **2**, 177–181.

Smith, A. (2016), Public prediction for the future of workforce automation, Technical report, Pew Research Center.

Sparrow, R. D., Adekunle, A. A. & Berry, R. J. (2016), Leopard: Lightweight encryption operation permutation addition rotation and diffusion, *in* '2016 10th International Conference on Signal Processing and Communication Systems (ICSPCS'.

Sparrow, R. D., Adekunle, A. A., Berry, R. J. & Farnish, R. J. (2016), A novel block cipher design paradigm for secured communication, *in* '2016 Annual IEEE Systems Conference (SysCon)', pp. 1–6.

Stallings, W. (2015), *Operating Systems: Internals and Design Principles*.

Stonebraker, M., Cetintemel, U. & Zdonik, S. (2005), 'The 8 requirements of real-time stream processing'.

Strength (2016).
URL: *https://en.oxforddictionaries.com/definition/strength*

Sugita, M., Kobara, K., Uehara, K., Kubota, S. & Imai, H. (2000), Relationships among differential, truncated differential, impossible differential cryptanalyses against word-oriented block ciphers like rijndael, e2., *in* 'AES Candidate Conference'.

Sundell, M., Kuivalainen, J., Mäkelä, J., Gervais, A., Orava, J. & Hyppönen, M. (2016), 'White paper on industrial automation security in fieldbus and field device level', Online.
URL: *https://www.vacon.com/imagevaultfiles/id_3695/cf_2/vacon-white-paper-on-industrial-automation-securit.pdf*

Swenson, C. (2008), *Mordern Cryptanalysis: Technique for Advance Code Breaking*.

Tan, S. L. & Anh, T. N. B. (2009), Real-time operating system (rtos) for small (16-bit) microcontroller, *in* 'IEEE 13th International Symposium on Consumer Electronics'.

Union, I. T. (2016), 'Radio regulations'.

Vanhoef, M. & Piessens, F. (2017), 'Key reinstallation attacks: Breaking wpa2 by forcing nonce reuse in wpa2'.

Veen, C. V. (2012), 'Remote sensing: All eyes on munich'.
URL: *http://www.headwallphotonics.com/blog/bid/190790/RemoteSensingAllEyesonMunich*

Webster, A. F. & Tavares, S. E. (1986), *On the Design of S-Boxes*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 523–534.

Wei, M. & Wang, W. (2015), Safety can be dangerous: Secure communications impair smart grid stability under emergencies, *in* '2015 IEEE Global Communications Conference (GLOBECOM)'.

Wilhelm, R., Engblom, J., Ermedahl, A., Holsti, N., Thesing, S., Whalley, D., Bernat, G., Ferdinand, C., Heckmann, R., Mitra, T. et al. (2008), 'The worst-case execution-time problem - overview of methods and survey of tools'.

Williams, R. (2006), *Real-Time Systems Development*.

Winzer, R. (2015), Unmanned reconnaissance from the air, Technical report, Crypto AG.

Won, J., Seo, S.-H. & Bertino, E. (2015), A secure communication protocol for drones and smart objects, *in* 'Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security'.

Woods, D. L., Wyma, J. M., Yund, E. W., Herron, T. J. & Reed, B. (2015), 'Factors influencing the latency of simple reaction time', *Frontiers in Human Neuroscience* **9**, 131.
URL: *http://journal.frontiersin.org/article/10.3389/fnhum.2015.00131*

X.509 (2014), 'Information technology open systems interconnection the directory: Public-key and attribute certificate frameworks'.

X.800 (1991), 'Data communication networks: Open systems interconnection (osi) security structure and applications'.

Yap, W.-S., Yeo, S. L., Heng, S.-H. & Henricksen, M. (2014), 'Security analysis of gcm for communication', *Security and Communication Networks* **7**(5), 854–864.
URL: *http://dx.doi.org/10.1002/sec.798*

Zalman, R. & Mayer, A. (2014), A secure but still safe and low cost automotive communication technique, *in* 'Design Automation Conference (DAC), 2014 51st ACM/EDAC/IEEE'.

Zetter, K. (2015), 'Researchers hack a model s, but tesla's already released a patch'.
URL: *https://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/*

Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B. & Verbauwhede, I. (2015), 'Rectangle: a bit-slice lightweight block cipher suitable for multiple platforms', *Science China Information Sciences* **58**(12), 1–15.
URL: *http://dx.doi.org/10.1007/s11432-015-5459-7*

Zhou, Y. & Feng, D. (2005), 'Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing'.

Zhu, B., Tan, Y. & Gong, G. (2013), *Cryptology and Network Security: 12th International Conference, CANS 2013, Paraty, Brazil, November 20-22. 2013. Proceedings*, Springer International Publishing, Cham, chapter Revisiting MAC Forgeries, Weak Keys and Provable Security of Galois/Counter Mode of Operation, pp. 20–38.

Zouhri, O., Benhadou, S. & Medromi, H. (2017), *A New Adaptative Security Protocol for UAV Network*, Springer Singapore, Singapore, pp. 649–657.

A Appendix A: An Instance of The Performance Requirements of Each Individual Task of The Static to Static Real-Time System Problem Scenario

Task ID	Task	Category	Trigger Event Task ID	Response Task ID	Maximum Deadline Estimate
1	Initialise System	Process	8	2	500 μs
2	Start Compressor and Feeder	Input	1	3	10 ms
3	Convey Material to Silo	Process	2	4	1 ms
4	Sense Ignition Source	Input	3	5	5 ms
5	Transmit Signal to Controller	Input	4	6	30 μs
6	Interpret Signal	Process	5	7	5 ms
7	Activate Actuators	Output	6	8	1 ms
8	Shutdown System	Output	6	8	1 ms
Worst Case Execution Time					**24 ms**

B Appendix B: The Impact of Communication Latency on Real-Time Teleoperation Over a Single Communication Link Experiment Plan

Aim: To analyse how contemporary security construct impact the latency induced on a simplex single hop communication link on real-time teleoperation and telemetry.

Hypothesis: The null hypothesis is that security constructs will have no impact on the communication latency in a single hop simplex communication link. The alternative hypothesis is that the security construct will have an impact on the communication latency in a single hop simplex communication link.

Assumptions: Ideal communication link between the transmitter and receiver nodes and are one hundred metres in distance apart. The communication medium between the transmitter and receiver is copper cabling. FIFO task scheduler used by microcontrollers.

Method: Measurement based analysis undertaken in the emulated Proteus ISIS 8 emulator that measured the overall latency incurred by the system with the implementation of contemporary cryptographic methods. The measurement based technique selected for this test set a pin high at the beginning of the encryption or decryption process and set the pin low when the operation was complete; the duration of the process was analysed through the use of an oscilloscope and a timer counter on the transmitter and receiver microcontroller.

The communication link between the transmitter and receiver was simulated with the Serial Peripheral Interface (SPI) to send data between transmitter and receiver node; this was selected to mimicked an ideal wireless communication channel with synchronous data transmission rate. The simulation of the communication link was achieved through the hexadecimal files uploaded onto the microcontrollers derived from the implementation of the C programme selected to code the SPI communication at specified transmission rate through the application of the SPI divisor; this divided the frequency of oscillation by the SPI divisor to derive the transmission rate for the transmitter and receiver device.

Apparatus: The apparatus required for this test is listed in Table B.1. Configuration of the components selected for this test in the Proteus ISIS 8 emulator are specified in Table B.2 and B.3

Table B.1: Apparatus required for test procedure

Item	Quantity
Windows 7 Intel Pentium 2.1 GHz processor	1
Proteus ISIS 8 Simulation Package	1
PIC18F45K22 Microcontroller	2
Timer Counters	2
Virtual Oscilloscope	1
Light Emitting Diodes (LED)	3
Push Button	1

Table B.2: Configuration of components for no security test

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled	1 MHz 4 MHz 8 MHz
Serial Peripheral Interface (SPI) Configurations	**Test 1:** Divisor of 4 **Test 2:** Divisor of 16 **Test 3:** Divisor of 64
Packet Size	36 Bytes

Table B.3: Configuration of components with security test

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled	1 MHz 4 MHz 8 MHz
Serial Peripheral Interface (SPI) Configurations	Divisor of 4
Packet Size	36 Bytes 52 Bytes 84 Bytes
AEAD Constructs	GCM-AES-128 CCM-AES-128 TinyAEAD 3 rounds (AES-128) TinyAEAD 5 rounds (AES-128) TinyAEAD 10 rounds (AES-128)

Table B.4: Configuration of components for comparison against mathematical model and simulation test

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled	20 MHz
Serial Peripheral Interface (SPI) Configurations	Divisor of 4
Packet Size	36 Bytes 52 Bytes 84 Bytes
AEAD Constructs	TinyAEAD 3 rounds (AES-128)

Procedure: The procedure was conducted sequentially with the following steps:

1. Configure the SPI settings in the C programme and compile the programme to obtain the hexadecimal file.
2. Set configuration of the crystal frequency used by the microcontrollers and upload the hexadecimal files in the Proteus ISIS 8 emulator by clicking on the device and setting the parameters specified.
3. Begin the emulation of the system.
4. Press the push button to initialise a packet transmission from the transmitter to the receiver.
5. Watch the oscilloscope trace to identify if the packet has been transmitted across the SPI output pin of the transmitter node or the SPI input pin of the receiver node.
6. View the timer on the transmitter and receiver devices to obtain the time taken for a message to be encrypted at the transmitter and decrypted at the receiver.
7. Record the observed time for the operation to complete.

Recorded data for no security tests

Crystal Frequency (MHz)	SPI divisor of 4 time (ms)	SPI Divisor of 16 time (ms)	SPI divisor of 64 time (ms)
1	2.9	4.6	11.3
4	0.8	1.2	2.8
8	0.4	0.6	1.4

Crystal Frequency (MHz)	SPI divisor of 4 time (ms)	SPI Divisor of 16 time (ms)	SPI divisor of 64 time (ms)
1	6.0	9.2	22.6
4	1.5	2.3	5.7
8	0.8	1.1	2.9

Crystal Frequency (MHz)	SPI divisor of 4 time (ms)	SPI Divisor of 16 time (ms)	SPI divisor of 64 time (ms)
1	12.0	18.3	45.2
4	3.0	4.6	11.3
8	1.5	2.2	5.7

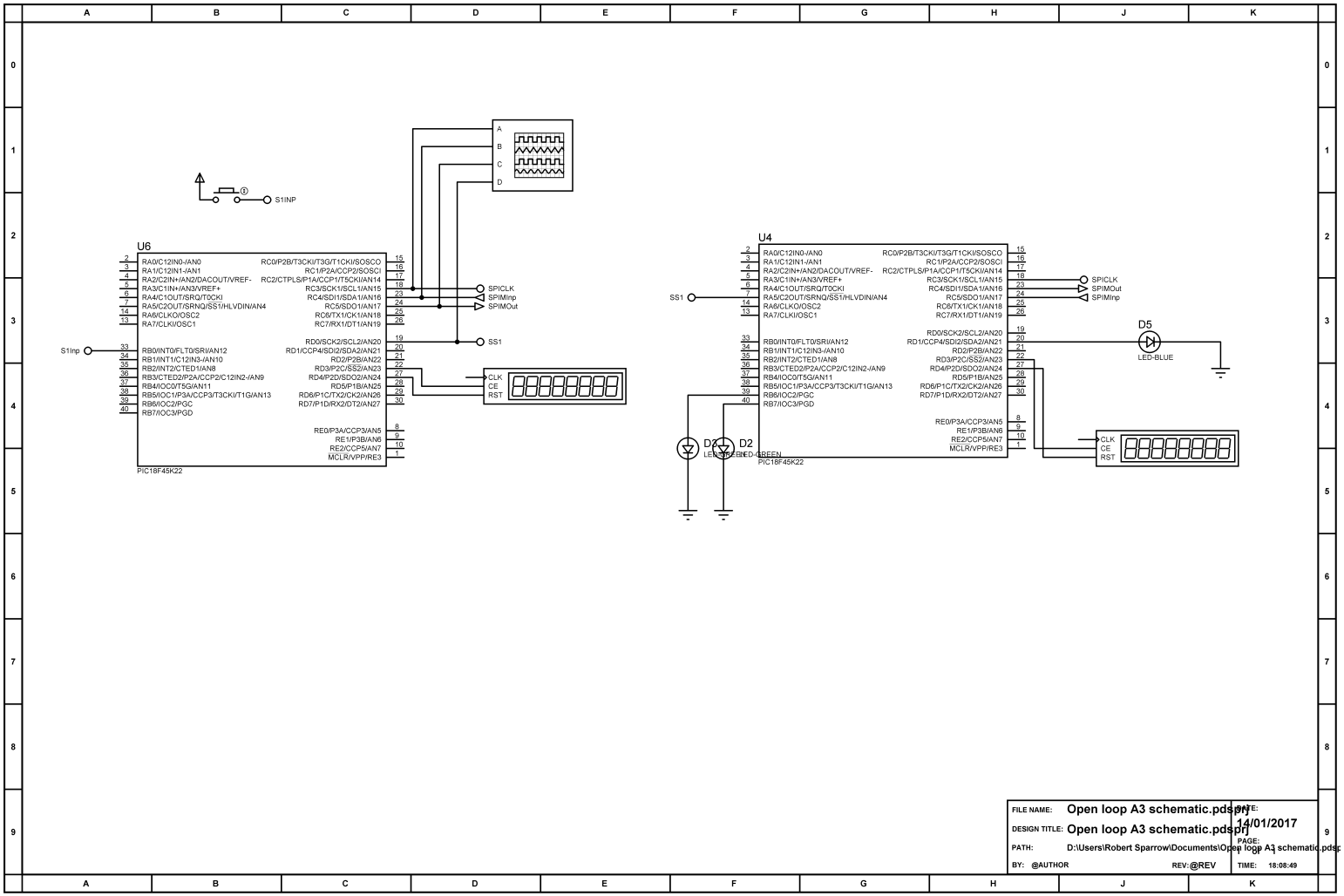
Recorded data for security tests

Packet Size	GCM-AES-128 time (ms)	CCM-AES-128 time (ms)	TINY AEAD 10 rounds time (ms)	TINY AEAD 5 rounds time (ms)	TINY AEAD 3 rounds time (ms)	Crystal Frequency (MHz)
16	361.5	73.9	61.5	32.5	20.9	8
32	490.2	103.6	92.1	48.4	31.1	8
64	753.1	162.8	153	80.4	51.5	8

Packet Size	GCM-AES-128 time (ms)	CCM-AES-128 time (ms)	TINY AEAD 10 rounds time (ms)	TINY AEAD 5 rounds time (ms)	TINY AEAD 3 rounds time (ms)	Crystal Frequency (MHz)
16	723.1	147.8	123.7	65	41.9	4
32	980.4	220.7	184.2	96.8	63	4
64	1506.3	325.7	306.1	160.9	102.9	4

Packet Size	GCM-AES-128 time (ms)	CCM-AES-128 time (ms)	TINY AEAD 10 rounds time (ms)	TINY AEAD 5 rounds time (ms)	TINY AEAD 3 rounds time (ms)	Crystal Frequency (MHz)
16	2892.6	591.3	492.4	260	167.6	1
32	3928.1	829.2	736.8	387.7	249.1	1
64	6025.3	1302.9	1224.4	640.3	412.3	1

Schematic


A
B
C
D
S1INP
U6
RA0/C12IN0-/AN0
RA1/C12IN1-/AN1
RA2/C2IN+/AN2/DACOUT/VREF-
RA3/C1IN+/AN3/VREF+
RA4/C1OUT/SRQ/T0CKI
RA5/C2OUT/SRNQ/SS1/HLVDIN/AN4
RA6/CLKO/OSC2
RA7/CLKI/OSC1
RC0/P2B/T3CKI/T3G/T1CKI/SOSCO
RC1/P2A/CCP2/SOSCI
RC2/CTPLS/P1A/CCP1/T5CKI/AN14
RC3/SCK1/SCL1/AN15
RC4/SDI1/SDA1/AN16
RC5/SDO1/AN17
RC6/TX1/CK1/AN18
RC7/RX1/DT1/AN19
RD0/SCK2/SCL2/AN20
RD1/CCP4/SDI2/SDA2/AN21
RD2/P2B/AN22
RD3/P2C/SS2/AN23
RD4/P2D/SDO2/AN24
RD5/P1B/AN25
RD6/P1C/TX2/CK2/AN26
RD7/P1D/RX2/DT2/AN27
RB0/INT0/FLT0/SRI/AN12
RB1/INT1/C12IN3-/AN10
RB2/INT2/CTED1/AN8
RB3/CTED2/P2A/CCP2/C12IN2-/AN9
RB4/IOC0/T5G/AN11
RB5/IOC1/P3A/CCP3/T3CKI/T1G/AN13
RB6/IOC2/PGC
RB7/IOC3/PGD
RE0/P3A/CCP3/AN5
RE1/P3B/AN6
RE2/CCP5/AN7
MCLR/VPP/RE3
PIC18F45K22
S1Inp
SPICLK
SPIMInp
SPIMOut
SS1
CLK
CE
RST
U4
SS1
SPICLK
SPIMOut
SPIMInp
D5
LED-BLUE
D2
LED-GREEN
D2
LED-GREEN
PIC18F45K22
CLK
CE
RST
FILE NAME: Open loop A3 schematic.pdsprj
DESIGN TITLE: Open loop A3 schematic.pdsprj
PATH: D:\Users\Robert Sparrow\Documents\Open loop A3 schematic.pdsprj
BY: @AUTHOR
REV: @REV
DATE: 14/01/2017
PAGE: 1 OF 1
TIME: 18:08:49

C Appendix C: The Impact of Latency on Real-Time Teleoperation over Half-Duplex Dual-Communication Link Experiment Plan

Aim: To analyse how contemporary security construct impact the latency induced on a dual-communication single hop link on real-time teleoperation and telemetry.

Hypothesis: The null hypothesis is that the security constructs will not impact on the communication latency recorded for a real-time teleoperation and telemetry application with half-duplex dual communication links; the alternative hypothesis to this is that the security construct will have an impact on the communication latency recorded for a real-time teleoperation and telemetry application with half-duplex dual communication links.

Assumptions: Ideal communication link between the transmitter and receiver nodes and are one hundred metres in distance apart. The communication medium between the transmitter and receiver is copper cabling. FIFO task scheduler used by microcontrollers.

Method: Measurement based analysis undertaken in the emulated Proteus ISIS 8 emulator that measured the overall latency incurred by the system with the implementation of contemporary cryptographic methods. The measurement based technique selected for this test set a pin high at the beginning of the encryption or decryption process and set the pin low when the operation was complete and send the feedback to the transmitter node; in addition, this test analyses the impact of delay on the operation of an actuator controlled remotely. The duration of the process was analysed through the use of an oscilloscope and a timer counter on the transmitter and receiver microcontroller.

The communication link between the transmitter and receiver was simulated with the Serial Peripheral Interface (SPI) to send data between transmitter and receiver node; this was selected to mimicked an ideal wireless communication channel with synchronous data transmission rate. The simulation of the communication link was achieved through the hexadecimal files uploaded onto the microcontrollers derived from the implementation of the C programme selected to code the SPI communication at specified transmission rate through the application of the SPI divisor; this divided the frequency of oscillation by the SPI divisor to derive the transmission rate for the transmitter and receiver device.

The pulse width modulation was selected to variate the speed of the actuator in the emulation; in this instance, the actuator is a direct current motor. The pulse width modulation is influenced by the potentiometer that is feedback into the transmitter node to calculate

the new set-point value to be transmitted to the receiver and set for the actuator.

Apparatus: The apparatus required for this test is listed in Table C.1. Configuration of the components selected for this test in the Proteus ISIS 8 emulator are specified in Table C.2, C.3 and C.4.

Table C.1: Apparatus required for test procedure

Item	Quantity
Windows 7 Intel Pentium 2.1 GHz processor	1
Proteus ISIS 8 Simulation Package	1
PIC18F45K22 Microcontroller	2
Timer Counters	2
Virtual Oscilloscope	2
Light Emitting Diodes (LED)	5
Logic Counter	8
DC motor	1
Diode	1
BUZ 10 MOSFET	1
10 uf Capacitor	1
100 nf Capacitor	1
100 ohm Potentiometer	1

Table C.2: Configuration of components for no security test

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled	8 MHz
Serial Peripheral Interface (SPI) Configurations	Divisor of 4
Packet Size	36 Bytes 52 Bytes 84 Bytes

Table C.3: Configuration of components with security test

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled	8 MHz
Serial Peripheral Interface (SPI) Configurations	Divisor of 4
Packet Size	36 Bytes 52 Bytes 84 Bytes
AEAD Constructs	CCM-AES-128 TinyAEAD 3 rounds (AES-128) TinyAEAD 5 rounds (AES-128) TinyAEAD 10 rounds (AES-128)

Table C.4: Configuration of components for comparison against mathematical model and simulation test

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled	64 MHz
Serial Peripheral Interface (SPI) Configurations	Divisor of 4
Packet Size	36 Bytes 52 Bytes 84 Bytes
AEAD Constructs	CCM-AES-128 TinyAEAD 3 rounds (AES-128)

Procedure: The procedure was conducted sequentially with the following steps:

1. Configure the SPI settings in the C programme and compile the programme to obtain the hexadecimal file.

2. Set configuration of the crystal frequency used by the microcontrollers and upload the hexadecimal files in the Proteus ISIS 8 emulator by clicking on the device and setting the parameters specified.

3. Begin the emulation of the system.

4. Set/adjust the potentiometer to adjust the reading to the transmitter node; observe if the values on PORTD variates to the change in the potentiometer value.

5. Observe the oscilloscope trace to identify if the packet has been transmitted across the SPI output pin of the transmitter node or the SPI input pin of the receiver node.

6. Check the decryption and message integrity checks are computed correctly through the LED applied on PORTB.
7. View the timer on the transmitter and receiver nodes to obtain the time taken for a message to be encrypted at the transmitter and decrypted at the receiver.
8. Observe if the speed of the motor variates to the change of the potentiometer using the potentiometer to observe the change in the pulse width modulation pin.
9. Record the observed time for the operation to complete.

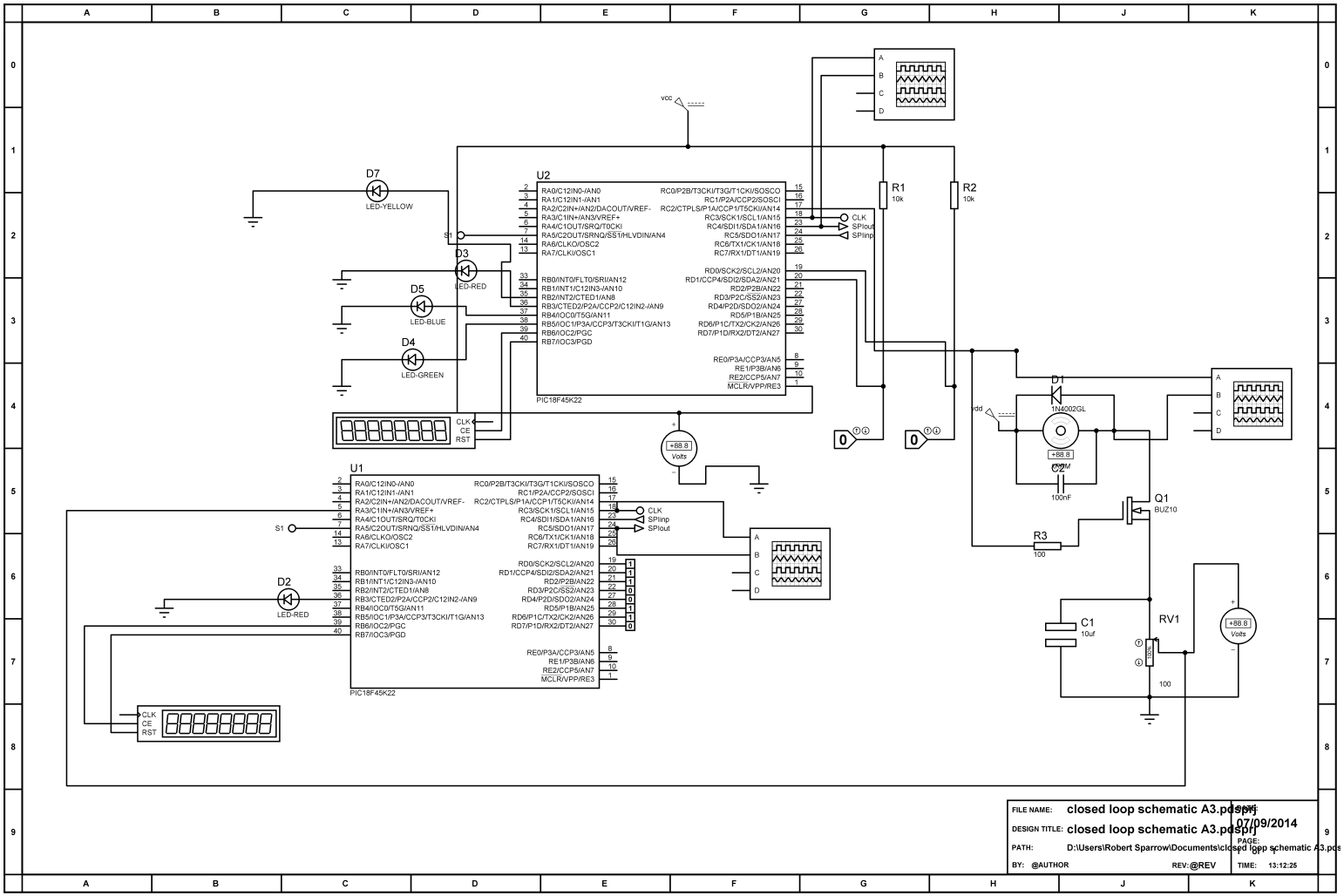
Recorded data for tests

Packet Size	No security (ms)	CCM-AES-128 (ms)	TinyAEAD 10 rounds (ms)	TinyAEAD 5 rounds (ms)	TinyAEAD 3 rounds (ms)
36	180.4	254.2	241.1	211.1	201.5
52	180.7	284.5	273.2	229.8	212.5
84	181.7	345.5	335.6	263	234.1

Recorded data for the comparison of model and simulation test

Packet size	Crystal Frequency (MHz)	No security (ms)	Model TinyAEAD 3 rounds (ms)	Simulation TinyAEAD 3 rounds (ms)	Model CCM-AES-128 (ms)	Simulation CCM-AES-128 (ms)
36	64	22.8	25.9	25.2	32.4	31.8
52	64	23.4	27.1	26.6	36.1	35.6
84	64	24.6	29.9	29.2	43.8	43.3

Schematic


U2
PIC18F45K22
U1
PIC18F45K22
D7
LED-YELLOW
D3
LED-RED
D5
LED-BLUE
D4
LED-GREEN
D2
LED-RED
D1
1N4002GL
R1
10k
R2
10k
R3
100
C1
10uf
C2
100nF
RV1
100
Q1
BUZ10
S1
vcc
CLK
CE
RST
SPIout
SPIinp
Volts
FILE NAME: closed loop schematic A3.pdsprj
DESIGN TITLE: closed loop schematic A3.pdsprj
PATH: D:\Users\Robert Sparrow\Documents\closed loop schematic A3.pds
BY: @AUTHOR
REV: @REV
DATE: 07/09/2014
TIME: 13:12:25

D Appendix D: The Impact of Homogeneous and Heterogeneous Configuration on the Instantaneous Packet Throughput Over a Point to Point Communications Link Experiment Plan

Aim: To analyse how homogeneous and heterogeneous processing and transmission rates impact on on the instantaneous packet throughput recorded for a point to point communication link.

Hypothesis: The null hypothesis is that the heterogeneous configuration of the processing and transmission rate would not have an impact on the number of instantaneous packets recorded by the receiving device in comparison to the homogeneous configuration. The alternative hypothesis is that heterogeneous configuration of the processing and transmission rate would have an impact on the number of packets recorded by the receiver in comparison to the homogeneous configuration.

Assumptions: Ideal communication link between the transmitter and receiver nodes and are one hundred metres in distance apart. The communication medium between the transmitter and receiver is wireless communication operating at 2.4 GHz frequency.

Method: Configuration of the components selected are as follows, a crystal frequency of 2 MHz and 4 MHz was selected to reflect different processing frequencies used in low energy real-time teleoperation and telemetry systems with packet sizes of thirty-six bytes sampled; which is commonly used for low latency real-time teleoperation systems. The Universal Asynchronous Receiver Transmitter (UART) was selected as the serial communication methods between the transmitter and receiver with baud rates of 9,600 and 4,800 symbols per second were selected to reflect different transmission speeds of the communication links. The homogeneous processing and transmission rate test configured each intermediate node with crystal frequency of 4 MHz with a homogeneous transmission baud rate of 9600 symbols per second for the transmission rate. The number of packets recorded was achieved with through measurment based analysis of setting an output pin low to high once the message has been successfully decrypted and passed the integrity and authentication checks.

Apparatus: The apparatus required for this test is listed in Table E.1. Configuration of the components selected for this test in the Proteus ISIS 8 emulator are specified in Table E.2.

Table D.1: Apparatus required for test procedure

Item	Quantity
Windows 7 Intel Pentium 2.1 GHz processor	1
Proteus ISIS 8 Simulation Package	1
PIC18F45K22 Microcontroller	2
Counters	2
Stopwatch (Simulated)	1
Virtual Oscilloscope	1

Table D.2: Configuration of components

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled (One configuration selected for all microcontrollers for homogeneous configuration. Heterogeneous configuration from start node (5 MHz) to end node (1 MHz) configuration setting as listed)	5 MHz 4 MHz 3 MHz 2 MHz 1 MHz
Baud Rate (bps) (One configuration selected for all microcontrollers for homogeneous configuration. Heterogeneous configuration from start node (9600 bps) to end node (110 bps) configuration setting as listed)	9600 2400 1200 600 300 110
Packet Size	36 Bytes

Procedure: The procedure was conducted sequentially with the following steps:

1. Configure the UART settings and the communication method in the C programme and compile the programme to obtain the hexadecimal file.

2. Set configuration of the crystal frequency used by the microcontrollers and upload the hexadecimal files in the Proteus ISIS 8 emulator by clicking on the device and setting the parameters specified.

3. Begin the emulation of the system.

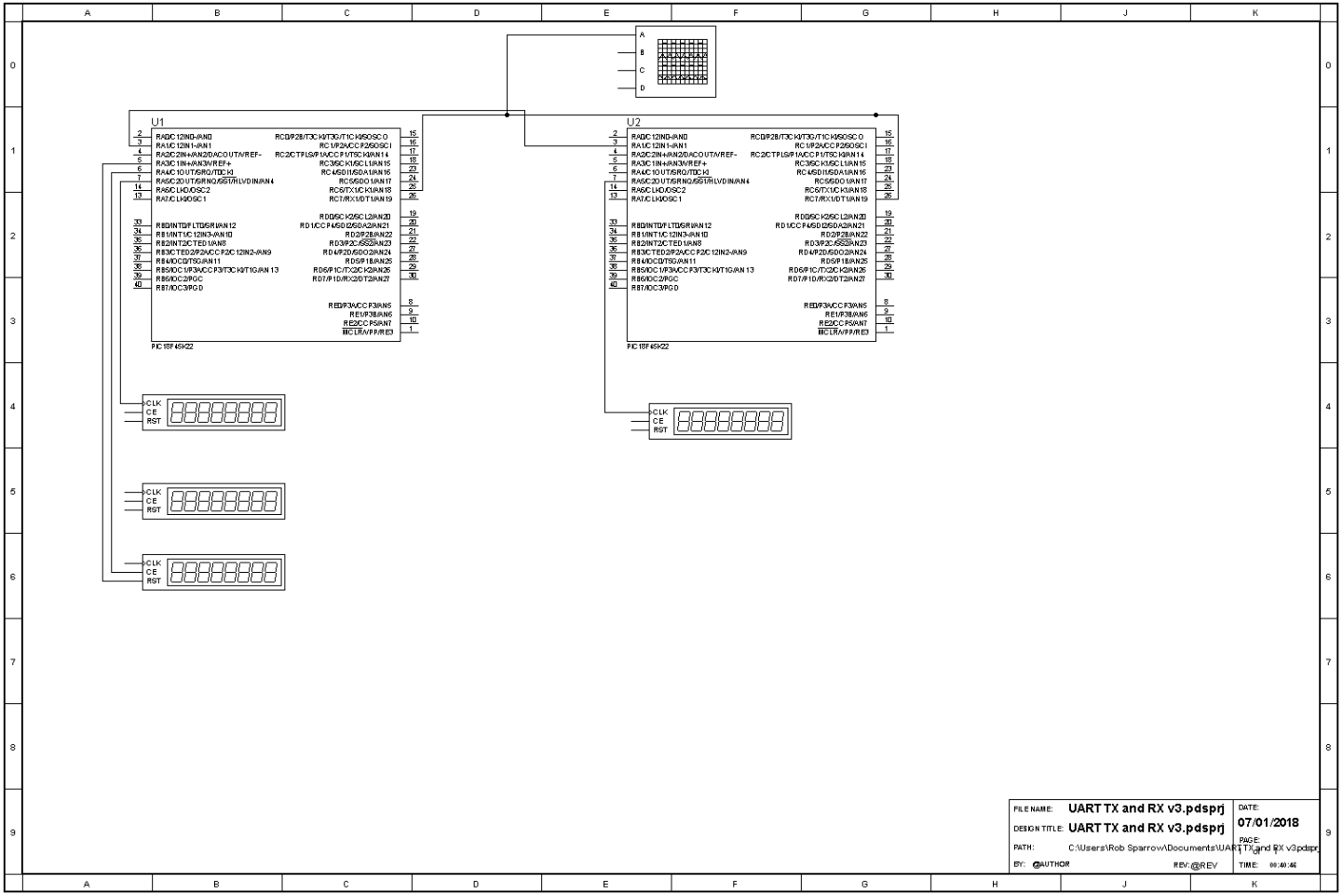
4. Observe the oscilloscope trace to identify if the packet has been transmitted across the SPI output pin of the transmitter node or the SPI input pin of the receiver node.

5. Pause the simulation once the timer has reached sixty seconds.

6. View counter on all nodes to obtain the number of instantaneous packets received in the sixty second time period.

7. Record the measurements.

Schematic


U1
U2
PIC18F45K22
PIC18F45K22
CLK
CE
RST
FILE NAME: UART TX and RX v3.pdsprj
DESIGN TITLE: UART TX and RX v3.pdsprj
PATH: C:\Users\Rob Sparrow\Documents\UART TX and RX v3.pdspr
BY: @AUTHOR
REV: @REV
DATE: 07/01/2018
PAGE:
TIME: 00:40:46

E Appendix E: The Impact of Multiple Hop Propagation with Homogeneous and Heterogeneous Transmission and Processing Rates on Instantaneous Packet Throughput Experiment Plan

Aim: To investigate homogeneous and heterogeneous processing and transmission rates on on the instantaneous packet throughput recorded for multiple hop communication links.

Hypothesis: The null hypothesis presented is that the increased number of nodes on the communication link will not have an impact on the number of instantaneous packets received for homogeneous and heterogeneous configuration methods. The alternative hypothesis is that the increased number of nodes on the communication link will have an impact on the number of instantaneous packets received for homogeneous and heterogeneous configuration methods.

Assumptions: Ideal communication link between the transmitter and receiver nodes and are one hundred metres in distance apart. The communication medium between the transmitter and receiver is wireless communication operating at 2.4 GHz frequency.

Method: Configuration of the components selected are as follows, crystal frequency of 1 MHz, 2 MHz, 3 MHz, 4 MHz and 5 MHz was selected with packet sizes of thirty-six bytes sampled to reflect processing rates and packet sizes used for low-powered real-time teleoperation communications. The Universal Asynchronous Receiver Transmitter (UART) was selected as the serial communication methods between the transmitter and receiver with baud rates of 2,400, 1,200, 600, 300 and 110 symbols per second were selected to reflect different transmission speeds of the heterogeneous communication links.

Two tests were conducted in this section; first, the processing rate of the computational device was examined with the comparison of homogeneous and heterogeneous processing on the instantaneous packet throughput over a multiple-hop communication link. The second test investigated how homogeneous and heterogeneous transmission rates influence the instantaneous throughput recorded over multiple-hop propagation. All timings and instantaneous packet throughput measurements were taken from the simulator used. Metrics used for the experimentation are seconds for the time frame sample. Appendix F illustrates the schematic of the simulated test platform. The homogeneous processing rate test configured each intermediate node with crystal frequency of 5 MHz; the heterogeneous processing rate varied the crystal frequency of each node by 1 MHz (i.e start node 5

MHz, intermediate node one 4 MHz, intermediate node two 3 MHz).

Apparatus: The apparatus required for this test is listed in Table E.1. Configuration of the components selected for this test in the Proteus ISIS 8 emulator are specified in Table E.2.

Table E.1: Apparatus required for test procedure

Item	Quantity
Windows 7 Intel Pentium 2.1 GHz processor	1
Proteus ISIS 8 Simulation Package	1
PIC18F45K22 Microcontroller	2-5
Counters	2-5
Stopwatch (Simulated)	1
Virtual Oscilloscope	5

Table E.2: Configuration of components

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled	5 MHz 4 MHz 3 MHz 2 MHz 1 MHz
Baud Rate	9600 2400 1200 600 300 110
Packet Size	36 Bytes

Procedure: The procedure was conducted sequentially with the following steps:

1. Configure the UART settings and the communication method in the C programme and compile the programme to obtain the hexadecimal file.
2. Set configuration of the crystal frequency used by the microcontrollers and upload the hexadecimal files in the Proteus ISIS 8 emulator by clicking on the device and setting the parameters specified.
3. Begin the emulation of the system.
4. Observe the oscilloscope trace to identify if the packet has been transmitted across the SPI output pin of the transmitter node or the SPI input pin of the receiver node.

5. Pause the simulation once the timer has reached sixty seconds.
6. View counter on all nodes to obtain the number of instantaneous packets received in the sixty second time period.
7. Record the measurements.

Recorded data for the number of instantaneous packets received using synchronous processing rate for a 36 byte packet size tests over a multiple hop link

Hop Number	Processing Frequency (MHz)	Sample Time (Seconds)	Packet Size	Number of Packets
1	5	60	36	512
2	5	60	36	256
3	5	60	36	255
4	5	60	36	254
5	5	60	36	253

Recorded data for the number of instantaneous packets received using asynchronous processing rate for a 36 byte packet size tests over a multiple hop link

Hop Number	Processing Frequency (MHz)	Sample Time (Seconds)	Packet Size	Number of Packets
1	5	60	36	512
2	4	60	36	256
3	3	60	36	147
4	2	60	36	97
5	1	60	36	49

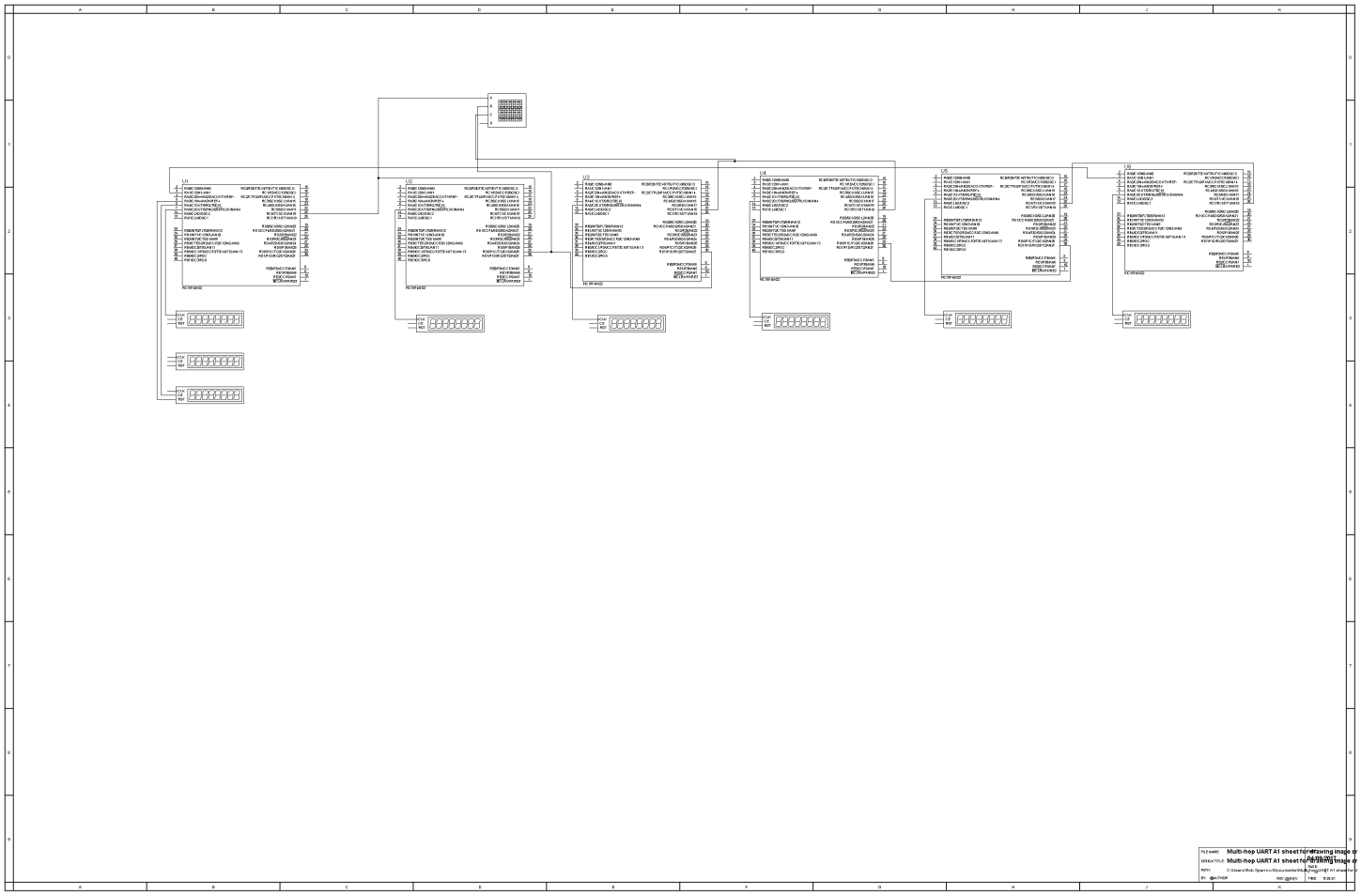
Recorded data for the number of instantaneous packets received using synchronous transmission rate for a 36 byte packet size tests over a multiple hop link

Hop Number	Processing Frequency (MHz)	Sample Time (Seconds)	Packet Size	Baud Rate	Number of Packets
1	4	60	36	9600	410
2	4	60	36	9600	205
3	4	60	36	9600	203
4	4	60	36	9600	202
5	4	60	36	9600	201

Recorded data for the number of instantaneous packets received using asynchronous transmission rate for a 36 byte packet size tests over a multiple hop link

Hop Number	Processing Frequency (MHz)	Sample Time (Seconds)	Packet Size	Baud Rate	Number of Packets
1	4	60	36	9600	410
2	4	60	36	4800	205
3	4	60	36	2400	98
4	4	60	36	1200	55
5	4	60	36	600	19

Schematic



F Appendix F: Analysis of the Multiple Hop Propagation Methods on Real-Time Teleoperation and Telemetry Experiment Plan

Aim: To analyse how contemporary cryptographic construct impact on the instantaneous packet throughput recorded over a multiple hop heterogeneous communication link.

Hypothesis: The null hypothesis presented for this investigation is that the security service selected will not have an impact on the number of instantaneous packets recorded at each intermediate node on the communication link. The alternative hypothesis is that the security service selected will have an impact on the number of instantaneous packets recorded at each intermediate node on the communication link.

Assumptions: Ideal communication link between the transmitter and receiver nodes and are one hundred metres in distance apart. The communication medium between the transmitter and receiver is wireless communication operating at 2.4 GHz frequency.

Method: Measurement based analysis undertaken in the emulated Proteus ISIS 8 emulator that tallied the number of successful instantaneous packets received over a specified period of time; each node records increments a counter each time a message has successfully been decrypted and the message authentication code is correct. The instantaneous packet throughput recorded was taken from a sixty second observation based on simulation time. The transmission of the packets between each node on the network was observed with an oscilloscope.

The communication link between the transmitter and receiver was simulated with the Serial Peripheral Interface (SPI) to send data between transmitter and receiver node; this was selected to mimicked an ideal wireless communication channel with synchronous data transmission rate. The simulation of the communication link was achieved through the hexadecimal files uploaded onto the microcontrollers derived from the implementation of the C programme selected to code the SPI communication at specified transmission rate through the application of the SPI divisor; this divided the frequency of oscillation by the SPI divisor to derive the transmission rate for the transmitter and receiver device.

Apparatus: The apparatus required for this test is listed in Table F.1. Configuration of the components selected for this test in the Proteus ISIS 8 emulator are specified in Table F.2, F.2 and F.4.

Table F.1: Apparatus required for test procedure

Item	Quantity
Windows 7 Intel Pentium 2.1 GHz processor	1
Proteus ISIS 8 Simulation Package	1
PIC18F45K22 Microcontroller	5
Counters	2
Stopwatch (Simulated)	1
Virtual Oscilloscope	5
Light Emitting Diodes (LED)	5

Table F.2: Configuration of components for no security test

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled	4 MHz
Serial Peripheral Interface (SPI) Configurations	Divisor of 16
Transmission Rate (Kbps)	250
Packet Size	36 Bytes 84 Bytes

Table F.3: Configuration of components with security test

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled	4 MHz
Serial Peripheral Interface (SPI) Configurations	Divisor of 16
Transmission Rate (Kbps)	250
Packet Size	36 Bytes 84 Bytes
AEAD Constructs	CCM-AES-128 TinyAEAD 3 rounds (AES-128)

Table F.4: Configuration of components for comparison against mathematical model and simulation test

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled	64 MHz
Serial Peripheral Interface (SPI) Configurations	Divisor of 4
Packet Size	36 Bytes 84 Bytes
AEAD Constructs	CCM-AES-128 TinyAEAD 3 rounds (AES-128)

Procedure: The procedure was conducted sequentially with the following steps:

1. Configure the SPI settings in the C programme and compile the programme to obtain the hexadecimal file.
2. Set configuration of the crystal frequency used by the microcontrollers and upload the hexadecimal files in the Proteus ISIS 8 emulator by clicking on the device and setting the parameters specified.
3. Begin the emulation of the system.
4. Observe the oscilloscope trace to identify if the packet has been transmitted across the SPI output pin of the transmitter node or the SPI input pin of the receiver node.
5. Check the decryption and message integrity checks are computed correctly through the LED applied on PORTB.
6. Pause the simulation once the timer has reached sixty seconds.
7. View counter on all nodes to obtain the number of instantaneous packets received in the sixty second time period.
8. Record the measurements.

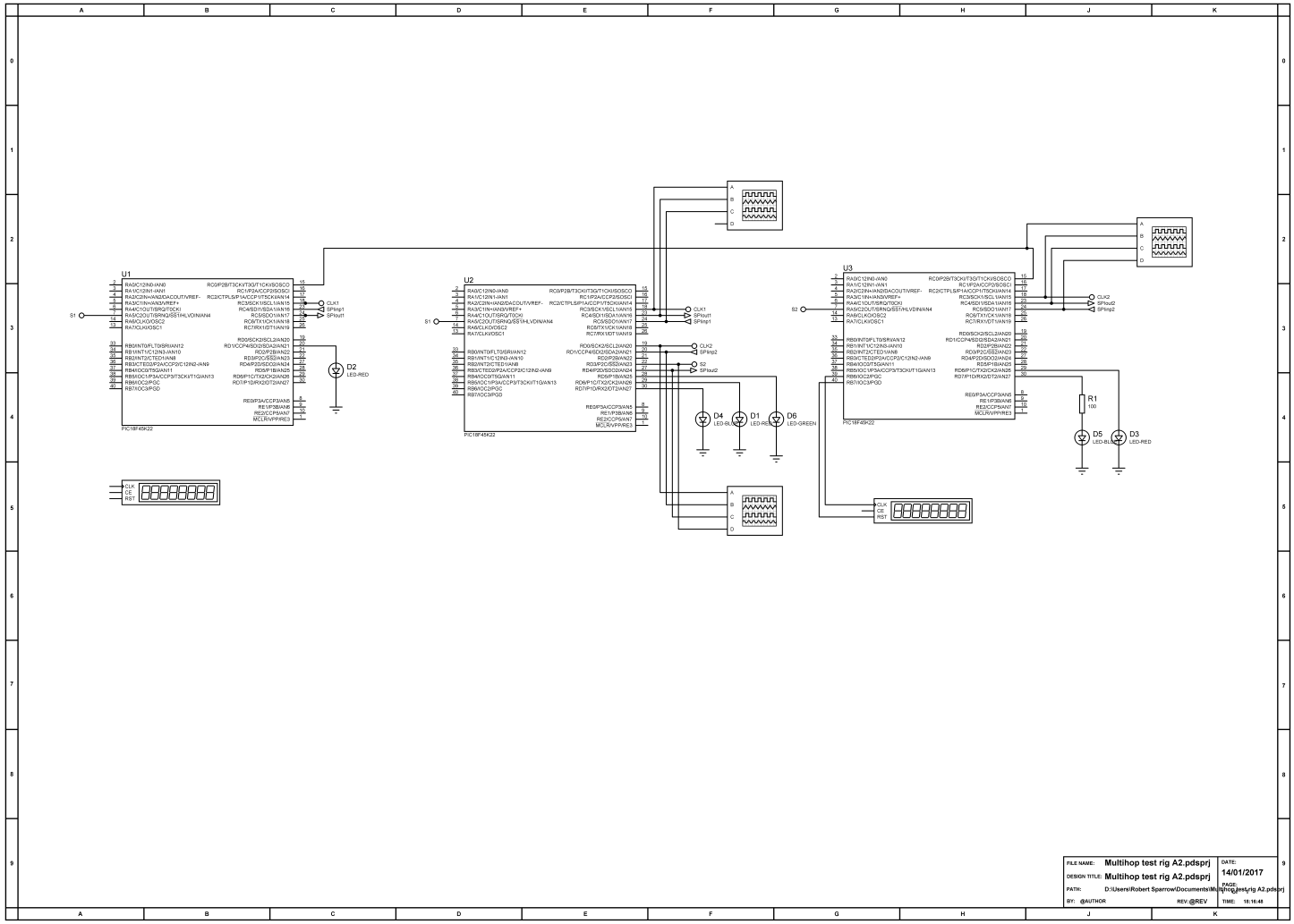
Recorded data for the number of instantaneous packets received using asynchronous processing rate for a 36 byte packet size tests

Number of Hops	No security	TinyAEAD 3 round	TinyAEAD 5 round	TinyAEAD 10 round	CCM-AES-128	No security model	TinyAEAD 3 round model	CCM-AES-128 model
Start Node	100	91	89	67	66	97	91	66
1 hop	49	46	45	36	36	52	47	26
2 hop	32	31	29	25	25	35	33	23
3 hop	25	23	21	19	19	28	27	21
4 hop	20	19	17	15	15	24	24	19
End Node	16	16	16	13	12	22	22	18

Recorded data for the number of instantaneous packets received using asynchronous processing rate for a 84 byte packet size tests

Number of Hops	No security	TinyAEAD 3 round	TinyAEAD 5 round	TinyAEAD 10 round	CCM-AES-128	No security model	TinyAEAD 3 round model	CCM-AES-128 model
Start Node	97	82	57	63	62	97	82	62
1 hop	48	38	33	31	30	52	39	23
2 hop	31	26	22	21	19	35	30	21
3 hop	23	20	15	17	14	28	25	19
4 hop	19	15	14	13	12	24	22	18
End Node	16	13	12	10	10	22	20	17

Schematic


U1
PIC18F45K22
U2
PIC18F45K22
U3
PIC18F45K22
S1
S2
D2
LED-RED
D4
LED-GLOW
D1
LED-RED
D6
LED-GREEN
D5
LED-BLUE
D3
LED-RED
R1
100
CLK1
SPIout1
SPIin1
CLK2
SPIout2
SPIin2
FILE NAME: Multihop test rig A2.pdsprj
DESIGN TITLE: Multihop test rig A2.pdsprj
PATH: D:\Users\Robert Sparrow\Documents\Multihop test\rig A2.pdsprj
BY: @AUTHOR
REV:@REV
DATE: 14/01/2017
PAGE:
TIME: 16:16:48

G Appendix G: An Instance of Performance Requirements of Each Individual Task of The Static to Mobile and Mobile to Static Real-Time System Problem Scenarios

Task ID	Task	Category	Trigger Event Task ID	Response Task ID	Maximum Deadline Estimate
1	Initialise System	Process	-	2	500 μs
2	Human Adjusts Control of UAV	Input	1	3	2 ms
3	Transmission of Teleoperation Data Packet	Process	2	4	30 μs
4	Computation of Received Teleoperation Data Packet	Process	3	5	2 ms
5	Adjust Actuators in Response to Teleoperation Data Packet	Output	4	6	5 ms
6	Captures Sensed Data	Input	1	7	50 ms
7	Packetised Sensed Data	Process	7	8	25 ms
8	Transmit Telemetry Data	Process	8	9	30 μs
9	Process Telemetry Data	Process	9	10	25 ms
10	Displays Acquired Telemetry Data	Output	10	6	12 ms
Worst Case Execution Time					121 ms

H Appendix H: The Impact of a Secure Communication Link on the Operational Performance of a Semi-Autonomous Mobile End-Point Experiment Plan

Aim: To analyse the impact of secure communication on the operational performance of a semi-autonomous mobile end-point

Hypothesis: The null hypothesis presented is that the secure communication link would not have the same impact on the responsiveness between the command sent and the action undertaken based on the command sent to the mobile ground vehicle. The alternative hypothesis is that the secure communication link will have the same impact on the responsiveness between the command sent and the action undertaken based on the command sent to the mobile ground vehicle.

Assumptions: None stated

Method: The test platform selected for this experiment was a simulated environment with the robot simulator software selected Papini (2016). The operation of the robot in this scenario was an autonomous mobile ground vehicle that followed a series of commands to drive from the start position to the exit point in a maze. Input delays of twenty-one milliseconds and one hundred and ninety milliseconds and seven hundred milliseconds was implemented into the semi-autonomous script to reflect the additional delay incurred from the autonomous vehicle to process TinyAEAD-AES-128 at three rounds, CCM-AES-128 and GCM-AES-128 per task conducted in the pre-computed script used by the semi-autonomous mobile end-point. The same start position is initiated for each test with the delay of the AEAD constructs applied per command initiated from the command script used for all tests.

Measurement recorded of the path taken by the semi-autonomous ground vehicle and the time required to complete the task. The start and exit positions for the robot to exit the maze were the same for all tests conducted. All timings were taken from a real-world clock.

Manoeuvres Examined: The manoeuvres performed in this test examined the time required for a mobile ground vehicle to follow a pre-determined script to navigate out of a maze; however, at each command, the delay of the security service is applied to reflect the latency incurred from a secured communication link with different AEAD constructs selected. The trace of the unmanned ground vehicle is recorded to ascertain how the delay

impacts on the operation performance of the semi-autonomous vehicle.

Apparatus: The apparatus required for this test is listed in Table H.1. Configuration of the components selected for this test in the robot simulator are specified in Table H.2

Table H.1: Apparatus required for test procedure

Item	Quantity
Windows 7 Intel Pentium 2.1 GHz processor	1
Robot Simulator	1
Robot	1
Maze	1
Stopwatch	1
Autonomous script	1

Table H.2: Configuration of components

Item	Configuration
Security Constructs	TinyAEAD 3 rounds (AES-128) CCM-AES-128
Delays (Per task complete)	21 millisecond (TinyAEAD) 74 milliseconds (CCM-AES-128)

Test Procedure: The procedure was conducted sequentially with the following steps:

1. Start the robot simulator and select the maze example from the per-selected list.
2. Set the delays of the security service for each command imitated on the default per-configured autonomous script that the robot will follow.
3. Start the robot simulation and the real-world stopwatch.
4. Observe the automated process; pause the stopwatch once the semi-autonomus vehicle has left the maze.
5. Record the observed time for the operation to complete.

I Appendix I: The Impact of Non-Ideal Channel Characteristics on Instantaneous Packet Throughput Experiment Plan

Aim: To analyse how non-ideal communication links impact on the message during propagation across the communication link.

Hypothesis: The null hypothesis proposed in this analysis is that the non-ideal channel characteristics will not reduce the number of packets received by the receiver over the same sample time analysed in comparison to the number of packets recorded under ideal channel conditions. The alternative hypothesis is that the non-ideal channel characteristics will reduce the number of packets received by the receiver over the same sample time analysed in comparison to the number of packets recorded under ideal channel conditions.

Assumptions: The transmitter and receiver nodes and are one hundred metres in distance apart. The communication medium between the transmitter and receiver is wireless communication operating at 2.4 GHz frequency. FIFO task scheduler used by microcontrollers.

Method: Measurement based analysis undertaken in the emulated Proteus ISIS 8 emulator that tallied the number of successful instantaneous packets received over a specified period of time; each node records increments a counter each time a message has successfully been decrypted and the message authentication code is correct. The instantaneous packet throughput recorded was taken from a sixty second observation based on simulation time. The transmission of the packets between each node on the network was observed with an oscilloscope.

The communication link between the transmitter and receiver was simulated with the Serial Peripheral Interface (SPI) to send data between transmitter and receiver node; this was selected to mimicked an ideal wireless communication channel with synchronous data transmission rate. The simulation of the communication link was achieved through the hexadecimal files uploaded onto the microcontrollers derived from the implementation of the C programme selected to code the SPI communication at specified transmission rate through the application of the SPI divisor; this divided the frequency of oscillation by the SPI divisor to derive the transmission rate for the transmitter and receiver device.

An intermediate microcontroller was placed between the transmitter and receiver to intercept the message and mimic the impact of a non-ideal communication link to the message.

The interference level was analysed as the non-ideal channel characteristic as it is known that interference contributes towards packet corruption and error as it propagates over the communication medium. The non-ideal channel characteristics of the communication link were derived from a binomial distribution with value of thirty-four per cent, fourteen per cent and two per cent. A random number generator was selected to generate a random number within a byte value of 0 to 255; if the number was within or under the percentage value set for the non-ideal communication link, the packet was modified to reflect packet corruption; otherwise the message was unaffected.

The second variable analysed was jitter; similar to the packet corruption test, the same probability percentages are chosen; however, this test varies the inter-arrival time of the message by delaying the packet at the intermediate hop before propagating to the receiver device. The initial delay sampled in this test was seven milliseconds for thirty-four per cent probability, nine milliseconds for fourteen per cent probability and ten milliseconds for two per cent probability.

Apparatus: The apparatus required for this test is listed in Table I.1. Configuration of the components selected for this test in the Proteus ISIS 8 emulator are specified in Table I.2.

Table I.1: Apparatus required for test procedure

Item	Quantity
Windows 7 Intel Pentium 2.1 GHz processor	1
Proteus ISIS 8 Simulation Package	1
PIC18F45K22 Microcontroller	3
Counters	1
Stopwatch (Simulated)	1
Virtual Oscilloscope	1

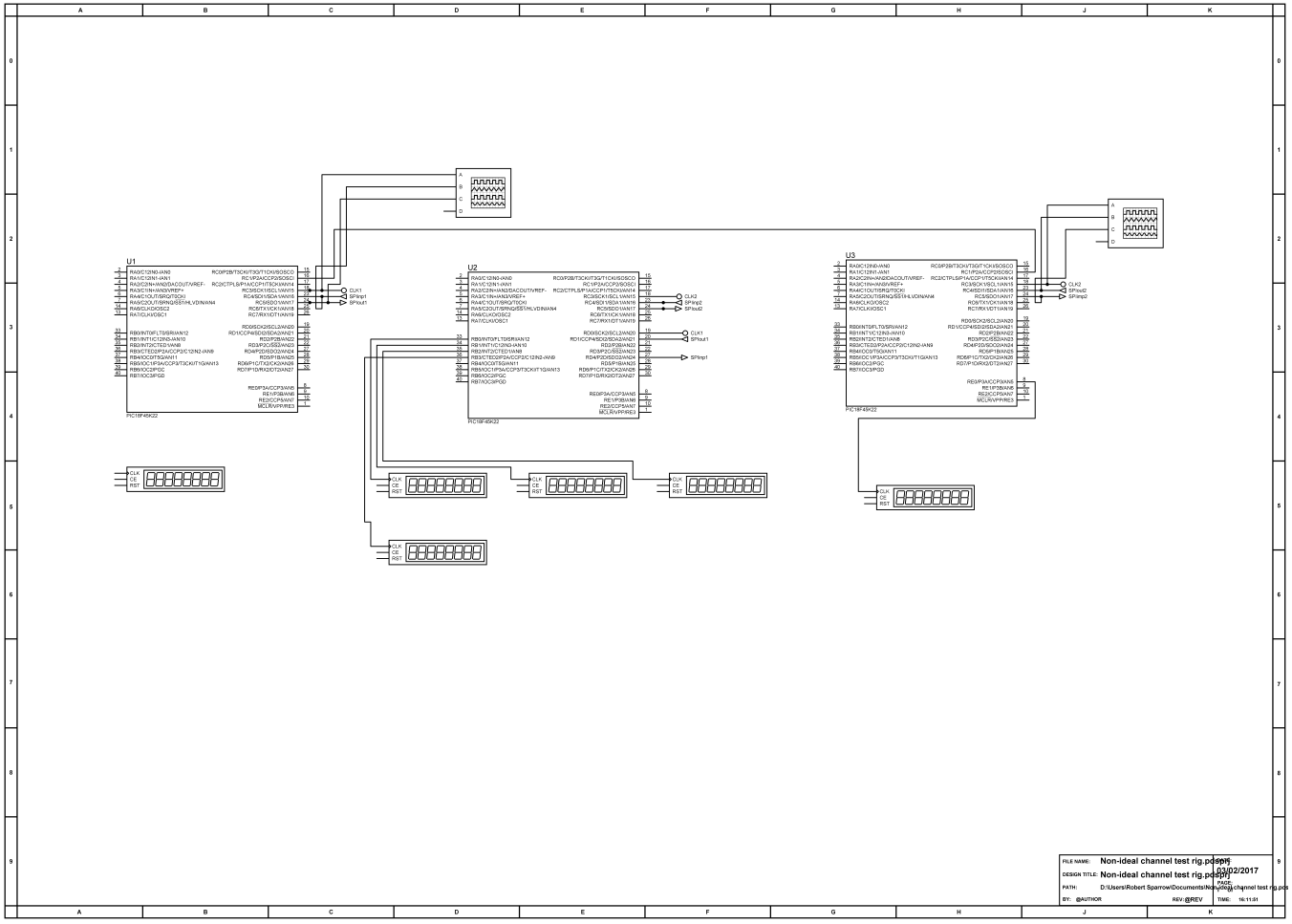
Table I.2: Configuration of components

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled	4 MHz
Serial Peripheral Interface (SPI) Configuration	Divisor of 4
Transmission rate (Kbps)	250
Packet Size	36 Bytes

Procedure: The procedure was conducted sequentially with the following steps:

1. Configure the SPI settings and the communication method in the C programme and compile the programme to obtain the hexadecimal file.
2. Set configuration of the crystal frequency used by the microcontrollers and upload the hexadecimal files in the Proteus ISIS 8 emulator by clicking on the device and setting the parameters specified.
3. Begin the emulation of the system.
4. Observe the oscilloscope trace to identify if the packet has been transmitted across the SPI output pin of the transmitter node or the SPI input pin of the receiver node.
5. Pause the simulation once the timer has reached sixty seconds.
6. View counter on all nodes to obtain the number of instantaneous packets received in the sixty second time period.
7. Record the measurements.

Schematic


U1
PIC18F46K22
U2
PIC18F46K22
U3
PIC18F46K22
CLK1
SPIout1
SPIinp1
CLK2
SPIout2
SPIimp2
FILE NAME: Non-ideal channel test rig.pcspr
DESIGN TITLE: Non-ideal channel test rig.pcspr
PATH: D:\Users\Robert Sparrow\Documents\Non-ideal channel test rig.pcs
BY: @AUTHOR
REV: @REV
DATE: 03/02/2017
PAGE: 1 OF 1
TIME: 16:11:01

J Appendix J: Real-World Validation of The Maximum Communication Range for Real-Time Teleoperation and Telemetry Communications at Various Antenna Placements and Sensitivities Experiment Test Plan

Aim: To analyse the impact of the transmission power used to broadcast the wireless communication medium to the receiver device and what variables influence the maximum broadcast range and operational use of real-time teleoperation and telemetry

Hypothesis 1: The null hypothesis presented in this investigation is that the higher the vertical placement of the antenna; the further the communication range between the transmitter and receiver would be. The alternative hypothesis is that higher the vertical placement of the antenna; the closer the communication range between the transmitter and receiver would be.

Hypothesis 2: The null hypothesis presented in this test is that the omni-directional antenna with gain will not have an increased communication range than the omni-directional antenna with no gain. The alternative hypothesis is that the omni-directional antenna with gain will have an increased communication range than the omni-directional antenna with no gain.

Assumptions: It is assumed for this analysis that line of sight communication links are selected to conduct communication between the transmitter and receiver and the free space model is applicable for the analysis of the communication link as the operational height of a UAV and the CAA regulations would prevent the device being piloted in areas that may obstruct the wireless signal.

Method: The maximum broadcast range of the wireless communication medium was analysed through mathematical modelling with the the free space path loss calculation to derive the loss of signal strength through free space with no obstacles to cause refraction of deflection; this model was selected because the emphasis of this analysis was to identify the maximum theoretical communication range of a 2.4 GHz wireless broadcast range at various transmission powers under ideal communication channel conditions as a benchmark analysis. Selection of the free-space path loss for this analysis was chosen in order to ascertain the maximum theoretical distance of a communication signal to a mobile UAV over a point to point communication link with minimal interference and objects obstructing the communication signal as the mobile UAV would be operational in scenarios outside of urban areas in order to comply with the CAA regulations.

The link budget calculation was selected to factor the gains and losses of the communication link; this includes the transmission power, receiver sensitivity, antenna gain and the free space loss of the system. The link budget calculation was selected for this analysis to derive a holistic viewpoint of the theoretical transmission power required to propagate the signal to the receiver device with the consideration of antenna gain and free space path loss; this model quantifies signal gain and loss as it propagates across the communication link; therefore, the modelled answers give an indication of how antenna gains contribute towards the required transmission power to propagate the signal over a given distance; this is important in the context of real-time teleoperation and telemetry as the reduction in the transmission power and antenna gain could prolong the operational lifetime of the system and increase the maximum distance for communications.

Validation of the mathematical model was conducted in a real-world environment. The test platform was created with a Raspberry Pi configured as the transmitter device and a Linux 2.4 GHz Ubuntu laptop as the receiver device. The TP-Link TL-WN722N 3 dBi omni-directional high gain antenna dongles was selected for line of sight communication; the IEEE standard 802.11g was chosen as the communication protocol. The frequency selected for the communication channel was 2.4 GHz to replicate conventional short range wireless communication systems. One Raspberry Pi is configured as an wireless access point and the other Raspberry Pi is a client that associated with the wireless access point in order to transfer messages over the same communication link. Vertical placement of the antenna was set at zero metres, one metre, and two metres above ground. One hundred ping commands were sent from the transmitter and receiver; the average of five tests was taken for the results. The packet size selected for the ping test was fifty-six bytes. The percentage of successfully ping command between the transmitter and receiver was recorded.

The height of the antenna placements were sets to one metre above the ground with a transmission power of 0 dBm was sampled. Intervals of ten metres in distance was sampled over a total distance of one hundred and twenty metres. The received signal level of the transmission link was recorded with the wavemon software package in Linux.

Apparatus: The apparatus required for this test is listed in Table J.1. Configuration of the components selected for this test in the Proteus ISIS 8 emulator are specified in Table J.2

Table J.1: Apparatus required for test procedure

Item	Quantity
Linux 2.4 GHz Inter I7 processor with Ubuntu operating system	1
Raspberry Pi 2 Model B	2
TP-Link TL-WN722N 3 dBi omni-directional high gain antenna dongles	2
Wi-Pi 0 dBi omni-directional antenna dongles	2
Ladders (2 metres height)	2
Battery Packs	2
Wavemon software	1

Table J.2: Configuration of components

Item	Configuration
Raspberry Pi 2 Model B Processing Frequency	1 GHz
Transmission Power	0 dBm
Packet Size	56 Bytes
Antenna Sensitivity	3 dBi 0 dBi
Antenna Configuration	Directional Omni-directional
Antenna Placement Above Ground	0.1 metre 1 metre 2 metre
Communication Protocol	802.11g
Communication Frequency	2.412 GHz (Channel 1)

Procedure: The procedure was conducted sequentially with the following steps:

1. Configure the Raspberry Pi and initiate association of the client device with the access point device.
2. Initiate a ping command to check the connection is established and communications is initiated.
3. Measure a ten metre waypoints between the access point and the client device.
4. Place the client device at the waypoint measured in step 3.
5. Remote access into the client device using secure shell protocol (SSH) and set the ping command to initiate 100 times.

6. Execute the command.

7. Once the one hundred ping messages have been complete, record the ping statistics generated

8. Repeat the process until the connectivity is lost and record the maximum distance obtained.

9. Reconfigure the vertical placement of the antenna position and/or the transmission power and/or the antenna configuration of the communication devices and repeat the test until all variations are complete.

Recorded data for the percentage of successful packet deliveries at various vertical antenna heights at a 0 dBm transmission power

Independent Variable	Dependent Variables		
Distance (Metres)	0.1 Metre Packet Received	1 Metre Packet Received	2 Metre Packet Received
10	100	99	99
20	95	99	99
30	85	99	99
40	75	99	99
50	59	99	99
60	0	99	99
70	0	94	99
80	0	93	99
90	0	91	99
100	0	89	99
110	0	87	99
120	0	86	99
130	0	84	99
140	0	83	99
150	0	82	99
160	0	67	99
170	0	0	99
180	0	0	97
190	0	0	90
200	0	0	90
210	0	0	86
220	0	0	86
230	0	0	86
240	0	0	86
250	0	0	84
260	0	0	84
270	0	0	84
280	0	0	84

Recorded data for Directional versus Omni-Directional antenna range test

Independent Variable	Dependent Variables	
Distance (Metres)	Omni-Directional Antenna Signal Level	Directional Antenna Signal Level
10	-58	-41
20	-58	-41
30	-59	-42
40	-60	-42
50	-61	-44
60	-63	-46
70	-63	-45
80	-63	-45
90	-61	-45
100	-61	-46
110	-62	-48
120	-60	-49

K Appendix K: Energy Usage of The Communication Components Experiment Plan

Aim: To profile the energy cost of processing and the cost of communication for real-time teleoperaiton and telemetry.

Hypothesis: The null hypothesis presented is that the power consumption for the processing of data is greater than the power consumption for the communication of data. The alternative hypothesis is that the power consumption for the communication of data is greater than the power consumption for the processing of data.

Assumptions: None stated.

Method: The test platform selected for the test was a real-world PIC18F45K22 microcontroller with a Microchip MRF24WB0MA wireless 802.11g transceiver as the wireless module selected. Packet size of five hundred bytes was sampled to reflect the 802.11 Wi-Fi packet structure. Crystal frequencies of 1 MHz, 4 MHz, 8 MHz and 16 MHz were sampled. The crystal frequencies sampled were multiplied by the phase lock loop (PLL) to multiply the initial crystal frequency sampled by four. Current draw of the components was measured in milliamps and converted to power in milliwatts (mW).
Apparatus: .

Table K.1: Apparatus required for test procedure

Item	Quantity
Windows 7 Laptop with Intel Pentium 2.1 GHz processor	1
Wireless Access Point	1
Mikroelectronica PIC C Compiler	1
PIC18F45K22	1
Microchip MRF24WB0MA wireless 802.11g transceiver	1
Multimeter	1

Table K.2: Configuration of components for no security test

Item	Configuration
PIC18F45K22 Microcontrollers Crystal Frequency Sampled (MHz)	1, 4, 8 ,16
Phase Lock Loop	Yes (x4 Multiplier)
Packet Size	500 Bytes
Sampled units	Milliamps (Current) Milliwatts (Power)
Communication Protocol	802.11

Procedure: The procedure was conducted sequentially with the following steps:

1. Assemble the components to recreate the schematic presented in this Appendix.
2. Compile the C programme in the Mikroelektronika IDE.
3. Copy the compiled C programme (hexadecimal file) to the target microcontroller.
4. Reset microcontroller on the target board
5. Synchronise the microcontroller to the access point
6. Upload telemetry data from the microcontroller to the Access Point which is displayed on a telemetry webpage interface.
7. Measure the current draw from the microcontroller.
8. Record the observed measurement.
9. Repeat steps 1-8 and measure the current draw of the transceiver used for communication between the microcontroller and access point.

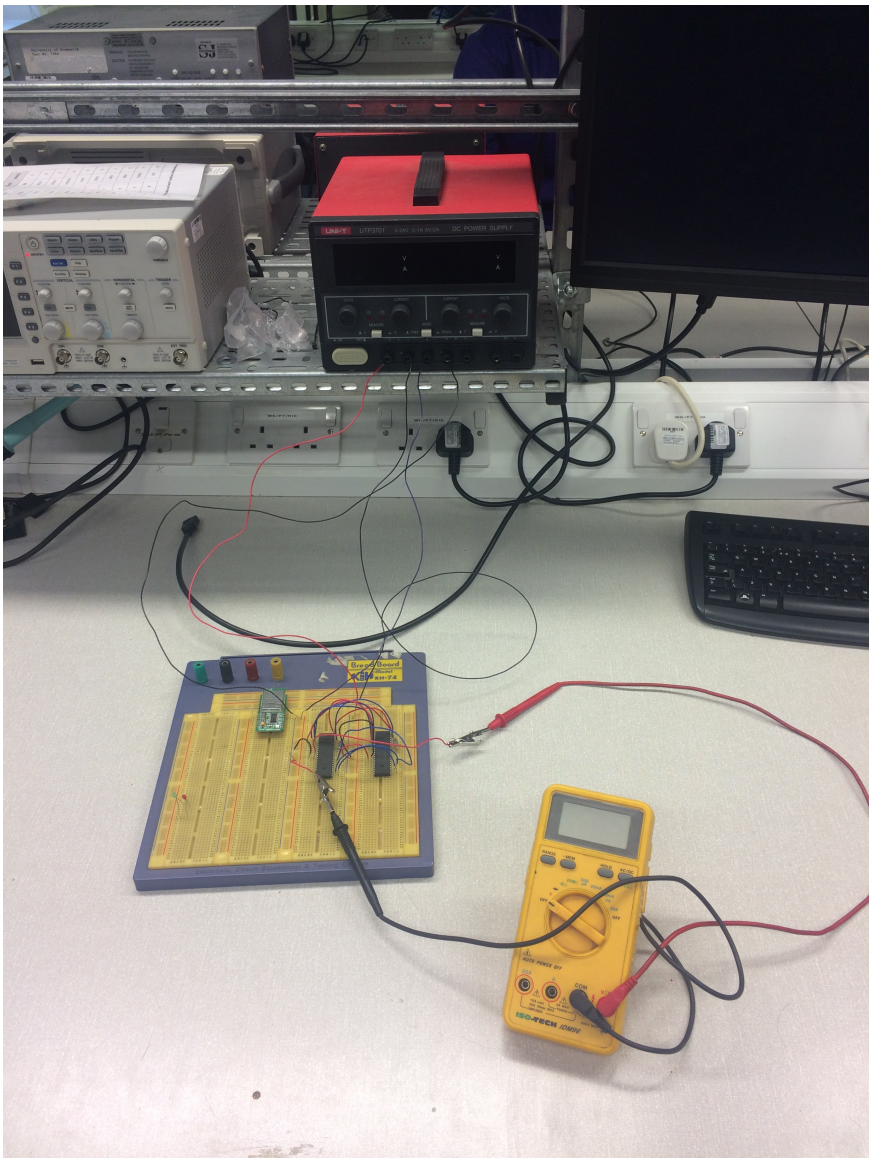
Recorded data for idle communication tests

Independent Variable	Dependent Variables	
Crystal Frequency (MHz)	**Microcontroller Power Consumption (mW)**	**Communication Power Consumption (mW)**
1	0.1	5.4
4	0.2	5.4
8	0.4	5.7
16	0.6	6.0
20	0.8	6.1

Recorded data continuous communication tests

Independent Variable	Dependent Variables	
Component	**Mean (mW)**	**Standard Deviation**
Microcontroller	0.40	0.27
Transceiver	5.68	0.32

Visual Schematic



L Appendix L: The Impact of Secure Communication Links on the Operational Performance of a Manual Controlled Mobile End-Point Experiment Plan

Aim: To analyse the impact of secure communication on the operational performance of a manual controlled mobile end-point.

Hypothesis: The null hypothesis presented in this investigation is that the application of secure communication links will not have an impact on the operational performance characteristics of a mobile end-point. The alternative hypothesis is that the application of secure communication links will have an impact on the operational performance characteristics of a mobile end-point.

Assumptions: None sated.

Method: The test platform selected for this experiment was a computer simulator called FlightGear with the fixed wing Piper J3 cub selected as the aircraft. The user interface chosen for this test was a generic two axis joystick to control the operation of the simulation aircraft; an Arduino Uno development board with an ATMega328p microcontroller to read the analogue input from the joystick through the analogue to digital converter and pass the reading to the simulation software over the USB interface. A 16 MHz crystal frequency was selected as the processing frequency of the Arduino microcontroller.

The speed of the plane at full throttle was eighty miles per hour (thirty-six metres per second). TinyAEAD at three rounds and CCM were selected as the security construct for this test with the AES-128 selected as the block cipher used by the AEAD constructs. Delays of fifteen milliseconds and thirty-five milliseconds were selected to simulate the time required by TinyAEAD at three rounds and CCM to process a forty-eight byte payload message on the ATMega328p microcontrolloer. Ground altitude above sea level was four hundred feet (one hundred and twenty two metres) . Flight heights of the UAV was set to five hundred and sixty four feet (fifty metres), seven hundred and twenty-eight feet (one hundred metres) above ground altitude was selected to reflect the constraints of the operating range set by the CAA regulations.

Measurements recorded for this test focused on the response of the mobile end-point to complete the task through the additional distance travelled by the mobile device. Sample time of the measurements recorded by the data loggers in the simulation was five millisecond intervals. All measurements were recorded based on the simulation clock time.

Manovers Examined: The manovers performed in this test examined the ascent and decent of the UAV from the specified heights. The decent from the fixed heights was held for a five second time period before the auto-pilot was initiated to restore the UAV to its original flight height for the test conducted. Alternative man overs examined in this simulation is the roll of the UAV from a 360 degree axis whilst performing a horizontal turn and the heading of the UAV to determine the direction that the mobile end-point is facing during the horizontal turn. All altenative manovers were held for five second and manually controlled to the original start position.

Apparatus: The apparatus required for this test is listed in Table L.1. Configuration of the components selected for this test in the FlightGear simulator are specified in Table L.2

Table L.1: Apparatus required for test procedure

Item	Quantity
Windows 7 Intel Pentium 2.1 GHz processor	1
Arduino Uno (ATMega328p microcontroller)	1
Joystick	1
16 MHz Crystal Oscillator	1
FlightGear Simulator	1
Piper J3 Cub (Plane Chosen in FlightGear Simulator)	1
Data Logger (in FlightGear Simulator)	1
Stopwatch (in FlightGear Simulator)	1

Table L.2: Configuration of components

Item	Configuration
Arduino Uno (ATMega328p)	16 MHz
Hardware Communication Method	Universal Serial Bus
Packet Size	36 Bytes 52 Bytes 84 Bytes
AEAD Constructs	TinyAEAD 3 rounds (AES-128) (15 millisecond delay) CCM-AES-128 (35 millisecond delay)
Fixed Speed of the UAV	36 Metres per second
Joystick Configuration	x4 Analogue to Digital Converter Pins up, down, left and right direction.

Test Procedure: The procedure was conducted sequentially with the following steps:

1. Assemble the test apparatus to reflect the test schematic represented.
2. Programme the Arduino Uno board with the associated time delays to reflect the delay incurred by TinyAEAD configured with AES-128 at three rounds and standardised CCM-AES-128.
3. Open FlightGear Simulator and start a new flight session with the Piper J3 Cub selected as the aircraft.
4. Begin the flight simulation.
5. Configure the auto-pilot to reach the specified altitude for the test conducted and await for the aircraft to ascend to the specified height.
6. Once the aircraft has reached the specified altitude; set the data logger to record the flight data and assume manual control of the aircraft.
7. Perform the specified manouver for five seconds using the software stopwatch to record the time duration.
8. Initiate the auto-pilot to restore the aircraft to its original start position.
9. Record the observed time for the operation to complete.

M Appendix M: The Relationship Between the Vertical Height of the Mobile Device and the Number of Picture Samples

Aim: To to ascertain the coverage area of the image taken by an optical camera at various horizontal heights; the resolutions obtained from the image capture and the file size of the telemetry file

Hypothesis: The null hypothesis proposed in this investigation is that the higher the vertical placement of the optical camera; the greater the coverage area is at the cost of a reduced resolution of the picture details (i.e. buildings, scenery, people, etcetera). The alternative hypothesis is that the higher the vertical placement of the optical camera; the greater the coverage with no cost in resolution of the picture detail.

Assumptions: It is assumed that the aspect ratio of the models are scaled correctly to manufactures specifications.

Method: The test investigated the picture quality obtained from the two cameras at varying specified heights specified to determine how the vertical height of the mobile platforms influences the picture quality. Two cameras were selected for this test, the Raspberry Pi colour (RGB) camera and the Raspberry Pi infra-red (IR) camera; both cameras had a picture quality of five megapixels and a viewing angle of sixty degrees and image resolution of 2,592×1,944 pixels. The model scene selected was a 1:148 ratio with three heights scaled to reflect a mobile real-time application flying at heights of eighty metres, one hundred metres and one hundred and twenty metres. No post processing was undertaken on the pictures. No compression techniques were used for the image file. The apparatus required for this test is listed in Table M.1. Configuration of the components selected for this test are specified in Table M.2

Table M.1: Apparatus required for test procedure

Item	Quantity
Raspberry Pi	1
5 Megapixel RGB Camera	1
5 Megapixel IR Camera	1
Variable Stand	1

Table M.2: Configuration of components

Item	Configuration
Raspberry Pi Processing Frequency	1 GHz
Aperture Angle of Cameras	60 Degrees
Ratio of Model Scene	1:148
Image Resolution	2,592×1,944 pixels
Vertical Heights Sampled (In reference to Ratio of Model Scene)	80 Metres 100 Metres 120 Metres

Procedure: The procedure was conducted sequentially with the following steps:

1. Create the model scene and present it for the experiment.
2. Calibrate the height of the vertical stand in reference to the aspect ratio of the models selected.
3. Configure the Raspberry Pi with the RGB or IR camera.
4. Place camera lens in a horizontal position, facing the model scene created on the vertical stand.
5. Take picture.
6. Repeat steps 1-5 with alternative camera selection or at different vertical height until all data samples are colelcted.
7. Analyse results.

N Appendix N: Performance Metrics of the Cipher-Text Output of the AES-128 block cipher Experiment Plan

Aim: To profile the performance metrics of the AES-128 block cipher.

Hypothesis: The AES-128 standardised block cipher performance metrics increased as the number of rounds selected increases. The AES-128 block cipher is resilient against a strict avalanche criterion test.

Assumptions: A message size of 256 bytes is selected to reflect the maximum packet size for a MAVlink communication protocol for real-time teleoperation and telemetry.

Method: The application of the strict avalanche test method was selected to analyse the change in the known plain-text input and cipher-text output of the block ciphers investigated; this is to determine if there is any correlation that a change in a particular bit position of the known plain-text is more or less than a fifty percent change in the cipher-text output. The test changed one byte of a zero payload message, encrypted the message through AES-128 block cipher and stored the output into a text file. The byte positions are reset back to their default set values before the next byte position is changed; therefore, a change of one byte position at a time that propagates throughout the payload.

Measurements methods selected for this test was the entropy to measure the uncertainty in the cipher-text output; arithmetic mean of the weighting of zero and ones in the binary cipher-text output and the serial correlation to measure if there is a correlated trend in the cipher-text outputs. All cipher-text outputs were recorded into a text file and analysed with the entropy number tester.
Apparatus: .

Table N.1: Apparatus required for test procedure

Item	Quantity
Windows 7 Intel Pentium 2.1 GHz processor	1
Microsoft Visual Studio 2010 edition	1
Entropy Number Tester	1

Table N.2: AES-Configuration

Item	Configuration
Block Size (Bits)	128
Number of Rounds Sampled	1-10
Message Input	256 Bytes
Plain-Text input	All zero (except for the index value that is flipped under the strict avalanche criterion, which has a byte value of all ones).
Key Value	All zeros
Mode of Operation	Electronic Code Book (ECB)

Procedure: The procedure was conducted sequentially with the following steps:

1. Configure the block cipher parameters as specified in the apparatus configuration
2. Set the number of iterations (rounds) for the AES-128 block cipher
3. Compile the C programme
4. Execute C programme
5. Locate text file with cipher-text output
6. Copy the cipher-text file into the entropy number test file path location
7. Execute the entropy number tester programme to analyse the cipher-text output collated in the text file
8. Record the observed measurement.
9. Repeat steps 1-8 for the specified number of rounds analysed.

Recorded data for strict avalanche test

Independent Variable	Dependent Variables		
Number of Rounds	Entropy (bits)	Arithmetic Mean (bits)	Serial Correlation
1	1.3	14.3	-0.14
2	4.0	144.0	0.06
3	7.1	124.9	0.05
4	7.1	123.3	0.03
5	7.3	133.1	0.02
6	7.2	129.0	0.09
7	7.1	119.9	0.03
8	7.2	126.6	-0.02
9	7.1	131.2	0.00
10	7.1	123.9	-0.02

O Appendix O: Linear Approximation Bias Table of the Substitution-Box

		Input Mask															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Output Mask	**0**	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	25	0	37.5	37.5	37.5	62.5	62.5	62.5	37.5	62.5	0	0	0	25
	2	0	0	37.5	62.5	62.5	62.5	0	75	0	0	62.5	37.5	62.5	62.5	25	0
	3	0	0	37.5	37.5	75	25	37.5	37.5	37.5	37.5	0	0	62.5	62.5	0	0
	4	0	62.5	0	37.5	0	37.5	0	62.5	62.5	0	87.5	0	37.5	0	62.5	0
	5	0	62.5	0	62.5	37.5	25	62.5	0	25	62.5	0	37.5	37.5	0	37.5	0
	6	0	37.5	62.5	0	37.5	0	0	62.5	37.5	0	0	62.5	0	87.5	62.5	0
	7	0	37.5	37.5	0	0	62.5	62.5	0	25	37.5	62.5	0	0	37.5	62.5	25
	8	0	37.5	25	37.5	37.5	0	62.5	0	0	37.5	0	62.5	37.5	0	37.5	75
	9	0	62.5	0	62.5	0	37.5	75	62.5	62.5	25	37.5	0	62.5	0	62.5	0
	10	0	37.5	62.5	0	25	37.5	37.5	0	0	37.5	62.5	0	75	37.5	37.5	0
	11	0	62.5	62.5	0	62.5	0	0	62.5	37.5	0	0	87.5	0	37.5	37.5	0
	12	0	75	0	25	37.5	62.5	37.5	62.5	37.5	37.5	37.5	37.5	0	0	0	0
	13	0	0	0	25	0	0	75	0	0	75	0	0	75	0	0	0
	14	0	0	62.5	37.5	0	0	62.5	37.5	62.5	37.5	0	0	37.5	62.5	25	25
	15	0	75	37.5	62.5	37.5	62.5	0	25	0	0	62.5	62.5	62.5	62.5	0	0

P Appendix P: Linear Approximation Bias Table of the Integer Addition

		Input Mask															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Output Mask	**0**	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	4	0	0	0	0	0	25	0	25	0	0	0	0	0	0	0	0
	5	0	0	0	0	0	75	0	75	0	0	0	0	0	0	0	0
	6	0	0	0	0	0	25	0	25	0	0	0	0	0	0	0	0
	7	0	0	0	0	0	25	0	25	0	0	0	0	0	0	0	0
	8	0	0	0	0	0	0	0	0	0	37.5	25	37.5	0	37.5	25	37.5
	9	0	0	0	0	0	0	0	0	0	87.5	0	62.5	0	87.5	0	62.5
	10	0	0	0	0	0	0	0	0	0	37.5	75	62.5	0	37.5	75	62.5
	11	0	0	0	0	0	0	0	0	0	37.5	0	37.5	0	37.5	0	37.5
	12	0	0	0	0	0	0	0	0	0	37.5	25	37.5	0	37.5	25	37.5
	13	0	0	0	0	0	0	0	0	0	37.5	0	62.5	0	37.5	0	62.5
	14	0	0	0	0	0	0	0	0	0	37.5	25	12.5	0	37.5	25	12.5
	15	0	0	0	0	0	0	0	0	0	37.5	0	37.5	0	37.5	0	37.5

Q Appendix Q: Rule Set Configuration for the Privacy Cryptographic Unit Expert System

Mapping 1

Paranoia Stimuli Classification	Interference Stimuli Classification	Linear Value (%)	Non-Linear Value (%)
No Threat	No Threat	0.0%	0.0%
No Threat	Low Threat	1.5%	0.7%
No Threat	Medium Threat	3.0%	3.0%
No Threat	High Threat	4.5%	9.0%
No Threat	Very High Treat	5.0%	27.0%

Mapping 2

Paranoia Stimuli Classification	Interference Stimuli Classification	Linear Value (%)	Non-Linear Value (%)
Low Threat	No Threat	-1.5%	-0.7%
Low Threat	Low Threat	0.0%	0.0%
Low Threat	Medium Threat	1.5%	0.7%
Low Threat	High Threat	3.0%	3.0%
Low Threat	Very High Treat	4.5%	9.0%

Mapping 3

Paranoia Stimuli Classification	Interference Stimuli Classification	Linear Value (%)	Non-Linear Value (%)
Medium Threat	No Threat	-3.0%	-3.0%
Medium Threat	Low Threat	-1.5%	-0.7%
Medium Threat	Medium Threat	0.0%	0.0%
Medium Threat	High Threat	1.5%	0.7%
Medium Threat	Very High Treat	3.0%	3.0%

Mapping 4

Paranoia Stimuli Classification	Interference Stimuli Classification	Linear Value (%)	Non-Linear Value (%)
High Threat	No Threat	-4.5%	-9.0%
High Threat	Low Threat	-3.0%	-3.0%
High Threat	Medium Threat	-1.5%	-0.7%
High Threat	High Threat	0.0%	0.0%
High Threat	Very High Treat	1.5%	0.7%

Mapping 5

Paranoia Stimuli Classification	Interference Stimuli Classification	Linear Value (%)	Non-Linear Value (%)
Very High Threat	No Threat	-5.0%	-27.0%
Very High Threat	Low Threat	-4.5%	-9.0%
Very High Threat	Medium Threat	-3.0%	-3.0%
Very High Threat	High Threat	-1.5%	-0.7%
Very High Threat	Very High Treat	0.0%	0.0%

R Appendix R: Simulating and Modelling the Impact of Security Constructs on Latency for Open Loop Control

Conference paper 1: Simulating and Modelling the Impact of Security Constructs on Latency for Open Loop Control

Published in: IEEE 6th Computer Science and Electronic Engineering Conference (CEEC) 2014, Colchester, Essex

Presented on: 26th September 2014

Abstract: Open loop control has commonly been used to conduct tasks for a range of Industrial Control Systems (ICS). ICS however, are susceptible to security exploits. A possible countermeasure to the active and passive attacks on ICS is to provide cryptography to thwart the attacker by providing confidentiality and integrity for transmitted data between nodes on the ICS network; however, a drawback of applying cryptographic algorithms to ICS is the additional communication latency that is generated. The proposed solution presented in this paper delivers a mathematical model suitable for predicting the latency and impact of software security constructs on ICS communications. The proposed model has been tested and validated against a software simulated open loop control scenario, the results obtained indicate on average a 1.3 percentage difference between the model and simulation.

Simulating and Modelling the Impact of Security Constructs on Latency for Open Loop Control

R.D.Sparrow, A.A.Adekunle, R.J.Berry and R.J.Farnish
The Wolfson Centre for Bulk Solids Handling Technology,
University of Greenwich,Chatham Maritime,
Chatham, Kent ME4 4TB, England, UK
{r.d.sparrow, a.a.adekunle, r.j.berry, r.j.farnish} @gre.ac.uk

***Abstract*—Open loop control has commonly been used to conduct tasks for a range of Industrial Control Systems (ICS). ICS however, are susceptible to security exploits. A possible countermeasure to the active and passive attacks on ICS is to provide cryptography to thwart the attacker by providing confidentiality and integrity for transmitted data between nodes on the ICS network; however, a drawback of applying cryptographic algorithms to ICS is the additional communication latency that is generated. The proposed solution presented in this paper delivers a mathematical model suitable for predicting the latency and impact of software security constructs on ICS communications. The proposed model has been tested and validated against a software simulated open loop control scenario, the results obtained indicate on average a 1.3 percentage difference between the model and simulation.**

***Index Terms*—Industrial Control Systems, Real-Time communication, Impact modelling.**

I. Introduction

OPEN loop control is used in a range of Industrial Control Systems (ICS), to conduct tasks ranging from data acquisition to the operation of an actuator. Variations of ICS include Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC). ICS previously have been immune from potential security breaches due to their isolation from enterprise networks; however, with the presence of "the internet of things" being more predominant, ICS could be susceptible to the same attacks as enterprise networks [1].

ICS interact using a fieldbus protocol (e.g. Profibus, Modbus), mos which must take into consideration the real time and non-real time requirements of a system [2], [3] as failure to achieve real time constraints could be catastrophic [4].

The contribution of this paper is a mathematical model for predicting and calculating the impact of software based security constructs using block ciphers, on the overall latency of open loop control systems; enabling practitioners to model the impact of software security constructs without the time and expense required to conduct simulation or real world testing.

The structure of this paper is organised as follows: Section II introduces the terms and phrases discussed in this paper. Section III introduces relevant literature. Section IV introduces the proposed mathematical model with Section V discussing the test methodology used. Section VI discuses and analyses the results obtained from comparative testing of the proposed mathematical model with the simulation conducted. Section VII applies the proposed mathematical model as a predictive tool. Section VIII discusses the findings obtained. Section IX concludes.

II. Preliminary

This section defines the terms used throughout this paper.

- *Real Time Constraints:* is a computing system whose correct behaviour depends not only on the value of the computation but also on the time at which outputs are produced. The deadline of less than ten milliseconds (i.e <10ms) represents the real time constraints in this paper. [5]
- *Non Real Time Constraints:* is a computing system whose correct behaviour depends only on the value of the computation. A deadline of greater than ten milliseconds (>10ms) and below one hundred milliseconds (<100ms) represents the limits for non real time requirements in this paper. [Op cit 5]
- *Latency:* The duration taken for data to travel from transmitter to receiver.
- *Confidentiality:* Confidentiality in this paper refers to using encipherment methods in order to thwart an unauthorised entity understanding the content of the payload of the data frames transmitted.
- *Integrity:* In this paper integrity is determining whether communicated data has been altered in transit at the receiving node.
- *Authentication:* The proof that a device on the network is legitimately eligible to communicate with other eligible devices on the same network.

978-1-4799-6692-9/14/$31.00 ©2014 IEEE

- *AEAD concept:* The Authenticated Encryption with Associated Data (AEAD) concept provides both symmetric cryptographic security data services to transmitted packetised data.

III. Literature Review

Section III examines current literature presented by other researchers and identifies research gaps. The literature review consists of three parts, first the current methodologies undertaken by other researchers, second the introduction of AEAD constructs and finally a conclusion of the literature review. A method proposed by Swaminathan [6] uses the 56-bit Data Encryption Standard (DES) cipher in a symmetric cryptography approach to provide security in fieldbus networks; however, there is limited information regarding the test plan or the results to clarify whether this approach is suited for fieldbus communications from a real time or non real time prospective. In addition, the National Institute of Standards and Technology (NIST) have withdrawn the use of the DES cipher as a standard [7]; Van De Zande [8] commented on the associated vulnerabilities with DES and why it is no longer enforced as a standard, therefore suggesting the use of the DES algorithm is no longer suited for modern fieldbus networks.

Hong et al [9] investigated the impact of using cryptographic algorithms on SCADA devices and how this influences the performance of the embedded device. The research undertakes a comparison between two block ciphers, the Advanced Encryption Standard (AES) and SEED. The block ciphers are utilised in the Cipher Block Chaining (CBC) mode for confidentiality security services. Integrity security services are generated using a message authentication code (MAC) and a hashed message authentication code (HMAC). HMAC uses the Message Digest 5 (MD5) algorithm. The test conducted by Hong et al, was performed on devices that were not computationally limited; the comparison was made between a desktop computer and an Intel Xscale PXA270 embedded processor. In addition the size of the packet used for the test was fixed at 96 bytes; as there was no change to the variables used in this investigation it is difficult to gauge the behaviour of security algorithms on the operation of generic fieldbus communication protocols using microcontrollers.

Wang [10] investigates the security vulnerabilities associated with SCADA systems, with remote hacking being deployed to gain unauthorised access to the actuator on the ICS through the remote terminal units. Security vulnerabilities identified by Wang focus on the computational limitations currently present with ICS networks and discusses how these devices were not designed with security services as a primary consideration. The approach taken to overcome the shortfalls mentioned by Wang, involves a master SCADA device to distribute symmetric keys to slave SCADA devices with various customised approaches dependent on the type of ICS network. With the limited test results presented in the paper, it is difficult to infer whether the approaches specified are best suited for the context of ICS. Furthermore, the use of symmetric key management can also impact on the computational requirements associated with ICS. This was not considered in the report

Zeng and Chow [11], propose a mathematical model to calculate the trade-off of performance when security constructs are applied to wireless Network Control Systems (NCS). Problems discussed in this literature focus on the vulnerabilities of the transmission medium as wireless communication systems have been known to be susceptible to passive and active security threats. This problem is further imposed as Zeng and Chow state that NCS were designed without the consideration of security in mind. The proposed solution by Zeng and Chow presents a mathematical model to calculate the trade-off between security algorithms and the performance of the ICS. The tests conducted uses three cryptographic algorithms being DES, 3DES and AES using the Electronic Code Book (ECB) mode of operation with results obtained from the simulation programme Simulink. Results presented in this paper presents ambiguity with minimal data presenting how accurate the model is in comparison to the software simulation, therefore it is difficult to infer whether the proposed trade-off model is suited for the context of industrial control systems. In addition DES and 3DES constructs are no longer standardised due to their known security vulnerabilities.

This paragraph introduces the AEAD concepts with two examples being Counter with cipher block chaining (CCM) and TinyAEAD. CCM is a NIST standardised AEAD construct designed to provide integrity and confidentiality using a 128-bit block cipher [12]. The TinyAEAD construct is designed to provide confidentiality and integrity services using block ciphers of various bit lengths [13]. This construct can be configured to run at a reduced specified number of block cipher iterations in order to enhance the processing speed of the construct. In addition TinyAEAD provides flexibility and adaptability that can be applied to a broad range of contexts.

A conclusion from the literature review is that the approaches currently undertaken to understand the impact of security algorithms on constrained ICS show ambiguity with minimal test results available to identify any relationships or proof that the approaches discussed have been justified for this context. This problem is a reoccurring theme amongst existing literature as the model or results are bespoke scenarios. Current models are unduly complex, therefore, there is a requirement for simplified mathematical models.

IV. Proposed Communication Latency Model

This section introduces the proposed mathematical model to calculate communication latency introduced by security constructs on open loop control systems. The proposed mathematical model is designed to take into consideration factors influencing the overall latency of the system whilst allowing

for flexibility for the parameters used; making it advantageous as it can calculate latency for any open loop control system. To calculate the total delay latency (τdl) for a single hop open loop control system, the equation calculates a subtotal comprising of the instruction cycle time (δ) (at a specified crystal frequency) for a microcontroller to process and transmit one byte of data across to the receiving microcontroller; the time to transmit the data across the chosen physical medium (η) and the time to process a byte of data though the security algorithm (ψ) is added. The size of the packet ($\triangle$) must be multiplied by the sub total latency acquired from ($\eta + \delta + \psi$), as this will calculate the result for a desired packet length size in bytes. The transmission delay is calculated by dividing the speed of the transmission medium (ν) (e.g. the speed of electrons through a copper cable or the vacuum of the speed of light) by the distance of the link (ℓ).

$$\tau dl = (\triangle(\eta + \delta + \psi)) + \frac{\nu}{\ell} \quad (1)$$

Equation 1: Calculating communication latency introduced by security constructs for a single hop open loop control

$\tau dl = Total\ delay\ latency\ (ms)$
$\triangle = Packet\ size\ (bytes)$
$\eta = Physical\ layer\ process\ time\ cost\ (ms)$
$\delta = Instruction\ cycle\ time\ cost\ (ms^{-1})$
$\psi = Security\ algorithm\ process\ time\ cost\ (ms)$
$\nu = Transmission\ medium\ delay\ (ms)$
$\ell = Link\ Distance\ (meters)$

V. Testing Methodology

In this section the methodology, apparatus, parameters and scenario used in the validation of the proposed mathematical model is introduced. The simulation programme used is Proteus ISIS 8 professional with the Microchip PIC18F45K22 series selected as the microcontroller of choice. The Serial Peripheral Interface (SPI) was selected as part of the physical layer (i.e OSI model) used to pass data between the transmitting and receiving microcontrollers. The AEAD security constructs used are CCM and TinyAEAD running AES (128-bit key variant).

The testing structure examines the latency for the transmitting microcontroller to process and transmit the packet, the duration of the packet to propagate to the receiving microcontroller and to process the received packet. The impact of the software security constructs on latency is measured in milliseconds. All timings are taken from the simulator used.

The test procedure examines the effect of software security services on ICS by using three SPI divisor settings of 4, 16 and 64 and data frame sizes of 36, 52 and 84 bytes. Crystal frequencies of 1 MHz, 4 MHz and 8 MHz were selected to represent realistic industry microcontroller frequencies. It is assumed for this test scenario that the communication medium is copper cabling travelling at the speed of electrons (100m in length).

VI. Results and Analysis of Testing

Section VI presents the data obtained from undertaking the testing methodology as discussed in the aforementioned section and infers the meaning of the data obtained. Figure 1 graphs the total latency in time required to process a 36 byte data frame without security on the PIC18F45K22 microcontroller. The zero integer on the horizontal axis represents the real time requirement deadline, negative integers represent the time less than the real time constraint, positive integers represent time greater than the real time constraint. Results displayed in Figure 1 indicate that overall the majority of the packet sizes using different crystal frequencies and SPI clock divisors met the real time constraints with only the 1 MHz crystal frequency at the SPI divisor of 64 not achieving the real time requirements.

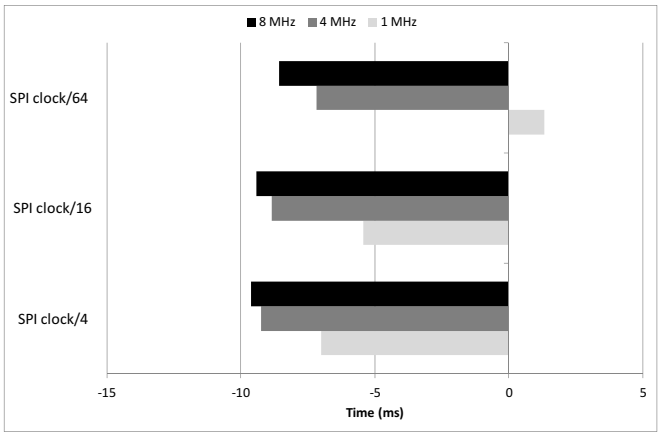


Figure 1. Communication latency for a simulated single hop link without security (36 byte packet length)

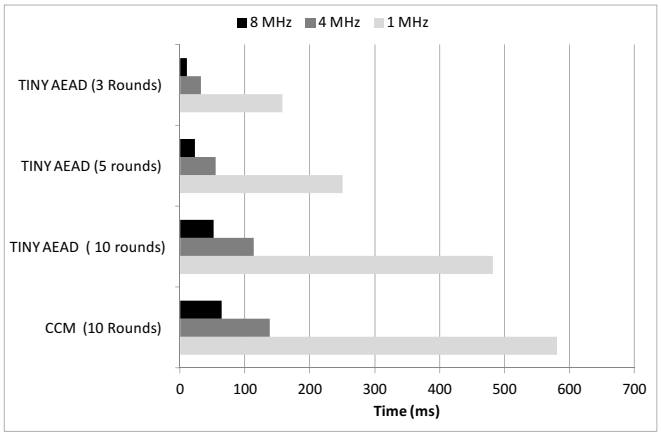


Figure 2. End to end communication time for specified AEAD constructs on a simulated single hop link (36 byte packet length)

Figure 2 graphs the influence of security algorithms when applied to the communicating microcontrollers, indicating a change in the overall communication latency. The 8 MHz crystal frequency is better suited for meeting the real time requirements of a fieldbus network incorporating any of the

security algorithms utilised for this investigation. The 4 MHz crystal frequency is only suited for non real time requirements running TinyAEAD at three and five rounds. The 1 MHz crystal frequency is unsuitable for either constrained time.

Figure 3 graphs the result for a packet size of 52 bytes without security applied. The 8 MHz and 4 MHz crystal frequencies achieved the real time constraints, however the 1 MHz crystal frequency using the SPI divisor of 64 did not achieve the real time constraints.

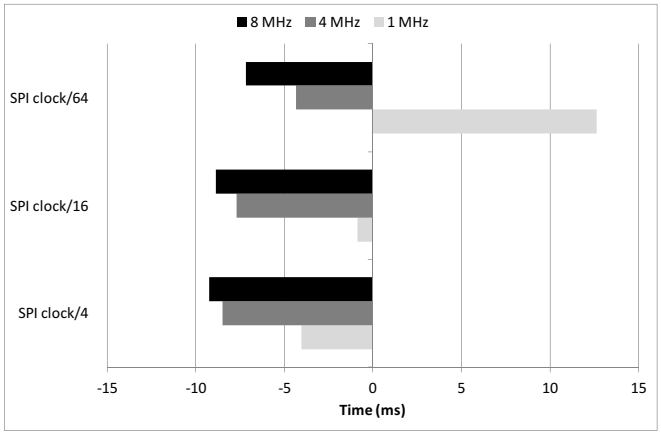


Figure 3. Communication latency for a simulated single hop link without security (52 byte packet length)

The data in Figure 4 indicates that none of the tested AEAD security constructs met the real time constraints. The 8 MHz test running CCM shows it is within the non real time constraints, whilst the TinyAEAD construct running three rounds at 8 MHz is four times as fast in comparison to CCM.

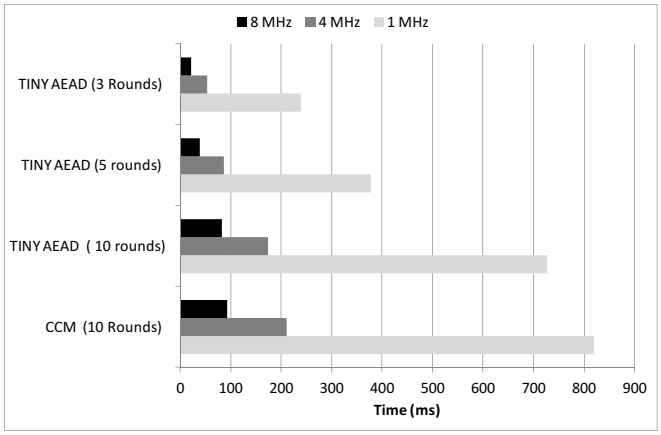


Figure 4. End to end communication time for specified AEAD constructs on a simulated single hop link (52 byte packet length)

Figure 5 displays the effect of a 84 packet size has on the operation of the microcontrollers with lower crystal frequencies having the larger latency times. Configuring the SPI with a divisor of 64 resulted in the largest latency times.

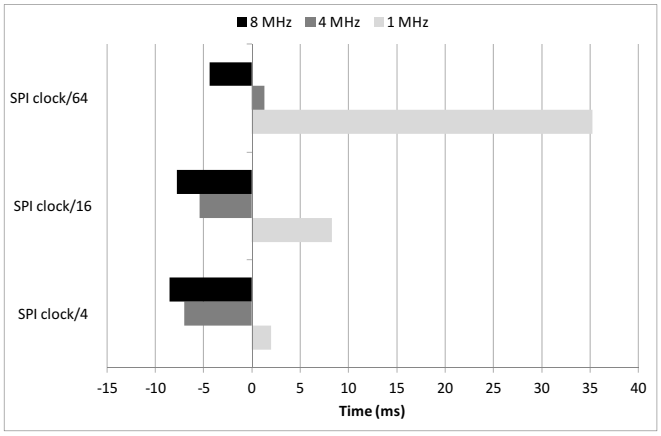


Figure 5. Communication latency for a simulated single hop link without security (84 byte packet length)

Figure 6 illustrates the impact of using AEAD constructs for a 84 byte packet size. Using TinyAEAD and CCM for ten round configuration is not suitable for meeting real time or non real time requirements for any of the specified crystal frequency used. Utilising TinyAEAD at five rounds is suited for an 8 MHz crystal frequency whilst the three round configuration is suited for both 8 MHz and 4 MHz crystal frequencies.

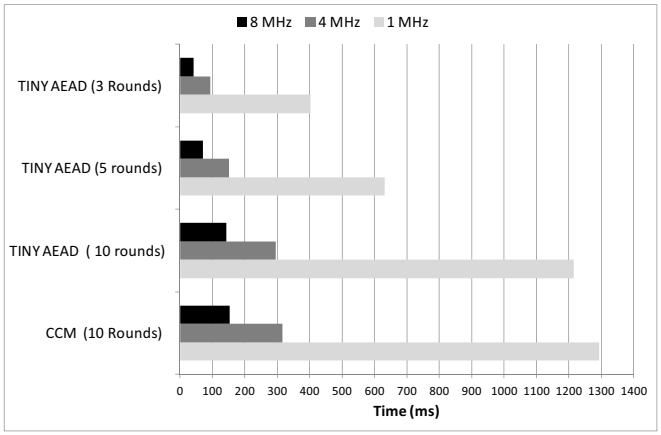


Figure 6. End to end communication time for specified AEAD constructs on a simulated single hop link (84 byte packet length)

Concluding from the simulation results, the next set of results compares the proposed mathematical model against the simulation results obtained for calculating the latency for packets without security. The tests had been conducted using a PIC18F45K22 with a fixed 36 byte packet size. The SPI was selected as the physical medium between the two microcontrollers with three different divisors selected, being 4, 16 and 64. Crystal frequencies of 1 MHz, 4 MHz and 8 MHz have been selected. The communication medium selected is copper cabling at the speed of electrons (100m in length).

Data displayed in Table I states the times calculated using

the model and the times reported by the simulation. The data indicates that the times calculated and reported are correlated. The symbol σ represents standard deviation.

Table I
36 BYTE PACKET SIZE TIME COMPARISON USING SPI DIVISOR OF 4

CRYSTAL FREQUENCY (MHz)	PROPOSED MODEL RESULTS (ms)	SIMULATION RESULTS (ms)	DIFFERENCE IN RESULTS (%)	MEAN (MS)	σ
1	2.928	2.992	2.13	2.960	0.045
4	0.736	0.748	1.60	0.742	0.008
8	0.368	0.374	1.60	0.371	0.004

The comparison is based on a 16 byte packet size with the three ranges of crystal frequency being 1 MHz, 4 MHz and 8 MHz and SPI clock divisors being 4, 16 and 64.

Data obtained and displayed in Table II correlates the results obtained from the model to be accurate in comparison to the simulation. The times calculated using the model was over two percent difference between the model and the time acquired from the simulation.

Table II
36 BYTE PACKET SIZE TIME COMPARISON USING SPI DIVISOR OF 16

CRYSTAL FREQUENCY (MHz)	PROPOSED MODEL RESULTS (ms)	SIMULATION RESULTS (ms)	DIFFERENCE IN RESULTS (%)	MEAN (MS)	σ
1	4.512	4.592	1.61	4.552	0.065
4	1.136	1.148	1.04	1.142	0.008
8	0.560	0.574	2.43	0.567	0.009

Table III conducts the same test procedure using a SPI divisor of 64.

Table III
36 BYTE PACKET SIZE TIME COMPARISON USING SPI DIVISOR OF 64

CRYSTAL FREQUENCY (MHz)	PROPOSED MODEL RESULTS (ms)	SIMULATION RESULTS (ms)	DIFFERENCE IN RESULTS (%)	MEAN (MS)	σ
1	11.248	11.312	0.56	11.280	0.045
4	2.816	2.828	0.42	2.882	0.008
8	1.408	1.414	0.42	1.411	0.004

Comparison of the results obtained from the model and simulation indicate that the accuracy of the results calculated using the model is within an average 1.3 percentage difference of the results generated by the output of the simulation, with increased lower percentage differences being obtained for the longer time durations. These results indicate that the model is suited for calculating the total communication latency generated without the implementation of AEAD security for the simulated scenario.

The SPI clock divisor also influences latency, with the smaller SPI divisor showing reduced latency in comparison with the larger SPI divisors. This is particularly noticeable when the size of the packet length increases, as the 64 SPI divisor on a 1 MHz crystal frequency causes initial difficulty without any security algorithm attached and this also has an influence on the 4 MHz and 8 MHz frequencies. Therefore this suggest that higher crystal frequencies would be more preferable for a larger SPI divisor is required, or use the smallest SPI divisor possible in order to provide the least communication latency.

Crystal frequency influences the packet processing latency delay with packets being transmitted with and without security. This is represented throughout each Figure; showing a relationship between the configuration of the crystal frequency and the outcome of the results.

VII. PREDICTIVE MODELLING

Section VII discusses the process of comparing the proposed mathematical model calculation in direct comparison to a result obtained from simulation. The PIC18F45K22 microcontroller can use a maximum crystal frequency of 64 MHz [14] and can be calculated using the mathematical model that the implementation of any of the security constructs would be suitable for a small packet size; however, on larger packets the TinyAEAD construct is better suited to meeting the real time requirements due to its flexibility in its design by reducing the round settings to reduce latency. To verify this hypothesis a comparison is undertaken between the simulation and the mathematical model using the underlying block cipher in TinyAEAD construct at three rounds, three packet sizes being 36, 52, 84 bytes, a 20 MHz crystal frequency and SPI divisor of 4.

Calculating the SPI latency can be achieved by two methods: dividing the microcontroller frequency of oscillation by the SPI divisor or using the calculated Million Instructions Per Seconds (MIPS), this is shown in Equation 2 and 3.

$$Fo = \Upsilon/\alpha \tag{2}$$

Equation 2: Frequency of oscillation calculation for SPI

$$MIPS = ((\frac{1}{\Upsilon/\partial})\alpha)^{-1} \tag{3}$$

Equation 3: MIPS calculation for SPI

Two approaches to calculating the SPI latency have been formulated; Equation 2 calculates the frequency of oscillation (Fo) by taking the crystal frequency (Υ) of the microcontroller and dividing by the SPI clock divisor (α). Equation 3 calculates the MIPS; the crystal frequency (Υ) is divided by the microcontroller instructions per cycle (∂); the value obtained is then divided by one. The SPI divisor (α) is then multiplied with the value obtained to derive the instruction cycle time. The value is then inverted to derive the MIPS.

For this scenario the crystal frequency of 20 MHz (5 MIPS) was selected using a PIC18F45K22 microcontroller. The instruction cycle time per bit over the SPI is 0.2 nanoseconds using 5 MIPS. The latency for a whole byte is calculated by multiplying the 0.2 nanoseconds by eight, resulting in a total latency of 1.6 microseconds per byte. Table IV displays the results obtained from the predictive modelling with security included.

Table IV
COMPARATIVE RESULTS OF MODEL VS SIMULATION FOR SOFTWARE IMPLEMENTATION OF TINYAEAD (3 ROUNDS)

PACKET SIZE (bytes)	PROPOSED MODEL RESULTS (ms)	SIMULATION RESULTS (ms)	DIFFERENCE IN RESULTS (%)	MEAN (MS)	σ
36	8.640	8.642	0.02%	8.641	0.001
52	12.792	12.784	0.06%	12.788	0.005
84	21.336	21.302	0.17%	21.319	0.024

As presented in Table IV, the accuracy of the model in contrast to the simulation shows an accurate measurement to one decimal place; however, the measurement of the impact of security constructs using larger packet sizes shows that at a 20 MHz crystal frequency, packet lengths under the size of 36 bytes are only feasible for real time requirements of a fieldbus communication network. The 52 and 84 byte packet lengths are more suited to non real time requirements.

VIII. DISCUSSION

Data obtained from the tests reported in this paper suggests latency induced by AEAD constructs affect the communication of open loop control systems. A contrived scenario applicable to the context of semi-autonomous control is the use of a fixed wing unmanned aerial vehicles (UAV) which is piloted from a remote base station to the drone. Figure 7 represents the minimal distance travelled to perform a set action on the UAV with and without specified software AEAD constructs.

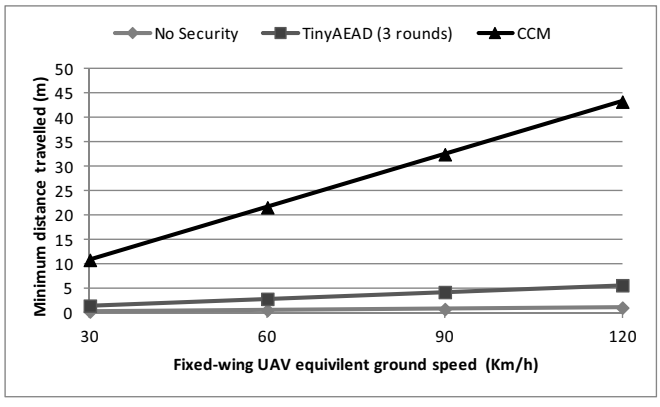


Figure 7. Minimum distance travelled by a fixed wing UAV before execution of a telecommand with and without secure communication

Using the parameters of a PIC18F45K22, an 84 byte packet length and a crystal frequency of 1 MHz the results indicate that the latency induced by the security constructs increased the minimum distance travelled by the fixed winged UAV before the command is performed. CCM had the most effect, with the minimum distance travelled increasing significantly in comparison to TinyAEAD at three rounds.

IX. CONCLUSION

The equation proposed in this paper demonstrates an accurate measurement of the total time impact of the desired packet length with and without security measures applied and also takes into consideration security algorithms that can be customised for a set purpose.

In conclusion from the results obtained TinyAEAD running at a crystal frequency of 20 MHz is suitable towards operating within the real time requirements specified in this paper up to packet sizes of 54 bytes. This therefore infers that the use of adjustable AEAD constructs can meet the specified real time constraints set in this paper, whilst fixed AEAD constructs are not suited.

The mathematical model is applicable towards calculating the impact of security constructs on open loop control by either inputting the variables to generate the total time delay to define the ideal parameters based on the total delay time required. Therefore, this proposed approach enables readers and practitioners to use this model as a method of accurately measuring the impact without having to expend time and resources.

REFERENCES

[1] M. Ozturk and P. Aubin. Scada security:challenges and solutions, June 2011.
[2] E. Tovar and F. Vasques. Real-time fieldbus communications using profibus networks. *IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS*, 46:1241–1251, 1999.
[3] B. Galloway and G. P. Hancke. Introduction to industrial control networks. *ATIONS SURVEYS & TUTORIALS, VOL. 1*, 15:860–879, 2013.
[4] B. Miller and D. Rowe. A survey scada of and critical infrastructure incidents. In *RIIT '12 Proceedings of the 1st Annual conference on Research in information technology*, 2012.
[5] Profinet real-time communication, December 2006.
[6] P. Swaminathan, K. Padmanabhan, S. Ananthi, and R. Pradeep. The secure field bus (secfb) protocol - network communication security for secure industrial process control. In *TENCON 2006. 2006 IEEE Region 10 Conference*, 2006.
[7] Data encryption standard (des), October 1999.
[8] P. Van De Zande. The day des died. Technical report, System Administration, Networking, and Security Institute, 2001.
[9] S. Hong, M. Lee, and D. Shin. Experiments for embedded protection device for secure scada communication. In *Power and Energy Engineering Conference (APPEEC), 2010 Asia-Pacific*, 2010.
[10] Wang.Y. sscada: Securing scada infrastructure communications. *Int. J. Communication Networks and Distributed Systems*, 6:59–78, 2011.
[11] W Zeng and Y. Chow, M. A trade-off model for performance and security in secured networked control systems. In *IEEE International Symposium on Industrial Electronics (ISIE),*, 2011.
[12] Recommendation for block cipher modes of operation: The ccm mode for authentication and confidentiality.
[13] A. Adekunle and S. Woodhead. An aead cryptographic framework and tinyaead construct for secure wsn communication. In *Wireless Advanced (WiAd)*, 2012.
[14] Microchip. Pic18(l)f2x/4xk22 data sheet. Technical report, Microchip Technology Inc, 2012.

S Appendix S: Simulating and Modelling the Impact of Secure Communication Latency for Closed Loop Control

Conference paper 2: Simulating and Modelling the Impact of Secure Communication Latency for Closed Loop Control

Published in: IEEE 6th International Conference on Internet Technologies & Applications 2015, Wrexham, Wales

Presented on: 11th September 2015

Abstract: Closed loop control systems have been implemented to conduct a variety of tasks (e.g. manufacturing and automation). Industrial Control System (ICS) have been used to regulate a closed loop process; however, ICS are exposed to the same security vulnerabilities associated with enterprise networks. Cryptography has been deployed to overcome the associated data communication weaknesses between each ICS node through the use of block ciphers; however, the drawback of applying cryptographic algorithms to ICS is the additional communication latency. This paper investigates the relationship between security constructs and latency for closed loop control system with test conducted in a simulated environment. A case scenario is illustrated to demonstrate the impact of the results obtained to a real world context.

Simulating and Modelling the Impact of Secure Communication Latency for Closed Loop Control

R.D.Sparrow, A.A.Adekunle, R.J.Berry and R.J.Farnish
The Wolfson Centre for Bulk Solids Handling Technology,
University of Greenwich,Chatham Maritime,
Chatham, Kent ME4 4TB, England, UK
{r.d.sparrow, a.a.adekunle, r.j.berry, r.j.farnish} @gre.ac.uk

***Abstract*—Closed loop control systems have been implemented to conduct a variety of tasks (e.g. manufacturing and automation). Industrial Control System (ICS) have been used to regulate a closed loop process; however, ICS are exposed to the same security vulnerabilities associated with enterprise networks. Cryptography has been deployed to overcome the associated data communication weaknesses between each ICS node through the use of block ciphers; however, the drawback of applying cryptographic algorithms to ICS is the additional communication latency. This paper investigates the relationship between security constructs and latency for closed loop control system with test conducted in a simulated environment. A case scenario is illustrated to demonstrate the impact of the results obtained to a real world context.**

***Index Terms*—closed loop control, real-time systems, computational constraints, security constructs**

I. Introduction

Closed loop control systems are implemented in a variety of sectors to provide feedback from a set process. With closed loop control providing autonomous actions based on feedback from an actuator, this method is suitable for monitoring a continuous process without human intervention. Closed loop control has commonly been identified in Industrial Control Systems (ICS) (e.g. computer aided manufacturing). With devices becoming interconnected, one of the most challenging aspects of ICS is the exposed security vulnerabilities, this is due to the increase of cyber crime and availability of open designs [1].

Increased threats to ICS are also becoming more frequent [2] with statistics reported indicating that cyber attacks against control systems has increased. The System Administration Networking and Security Institute (SANS) survey indicates a minimum of one or two security breaches against ICS has occurred within the past twelve months [3]. Safety of industrial networks is critical as undetected corruption of data packets during transmission can cause damage to equipment, environment and human health [4]. This paper investigates how software based security algorithms using block ciphers impact the overall communication latency of closed loop control systems. A mathematical model is proposed to aid practitioners to predict the effects of security constructs on closed loop control systems without the requirement and cost of implementing an experimentation platform.

The structure of this paper is organised as follows: Section II introduces the terms and phrases discussed in this paper. Section III discusses a system safety case scenario with Section IV reviewing relevant literature. Section V discusses the experimentation procedure with Section VI analysing the results obtained. Section VII introduces the proposed mathematical mode with Section VIII conducting a comparative experiment of the proposed mathematical model against the simulation. Section IX examines the mathematical model as a predictive tool. Section X discusses the impact of the results to the context of the case scenario. Section XI concludes.

II. Preliminary

This section defines the terms used throughout this paper.

- *Real-Time Constraints:* is a computing system whose correct behaviour depends not only on the value of the computation but also on the time at which outputs are produced.
- *Non Real-Time Constraints:* is a computing system whose correct behaviour depends only on the value of the computation.
- *Latency:* The duration taken for data to travel from transmitter to receiver.
- *Confidentiality:* Confidentiality in this paper refers to using encipherment methods in order to thwart an unauthorised entity understanding the content of the payload of the data frames transmitted.
- *Integrity:* In this paper integrity is determining whether data has been altered in transit at the receiving node.
- *Authentication:* The proof that a device on the network is legitimately eligible to communicate with other eligible devices on the same network.
- *AEAD concept:* The Authenticated Encryption with Associated Data (AEAD) concept provides both confidentiality and integrity security data services to transmitted packetised data.

III. System Safety Case Scenario

The following section considers a scenario where a closed loop control system is used to automate a safety critical process. Dust explosions in bulk solids powder handling can result in personal injury or death and loss of plant. The adoption of legislation to mitigate the effects of such events is now widespread and many technical approaches can be applied to ensure plant safety. The scenario uses a suite of these counter-measures commonly found in industry. Figure 1 illustrates, the main components found in many plants (i.e. air mover, powder feeder, pneumatic conveying pipeline and reception vessel).

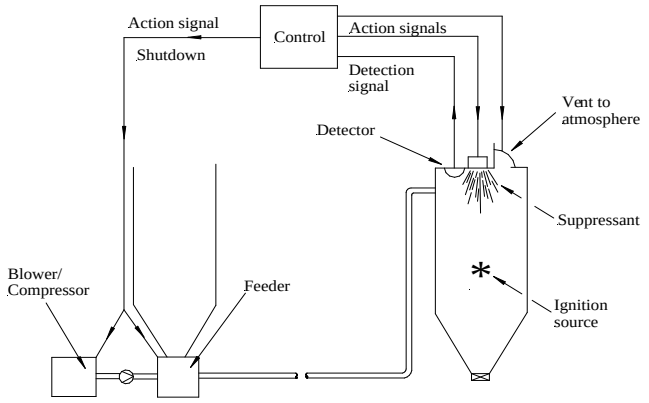


Figure 1. Schematic of a process plant for bulk solids powder handling

Best practice dictates that in the event of a rapid pressure rise being detected (i.e. the initiation of a dust explosion) a range of counter-measures should be activated. The energy released during a dust explosion is such that an over-pressure capable of destroying the plant can develop on average within a tenth of a second (e.g. polyester can attain a maximum explosion pressure of 6.1 bar at a rate of 85 bar/sec) [5] thus the response time for detection and actuation of counter-measures is a critical factor for the safety of staff and the safe operation of the plant.

IV. Literature Review

Section IV introduces literature relevant to the context of this paper with focus on confidentiality, integrity and authentication in closed loop control and methods of modelling utilised. The literature review is sectioned into three parts; firstly the current approaches undertaken by other researchers, secondly the introduction of the AEAD constructs and finally a conclusion of the literature undertaken. Ma et al focus on mechanisms for providing security to real-time systems; the authors propose the Adaptive Risk Control and Security Management concept (ARCSM) [6]. This approach targets current security vulnerabilities for insecure environments without compromising the real-time element of embedded systems. This is achieved by using a two tier feedback control framework on each node on the network. Experimentation conducted by the authors examine the time and energy required by cryptographic constructs and how this influences the operation of the embedded system. The results obtained from their research show that the ARCSM approach is better suited for open loop control with varying run-time performance; however, the security constructs tested in this paper only utilises legacy security constructs, raising questions to how contemporary cryptographic constructs would behave in this context. It is also noted that a high end specification ARM S3C2440 microprocessor was selected for experimentation.

A method to overcoming deception attacks in closed loop control systems is presented by Pang et al using their secure networked predictive control system (SNPCS) [7]. The research conducted by the authors provides confidentiality, integrity and authentication to data by using a software implementation of the Data Encryption Standard (DES), Message Digest version 5 (MD5) and a time-stamp. The Recursive Networked Predictive Control (RNPC) is utilised to compensate for the control system performance from the deception attacks. Experimentation was performed on an internet based control rig with results showing the implemented countermeasure was suitable; however, it is unknown whether this security approach is suited against other attacks vectors. The comparison between the authors method and other software security constructs is not explicitly explained. The implementation of a time-stamped authentication system is also a security vulnerability due to synchronisation of two time zones. An attacker could craft their own packet using the same time-stamp and spoof a legitimate device with the possibility of the packet still passing the authentication procedure.

Gupta et al [8] assesses the performance of data and time sensitive wireless network control systems with the presence of information security. The issues examined by the authors emphasise the security vulnerability of wireless broadcast to transmit data over the internet from the Network Control System (NCS) as the broadcast signal can be detected by anyone within range. This is further exposed as NCS had been designed without consideration of security in mind, allowing for the attacker to compensate the device remotely. A proposed solution by the authors uses security constructs DES and Triple Data Encryption Standard (3DES) operating in the Electronic Code Book (ECB) mode on a closed loop control testbed intelligent space (ispace). Results obtained suggest that the security constructs investigated have a slight impact on the timing of the closed loop control system with overhead of 9% to 18%. The focus of the research conducted by the au tours is for securing NCS traffic over the internet. The security constructs used are no longer standardised due to their known security vulnerabilities and the ECB mode of operation is also susceptible to known plain text attacks.

An approach undertaken by Dhand et al [9] examines the impact of communication delay on real-time distributed control systems. Current problems discussed by the authors focuses on the challenge of minimising delay within a

control loop and how time delays are not always specific to the controller alone but also from transmission and sensor delays. The solution presented in this literature uses the Auto-regressive Integrated Moving Average (ARIMA) to forecast the communication delay a control loop. Experimentation was performed using the national instruments Data Socket Transport Protocol (DSTP) at the application layer, the Transmission Communication Protocol (TCP) for the transport layer and Ethernet for the data link layer. Results had been acquired by using minilab 15 and Simulink. The impact of security constructs on the operation of real-time control networks has been overlooked as the focus of the model is for communication latency.

This paragraph introduces the AEAD concepts with two paradigms being presented; the fixed standardised approach of Counter with cipher block chaining (CCM) and the adjustable and flexible approach of TinyAEAD. CCM is a National Institute of Standards and Technology (NIST) standardised AEAD construct designed to provide integrity and confidentiality using a 128-bit block cipher [10]. The TinyAEAD construct is designed to provide confidentiality and integrity services using block ciphers of varying bit length [11]. This construct can be configured to run at a reduced specified number of block cipher iterations in order to enhance the processing speed of the construct. In addition TinyAEAD provides flexibility and adaptability that can be applied to a broad range of contexts.

Concluding from the literature review undertaken two areas have been identified as areas to conduct further research; firstly the requirement for test with modernised cryptographic constructs is required as the literature uses constructs that are no longer standardised. Secondly a mathematical model is required to predict and disclose the impact of security constructs on closed loop control systems as current models do not take this into consideration.

V. Experimentation Procedure

Section V discusses the experimentation procedure conducted and the apparatus selected. The simulation programme used is Proteus ISIS 8 professional with the Microchip PIC18F45K22 selected as the microcontroller of choice. The Serial Peripheral Interface (SPI) has been selected as the physical medium used to transport the data between microcontrollers. Software security constructs evaluated in this paper focus on variation of the Advanced Encryption Standard (AES) using a 128-bit key. Modes of operation examined were CCM and TinyAEAD. The selected closed loop control approach used is the Proportional-Integral-Derivative (PID).

The experimentation examines latency for a transmitting microcontroller to process and transmit the packet, the duration of the packet to propagate to the receiving microcontroller to process the received packet and perform the feedback action. The metric utilised for measuring the impact software security constructs on latency is measured in milliseconds. All timings are taken from the simulator used.

Packet sizes of 36, 52 and 84 bytes in length were sampled to mimic ICS protocols with SPI divisor of 4 to output the data at the fastest configuration setting. The crystal frequency sampled was 8 MHz to replicate a low frequency micro-controller. Finally it is assumed for this test scenario that the communication medium used to transmit between the microcontrollers uses copper cabling of 100m in length.

VI. Results and Analysis of Experimentation

This section analyses the data obtained from undertaking the experimentation procedure. Table I illustrates the latency for varying packet sizes using an SPI divisor of 4 without security constructs applied. Table I is used as a benchmark as the real-time operation of a closed loop control network without security.

Table I
Total simulated communication latency for a simulated single hop closed loop feedback link without security

Packet size (bytes)	Time (ms)
36 Bytes	180.4
52 Bytes	180.7
84 Bytes	181.7

Data in Figure 2 presents the communication latency generated by software security constructs for a 36 byte packet. The zero on the x-axis reflects the time recorded for no security for a 36 byte packet. It is inferred that the communication latency has increased with longer latency recorded for CCM and TinyAEAD at ten rounds, whilst TinyAEAD at five and three rounds had the smallest impact. TinyAEAD had the least latency overhead of 12% whilst CCM incurred an overhead of 29%.

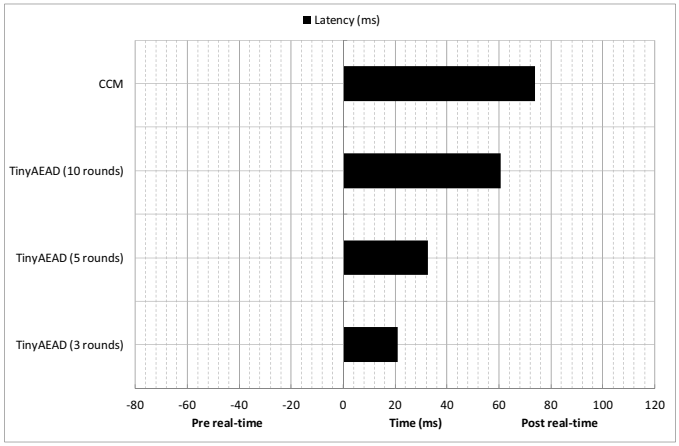


Figure 2. Simulated communication latency for a simulated single hop closed loop feedback link with security (36 byte packet length)

Figure 3 graphs the results using a packet size of 52 bytes. The security constructs examined have shown an increased

in the total communication latency with noticeable difference between TinyAEAD at three rounds and CCM. TinyAEAD at 3 rounds incurred the smallest latency overhead of 25% with CCM incurring the biggest latency overhead of 37%.

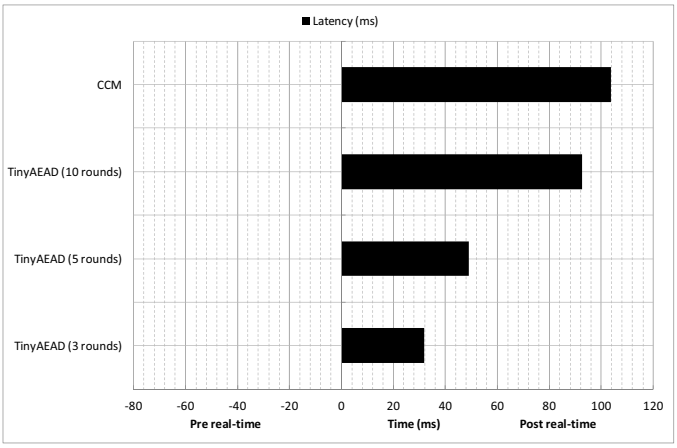


Figure 3. Simulated communication latency for a simulated single hop closed loop feedback link with security (52 byte packet length)

Figure 4 illustrates the impact of software security constructs using an 84 byte packet size. The graphs indicates that CCM and TinyAEAD both running at ten rounds has the biggest increase in the communication latency. TinyAEAD using three rounds has the least communication latency. Tiny AEAD at three rounds has the smallest impact on latency overhead with 33% increase, whilst CCM had the biggest impact on latency with 48% increase.

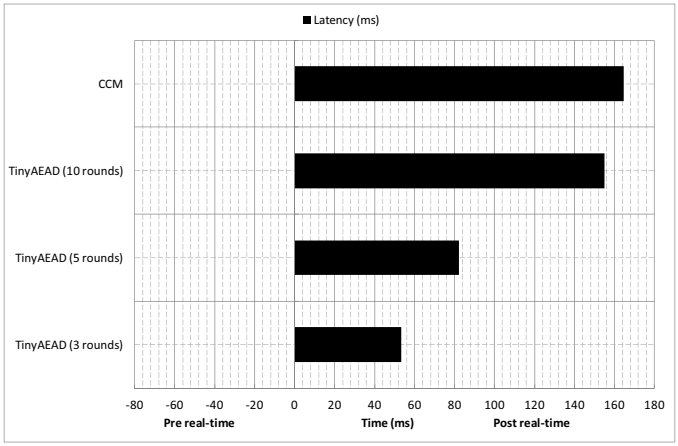


Figure 4. Simulated communication latency for a simulated single hop closed loop feedback link with security (84 byte packet length)

Analysing the results obtained from the experimentation adjustable cryptographic constructs are better suited to minimising communication latency in comparison to standardised constructs. Packet size also influences the latency generated with the smaller packet sizes processed faster than larger sized packet.

VII. Proposed Communication Latency Model

This section introduces the proposed mathematical model to calculate latency introduced by security constructs on communication link of closed loop control. The model is designed to take into consideration factors influencing the overall latency of the system whilst allowing for flexibility for the parameters used; making it advantageous as it can calculate latency for a closed loop control system.

$$\tau l = (\triangle\,(\eta + \delta + \psi)) + \frac{\nu}{\ell} + F \tag{1}$$

Formula 1: Calculating communication latency introduced by security constructs for a single hop closed loop control

The total latency is represented as (τl) with the instruction cycle time (at a specified clock frequency) is (δ). The transmission time of the data is represented as (η) and the time to process a byte of data though the security algorithm is (ψ). The size of the packet is $(\triangle)$ with the propagation delay (e.g. the speed of electrons through a copper cable or the vacuum of the speed of light) represented as (ν). The distance of the link in meters is (ℓ). The round trip time is (F).

VIII. Comparison between Proposed Model and Simulation Results

Utilising the proposed model presented in Formula 1; Table II compares the results obtained from the proposed model against the simulated results. The results take into consideration the latency incurred from the software security construct TinyAEAD at three rounds. A crystal frequency of 8 MHz was sampled. SPI divisors of 4 sampled with packet sizes of 36, 52 and 84 bytes examined.

Table II
Model versus Simulation results for varying packet sizes

Packet Size (bytes)	Proposed model results (ms)	Simulated results (ms)	Difference in results (%)
36	202.3	201.5	0.39
52	213.6	212.5	0.51
84	236	234.1	0.80

Data displayed in Table II compares the outcome achieved from the proposed mathematical model and the simulated tests. Results indicate calculated and recorded results correlate.

Comparison of the proposed mathematical model and the simulation results indicate that the results calculated from the model is within an average percentage of 0.56%. This infers that the model is a good predictor for calculating the communication latency for closed loop control with the inclusion of AEAD security constructs.

Summary of the experimentation conducted indicates that a range of factors influence the communication latency generated. Packet size contributes the total latency with results

indicating the larger sized packets have the biggest increase in latency in comparison to smaller packets. This indicates that protocols with larger payloads may not be best suited to meeting the real-time requirements of closed loop control systems.

IX. Predictive Modelling

This section uses the proposed model as a predictive tool against the results obtained from the simulation. The PIC18F45K22 microcontroller can use a maximum crystal frequency of 64 MHz [12] and the communication latency can be calculated by using the proposed model. The crystal frequency and packet size sampled has strong correlation with the latency output. To validate this hypothesis a contrived scenario has been derived with a PIC18F45K22 microcontroller operating at a crystal frequency of 32 MHz. TinyAEAD at three rounds has been selected as the security construct of choice as it better suited to meeting real-time constraints. Three packet sizes are selected for this test, being 36, 52 and 84 bytes in length. The SPI divisor has been set to 4. σ represents standard deviation in Table III.

Table III
Comparative results of model versus simulation for software implementation of TinyAEAD (3 rounds)

Packet Size (bytes)	Proposed Model Results (ms)	Simulated Results (ms)	Difference in Results (%)	Mean (ms)	σ
36	49.9	50.4	0.97	50.1	0.35
52	51.5	53.1	1.13	52.3	1.13
84	53.4	58.5	5.11	57.1	1.90

From the data obtained in Table III, the model is better suited for predicting the latency for small packet sizes, whilst larger packet sizes show an increased percentage difference between the proposed result and the simulated result. Utilising the specified crystal frequency for this scenario suggests that the real-time constraints in Table I would be meet. It is also inferred that the model is suited to predicting the latency incurred utilising different crystal frequencies.

X. Discussion

Section X examines the potential impact of applying security constructs to the system case scenario presented in Section III. The real-time requirement for this scenario is 25 milliseconds [13] before the pressure begins to incline, therefore this value is used to mimic a real world scenario. The results obtained in Section IX suggest that a 32 MHz crystal frequency was not suitable for meeting the real-time requirements for this context; however, for this case scenario the maximum crystal frequency of 64 MHz has been selected for the PIC18F45K22. A direct comparison between AEAD constructs CCM at ten rounds and TinyAEAD at three rounds were selected with packet sizes samples of 36, 52 and 84 bytes in size selected measure the effect of changing the crystal frequency.

Figure 5 results indicates that the selection of the most suitable security construct is required to meet the real-time requirements of a system with TinyAEAD impacting less on the latency in comparison to CCM.

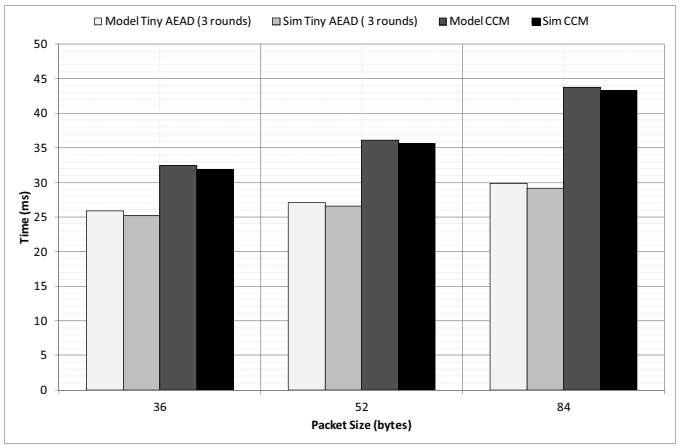


Figure 5. Model versus simulation of security construct impact for case scenario

Data illustrated in Figure 5 suggests that TinyAEAD would meet the real-time constraints using a packet size of 36 byte length only. The results obtained from the mathematical model correlate with the simulation, inferring that this model is applicable for predictive impacts.

As discussed throughout this paper the addition of security constructs on closed loop control increases the latency incurred. A result of missing the real-time constraints could impact on safety and operation of the staff and the plant. Figure 6 shows a consequence of compromising plant safety as shown in the DeBruce Grain Co incident in Haysville, Kansas.

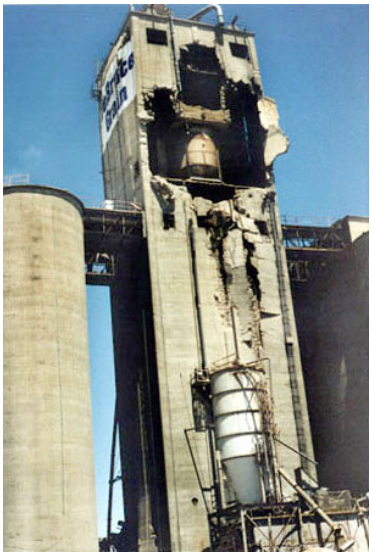


Figure 6. DeBruce Grain Co dust explosion incident [14]

XI. Conclusion

The proposed mathematical model presented in this paper is suitable for calculating the impact of security constructs for varying packet lengths and security constructs. Due to the flexibility of the model users can predict the impact of communication latency with the addition of security constructs applied without having to invest in a simulator or real world closed loop control system.

Concluding from the data obtained the impact of security constructs on closed loop control systems is significant with the overall communication latency increasing. The consequence of inducing delay on a real-time closed loop control system can be catastrophic as presented in the case scenario and therefore raises further questions regarding systems safety.

Consideration of the security construct is crucial towards the latency generated as the incorrect selection can cause a bigger impact on latency, causing disruption to the operation of the system and potential safety implications.

References

[1] A Cardenas, S Amin, and S Sastry. Research challenges for the security of control systems. In *Proceedings of the 3rd conference on Hot topics in security*, 2008.

[2] T Morris and W Gao. Industrial control system cyber attacks. In *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research*, 2013.

[3] M Luallen and D Harp. Breaches on the rise in control systems: A sans survey. Technical report, System Administration, Networking, and Security Institute, 2014.

[4] M. Franekova. Safety and security profiles of industry networks used in safety critical-applications. *Transport Problems*, 4:25–32, 2008.

[5] The Wolfson Centre for Bulk Solids Handling. Pneumatic conveying short course.

[6] Y Ma, W Jiang, N Sang, and X Zhang. Arcsm: A distributed feedback control mechanism for security critical real-time system. In *10th IEEE International Symposium on Parallel and Distributed Processing with Applications*, 2012.

[7] Z Pang and G Lui. Design and implimentation of secure network predictive control systems under deception attacks. *IEEE Transactions on Control Systems Technology*, 20:1334–1342, 2012.

[8] R.A Gupta, AK. Agarwal, Mo-Yuen Chow, and Wenye Wang. Performance assessment of data and time-sensitive wireless distributed networked-control-systems in presence of information security. In *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pages 1–7, 2007.

[9] R. Dhand, G. Lee, and G. Cole. Communication delay modelling and its impact on real-time distributed control systems. In *ADVCOMP 2010 : The Fourth International Conference on Advanced Engineering Computing and Applications in Sciences*, 2010.

[10] Recommendation for block cipher modes of operation: The ccm mode for authentication and confidentiality.

[11] A. Adekunle and S. Woodhead. An aead cryptographic framework and tinyaead construct for secure wsn communication. In *Wireless Advanced (WiAd)*, 2012.

[12] Microchip. Pic18(l)f2x/4xk22 data sheet. Technical report, Microchip Technology Inc, 2012.

[13] H.J Hienrich. Ablauf von gas- und staubexplosionen gemeinsamkeiten und unterschiede. In *Sichere Handhabung brennbare Stäube, Band I, VDI Verlag, W. Germany.*, 1988.

[14] B Sturner, December 1998.

T Appendix T: Study of Two Security Constructs on Throughput for Wireless Sensor Multi-Hop Networks

Conference paper 3: Study of Two Security Constructs on Throughput for Wireless Sensor Multi-Hop Networks

Published in: IEEE 38th International convention on information and communication technology, electronics and microelectronics, Opatija, Croatia

Presented on: 27th May 2015

Abstract: With the interconnection of devices becoming more widespread in society (e.g. internet of things), networked devices are used in a range of environments from smart grids to smart buildings. Wireless Sensor Networks (WSN) have commonly been utilised as a method of monitoring a set processes. In control networks WSN have been deployed to perform a variety of tasks (i.e. collate and distribute data from an event to an end device). However, the nature of the wireless broadcast medium enables attackers to conduct active and passive attacks. Cryptography is selected as a countermeasure to overcome these security vulnerabilities; however, a drawback of using cryptography is reduced throughput. This paper investigates the impact of two software authenticated encryption with associated data (AEAD) security constructs on packet throughput of multiple hop WSN, being counter with cipher block chaining and message authentication code (CCM) and TinyAEAD. Experiments were conducted in a simulated environment. A case scenario is also presented in this paper to emphasise the impact in a real world context. Results observed indicate that the security constructs examined in this paper affect the average throughput measurements up to three hops.

MIPRO 2015, 25-29 May 2015, Opatija, Croatia

Study of Two Security Constructs on Throughput for Wireless Sensor Multi-Hop Networks

R.D.Sparrow, A.A.Adekunle, R.J.Berry and R.J.Farnish
The Wolfson Centre for Bulk Solids Handling Technology,
University of Greenwich,Chatham Maritime,
Chatham, Kent ME4 4TB, England, UK
{r.d.sparrow, r.j.berry, r.j.farnish} @gre.ac.uk

***Abstract*—With the interconnection of devices becoming more widespread in society (e.g. internet of things), networked devices are used in a range of environments from smart grids to smart buildings. Wireless Sensor Networks (WSN) have commonly been utilised as a method of monitoring a set processes. In control networks WSN have been deployed to perform a variety of tasks (i.e. collate and distribute data from an event to an end device). However, the nature of the wireless broadcast medium enables attackers to conduct active and passive attacks. Cryptography is selected as a countermeasure to overcome these security vulnerabilities; however, a drawback of using cryptography is reduced throughput. This paper investigates the impact of two software authenticated encryption with associated data (AEAD) security constructs on packet throughput of multiple hop WSN, being counter with cipher block chaining and message authentication code (CCM) and TinyAEAD. Experiments were conducted in a simulated environment. A case scenario is also presented in this paper to emphasise the impact in a real world context. Results observed indicate that the security constructs examined in this paper affect the average throughput measurements up to three hops.**

***Index Terms*—Networked Control Systems, Wireless Sensor Networks, AEAD constructs.**

I. Introduction

Wireless Sensor Networks (WSN) have commonly been used in control and instrumentation tasks such as obtaining measurements to transmitting data across multiple wireless devices. The application for WSN have been deployed in control systems to remote monitor; however, due to the nature of the wireless broadcast medium utilised , potential attackers could conduct passive and active attacks to compromise the operation of the system [1].

Many challenges and issues have been documented outlining the current vulnerabilities and constraints associated with WSN, including limited computational power, trust of intermediately devices and the physical medium utilised to broadcast data [2]. The requirement for reliability in WSN is critical with a variety of security challenges that require addressing whilst maintaining the operation of the system [3]. High throughput applications are currently utilised over wireless mediums (e.g. video streaming), with emphasis on quality of service (QoS). WSN can be deployed to relay streaming data to devices outside the range of the broadcasting node and maintain an acceptable quality of experience (QoE) for the end user.

This paper investigates the effect of two software security measures on WSN with focus on Authenticated Encryption with Associated Data (AEAD) concept and how their implementation influences packet throughput of a WSN. Reasons for undertaking this investigation is to record the behaviour of packet throughput dependent applications (i.e throughput measures the successful message deliveries over a communication medium) with AEAD constructs implemented over multiple wireless hops. A mathematical model is proposed to predict packet throughput for multiple hop WSN communications.

The structure of this paper is organised as follows: Section II introduces the terms and phrases discussed in this paper and a relevant case scenario. Section III introduces relevant literature, Section IV introduces the proposed mathematical model. Section V discusses the experimentation methodology. Section VI analyses the results obtained from the simulation conducted with comparison against the proposed mathematical model. Section VII examines the mathematical model as a predictive tool. Section VIII discusses the impact in relation to the case scenario Section IX concludes.

II. Preliminary

This section defines the terms used throughout this paper and presents the context of the case scenario. The Authenticated Encryption with Associated Data (AEAD) concept provides symmetric cryptographic security services to transmitted packetised data. AEAD combines confidentiality and integrity resulting in a secure communication channel. Confidentiality as an encrypting function is thought secure if an adversary is unable to distinguish the ciphertexts from a bit string chosen uniformly at random, from the set of all possible bit strings of a specified length, under a chosen plaintext attack. For the purpose of this paper, an integrity check function is thought secure if it is computationally infeasible to perform an existential forgery under an adaptive chosen ciphertext attack.

Two AEAD paradigms are presented in this paper, they are Counter with cipher block chaining (CCM) and

TinyAEAD. CCM is a National Institute of Standards and Technology (NIST) standardised AEAD construct designed to provide integrity and confidentiality using a 128-bit block cipher [4]. The TinyAEAD construct is designed to provide confidentiality and integrity services using block ciphers of various bit lengths [5]. This construct can be configured to run at a reduced specified number of block cipher iterations in order to enhance the processing speed of the construct. In addition TinyAEAD provides flexibility and adaptability that can be applied to a broad range of contexts.

The case scenario selected focuses on a circuit switched WSN multi-hop communication link viewed as using a linear logical network topology. It is assumed that nodes in the link are 100m due to limited battery power to transmit data over this distance, therefore multiple intermediate nodes are required to relay data between the source and destination nodes [6]. Figure 1 illustrates the case scenario.

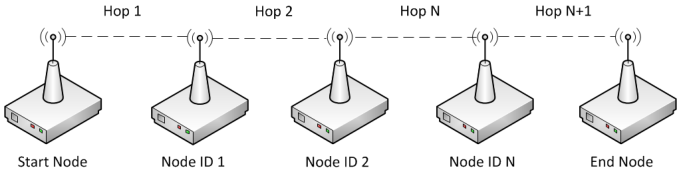


Figure 1. Illustrative concept of a circuit switched linear WSN multi-hop topology

In reference to Figure 1 the Start Node transmits a continuous flow of packets to node ID 1; the data is then transferred over *N* intermediate nodes before reaching the End Node. To secure the data being transmitted between each node, confidentiality, integrity and authentication is applied to prevent adversaries from viewing and modifying data in transit on the communication link; however, a drawback of introducing security is reduced throughput due to the additional processing time of the cryptographic process undertaken at each node during packet propagation.

III. Literature Review

This section introduces relevant literature related to the context of this paper with focus on confidentiality, integrity and authentication for WSN and the current mathematical models utilised to predict packet throughput over multi-hop networks.

Research conducted by Diaz et al [7] examines the attack vectors used against WSN with focus on the impact on power consumption and software execution time. The security vulnerabilities examined by the authors focuses on attacks against the physical and data link layer of the open systems interconnection (OSI) model. Three attack vectors are examined; link-noise, packet injection and direct attacks. Experimentation was conducted using SystemC to model the software execution time. A virtual WSN platform was created to examine collision, interrogation and Sybil attacks to analyse the effect on the power consumption and system performance. Two network topologies were also evaluated in this simulation; linear and mesh networks with each node utilising an ARM 926 processor and 802.15.4 transceiver (Zigbee). Results reported suggest that display power consumption varied depending on the network topology and attack selected.

A journal article presented by Pan et al [8] investigates WSN for healthcare. The main security vulnerability investigated in the article was providing confidentiality and integrity of patients data over a wireless broadcast medium as an attacker can conduct passive and active attacks to monitor and modify confidential data before arriving at its destination. The authors proposed solution uses a Feistel structure with two different methods, the first method incorporates an substitution box (Sbox) and the second method without a Sbox. Each Feistel cipher uses four rounds with a unique 32-bit key called at each round for encryption and decryption. Experimentation of the two Feistel constructs were conducted on an Atmel ATMega128L 8-bit microcontroller operating at 8 MHz crystal frequency. Comparative results against the Data Encryption Standard (DES) cipher suggests that the two Feistel ciphers are more suited to computational constrained WSN as the time taken to operate the encrypt and decrypt functions were faster than DES and memory consumption was also reduced.

An approach undertaken by Vu et al [9] presents a concept for simulation modelling of secure WSN. The focus of the research conducted in this paper examines their own bespoke simulation environment for modelling WSN, with emphasis on secure connectivity between each WSN. The security vulnerability discussed by the authors concentrates on active attack vectors (e.g. man-in-the-middle attacks) to determine what proportion of the WSN links remain secure. Five areas have been configured in the simulator being physical deployment, key establishment, node capture model, network analysis and a graphical user interface. Experimentation conducted by the authors suggests the results obtained for resilience against node capture for model and simulation correlate; however this methodology only take into consideration cryptographic key distribution only.

Research conducted by Marzi and Marzi [10] propose a security model for WSN using trust and reputation models (TRM). The issues highlighted by the authors emphasise the security vulnerabilities incurred by incorporating WSN into a networked environment (e.g. sinkhole attacks) and the computational constraints associated with WSN devices. The proposed solution utilises a Enhanced Bio-inspired Trust and Reputation Model (EBTRM) to calculate which node on the network is the most trustworthy before selecting the node to communicate with. The node also take into consideration if the communication was successful or unsuccessful and factor this into their computational model. Experimentation conducted reviewed the performance of the EBTRM against the Peer Trust System (PTS) and Bio-inspired Trust and Reputation Model (BTRM-WSN) using the TRMSim-WSN simulator. Results indicate that the EBTRM is suited for

selecting the correct trustworthy node in comparison to BTRM-WSN and PTS, even with a high percentage of malicious sensor deployed on the network; however, when compared to the average path length and energy consumption utilised the EBTRM consumed the most energy and took longer wireless paths than the BTRM-WSN approach.

Summary of the literature review undertaken suggests there is a requirement to investigate modern software security constructs suited for WSN as current approaches utilise constructs that are no longer standardised. Secondly, the current models for predicting throughput do not take into consideration the influence of the security constructs selected on the impact of packet throughput; suggesting an approach taking security into consideration is required. This suggests that an investigation is required to examine how modern cryptographic paradigms influences throughput over WSN.

IV. Proposed Mathematical Throughput Model

In this section we propose a mathematical model for predicting the total throughput of packets transmitted across multiple node WSN. The mathematical model presented in this paper utilises the exponential decay function to calculate the change of packet throughput over time (packets per second) for each wireless hop. This model takes into consideration that the wireless nodes would have no knowledge of the previous packet arrival (i.e. the amount of packets arrived at the previous hops), thus making the process memoryless. In addition it is assumed that the packet arrivals do not occur simultaneously, therefore, orderliness has been factored into this model.

The model is calculated by adding the initial packet throughout value for the initial start hop (N_o) divided by the time frame selected in seconds (e.g. per minute) (t) to calculate the packet arrival rate. The inverse of the value is obtained using -1/($\frac{N_o}{t}$) before using the value with the exponential function (e). The value obtained is then multiplied by the total throughput value of the previous wireless hop packet throughput (N_o) to calculate the rate change in packet throughput (r).

$$r = N_o e^{(-1/(\frac{N_o}{t}))} \tag{1}$$

Equation 1: Exponential decay calculation for estimating throughput rate of change per wireless hop

The final calculation is to subtract r from N_o to derive the new packet throughput measurement for N_{o+1} as formulated in Equation 2.

$$N_{o+1} = N_o - r \tag{2}$$

Equation 2: Calculation for estimating throughput per wireless hop

V. Experimentation Methodology

This section discusses the apparatus, metrics and context selected for the experimentation methodology. The programme selected is Proteus ISIS 8 professional with an emulated Microchip PIC18F45K22 selected as the microcontroller. The Serial Peripheral Interface (SPI) is selected as the physical layer (e.g. OSI model) to transmit and receive messages between each microcontroller on the WSN. The AEAD security algorithms used are CCM and TinyAEAD running AES (128-bit key variant). The communication channel for this experiment is simulated.

The experimentation methodology is used for observing packet throughput for ranging multiple nodes with and without software security measures applied. Packets are sent continuously and counted by the last hop device to measure how many packets have arrived at its destination within one minute time sample. All timings and packet throughput counts were taken from the simulator used. It is assumed for this scenario that no noise is present on the wireless channel and consequently all packets transmitted are received without loss or corruption.

Metrics used for the experimentation are seconds for the time frame of the experiment. The packet throughput is counted to measure how many packets arrived in the time frame and number of nodes to state how many intermediate devices were between the start and end node.

Configuration of the components selected are as follows, the crystal frequency selected is 4 MHz to replicate low powered industrial microcontrollers with packet sizes of 36, 52 and 84 bytes. A SPI divisor of 16 is chosen to replicate bandwidth of a wireless link of 250Kbps [11] as calculated using the formula obtained from previous research [12]. It is assumed that a 100m distance is between each wireless node. The experimentation methodology varied the number of intermediate nodes on the linear network, starting from one node to the maximum of five nodes.

VI. Results and Analysis of Experimentation

This section analyses the results obtained from the experimentation methodology discussed in the aforementioned section. Figure 2 illustrates the total throughput for a packet size of 36 bytes. Results presented in Figure 2 suggests that the number of intermediate nodes influences the total amount of successful packets being received within the time frame for a 36 byte packet with one hop showing the largest throughput count and five hops showing the smallest throughput count. The packet size has minimal impact based on the data presented. TinyAEAD at three rounds has a smaller impact on throughput than CCM.

Figure 3 presents data obtained from increasing the packet size to 52 bytes. The data indicates that security has reduced the throughput up to three nodes with CCM having the least throughput recorded. The larger hop counts show a minimal effect on the total throughput readings.

The data in Figure 4 represents results obtained for a 84 byte packet size. The results indicate CCM has a greater impact on

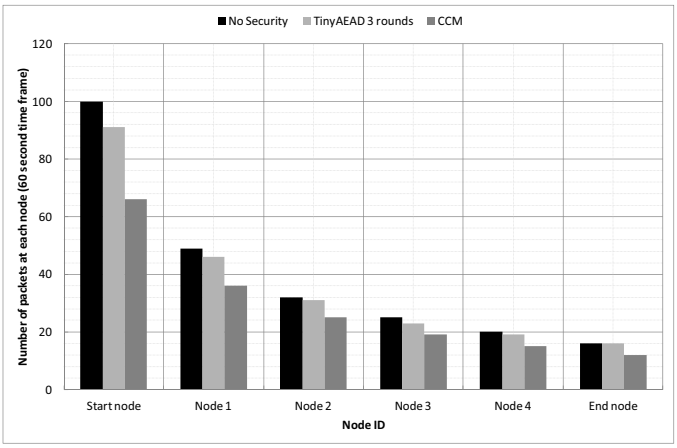


Figure 2. Simulation results for 36 byte packet lengths over multiple intermediate nodes for a sixty second time frame

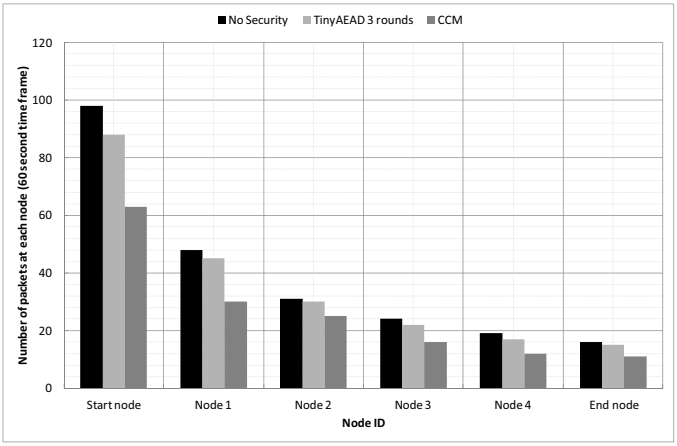


Figure 3. Simulation results for 52 byte packet lengths over multiple intermediate nodes for a sixty second time frame

the total throughput; it is also illustrated that larger packet sizes has ta larger decrease on throughput values in comparison to smaller packet sizes.

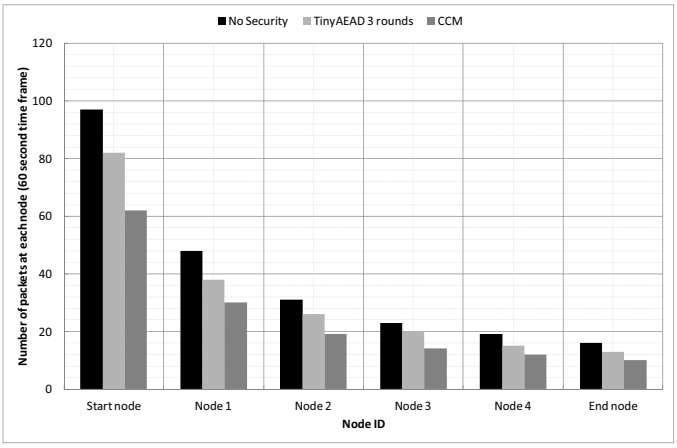


Figure 4. Simulation results for 84 byte packet lengths over multiple intermediate nodes for a sixty second time frame

The number of rounds utilised by the underlying block cipher used by the AEAD algorithms has a direct effect on the throughput values generated as the AEAD algorithms operating at reduced number of rounds outputted more packets in comparison to specified maximum number of rounds.

The quantity of intermediate nodes between the source and destination also has an influence on the total throughput value as the more nodes that were present in the network, the larger the reduction in the packet throughput; however, the AEAD algorithms had a greater impact for nodes closest to the Start Node, whilst nodes further away from the Start Node endured a minimal impact, suggesting that multiple hop wireless propagation over three nodes are suited to operating at stronger security configuration as the degradation of the packet throughput is reduced, whilst lower hop counts below three nodes are suited to lower security parameters as the effect on throughput is more noticeable.

Analysis of the results obtained from the simulation and the results acquired from the mathematical model is presented in Table 1. Table I compares the results for a 36 byte packet size over varying hop counts using a 250Kbps link.

Table I
NO SECURITY THROUGHPUT COMPARISON OF MATHEMATICAL MODEL VS SIMULATION (36 BYTES)

NUMBER OF NODES	SIMULATION RESULTS (PACKETS)	MODEL RESULTS (PACKETS)	CORRELATION COUNT
Start node	97	97	0.9998
1	48	52	
2	31	35	
3	23	28	
4	19	24	
5	16	22	

Data displayed in Table I suggests that the mathematical model correlates with the simulation results obtained up to three nodes. Correlation analysis indicates that the mathematical model and simulation results have a positive linear correlation. Table II shows the comparison data obtained from using TinyAEAD at three rounds.

Table II
TINYAEAD THREE ROUND THROUGHPUT COMPARISON OF MATHEMATICAL MODEL VS SIMULATION (36 BYTES)

NUMBER OF NODES	SIMULATION RESULTS (PACKETS)	MODEL RESULTS (PACKETS)	CORRELATION COUNT
Start node	91	91	0.9989
1	46	47	
2	31	33	
3	23	27	
4	19	24	
5	16	22	

Results in Table II indicates that the mathematical model correlates with the simulation up to three nodes. Correlation analysis suggests a positive linear correlation between the simulation and mathematical model. Table III compares data

obtained from simulation and modelling for CCM.

Table III
CCM THROUGHPUT COMPARISON OF MATHEMATICAL MODEL VS SIMULATION (36 BYTES)

NUMBER OF NODES	SIMULATION RESULTS (PACKETS)	MODEL RESULTS (PACKETS)	CORRELATION COUNT
Start node	66	66	0.9605
1	36	26	
2	25	23	
3	19	21	
4	15	19	
5	12	18	

Data illustrated in Table III indicates that the mathematical model is suited up to three nodes before difference increases. The correlation count between the simulation and mathematical model indicates a positive linear correlation between the two data samples.

Reviewing the comparison between the mathematical model and the simulation results, data obtained indicates that the mathematical model is better suited for calculating the throughput expected up to three nodes, this indicates that the mathematical model error increases as the number of nodes increases. Correlation analysis of the data obtained suggests the model and simulation have a positive correlation with no security and adjustable AEAD algorithms, whilst fixed AEAD algorithms have a lower positive correlation.

VII. PREDICTIVE MODELLING

This section utilises the mathematical model as a prediction tool for the total packet throughput over a select number of nodes over a period of time. Two experiments were conducted, first the prediction of throughput values over six nodes for varying packet sizes and security algorithms. A second experiment assesses the viability of the model as a predictive tool by varying the packet size, time frame, number of hops and rounds used by TinyAEAD. Table IV displays the data obtained for packet throughput values over six hops for a time frame of sixty seconds. The predictions were obtained using the first hop packet throughput value for each packet size and security construct obtained in Figures 2, 3 and 4 as a base reference for the variables used for the calculation.

Table IV
MATHEMATICAL MODEL VS SIMULATION RESULTS FOR THROUGHPUT MEASURED OVER INCREASED MULTIPLE NODES

NUMBER OF NODES	SECURITY CONSTRUCT	PACKET SIZE (BYTES)	PREDICTIVE MODEL RESULTS (PACKETS)	SIMULATION RESULTS (PACKETS)
6	CCM	36	11	16
7	TINYAEAD 3 ROUNDS	52	12	19
8	TINYAEAD 5 ROUNDS	84	7	12
9	TINYAEAD 10 ROUNDS	36	8	14

Results obtained from the predictive model and the simulation results suggest that the results do not correlate, this suggests that the mathematical model is not suited for predicting over five nodes. Table V tabulates data obtained from varying the time frame, rounds used for the underlying block cipher for TinyAEAD, size of the data packets and number of nodes were selected to indicate the viability of the mathematical model as a predictive tool.

Table V
MATHEMATICAL MODEL VS SIMULATION RESULTS FOR THROUGHPUT MEASUREMENTS OVER VARYING PARAMETERS

	TINYAEAD 3 ROUNDS	TINYAEAD 5 ROUNDS	TINYAEAD 10 ROUNDS
NUMBER OF HOPS	2	3	4
PACKET SIZE (BYTES)	36	52	84
SAMPLING TIMES (S)	120	180	240
PREDICTIVE MODEL RESULTS (PACKETS)	93	76	62
SIMULATION RESULTS (PACKETS)	92	80	63

Data presented in Table V indicates that the predictive results obtained from the proposed model correlate with the simulation results.

VIII. DISCUSSION

This section discusses the results obtained from experimentation and how they influence the case scenario of WSN previously discussed in Section II. To clarify how security impacts on packet throughput, Figure 5 graphs the instantaneous throughput measurements for a packet size of 36 bytes.

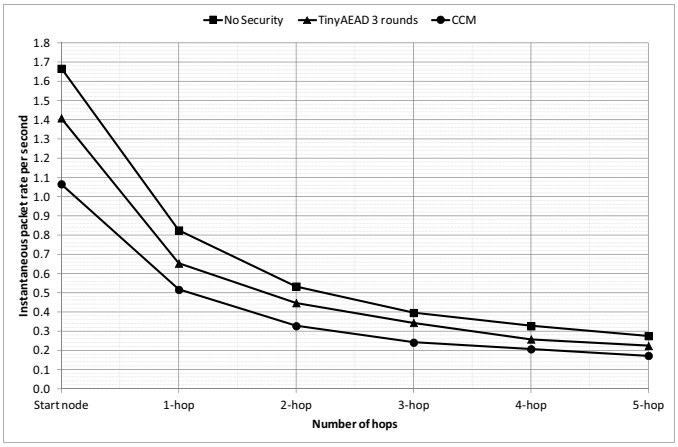


Figure 5. Instantaneous throughput measurements for 36 byte packet lengths over a sixty second time frame

Trends graphed in Figure 5 suggests that implementing security algorithms influences the initial rate of packets received

in the given time frame as no security has the highest throughput rate per second, however, the selection of the security algorithms also influences the instantaneous packet rate as TinyAEAD at three rounds outputs 0.3 packets per second faster than CCM from the initial start hop. The percentage difference between no security and CCM from the start node is 35% whilst the percentage difference between TinyAEAD and no security is 19%. This suggests that the initial impact of security algorithms on throughput is offset from the start node and propagates over multiple hops.

IX. Conclusion

The proposed mathematical model presented in this paper is suitable for calculating the impact of security algorithms using varying packet lengths and security algorithms up to four nodes in length. The amount of intermediate nodes on the network has influence on packet throughput measurements obtained with the number of packet arriving at each hop decaying exponentially; this indicates that the rate of throughput decreases with the increase in intermediary nodes.

Concluding from this investigation undertaken, it has been identified that the use of current standardised fixed AEAD algorithms impact on the throughout of WSN in comparison to adjustable AEAD algorithms, suggesting that current standardised AEAD algorithms using fixed parameters are not as suited in comparison to adjustable AEAD algorithms if packet throughput is a priority.

The mathematical model proposed contributes towards predicting the effect of security algorithms for variable sized WSN for a range of sampling time frames in simulation. Future work will validate the findings obtained on real world platform.

References

[1] A Blilat, A Bouayad, N Chaoui, and M El Ghazi. Wireless sensor network: Security challenges. In *Network Security and Systems (JNS2), 2012 National Days of*, pages 68–72, April 2012.

[2] S. Ahmad Salehi, M.A Razzaque, P. Naraei, and A Farrokhtala. Security in wireless sensor networks: Issues and challanges. In *Space Science and Communication (IconSpace), 2013 IEEE International Conference on*, 2013.

[3] K. Islam, Weiming Shen, and Xianbin Wang. Wireless sensor network reliability and security in factory automation: A survey. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 42(6):1243–1256, November 2012.

[4] Recommendation for block cipher modes of operation: The ccm mode for authentication and confidentiality.

[5] A. Adekunle and S. Woodhead. An aead cryptographic framework and tinyaead construct for secure wsn communication. In *Wireless Advanced (WiAd)*, 2012.

[6] R Purta, S Nagrecha, and G Madey. Multi-hop communications in a swarm of uavs. In *Proceedings of the Agent-Directed Simulation Symposium*, 2013.

[7] A Diaz, P. Sanchez, J. Sancho, and J. Rico. Design, automation test in europe conference exhibition. In *Wireless sensor network simulation for security and performance analysis*, pages 432–435, 2013.

[8] J. Pan, S. Li, and Z Xu. Security mechanism for a wireless-sensor-network based healthcare monitoring system. *Communications, IET*, 6(18):3274–3280, Dec 2012.

[9] Tuan Manh Vu, Carey Williamson, and Reihaneh Safavi-Naini. Simulation modeling of secure wireless sensor networks. In *Proceedings of the Fourth International ICST Conference on Performance Evaluation Methodologies and Tools*, 2009.

[10] H. Marzi and A Marzi. A security model for wireless sensor networks. In *Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2014 IEEE International Conference on*, 2014.

[11] Texas Instruments. 2.4 ghz ieee 802.15.4 / zigbee-ready rf transceiver, 2014.

[12] R Sparrow, A Adekunle, J Berry, R, and J Farnish, R. Simulating and modelling the impact of security constructs on latency for open loop control. In *Sixth Computer Science and Electronic Engineering Conference 2014 (CEEC'14)*, 2014.

U Appendix U: Balancing Throughput and Latency for an Aerial Robot over a Wireless Secure Communication Link

Conference paper 4: Balancing Throughput and Latency for an Aerial Robot over a Wireless Secure Communication Link

Published in: IEEE 2nd International Conference on Cybernetics CYBCONF 2015, Gdynia, Poland

Presented on: 25th June 2015

Abstract: With the requirement for remote control of unmanned aerial vehicles (UAV) becoming more frequent in scenarios where the environment is inaccessible or hazardous to human beings (e.g. disaster recovery); remote functionality of a UAV is generally implemented over wireless networked control systems (WNCS). The nature of the wireless broadcast allows attackers to exploit security vulnerabilities through passive and active attacks; consequently, cryptography is often selected as a countermeasure to the aforementioned attacks. This paper analyses simulation undertaken and proposes a model to balance the relationship between throughput and latency for a secure multi-hop communication link. Results obtained indicate that throughput is more influential up to two hops from the initial transmitting device; conversely, latency is the determining factor after two hops.

Balancing Throughput and Latency for an Aerial Robot over a Wireless Secure Communication Link

R.D.Sparrow, A.A.Adekunle, R.J.Berry and R.J.Farnish
The Wolfson Centre for Bulk Solids Handling Technology,
University of Greenwich,Chatham Maritime,
Chatham, Kent ME4 4TB, England, UK
{*r.d.sparrow, a.a.adekunle, r.j.berry, r.j.farnish*} *@gre.ac.uk*

***Abstract*—With the requirement for remote control of unmanned aerial vehicles (UAV) becoming more frequent in scenarios where the environment is inaccessible or hazardous to human beings (e.g. disaster recovery); remote functionality of a UAV is generally implemented over wireless networked control systems (WNCS). The nature of the wireless broadcast allows attackers to exploit security vulnerabilities through passive and active attacks; consequently, cryptography is often selected as a countermeasure to the aforementioned attacks. This paper analyses simulation undertaken and proposes a model to balance the relationship between throughput and latency for a secure multi-hop communication link. Results obtained indicate that throughput is more influential up to two hops from the initial transmitting device; conversely, latency is the determining factor after two hops.**

***Index Terms*—Unmanned Aerial Vehicles, Throughput, Latency, Security, Wireless .**

I. Introduction

Wireless Networked Control Systems (WNCS) have been commonly utilised to allow users to control the actions of an actuator remotely (e.g. unmanned aerial vehicles (UAV). Networking parameters are an important aspect of WNCS as control applications are sensitive to time delays and interferences [1], that affect the reliability and availability of the control systems. The broadcast nature of wireless communications poses security vulnerabilities that could be exploited through passive and active attacks.

With the integration of networks and control paradigms for WNCS, the balancing of these two paradigms is required to optimise the operational efficiency of the control network. This paper analyses simulation undertaken and proposes a model to balance the relationship between throughput and latency for a secure multi-hop communication link. The secure channel is provided by a cryptographic technique refereed to as Authenticated Encryption with Associated Data (AEAD).

The structure of this paper is organised as follows: Section II introduces the terms and phrases discussed in this paper. Section III discusses the case scenario used for this study, Section IV introduces relevant literature to the problem domain discussed. Section V outlines the experimentation procedure with Section VI discussing and analysing the results obtained from simulation. Section VII introducing the proposed mathematical model for predicting instantaneous throughput over multi-hop communication links. Section VIII undertakes comparative analysis of the proposed mathematical model with the simulation conducted. Section IX discusses the impact in relation to the case scenario. Section X concludes.

978-1-4799-8322-3/15/$31.00

II. Preliminary

This section defines the terms used throughout this paper.

- *Instantaneous Throughput*: in this paper instantaneous throughput is the amount of successfully delivered data packets at each node of a multi-hop communication link, measured in packets per minute.
- *Latency:* in this paper latency is the minimum propagation time on all electromagnetic signals imposed by the speed of light. This is summarised as $t = s/c_m$where t is equal to time, s is equal to the distance and c_m is equal to the speed of the medium.
- *Confidentiality:* Confidentiality in this paper refers to using encipherment methods in order to thwart an unauthorised entity understanding and changing the content of the payload of the data frames transmitted over the wireless communication channel.
- *Integrity:* In this paper integrity is determining whether communicated data has been altered in transit over the wireless communication channel between the first node to the end node.
- *Authentication:* The proof that a device on the network is legitimately eligible to communicate with other eligible devices on the same network.
- *AEAD concept:* The Authenticated Encryption with Associated Data (AEAD) concept provides both symmetric cryptographic security data services to transmitted packetised data. The security service combines confidentiality and integrity consequenting a

secure communication channel.

- *Balancing:* In this paper balancing refers to the distance that throughput is intersected by latency.

- *Quality of Service (QoS):* is to provide guarantees on the ability of a network to deliver predictable results (e.g. video stream from the UAV).

- *Quality of Experience (QoE):* the user's perspective of the overall value of the service provided, this is factored as response time for the UAV to change direction of flight.

III. Case Scenario

This section discusses a relevant case scenario applicable to context of this paper. The scenario introduces an application using WNCS where the requirement for throughput and latency is required to be optimal. WNCS have been used to control and operate actuators from a remote location; the scenario selected, is one where a fixed wing UAV is remotely piloted. Figure 1 illustrates the wireless open loop control scenario.

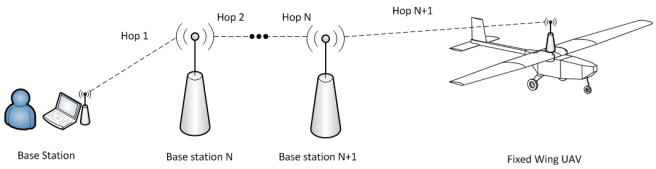


Fig. 1. Wireless open loop control scenario

Figure 1 shows a multi-hop propagation method to transmit control messages to the associated UAV. In this scenario command and control packet are transmitted at regular intervals from the controlling device to the UAV through a varying number of intermediate nodes. The relationship examined in this scenario is throughput and latency as the duration for packets being transmitted and received by the end node influences the response time of the UAV being controlled. With the wireless broadcast transmitting to devices within proximity, an attacker could passively monitor data between the start and end point and actively attack the link through multiple security vulnerabilities (e.g. replay attacks). The inclusion of confidentiality, integrity and authentication to provide a secure communication channel influences throughput and latency measurements, resulting in delay of commands being executed by the UAV. Motivation for conducting this research is to find the optimal balance between throughput and latency for WNCS.

The increase in latency affects the response time of an action from executing, this impacts the manoeuvrability of the UAV craft, thus affecting the QoE. Adjustment to throughput influences the UAV by the bandwidth consumption of the wireless link to transmit and receive messages over multiple wireless hops; influencing the power consumption of the UAV to transmit and receive messages and the QoS (i.e video stream from the UAV).

IV. Literature Review

This section introduces relevant literature to the context of this paper with focus on throughput, latency and security for wireless multi-hop open loop control systems. The literature review is sectioned into three parts, first the current approaches undertaken by other researchers, second the introduction of the AEAD constructs and finally a conclusion of the literature undertaken.

Douglas et al [2] introduce a high throughput path metric for multi-hop wireless routing by proposing their expected transmission count (ETX) metric. The ETX metric proposed by the authors differs from the minimum hop-count examined in this paper as characteristics of the link are taken into consideration, including link loss ratio, asymmetric loss ratio and interfacing with successful hops of multi-hop paths. These factors are utilised by the ETX metric to predict the total amount of packet retransmissions required per link. Experimentation conducted by the authors detail a schematic of a building using a 29-node wireless test-bed; each node is positioned on different floors and locations within the building. Each node utilises a Linux operating system with 802.11b wireless standard using an omni-directional antenna configured to transmit at 1Mbps and 1mW transmission power. Packet size of 193 bytes in total was sampled using the dynamic source routing protocol (DSR) and destination-sequenced distance vector routing protocol (DSDV). Results obtained from the experimentation procedure infers that the ETX procedure is better suited for finding higher throughput routes in comparison to minimum hop-count with a stronger correlation identified between the best static route and ETX. The authors have discussed that the ETX metric could be improved to take into consideration different packet sizes and bit-rates as results presented in this paper only considers fixed values.

Research conducted by Quang et al [3] examines the performance analysis of packet loss on WNCS. Problems examined by the authors investigate how packet loss impacts on the performance of the WNCS. The solution proposes a predictive algorithm for the Peripheral Integral Derivative (PID) at the forward loop to compensate the packet loss incurred. The authors use Matlab to simulate the effects of packet loss and how this influences the scenario examined, being an inverted pendulum system. Results graphed by the authors do not show clarity to the actual effects of packet loss on wireless networked control systems and whether their approach is suited to mitigate the effects of packet loss on a WNCS. The experimentation procedure and metrics utilised for this paper have not been specified to verify how packet loss can be overcome and how packet corruption influences

the operation of the control system.

Cai et al [4] discuss the challenge proposed with smart grid security in view of of Intelligent Electronic Devices (IED) for users to access the distribution level of the power network. Challenges discussed involve the design of network topology and security techniques for the network to fulfil reliability and real-time requirements. Vulnerabilities identified by the authors discuss the impact of a Distributed Denial of Service (DDOS) attack against smart grids with remote attackers transmitting additional packets to the control device. The solution proposed in this research adopts the Trustworthiness based Quality of Service (TQOS) routing protocol to ensure secure transmission is achieved. It is also stated that the use of symmetric encryption and decryption algorithm for the Supervisory Control And Data Acquisition (SCADA) command message it deployed, this comprised of a keyed-Hashed Message Authentication Code (HMAC). The simulation test platform Opnet was selected to conduct experimentation by replicating the TQOS protocol on point to point intelligent energy management (IEM) topology. Two topologies are created using eight and twenty four IEM nodes with different amount of attacking nodes deployed in each scenario. Variables analysed in this experiment are the communication end to end delay, varying encryption key lengths, processing speed of the CPU and security cost in terms of delay. The experimental testing conducted focused on the mathematical and simulation approach.

Research undertaken by Cheng et al [5] examine maximising throughput of UAV relaying networks with the load carry and deliver programme. The authors proposes a method of maximising throughput for delay tolerant networks called the "load-carry and deliver" (LCAD) and utilise this approach to understand the important factors contributing to a throughput maximising framework. The LCAD networking paradigm uses UAVs to relay packets between a source ground node and destination ground node over one or multiple UAV. Experimentation conducted by the authors uses a real world UAV fitted with an 802.11g wireless transceiver utilising a dipole antenna; with two computers for the source ground node and destination ground node. The UAV path for the flight experiment is conducted by a human pilot directing the UAV in a oval flight path of 700 yards (640m) long and 25 yard (23m) wide; each of the source and destination nodes are 550 yards (503m) apart. A fixed transmission rate of 6Mbps was selected with packet sizes of 1,500 bytes over the User Datagram Protocol over Internet Protocol (UDP/IP). Results obtained indicate that packet loss was more noticeable during the delivery stage from the UAV to the destination node as the time offset increases in comparison to the load stage. Finally the authors propose an empirical model that predicts link performance. This model takes into consideration factors including distance between the UAV and ground nodes and elevation angle of the UAV during flight. Results obtained suggest the model is robust in predicting the link performance at the physical layer of the Open Systems Interconnection model (OSI) stack over a single hop.

This paragraph introduces the AEAD concepts with two paradigms being presented; the fixed standardised approach of Counter with cipher block chaining (CCM) and the adjustable and flexible approach of TinyAEAD. CCM is a National Institute of Standards and Technology (NIST) standardised AEAD construct designed to provide integrity and confidentiality using a 128-bit block cipher [6]. The TinyAEAD construct is designed to provide confidentiality and integrity services using block ciphers of varying bit length [7]. This construct can be configured to run at a reduced specified number of block cipher iterations in order to enhance the processing speed of the construct. In addition TinyAEAD provides flexibility and adaptability that can be applied to a broad range of contexts.

Concluding from the literature review undertaken, methods undertaken by existing researchers focuses on the effect of packet loss or algorithms derived to reroute traffic based on traffic throughput metrics. Investigation to link performance has been discussed in the literature review at the physical layer; however, further research is required to understand the impact at the data link layer. Discussion of throughput models in the literature emphasise on single hop throughput only, further investigation is required to understand the effect over multi-hop. Minimal discussion of security countermeasures for WNCS has been presented in terms of suitability and effects on the control system. This paper investigates the balance between networking, security and control paradigms for WNCS through simulation and modelling as an indicator before consideration for real world experimentation.

V. Experimentation Procedure

This section discusses the apparatus, metrics and context selected for the experimentation. The simulation programme selected is Proteus ISIS 8 professional with the Microchip PIC18F45K22 selected as the microcontroller. The Serial Peripheral Interface (SPI) is selected as the physical layer (i.e. OSI model) to transmit and receive messages between each microcontroller on the WSN. The AEAD security constructs used are CCM and TinyAEAD running AES (128-bit key variant).

The experimentation structure examines the latency for the transmitting microcontroller to process and transmit the packet, the duration of the packet to propagate to the receiving microcontroller and to process the received packet. The impact of the software security constructs on latency is measured in milliseconds. All timings are taken from the simulator used.

Throughput is observed over multiple hops with and without software security measures applied. Packets are counted by the last hop device to measure how many packets have arrived at its destination within one minute time

sample. All timings and counting recorded are taken from the simulator used. It is assumed for this scenario that no noise is present on the wireless channel.

Metrics utilised for the test procedure are seconds for the sampling time of the test, packet count to measure how many packets arrived in the sample time and number of hops to state how many intermediate devices were between the start and end node.

Configuration of the components selected are as follows, the crystal frequency selected is 4 MHz to replicate low powered industrial microcontrollers with packet sizes of 36 and 84 bytes. A SPI divisor of 16 is chosen to replicate bandwidth of a wireless link of 250Kbps [8] as calculated using the following formula [9]. It is assumed that each hop is 100m. The test procedure varied the number of intermediate hops on the linear network, starting from one hop to the maximum of six hops. Sample time of sixty seconds was selected.

VI. Results and Analysis of Testing

Section VI reviews the results obtained from the test procedure discussed in Section V. The graphs presented draw comparison of latency induced for processing and transmitting packets against the instantaneous throughput measurements. The graphs in this section draws latency and throughput data for packets with no security and packets with security constructs. Figure 2 illustrates data obtained from latency versus throughput for a 36 byte packet size, the solid lines represent latency (left y-axis), the dashed lines represent throughput (right y-axis).

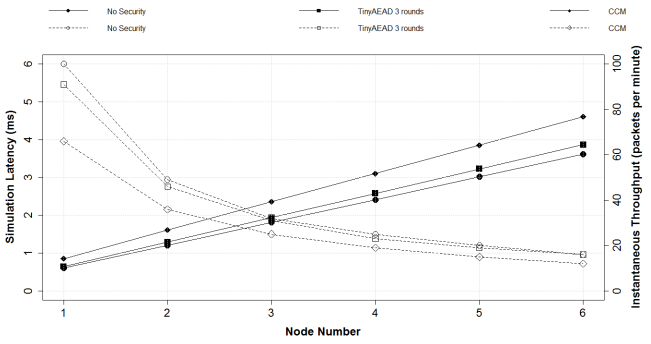


Fig. 2. Simulation results of throughput and latency for a 36 byte packet. Node 1 is the start node, Node 6 is the end node. The first hop is from Node 1 to Node 2

Data obtained in Figure 2 suggests that latency has minimal impact on instantaneous throughput up to two hops; however after three hops the latency influences the instantaneous throughput as the rate of decline reduces significantly. With latency increasing in relation to number of hops, the instantaneous throughput measurements for packets with no security and security begin to converge with TinyAEAD at three rounds obtaining the same instantaneous throughput measurements as no security. The instantaneous throughput difference between CCM and the other two approaches also reduces over the number of hops. Figure 3 illustrates the latency and instantaneous throughput trade off for a 84 byte packet size, the solid lines represents latency (left y-axis), the dashed lines represents instantaneous throughput (right y-axis)

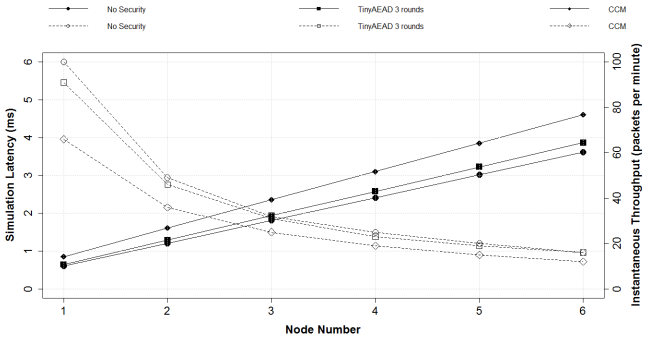


Fig. 3. Simulation results of throughput and latency for a 84 byte packet. Node 1 is the start node, Node 6 is the end node. The first hop is from Node 1 to Node 2

Results displayed in Figure 3 infer that latency has a reduce impact on instantaneous throughput up to two hops for no security an TinyAEAD at three rounds, however, latency for CCM intersects with the instantaneous throughput measurement for CCM before the second hop; this suggests that latency for CCM utilising a 84 byte packet has a larger impact than instantaneous throughput from two hops onwards.

Summarising from the tests conducted suggests the balance for optimised WNCS is two hops with throughput having priority before two hops; after two hops latency has more influence over throughput with the number of packets decreasing. The size of the packet also impacts on when the change between throughput and latency occurs as CCM using an 84 byte packet is only suited for one hop communications, whilst CCM using a 36 byte packet is better suited up to two hops.

The total throughput obtained over multiple hops obtained in Figure 2 and Figure 3 infers that convergence starts to occur as the number of hops increases; suggesting that even with the initial packet offset incurred from implementing security constructs ; the total throughput will equal the same with and without security the more intermediate node there are. This is particularly noticeable in Figure 2 as TinyAEAD at three rounds and no security converge on the sixth hop and CCM initial difference is reduced as the number of intermediate device increases.

VII. Proposed Model

This section proposes a mathematical model aimed for predicting the total throughput transmitted across multiple node WNCS. Motivation of deriving the proposed model is to

predict the total number of packets expected to arrive at the next hop without the requirement for conducting simulation or real world experimentation. Utilising this approach is cost effective and also reduces the time consumed to obtain and analyse data.

The mathematical model presented in this paper utilises the exponential decay function to calculate the change of the throughput measurement for each wireless hop. This model takes into consideration that the wireless nodes would have no previous knowledge of the previous packet arrival, thus making the process memoryless. In addition it is assumed that the packet arrivals do not occur simultaneously, therefore, orderliness has been factored into this model. Equation 1 shows the proposed model.

$$r = N_o e^{(^{-1}/(\frac{N_o}{t}))} \tag{1}$$

Equation 1: Exponential decay calculation for estimating throughput rate of change per wireless hop

The instantaneous throughout value for the previous hop is represented by (N_o); time in seconds is (t). $^{-1}/(\frac{N_o}{t})$ represent the inverse from the values calculated in the brackets. The exponential value is (e). The rate change in throughput is represented by (r).

The final calculation is to subtract r from N_o to derive the new throughput measurement for N_{o+1} as formulated in Equation 2.

$$N_{o+1} = N_o - r \tag{2}$$

Equation 2: Calculation for estimating throughput per wireless hop

VIII. Proposed Model versus Simulation

Section VIII draws comparison of the predictive capability of the proposed mathematical model against the simulation results obtained from the testing conducted in Section VI. Figure 4 graphs the comparison for instantaneous throughput with no security, TinyAEAD three rounds and CCM.

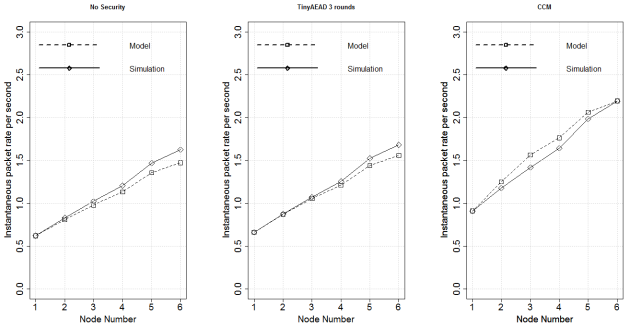


Fig. 4. Simulation versus Model results for throughput for a 36 byte packet

The graphs in Figure 4 show a positive correlation between the model and the simulation results. No security and TinyAEAD at three rounds correlate up to three hops before the model starts to under predict. Comparison between model and simulation for CCM suggests that the model over predicts after the first hop but converges at the sixth hop. Figure 5 displays the results for the simulation and model results for 84 byte packets.

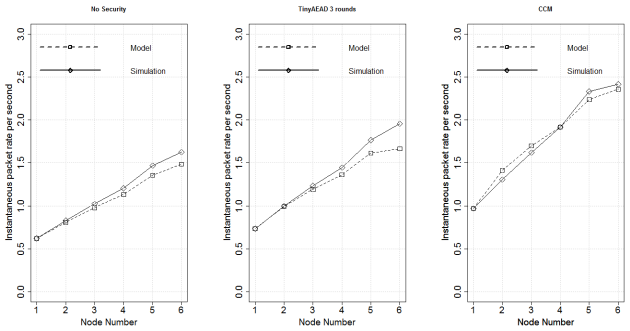


Fig. 5. Simulation versus Model results for throughput for a 84 byte packet

Results illustrated in Figure 5 suggest no security and TinyAEAD at three rounds correlate up to three hops before the model under-predicts the expected instantaneous throughput; however, data obtained for CCM suggests that the simulation and model results are correlated.

To clarify the suitability of the model, Pearson correlation analysis is selected as a statistical method to identify the strength of the relationship between the results obtained from the model and simulation, a results of -1 indicates a negative correlation, 0 indicates no correlation and 1 indicates positive correlation. Table 1 tabulates the outcome from the correlation analysis.

TABLE I
Correlation analysis of model and simulation results

Packet Length (bytes)	No Security Results	TinyAEAD 3 Rounds Results	CCM Results
36	0.999	0.998	0.960
84	0.999	0.998	0.968

Data displayed in Table I indicates that the correlation between the model and simulation results is a positive linear correlation, with a stronger correlation noted for no security in comparison to TinyAEAD at three rounds and CCM.

Summary of the comparison undertaken suggests that the proposed model is a good predictor for instantaneous number of packets over multiple wireless hops with a positive linear correlation between each set of results.

IX. Discussion

This section discusses the results obtained from the experimentation undertaken and apply the findings to the case scenario presented in Section III. As previously discussed, the QoS and QoE influence the operation of the UAV but at what distance does this effect become noticeable? To answer this question, the discussion examines the results obtained from the simulation and infers the maximum distance the UAV can travel before throughput and latency are unequal. Table 2 displays the maximum distance travelled by the UAV before the QoS and QoE become unbalanced.

TABLE II
TOTAL DISTANCE FOR BALANCE BETWEEN THROUGHPUT AND LATENCY FOR A 36 BYTE PACKET

CCM	TINYAEAD 3 ROUNDS	NO SECURITY
160m	200m	210m

As displayed in Table II the balance between throughput and latency varies with maximum distance for no security being 200m before the throughput and latency becomes unbalanced, whilst TinyAEAD at three rounds maximum distance is 170m and CCM at 140m. Table 3 tabulates the maximum distance travelled by the UAV for a 84 byte packet.

TABLE III
TOTAL DISTANCE FOR BALANCE BETWEEN THROUGHPUT AND LATENCY FOR A 84 BYTE PACKET

CCM	TINYAEAD 3 ROUNDS	NO SECURITY
140m	170m	200m

Results displayed in Table III indicate that the distance travelled without security applied is up to 200m, whilst TinyAEAD at three rounds is 150m and CCM 100m. It is inferred that security influences maximum parameter for the UAV before the QoS and QoE requirements are no longer fulfilled, resulting in an unresponsive UAV.

Results indicate that security constructs scale the total distance achievable by the UAV before the operation of the UAV is unattainable. It is also noted that security constructs using adjustable methods obtain more distance than fixed security constructs, suggesting that utilising adjustable cryptography is more adequate for aerial robotics.

X. Conclusion

The relationship between throughput and latency in WNCS influences the operation of the UAV with throughput being the determining up to two hops, whilst latency is the determining factor after two hops; inferring that the optimal balance between throughput and latency is achieved at two hops in the multi-hop scenario examined.

Selection of the security constructs is a determining factor on throughput and latency as adjustable security constructs are more suited if throughput is a priority; however, fixed approaches are better suited for WNCS with more intermediately nodes due to the convergence of the throughput measurements over a longer period of time.

The mathematical model presented in this paper is suited towards predicting the instantaneous throughput over a multi-hop communication link packets predicted over multiple intermediate node with and without security applications applied. Data obtained from the mathematical model allows practitioners to predict the throughput measurements without the expense of a simulated test platform or real world WNCS experimentation.

Future work is to conduct the experimentation undertaken in this paper in a real world scenario to verify the findings obtained.

References

[1] Y.A. Millan, F. Vargas, F. Molano, and E. Mojica. A wireless networked control systems review. In *Robotics Symposium, 2011 IEEE IX Latin American and IEEE Colombian Conference on Automatic Control and Industry Applications (LARC)*, 2011.

[2] J. Douglas, S, Daniel Aguayo, John Bicket, and Robert Morris. A high-throughput path metric for multi-hop wireless routing. In *Proceedings of the 9th ACM International Conference on Mobile Computing and Networking (MobiCom '03*, 2003.

[3] Nguyen Vu Anh Quang and Myungsik Yoo. Performance analysis of packet loss on wireless network control systems. In *Information and Communication Technology Convergence (ICTC), 2014 International Conference on*, 2014.

[4] Ziyuan Cai, Yizhou Dong, Ming Yu, and M. Steurer. A secure and distributed control network for the communications in smart grid. In *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on*, 2011.

[5] Chen-Mou Cheng, Pai-Hsiang Hsiao, H.T. Kung, and D. Vlah. Maximizing throughput of uav-relaying networks with the load-carry-and-deliver paradigm. In *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*, 2008.

[6] Recommendation for block cipher modes of operation: The ccm mode for authentication and confidentiality, 2004.

[7] A. Adekunle and S. Woodhead. An aead cryptographic framework and tinyaead construct for secure wsn communication. In *Wireless Advanced (WiAd)*, 2012.

[8] Texas Instruments. 2.4 ghz ieee 802.15.4 / zigbee-ready rf transceiver, 2014.

[9] R Sparrow, A Adekunle, J Berry, R, and J Farnish, R. Simulating and modelling the impact of security constructs on latency for open loop control. In *Sixth Computer Science and Electronic Engineering Conference 2014 (CEEC'14)*, 2014.

V Appendix V: The Affect of Two Cryptographic Constructs on QoS and QoE for Unmanned Control Vehicles

Conference paper 5: The Affect of Two Cryptographic Constructs on QoS and QoE for Unmanned Control Vehicles

Published in: IEEE 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, United Kingdom

Presented on: 25th June 2015

Abstract: Unmanned control vehicles are used for a variety of scenarios where the user can conduct a task from a remote location; scenarios include surveillance, disaster recovery and agricultural farming. The operation of unmanned vehicles is generally conducted over a wireless communication medium. The nature of the wireless broadcast allows attackers to exploit security vulnerabilities through passive and active attacks; consequently, cryptography is often selected as a countermeasure to the aforementioned attacks. This paper analyses simulation undertaken to identify the affect of cryptographic constructs on the Quality of Service (QoS) and Quality of Experience (QoE) of controlling an unmanned vehicle. Results indicate that standardised AEAD cryptographic approaches can increase the additional distance travelled by a unmanned vehicle over multiple hops communications up to 110 meters per second.

2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies

The Affect of Two Cryptographic Constructs on QoS and QoE for Unmanned Control Vehicles

R.D.Sparrow, A.A.Adekunle, R.J.Berry and R.J.Farnish
The Wolfson Centre for Bulk Solids Handling Technology,
University of Greenwich,Chatham Maritime,
Chatham, Kent ME4 4TB, England, UK
{r.d.sparrow, a.a.adekunle, r.j.berry, r.j.farnish} @gre.ac.uk

***Abstract*—Unmanned control vehicles are used for a variety of scenarios where the user can conduct a task from a remote location; scenarios include surveillance, disaster recovery and agricultural farming. The operation of unmanned vehicles is generally conducted over a wireless communication medium. The nature of the wireless broadcast allows attackers to exploit security vulnerabilities through passive and active attacks; consequently, cryptography is often selected as a countermeasure to the aforementioned attacks. This paper analyses simulation undertaken to identify the affect of cryptographic constructs on the Quality of Service (QoS) and Quality of Experience (QoE) of controlling an unmanned vehicle. Results indicate that standardised AEAD cryptographic approaches can increase the additional distance travelled by a unmanned vehicle over multiple hops communications up to 110 meters per second.**

***Index Terms*—Unmanned Vehicles, Security, Wireless, QoS, QoE**

I. Introduction

Unmanned control vehicles have been used in multiple environments where humans are unable to access directly, this include disaster recovery and remote surveillance [1]. Unmanned vehicles operate using manual, semi-autonomous and autonomous control; various implementation of unmanned vehicles have been developed which include Unmanned Aerial Vehicles (UAV) and Unmanned Ground Vehicles (UGV). Wireless relays are used to extend the range between the base station and vehicles [2], however, a secure communication channel is required to prevent known security vulnerabilities being exploited [3].

End users operating the unmanned vehicles require responsive and operational control to maintain guidance and movement of the travelling vehicle. Adjustment to the Quality of Service (QoS) and Quality of Experience (QoE) may disturb the elements contributing towards the operation of the unmanned vehicles; therefore causing uncoordinated and unstable control between the end users and unmanned control vehicle.

This paper examines the balance of QoS and QoE for unmanned vehicles and the implications of providing a secure communication channel on the operation of unmanned vehicles. The paper analyses the impact of secure communications on QoS and QoE over a multi-hop communication link in simulation. The secure channel is provided by a cryptographic technique refereed to as Authenticated Encryption with Associated Data (AEAD).

The structure of this paper is organised as follows: Section II introduces the term, phrases and case scenario used for this study. Section III presents existing literature to the problem scenario discussed, Section IV outlines the experimentation procedure. Section V discusses and analyses the results obtained from simulation with Section VI discussing the impact in relation to the case scenario. Section VII concludes.

II. Preliminary

This section defines the terms used throughout this paper and presents the context of the case scenario. The Authenticated Encryption with Associated Data (AEAD) concept provides symmetric cryptographic security services to transmitted packetised data. AEAD combines confidentiality and integrity resulting in a secure communication channel. Confidentiality as an encrypting function is thought secure if an adversary is unable to distinguish the ciphertexts from a bit string chosen uniformly at random, from the set of all possible bit strings of a specified length, under a chosen plaintext attack. For the purpose of this paper, an integrity check function is thought secure if it is computationally infeasible to perform an existential forgery under an adaptive chosen ciphertext attack.

Two AEAD paradigms are presented in this paper, they are Counter with cipher block chaining (CCM) and TinyAEAD. CCM is a National Institute of Standards and Technology (NIST) standardised AEAD construct designed to provide integrity and confidentiality using a 128-bit block cipher [4]. The TinyAEAD construct is designed to provide confidentiality and integrity services using block ciphers of various bit lengths [5]. This construct can be configured to run at a reduced specified number of block cipher iterations in order to enhance the processing speed of the construct. In addition TinyAEAD provides flexibility and adaptability that can be applied to a broad range of contexts.

The case scenario introduces two applications of unmanned vehicles which are UAV and UGV. Both scenarios use a

978-1-4799-8660-6/15 $31.00 © 2015 Crown Copyright
DOI 10.1109/NGMAST.2015.46

wireless network control systems to control and operate the vehicles from a remote location. A circuit switched multi-hop communication link is selected for the scenarios using a linear logical network topology. The fixed wing UAV scenario is presented in Figure 1.

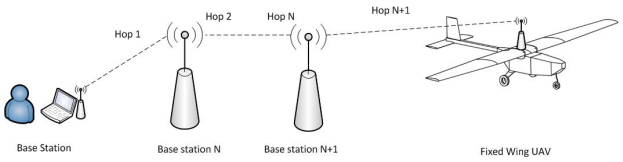


Figure 1. Illustrative concept of a circuit switched linear fixed wing UAV multi-hop topology

A multi-hop propagation method to transmit control messages to the associated fixed wing UAV. In this scenario command and control packet are transmitted at regular intervals from the controlling device to the fixed wing UAV through a varying number of intermediate nodes. A similar scenario for the UGV is presented in Figure 2.

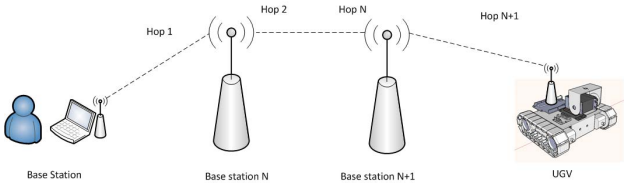


Figure 2. Illustrative concept of a circuit switched linear UGV multi-hop topology

The influence of cryptographic constructs on latency and how this influences on the response time of the unmanned vehicle is examined. As the wireless medium broadcasts to devices within proximity, an attacker could passively monitor data between the start and end point and actively attack the link through multiple security vulnerabilities (e.g. replay attacks). The inclusion of confidentiality, integrity and authentication to provide a secure communication channel influences latency and instantaneous throughput measurements, resulting in the delay of commands executed by the unmanned vehicle. Motivation for conducting this research is to balance QoS and QoE for unmanned control vehicles using secure communications.

The increase in latency affects the response time of an action, this impacts the manoeuvrability of the end device and affect the QoE. Adjustment to throughput influences the end device with the number of packets transmitted and received over multiple wireless hops; this affects QoS services (i.e video stream from the unmanned vehicle).

III. Literature Review

This section introduces relevant literature based on the context of this paper with focus on QoS and QoE for unmanned vehicles. The literature review is sectioned into two parts, first the current approaches undertaken by other researchers, followed by a summary of the literature undertaken.

A method for real-time video relay of UAV traffic surveillance systems through communication networks is proposed by Chen et al [6]. The authors use a UAV for traffic monitoring using a video feed from the UAV which is relayed to a ground station; the ground station forwards the video feed to a mobile communications tower before relaying to its intended destination. Two implementation methods are proposed and tested, first the mobile communication tower forwards the data directly to the end user using wireless communication; the second method forwards the video feed to a host web server before the end user queries the server for the video feed over a wired connection. Results suggests that the server implementation was better suited for limited bandwidth links using lower frames per second whilst higher frames per second on limited bandwidth links are not suited for either implementation method. The authors have also stated that security is a concern.

Bok et al propose a context-aware QoS control for wireless mesh networks of UAVs [7]. The authors discuss the issue of current QoS management methods in the context of UAVs with existing methods focused on the performance of the UAVs in a non-time dependent situation. The proposed solution by the authors uses a context-aware QoS scheme to adjust the priority of the messages based on process patterns. This is achieved by setting a flag value in the IP header to state the QoS priority of the system with a hierarchical mesh network topology to relay communications between the base-station and device on the network. The hierarchical network topology used in this context assigns roles to the UAVs on the network which are nodes and supernodes. Standard nodes use the queue manager for its own outgoing traffic only whilst supernodes communicate directory with the base station and standard nodes in its subgroup and is responsible for forwarding traffic of all nodes in its network. The work presented in this paper represent a prototype of the system.

QoS trade-offs for real-time video has been researched by Hansen and Hissam [8]. The problem examined by the authors is the changing requirements and needs of the end user over the course of time (e.g. emergency and first responder situations). A model is proposed by the authors for managing the QoS requirements as a means of quantifying QoE of the end user by proposing the Distributed Quality of Service Resource Allocation Model (D-Q-RAM). The D-Q-RAM proposes a method for solving optimisation problems in a distributed manner and is used in this papers context for bandwidth. The experimentation undertaken compares the frames per second against the image resolution for two different mission requirements. The Timed Averaged Unit (TAU) is created by the authors as a QoE metric. The test platform consists of six wireless routers and laptops operating at 2.4MHz. Each device was place 300m apart

using a mesh routing protocol with unicast UDP packets selected to transmit video traffic from the server to the end user. The change between the mission requirements occurs in increments during run time using four video flows from different radios. Results obtained suggest that the D-Q-RAM method is suited for adjusting the QoS requirements for the user but the TAU model does not take into consideration dropped frames.

Ibarrola et al examine web QoE evaluation in multi-agent network with validation of the International Telecommunication Union (ITU)-T G.1030 framework [9]. The authors propose an update of the current G.1030 standard by taking into consideration QoE of the user expectations and the user feedback. The authors undertook experiments using an emulation test platform to benchmark their modified version of the G.1030 framework with adjustments to the scaled session times for slow, medium and fast browsers to be applicable with present networks. Two experiments were conducted with participants first experiencing the slowest to fastest browser, then the second experiment fastest to slowest. All experiments undertaken used 49 random sessions with 11 skilled and 25 unskilled participants filling a questionnaire based on the experience of the system. Results indicate that additional delay has influence on download times with longer delays inducing longer download times. A relationship between QoS and QoE is defined by the authors based on previous experiences and user expectations with skilled workers having a higher QoE expectation than unskilled users. Authors suggest that the G.1030 framework required updating to meet modern day contexts.

The literature review suggests that elements of QoS and QoE have been investigated with proposed methods designed to accommodate for both metrics; however, the existing literature reviewed does not account for QoS and QoE with the integration of cryptographic processes. The context of the literature reviewed focused towards UAV only. This research investigates the effect of cryptographic constructs on the QoS and QoE of unmanned control vehicles. The packets size examined in this scenario focuses on a small size only to reduce the likelihood of packet corruption and delay obtained from larger packets [10].

IV. Experimentation Procedure

This section discusses the apparatus, metrics and context selected for the experiments. The simulation programme selected is Proteus ISIS 8 professional with the Microchip PIC18F45K22 selected as the microcontroller. The Serial Peripheral Interface (SPI) is selected as the physical layer (i.e. OSI model) to transmit and receive messages between each microcontroller on the network. The AEAD security constructs used are CCM and TinyAEAD running AES (128-bit key variant).

The test procedure examines the latency for the transmitting microcontroller to process and transmit the packet, the duration of the packet to propagate to the receiving microcontroller and to process the received packet. The impact of the software security constructs on latency is measured in metres per second travelled by the unmanned vehicle. All timings are taken from the simulator used.

Additional distance is observed in the experiments with and without security measures applied. Latency and instantaneous throughput is measured at each hop to measure the overall duration between the packets travelling from the source to the destination node and the amount of packets transmitted within a sixty second time sample. All timings and packet counts recorded are taken from the simulator used. It is assumed for this scenario that no noise is present on the wireless channel and the UGV vehicle is travelling at a top speed up to 30 mph and the UAV top speed up to 135 mph.

Metrics used for the test procedure are seconds for the sampling time of the test and number of hops to state how many intermediate devices were between the start and end node.

Configuration of the components selected are as follows, the crystal frequency selected is 4 MHz to replicate low powered industrial microcontrollers with packet sizes of 36 bytes. A SPI divisor of 16 is chosen to replicate bandwidth of a wireless link of 250Kbps [11] as calculated using the following formula [12]. It is assumed that each hop is 100m. The test procedure varied the number of intermediate hops on the linear network, starting from one hop to the maximum of six hops. Sample time of sixty seconds was selected.

V. Results and Analysis of Experiment

The results obtained from the simulation conducted are presented in this section. The graphs draw the effect of the AEAD cryptographic constructs on the operation of the unmanned vehicles in terms of the additional distance travelled by the unmanned vehicles before responding to the message received. Results are benchmarked in comparison to the distance travelled by the unmanned vehicles without security measures applied. Table 1 tabulates the distance travelled before responding to the command over multiple hops without security measured applied.

Table I
Distance travelled by unmanned vehicles before responding to the command (No Security)

Number of Hops	UGV (metres per second)	UAV (metres per second)
1	0.030	0.138
2	0.060	0.276
3	0.090	0.414
4	0.120	0.552
5	0.150	0.690
6	0.180	0.828

Figure 3 graphs the additional distance travelled by a UGV before acting upon the command. The x-axis represents the intermediate number of hops between the base station and

UGV; the y-axis represents the distance travelled by the UGV in metres per seconds (m/s) before responding to the command transmitted.

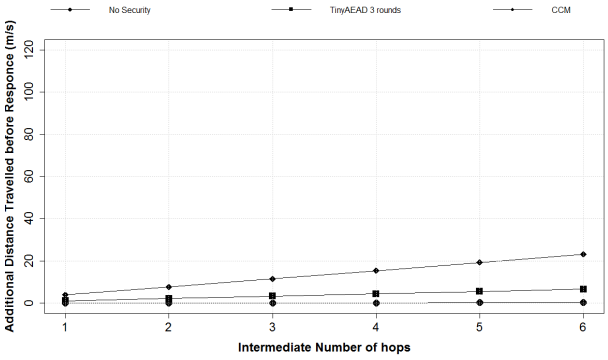


Figure 3. Simulation results of the additional distance incurred by a 30 mph UGV over multiple hops using a 36 byte packet

The results displayed in Figure 3 indicate that the AEAD constructs increase the distance travelled by the UGV before responding to the packet received. CCM has a greater influence with the additional distance incurred being greater than TinyAEAD operating at three rounds. The influence of the AEAD constructs on the distance travelled increases with more intermediate hops. Figure 4 graphs the additional distance travelled by a UAV before acting upon the command.

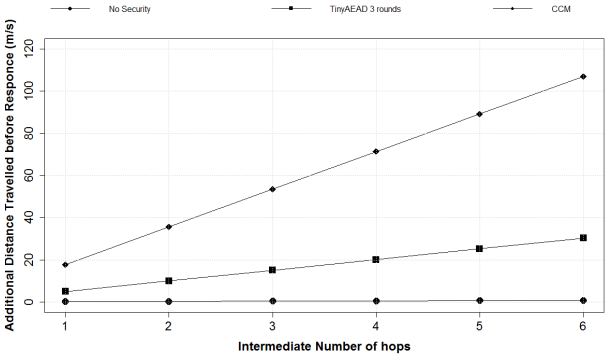


Figure 4. Simulation results of the additional distance incurred by a 135 mph fixed wing UAV over multiple hops using a 36 byte packet

Data obtained in Figure 4 suggests that the AEAD constructs increase the distance travelled by the fixed wing UAV before responding to the packet received. The TinyAEAD construct had a reduced impact in comparison to CCM with less distance travelled over each intermediate hop. The additional distance travelled increased with a larger number of intermediate hops between the base station and the fixed wing UAV.

Comparison of the two graphs presented in Figure 3 and Figure 4 indicates that the speed of the unmanned vehicles influences the additional distance incurred by the device before the command is acted upon as the distance travelled by the UAV with AEAD constructs was larger in comparison to the UGV. The number of intermediate hops between the base station and the unmanned vehicles also increases the distanced travelled by the unmanned vehicles, suggesting that the more intermediate hops there are on the network the more distance the unmanned vehicle travels before responding to the command.

Analysis of the two AEAD constructs in this experiment indicates that standardised fixed approach of CCM has a bigger impact in comparison to the adjustable TinyAEAD construct on the distance travelled by the unmanned vehicles; suggesting that the strength of the underlying block cipher influences the processing throughput.

VI. Discussion

The discussion uses the results obtained from the result and analysis of experiments and applies the findings to the case scenario presented in Section II. To examine the effect of security on QoS and QoE, instantaneous throughput is selected to sample the number of packets received at each hop in a sixty seconds time frame in relation to the distance travelled. It is assumed that the QoS is the instantaneous packet throughput from the base station to the vehicle; whilst QoE is the additional distance travelled by the vehicle before responding to the command. The effect of cryptography in terms of QoS and QoE for a 36 byte packet is presented in Figure 5.

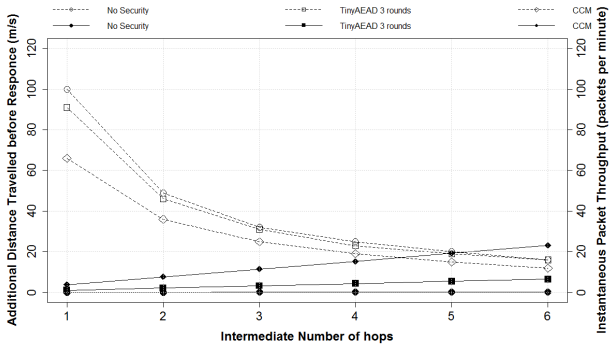


Figure 5. Balance of QoS and QoE of a UGV with and without secure communications. Additional distance travelled by the vehicle is represented by the filled line and the instantaneous throughput is represented by the dashed line

Data graphed in Figure 5 indicates that the instantaneous packet throughput and distance travelled by the UGV with CCM selected as the security measure intersect at four hops, whilst TinyAEAD at three rounds and no security measurements do not intersect up to the six hops sampled. This suggests that the trade-off for QoS and QoE is at least two hops less in comparison between TinyAEAD and no security. Figure 6 examines the scenario of a fixed wing UAV.

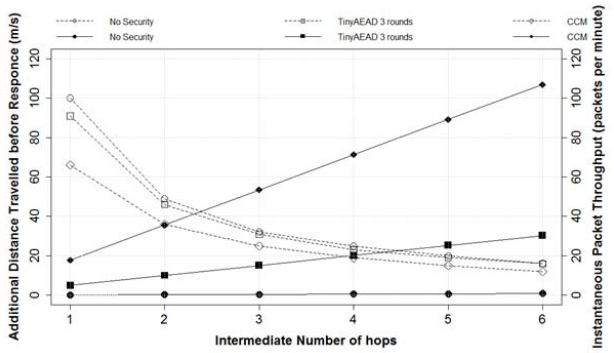


Figure 6. Balance of QoS and QoE of a fixed wing UAV with and without secure communications. Additional distance travelled by the vehicle is represented by the filled line and the instantaneous throughput is represented by the dashed line

Results displayed in Figure 6 suggests that the QoS and QoE trade-off using the CCM security measure is two hops, whilst TinyAEAD at three rounds intersects at four hops.

The discussion has highlighted two areas that contribute towards influencing the point where QoS is balanced with QoE; first the speed of the moving vehicle influences the point between balancing QoS and QoE. Secondly the selection of the cryptographic construct is important as constructs operating at fixed number of rounds reduce the number of hops travelled before the QoS and QoE balance is meet whilst adjustable cryptographic constructs are better suited for systems that require balancing for systems with more intermediate hops.

VII. Conclusion

The relationship between QoS and QoE is demonstrated through the additional distance travelled by the unmanned vehicles and the instantaneous throughput obtained. The selection of the unmanned vehicle as the speed of the vehicle has an influence on the balancing point between QoS and QoE.

Selection of the security constructs is a determining factor on the balance between QoS and QoE as adjustable security constructs is better suited for applications where the vehicle is travelling at a fast speed over small number of hops whilst fixed security constructs are better suited for situations where security of the vehicle is of priority.

Future work is to conduct the experimentation undertaken in this paper in a real world scenario to verify the findings obtained.

References

[1] G. Tuna, T.V. Mumcu, and K. Gulez. Design strategies of unmanned aerial vehicle-aided communication for disaster recovery. In *High Capacity Optical Networks and Enabling Technologies (HONET), 2012 9th International Conference on*, 2012.

[2] E. Pignaton de Freitas, T. Heimfarth, I.F. Netto, C.E. Lino, C.E. Pereira, A.M. Ferreira, F.R. Wagner, and T. Larsson. Uav relay network to support wsn connectivity. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on*, 2010.

[3] K. Hartmann and C. Steup. The vulnerability of uavs to cyber attacks - an approach to the risk assessment. In *Cyber Conflict (CyCon), 2013 5th International Conference on*, 2013.

[4] Recommendation for block cipher modes of operation: The ccm mode for authentication and confidentiality, 2004.

[5] A. Adekunle and S. Woodhead. An aead cryptographic framework and tinyaead construct for secure wsn communication. In *Wireless Advanced (WiAd)*, 2012.

[6] Yu Ming Chen, Liang Dong, and Jun-Seok Oh. Real-time video relay for uav traffic surveillance systems through available communication networks. In *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*, 2007.

[7] P.-B. Bok and Y. Tuchelmann. Context-aware qos control for wireless mesh networks of uavs. In *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*, 2011.

[8] J.P. Hansen and S.A. Hissam. Assessing qos trade-offs for real-time video. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a*, 2013.

[9] E. Ibarrola, F. Liberal, I. Taboada, and R. Ortega. Web qoe evaluation in multi-agent networks: Validation of itu-t g.1030. In *Autonomic and Autonomous Systems, 2009. ICAS '09. Fifth International Conference on*, 2009.

[10] J. Korhonen and Ye. Wang. Effect of packet size on loss rate and delay in wireless links. In *Wireless Communications and Networking Conference, 2005 IEEE*, 2005.

[11] Texas Instruments. 2.4 ghz ieee 802.15.4 / zigbee-ready rf transceiver, 2014.

[12] R Sparrow, A Adekunle, J Berry, R, and J Farnish, R. Simulating and modelling the impact of security constructs on latency for open loop control. In *Sixth Computer Science and Electronic Engineering Conference 2014 (CEEC'14)*, 2014.

W Appendix W: A Novel Block Cipher Design Paradigm for Secured Communication

Conference paper 6: A Novel Block Cipher Design Paradigm for Secured Communication

Published in: IEEE 10th International Systems Conference, Orlando, Florida, United States

Presented on: 17-24th April 2016

Abstract: Unmanned aerial vehicles (UAV) are commonly used to conduct tasks (e.g. monitor and surveillance) in various civilian applications from a remote location. Wireless communications (i.e. radio frequency) are often used to remotely pilot the UAV and stream data back to the operator. The characteristics of the wireless communication channel allows attackers to monitor and manipulate the operation of the UAV through passive and active attacks. Cryptography is selected as a countermeasure to mitigate these threats; however, a drawback of using cryptography is the impact on the real-time operation and performance of the UAV. This paper proposes the Permutation Substitution Network (PSN) design paradigm with an instance presented which is the Alternative Advanced Encryption Standard (AAES) and analysis of its performance against the standardised Substitution Permutation Network (SPN) design paradigm the Advanced Encryption Standard (AES). Results indicate that using the PSN paradigm is a feasible approach in comparison to the SPN design paradigm.

A Novel Block Cipher Design Paradigm for Secured Communication

R.D.Sparrow A.A.Adekunle, R.J.Berry and R.J.Farnish
The Wolfson Centre for Bulk Solids Handling Technology,
University of Greenwich,Chatham Maritime,
Chatham, Kent ME4 4TB, England, UK
{r.d.sparrow, a.a.adekunle, r.j.berry, r.j.farnish} @gre.ac.uk

***Abstract*—Unmanned aerial vehicles (UAV) are commonly used to conduct tasks (e.g. monitor and surveillance) in various civilian applications from a remote location. Wireless communications (i.e. radio frequency) are often used to remotely pilot the UAV and stream data back to the operator. The characteristics of the wireless communication channel allows attackers to monitor and manipulate the operation of the UAV through passive and active attacks. Cryptography is selected as a countermeasure to mitigate these threats; however, a drawback of using cryptography is the impact on the real-time operation and performance of the UAV. This paper proposes the Permutation Substitution Network (PSN) design paradigm with an instance presented which is the Alternative Advanced Encryption Standard (AAES) and analysis of its performance against the standardised Substitution Permutation Network (SPN) design paradigm the Advanced Encryption Standard (AES). Results indicate that using the PSN paradigm is a feasible approach in comparison to the SPN design paradigm.**

***Index Terms*—Unmanned Vehicles, Cryptography, Wireless, Construct design**

I. Introduction

Unmanned aerial vehicles (UAV) have become more frequent in scenarios that require tasks to be undertaken from a remote location (e.g. inaccessible areas) [1]. Digital control of UAV is becoming more frequent; wireless communication links use radio frequency (RF) links to transmit and receive messages between the operator and the UAV. Advisories within range may conduct passive and active attacks against the communication link due to the broadcast nature of the wireless communication channel [2].

Cryptography is selected to mitigate these attacks, however, the selection of the cryptographic algorithm had influenced the performance and operation of the UAV [3], [4]. The contributions of this paper are the permutation subsitution network (PSN) block cipher design paradigm, the alternative advanced encryption standard (AAES) and the first benchmark test between the substitution permutation network (SPN) and the PSN design paradigms.

The structure of this paper is organised as follows: Section II introduces the problem formulation. Section III conducts a problem analysis based on the problem formulation. Section IV presents existing literature relevant to the problem scope; Section V proposes the PSN block cipher design paradigm. Section VI presents the results obtained from the software benchmark experiments undertaken between SPN and PSN paradigms. Section VII discusses the impact of the benchmark results in the context of tactical UAV operations and performance. Section VIII concludes the paper.

II. Problem Formulation

This section introduces the problem formulation. The problem examined is UAV operated over a digital wireless communication channel from a remote location. The UK Civil Aviation Authority (CAA) policy states that the maximum operating range of the UAV is 500m (1640ft) line of sight distance and 120m (400ft) height [5]. The classification of a tactical UAV is based on the guidelines of the CAA regulations. Figure 1 presents an overview of the scenario.

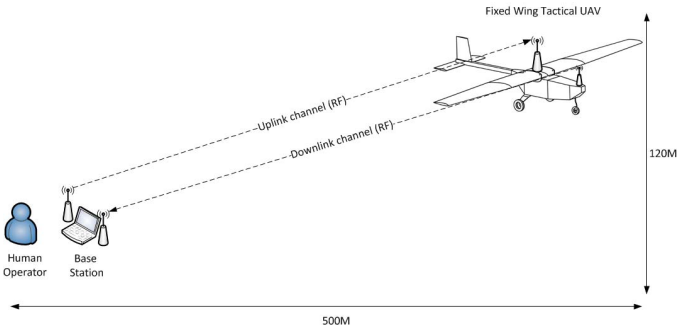


Figure 1. Illustrative concept of a point to point link for fixed wing UAV communication

A single hop point to point network is presented to transmit data between the base-station and the tactical UAV. The communication between the operator and the tactical UAV is full-duplex over two individual channels; a channel is designated as the uplink where command and control messages are transmitted between the base-station and UAV; the remaining channel is assigned as the downlink for streaming data (e.g. sensor readings) from the UAV to the base-station.

III. Problem Analysis

The UAV is susceptible to security vulnerabilities due to the nature of the wireless communication channel; both passive and active attacks can influence the operation of the UAV. Vulnerabilities identified in this paper are:

978-1-4673-9519-9/16/$31.00 ©2016 Crown

- Man-In-The-Middle attack:- Where an attacker intercepts, modifies and relays messages between the transmitter and receiver.
- Replay attack:- The attacker re-transmits the a previously transmitted message to the receiver in order to gain access to the device.
- Spoofing attack:- The attacker masquerades as a legitimate device through false messages.

A successful security attack may result in the UAV becoming unsafe and unreliable. The application of standardised security measures may not be suited for this scenario due to the real-time operational requirements of the UAV [6], [7].

The wireless communication channel broadcasts to devices within proximity, an attacker could passively monitor the data transmitted and undertake active attacks. Confidentiality, integrity and authentication are selected to provide a secure communication channel; however, the repercussions on the performance and operation of the UAV is a problem as the focus is targeted for tactical UAV devices; an instance of the performance and operation becoming affected is the maximum flight duration with tactical UAV devices have limited battery lifetime for the short mission duration.

IV. Literature Review

This section introduces literature releavent to the context of this paper with focus on methodologies used to secure the wireless communication channel for tactical UAV. The literature review is sectioned into two areas, first the current approaches undertaken by other researches, followed by a summary of the literature undertaken.

Pigatto et al [8] introduced sphere: a novel platform for improving safety and security on unmanned systems. The objective of the authors research was the implementation of safety and security of information for unmanned vehicles. The proposed solution presented in this research used two methods which are the central security unit (CSU) for authentication and communication security. Authentication is achieved when a request from the module to participate on the network is sent to the CSU; validation of the module is achieved through a CSU query to an internal database that stores module information before permission is approved or declined. Communication security is achieved by the same technique, however, the CSU queries the database for communication information before distribution of the secure keys is approved or declined and selects cryptographic methods suited for embedded or real-time sensitive systems. Test and cryptographic methodology has not been explicitly stated.

Rajatha et al [9] research focused on the authentication of Micro Aerial Vehicles (MAV) communication using Caesar cipher cryptography. The authors proposed a methodology for data encryption and authentication of MAV protocol messages between the ground station and the MAV using the Caesar cipher; this was achieved using a shift operator to rotate the character positions by a fixed number, referred to as a key. Authentication between the ground station and the MAV is proposed through the same chosen fixed number. The methodology selected by the authors is known to be vulnerable to modern cryptographic techniques used due to the widley known security vulnerabilities associated with the Caesar cipher. Test methodology and results have not been explicitly stated.

Fazal et al [10] proposed a design of a secured, high speed two way radio frequency (RF) data link for airborne vehicle communication. The authors identified design challenges which include anti-jam margins, line of sight constraints and attenuation of the RF signal. The solution derived by the authors used forward error correction to encode data to meet the data link real-time requirements; a direct sequence spread spectrum to reduce power density and have an increased resistance to interception as unauthorised users do not have the key required to spread the original signal. Two signal bands were selected which are the C-band (2-4 GHz) for command data uplink from the control terminal to the UAV and S Band (4-8 GHz) for the video downlink from the UAV to the control terminal. Tests conducted focused on five areas which were functional evaluation, range validation, interface checks and flight trials. The research presented was targeted at the physical layer of the Open Systems Interconnection (OSI) model.

Kim et al [11] introduce the symmetry structure layer design paradigm for SPN block cipher algorithms. The authors identified that the Advanced Encryption Standard (AES) block cipher does not use the same algorithm for encryption and decryption in comparison to a Feisel structure. The symmetry layer structure is proposed by the authors with the following objectives stated: The same AES algorithm to be used for encryption and decryption, enhance the security of AES, be easy to implement and not affect the performance of the cryptographic construct. The implementation of the symmetry layer uses Feisel structure characteristics to enable inverse operation using the same algorithm and is implemented after the fifth round of AES; after the sixth round of the encryption function the decryption operation is used for the last four rounds. Tests were conducted on a Windows XP Celeron 2.8 GHz, 700 MB RAM using Visual Studio 2005 C compiler; a file size of 30 MB was selected. Results indicate that the proposed solution had a 7% increase on the encryption and decryption time.

The literature review indicates that current research has highlighted the requirement for secure communication for unmanned vehicles is required with some consideration for operational and performance constraints; however, the cryptographic design methodology has not been explicitly stated or implemented in previous research reviewed to determine if the proposed solution is suited towards the context of remote controlled vehicles. This paper analyses a new design paradigm of cryptographic block ciphers for the application of

tactical UAV.

V. Design Paradigm

This section introduces the proposed design methodology used to derive a block cipher suited for UAV. This section is categorised into two sections, first the justification for the selection of SPN ciphers is discussed, followed by the explanation of the PSN design paradigm.

AES is a National Institute of Standards and Technology (NIST) standardised block cipher designed to provide confidentiality for a data size of 128-bits using cryptographic keys of 128, 192 or 256-bit sizes [12]. AES is a block cipher that uses the SPN design paradigm.

The SPN design paradigm consists of two functions based on Shannon's confusion and diffusion theory [13] which are substitution and permutation. The substitution box creates confusion by replacing the original plaintext character with a random character and diffusion is achieved through dispersion of the plaintext. The PSN uses the same principles from Shannon's theory by using substitution and permutation; however, the order of operation has been reconfigured to create diffusion before confusion. Derivation of the PSN paradigm is presented to identify how the order of the confusion and diffusion has influence on the ciphertext output.

The AES block cipher can be implemented in different arrangments as presented in Table 1.

Table I
Possible AES block cipher combinations

	SubBytes	ShiftRows	MixColumns
Combination 1	1	2	3
Combination 2	1	3	2
Combination 3	2	1	3
Combination 4	2	3	1
Combination 5	3	1	2
Combination 6	3	2	1

Table 1 presents six variations of the AES block cipher. The combinations listed in Table 1 are further categorised into three sub groups which are the SPN, PSN and the permutation substitution permutation network (PSPN). Combinations one and two fall under the SPN design paradigm as the order follows substitution before permutation; combination three and four comprise the PSPN design paradigm as permutation happens before and after the substitution. Combinations five and six are categorised under the PSN design paradigm as the permutation operations are undertaken before the substitution. The combination selected for this paper is combination six as this variation of the PSN paradigm is structured in a similar format to the SPN paradigm used for AES.

For this paper the block cipher AES was selected as it is the de-facto standard. AES uses the SPN paradigm and comprises of three functions which are the substitution byte, shift rows and mix columns. The substitution function is a non-linear substitution step where each byte is replaced with another according to a lookup . The shiftrows transposition step where each row of the state is shifted cyclically a certain number of steps. The mixcolumn is a mixing operation which operates on the columns of the state, combining the four bytes in each. The addroundkey is where each byte of the state is combined with the round key using bitwise exclusive or (XOR). A statistical comparison of the ciphertext outputs of the SPN paradigm using AES and the PSN paradigm using combination six was achieved using the paired t-test.

The test conducted changed the value of a individual byte position of a sixteen byte plain text message with the same value before each encryption call. The data from the ciphertext outputs were normalised against the random mean average for a byte of data (127.5 bits) before statistical analysis was conducted. Table 2 tabulates the output of the paired t-test.

Table II
Normalised paired-t-test comparison of SPN and PSN paradigms (95% confidence interval)

T-value	1.0519
Degrees of freedom	7
P-value	0.3278
Mean of differences	6.8

Results from the normalised paired t-test indicate that SPN and PSN paradigms are not significantly different; this therefore suggests that the PSN design paradigm is a suitable method for block ciphers. The generic pseudo code configuration of the SPN and PSN design paradigms are presented in Figure 2.

SPN design paradigm

```
Round(State, RKey)
{
SubByte(State);
ShiftRows(State);
MixColumn(State);
AddRKey(State, RKey);
}
SubByte(State);
ShiftRows(State);
MixColumn(State);
AddRKey(State, RKey);
```

PSN design paradigm

```
Round(State, RKey)
{
MixColumn(State);
ShiftRows(State);
SubByte(State);
AddRKey(State, RKey);
}
MixColumn(State);
ShiftRows(State);
SubByte(State);
AddRKey(State, RKey);
```

Figure 2. Pseudo code of the SPN paradigm (Left) and the PSN paradigm (Right)

VI. Results and Analysis of Experiment

This section discusses the result and analysis of the experiments undertaken. The experiment undertook a direct comparison between the SPN and PSN design paradigms. Implementation of the SPN and PSN design paradigms was achieved in software. The analysis of the results were conducted using statistical tests on the ciphertext output. The two statistical methods selected to draw comparison between the PSN and SPN design paradigms were the arithmetic mean and the serial-correlation test. The arithmetic mean formula and serial correlation formula is presented in Formula 1 and

Formula 2.

$$A = \frac{1}{n}\sum_{i=1}^{n} a_i$$

Formula 1: Arithmetic mean formula.

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{(n\sum x^2 - (\sum x)^2)(n\sum y^2 - (\sum y)^2)}}$$

Formula 2: Pearson's correlation coefficient formula

The arithmetic mean sums the bytes of the ciphertext output and divides by the file length; as the data is packaged into byte values; the ideal arithmetic mean for the ciphertext is 127.5-bits as half the value of a single byte is 127.5-bits. The serial correlation measures the extent to which each byte in the file depends upon the previous byte; the closer the value is to zero the more random the ciphertext output is as it is uncorrelated, correlation closer to positive or negative value of one indicates a non random output. Figure 3 plots the arithmetic mean comparison between SPN and PSN design paradigms at ten rounds using various byte sized messages.

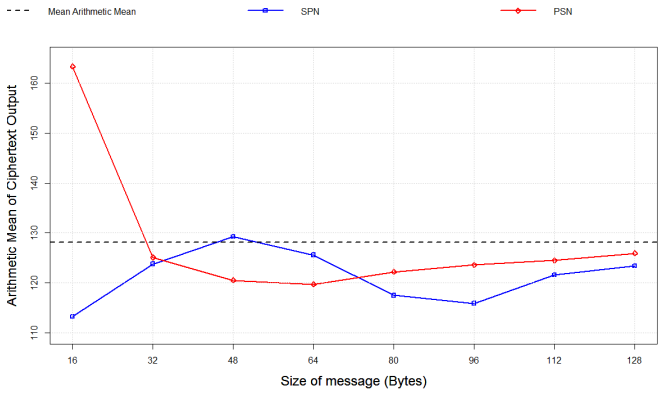


Figure 3. Comparison of the arithmetic mean of SPN and PSN using ten rounds with various byte sized messages

The mean result of the arithmetic mean tests for the SPN design paradigm is a mean total of 121.3 whilst the PSN design paradigm has a mean total of 128.1. The PSN paradigm is 0.6 bits difference from the ideal mean random in contrasts to the SPN paradigm of 6.2 bits difference. The standard deviation for the arithmetic mean for the SPN design paradigm is 5.4 whilst the PSN stricture is 14.4. The results from the standard deviation test indicate that the PSN paradigm is more consistent with its arithmetic mean output when compared to the SPN paradigm. Table 3 tabulates the results of the serial-correlation test between the SPN and PSN design paradigm at ten rounds using various byte sized messages.

Analysis of the serial correlation coefficient tests for the SPN design paradigm was -0.03 whilst the SPN design paradigm had a mean total of -0.01 correlation coefficient score. The standard deviation of the correlation coefficient scores indicates that SPN has a value of -0.60 whilst PSN has a value of -0.08.

Table III
COMPARISON OF SPN AND PSN DESIGN PARADIGMS USING TEN ROUNDS WITH VARIOUS BYTE SIZED MESSAGES

Size of message (Bytes)	Serial-Correlation SPN	Serial-Correlation PSN
16	-0.10	-0.46
32	0.04	0.16
48	-0.04	0.06
64	-0.04	0.05
80	-0.03	0.01
96	-0.07	-0.02
112	0.00	0.03
128	0.02	0.06

Summary of the experiments undertaken indicate that the PSN design paradigm is just as suited for generating random output as the SPN design paradigm from the preliminary statistical analysis undertaken. This suggests that it is feasible to select the PSN design paradigm to obtain a ciphertext output comparible to the SPN design paradigm.

VII. DISCUSSION

This discussion relates the results obtained from the experiments undertaken and applies the findings to the problem formulation and problem analysis focused towards tactical UAV with priority on the operational and performance requirements of the tactical UAV. The AAES block cipher is presented in this section with elaboration of its operation.

The PSN design methodology was used to derive the Alternative Advanced Encryption Standard (AAES) block cipher. The pseudo code configuration of AAES using the PSN design paradigm is presented in Figure 4.

AES Block Cipher

```
Round(State, RKey)
{
SubByte(State);
ShiftRows(State);
MixColumn(State);
AddRKey(State, RKey);
}
SubByte(State);
ShiftRows(State);
AddRKey(State, RKey);
```

AAES Block Cipher

```
Round(State, RKey)
{
MixColumn(State);
ShiftRows(State);
SubByte(State);
AddRKey(State, RKey);
}
SubByte(State);
ShiftRows(State);
AddRKey(State, RKey);
```

Figure 4. Pseudo code of conventional AES using the SPN paradigm (Left) and the AAES block cipher using the PSN paradigm (Right)

AAES first mixes the input data, followed by the permutation using the shift rows, the substitution follows before the bytes are XOR with the round key and the ciphertext is output. Generation of the substitution box is achieved using a method based on practitioners preference. The operation of the PSN methodology can be applied in three configurations which are standard AES configuration, the AAES configuration and a hybrid between PSN and SPN. The variation of the mixcolumn and shiftrows is also a valid combination of the PSN design paradigm.

A simulation has been undertaken to identify the affect of cryptographic services on the operation and performance of the tactical UAV, the investigation focuses on the number of packets transmitted and received by the UAV. The simulation selected the Microchip PIC18F45K22 selected as the microcontroller for the operator and tactical UAV. The Serial Peripheral Interface (SPI) is selected as the physical layer (i.e. OSI model) to transmit and receive messages between each microcontroller. The TinyAEAD construct was the selected AEAD construct due to its flexibility and adaptability of operating various cryptographic methods [14].

Metrics utilised for the test procedure are seconds for the sampling time of the test, packet count to measure how many packets arrived in the sample time of ten seconds. All timings are taken from the simulator used.

Configuration of the components selected are as follows, the crystal frequency selected is 4 MHz to replicate low powered microcontrollers with packet payload sizes of 16, 64 and 96 bytes chosen. Table 4 graphs the comparison between SPN and PSN design paradigms at ten rounds with various byte sized messages.

Table IV
PACKET COUNT COMPARISON BETWEEN SPN AND PSN DESIGN PARADIGMS (TEN SECOND SAMPLE TIME)

Number of Bytes in payload	Number of Packets (No Security)	Number of Packets (SPN)	Number of Packets (PSN)
16 bytes	3992	150	150
64 bytes	735	16	16
96 bytes	549	11	11

Results obtained indicate that the PSN design paradigm and the SPN design paradigm are correlated with the same number of packets generated; it can be inferred that the PSN design paradigm would be just as suited for the application of tactical UAV as the SPN design paradigm as it takes the same time to process through the cryptographic construct; this is because both paradigms utilised the same substitution and permutation functions; however, the order of the operation is modified.

It can also be inferred based on the preliminary cryptographic analysis undertaken that the PSN design paradigm is just as resilient against linear and differential cryptanalysis attacks as the SPN design paradigms uses the same technique of confusion and diffusion through permutation and substitution.

The impact on the operational and performance characteristics of the tactical UAV using the selected approaches indicates that both PSN and SPN design paradigms have an effect on the total number of packets received by the tactical UAV using TinyAEAD at ten rounds. The percentage difference between the test without security and using security is a minimal of 95% for 16 bytes, 97% difference for 64 bytes and 98% difference for 96 bytes. This suggests that the inclusion of cryptographic measures has a influence on the total amount of packets received.

VIII. CONCLUSION

The PSN design paradigm presented in this paper has been proposed; the PSN design paradigm and the SPN design paradigm indicates a strong statistical correlation and similar outcome for the processing time. The preliminary cryptanalysis undertaken, the indication is that the PSN paradigm is a valid methodology for block cipher design as the results obtained are comparable with the SPN design paradigm.

The affect of the cryptographic service on the operational and performance of the UAV has also been identified with both SPN and PSN design paradigms having the same influence with a minimum of a 95% packet reduction from the sampled selected. This suggests that cryptography has an influence on the operational and performance of the UAV and may impact on safety and reliability during flight.

Future work is to validate the PSN paradigm in a real world context.

REFERENCES

[1] Gurkan Tuna, Bilel Nefzi, and Gianpaolo Conte. Unmanned aerial vehicle-aided communications system for disaster recovery. *Journal of Network and Computer Applications*, 41:27 – 36, 2014.

[2] K. Mansfield, T. Eveleigh, T.H. Holzer, and S Sarkani. Unmanned aerial vehicle smart device ground control station cyber security threat model. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, pages 722–728, 2013.

[3] R Sparrow, A Adekunle, J Berry, R, and J Farnish, R. Simulating and modelling the impact of security constructs on latency for open loop control. In *Sixth Computer Science and Electronic Engineering Conference 2014 (CEEC'14)*, 2014.

[4] R.D. Sparrow, A.A. Adekunle, R.J. Berry, and R.J. Farnish. Study of two security constructs on throughput for wireless sensor multi-hop networks. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on*, pages 1302–1307, 2015.

[5] CAA. Unmanned aircraft system operations in uk airspace guidance, 2015.

[6] R.D. Sparrow, A.A. Adekunle, R.J. Berry, and R.J. Farnish. Balancing throughput and latency for an aerial robot over a wireless secure communication link. In *Cybernetics (CYBCONF), 2015 IEEE 2nd International Conference on*, pages 184–189, 2015.

[7] R.D. Sparrow, A.A. Adekunle, R.J. Berry, and R.J. Farnish. The affect of two cryptographic constructs on qos and qoe for unmanned control vehicles. In *Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on*, 2015.

[8] D.F. Pigatto, J. Smith, K.R. Lucas, and J. Castelo Branco. Sphere: A novel platform for increasing safety amp; security on unmanned systems. In *Unmanned Aircraft Systems (ICUAS), 2015 International Conference on*, pages 1059–1066, June 2015.

[9] B.S. Rajatha, C.M. Ananda, and S. Nagaraj. Authentication of mav communication using caesar cipher cryptography. In *Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference on*. 58-63, May 2015.

[10] M.M. Fazal, A.G. Pawar, and J. Prasad. Design of secured, high speed two way rf data link for airborne vehicle communication. In *Microwave and RF Conference, 2013 IEEE MTT-S International*, pages 1–4, December 2013.

[11] Gil-Ho Kim, Jong-Nam Kim, and Gyeong-Yeon Cho. Symmetry structured spn block cipher algorithm. In *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on*, volume 3, pages 1777–1780, 2009.

[12] Advanced encryption standard (aes).
[13] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.
[14] A. Adekunle and S. Woodhead. An aead cryptographic framework and tinyaead construct for secure wsn communication. In *Wireless Advanced (WiAd)*, 2012.

X Appendix X: LEOPARD: Lightweight Encryption Operation Permutation Addition Rotation and Diffusion

Conference paper 6: LEOPARD: Lightweight Encryption Operation Permutation Addition Rotation and Diffusion

Published in: IEEE 10th International Conferences on Signal Processing and Communication Systems, Brisbane, Australia

Presented on: 19-21th December 2016

Abstract: Tactical unmanned vehicles are commonly used to conduct tasks (e.g. monitor and surveillance) in various civilian applications from a remote location. The characteristics of the wireless communication link allows attackers to monitor and manipulate the operation of the unmanned vehicle through passive and active attacks. Cryptography is selected as a countermeasure to mitigate these threats; however, a drawback of using cryptography is the impact on the energy consumed by the unmanned vehicle as energy is often constrained and limits the duration of the mission time. This paper introduces the Lightweight Encryption Operation Permutation Addition Rotation and Diffusion (LEOPARD) cryptographic primitive with a benchmark performance analysis against the standardised Advanced Encryption Standard (AES). Results indicate that LEOPOARD is a feasible encryption approach in comparison to the AES encryption algorithm for unmanned vehicles with an average performance increase of 8%.

LEOPARD: Lightweight Encryption Operation Permutation Addition Rotation and Diffusion

R.D.Sparrow A.A.Adekunle and R.J.Berry
The Wolfson Centre for Bulk Solids Handling Technology,
University of Greenwich,Chatham Maritime,
Chatham, Kent ME4 4TB, England, UK
{r.d.sparrow, a.a.adekunle, r.j.berry} @gre.ac.uk

***Abstract*—Tactical unmanned vehicles are commonly used to conduct tasks (e.g. monitor and surveillance) in various civilian applications from a remote location. The characteristics of the wireless communication link allows attackers to monitor and manipulate the operation of the unmanned vehicle through passive and active attacks. Cryptography is selected as a countermeasure to mitigate these threats; however, a drawback of using cryptography is the impact on the energy consumed by the unmanned vehicle as energy is often constrained and limits the duration of the mission time. This paper introduces the Lightweight Encryption Operation Permutation Addition Rotation and Diffusion (LEOPARD) cryptographic primitive with a benchmark performance analysis against the standardised Advanced Encryption Standard (AES). Results indicate that LEOPOARD is a feasible encryption approach in comparison to the AES encryption algorithm for unmanned vehicles with an average performance increase of 8%.**

***Index Terms*—Cryptographic primitives, Unmanned Vehicles, Secure Communications, Energy Conservation, Encryption**

I. Introduction

The application of unmanned vehicles has become common in civilian scenarios that require teleoperation from remote location (e.g. hazardous or inaccessible areas) [1]. Wireless communication links are selected to communicate with unmanned vehicles through the use of radio frequency (RF) to transmit and receive messages between the base-station and mobile vehicle. Advisories within range may conduct passive and active attacks against the communication link due to the broadcast nature of the wireless communication link [2].

Cryptography is selected to mitigate these attacks, however, the selection of the cryptographic algorithm had influenced the performance and operation of the unmanned vehicle [3], [4]. As unmanned vehicles have limited energy supplies, the selection of standardised cryptographic approaches may not be suited for this context [5], [6]. The contributions of this paper are the Lightweight Encryption Operation Permutation Addition Rotation and Diffusion (LEOPARD) cryptographic primitive based on the Permutation Substitution Network (PSN) design paradigm [7] with comparison of the LEOPARD and standardised AES cryptographic primitive is presented.

The structure of this paper is organised as follows: Section II introduces the problem formulation. Section III conducts a problem analysis based on the problem formulation. Section IV presents existing literature relevant to the problem scope; Section V proposes the LEOPARD cryptographic primitive. Section VI presents the results obtained from the software benchmark experiments undertaken between LEOPARD and AES cryptographic primitives. Section VII discusses the impact of the benchmark results in the context of tactical UAV. Section VIII concludes the paper.

II. Problem Formulation

This section introduces the problem formulation. The problem examined is an unmanned aerial vehicle (UAV) operated over a digital wireless communication link from a remote location. The UK Civil Aviation Authority (CAA) policy states that the maximum operating range of the UAV is 500m (1640ft) line of sight distance and 120m (400ft) height [8]. The classification of a tactical UAV is based on the guidelines of the CAA regulations. Figure 1 presents an overview of the scenario.

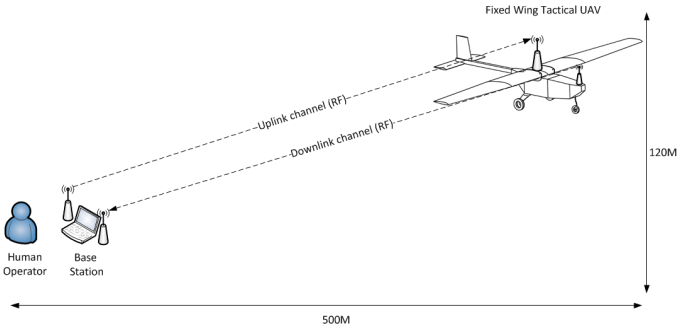


Figure 1. Illustrative concept of a point to point link for fixed wing UAV communication

A single hop point to point network is presented to transmit data between the base-station and the tactical UAV. The communication between the operator and the tactical UAV is full-duplex over two individual links; a link is designated as the uplink where command and control messages are transmitted between the base-station and UAV; the remaining link is assigned as the downlink for streaming data (e.g. sensor readings) from the UAV to the base-station. It is assumed that the maximum operation flight time for the tactical UAV in this context is not greater than 2 hours.

978-1-5090-0941-1/16/$31.00 ©2016 IEEE

III. Problem Analysis

The UAV is susceptible to security vulnerabilities due to the nature of the wireless communication link; both passive and active attacks can influence the operation of the UAV. Vulnerabilities considered in this paper include man-in-the-middle attacks, replay attacks and spoofing attacks

A successful security attack may result in the UAV becoming unsafe and unreliable. The application of standardised security measures may not be suited for this scenario due to the real-time operational requirements of the UAV [9], [10].

The wireless communication link broadcasts to devices within proximity, an attacker could passively monitor the data transmitted and undertake active attacks. Confidentiality, integrity and authentication are selected to provide a secure communication link; however, the repercussions on the performance and operation of the UAV is a problem as the focus is targeted for tactical UAV devices; an instance of the performance and operation becoming affected is the maximum flight duration with tactical UAV devices have limited battery lifetime for the short mission duration.

IV. Literature Review

This section introduces literature relevant to the context of this paper with focus on methodologies used to secure the wireless communication link for tactical UAV. The literature review is sectioned into two areas, first the current approaches undertaken by other researches, followed by a summary of the literature review undertaken.

Priyadharshini et al; introduce an energy and mobility based group key management in mobile ad-hoc networks [11]. The problem discussed by the authors is the issue of applying secure communications to mobile MANETs as the energy and mobility constraints and a requirement of an efficient key management scheme is required. The proposed solution presented by the authors was the energy and mobility based group key management which is an identification based key management scheme. Tests undertaken on the proposed scheme was undertaken in the simulation NS2. Results presented by the authors show the number of nodes participating in the MANET increased the latency generated for the key generation, this trend was also present for the energy consumption..

Jiang et al; research energy optimisation of security-critical real-time applications with guaranteed security protection [12]. The authors investigate the problem of the design of a secure and energy efficient real-time embedded system with the objective of minimising energy consumed based on the energy constraints on mobile applications such as UAV. The test platform selected by the authors was simulated based on the measurements obtained from a preliminary test of the time and energy readings of various security algorithms sampled on an ARM S3C2440 CPI operating at 500 MHz and 64 MB of RAM. Results from the preliminary results indicate that stream cipher RC4 consumed the least time and energy whilst triple data encryption standard (3DES) induced the longest time and had the highest energy consumption.

The impact of trust-based security association and mobility on the delay metric in MANET is presented by Nguyen et al; [13]. The problem discussed by the authors is the broadcast delay induced from broadcast authentication between devices on the MANET and the effect of the delay on the overall system. The proposed solution presented in this research is a mathematical model for analysing the delay of epidemic broadcasts in MANET and benchmarked against the results obtained from a simulated environment. Results presented by the authors indicates that the mathematical model and the simulation correlate for fixed density of nodes at varying velocities with larger delays reported at lower velocities. The density of nodes in an area influences the delay induced with larger density of nodes reducing the delay incurred. The security handshake delay measured indicated that the simulation results have a reduced effect for on the delay measured in comparison to the mathematical model results.

The literature review indicates that current research has highlighted the requirement for secure communication for unmanned vehicles is required with some consideration for operational and performance constraints; however, the cryptographic design methodology has not been explicitly stated or implemented in previous research reviewed to determine if the proposed solution is suited towards the context of remote controlled vehicles. This paper analyses a new design paradigm of cryptographic block ciphers for the application of tactical UAV.

V. Proposed Design

This section introduces the proposed LEOPARD design methodology for mobile platforms. This section is categorised into two sections, first the justification for the selection of AES block cipher is discussed, followed by the explanation of the LEOPARD block cipher design.

AES is a National Institute of Standards and Technology (NIST) standardised block cipher designed to provide confidentiality for a data size of 128-bits using cryptographic keys of 128, 192 or 256-bit sizes [14]. AES is a block cipher that uses the SPN design paradigm.

For this paper the block cipher AES was selected as it is the de-facto standard. AES uses the SPN paradigm and comprises of three functions which are the substitution byte, shift rows and mix columns. The substitution function is a non-linear substitution step where each byte is replaced with another according to a lookup. The shiftrows transposition step where each row of the state is shifted cyclically a certain number of steps. The mixcolumn is a mixing operation which operates on the columns of the state, combining the four bytes in each. The addroundkey is where each byte of the

state is combined with the round key using bitwise exclusive or (XOR).

The LEOPARD cryptographic primitive uses the permutation substitution network paradigm PSN presented in previous research [7]. The pseudo code configuration of LEOPARD and AES cryptographic primitives is presented in Figure 2.

AES

```
Round(State, RKey)
{
SubByte(State);
ShiftRows(State);
MixColumn(State);
AddRKey(State, RKey);
}
SubByte(State);
ShiftRows(State);
AddRKey(State, RKey);
```

LEOPARD

```
Round(State, RKey)
{
MixColumn(State);
AddRKeyAdd(State, RKey);
ShiftRows(State);
}
SubByte(State);
ShiftRows(State);
AddRKey(State, RKey);
```

Figure 2. Pseudo code of conventional AES cryptographic primitive (Left) and the LEOPARD cryptographic primitive (Right)

LEOPARD first mixes the input data, followed by the addition of the round key to the data stream; the permutation using the shift rows, the substitution follows before an additional permutation with the shiftrows in the final round. The bytes are XOR'd with the round key to derive the cipher-text is output. Generation of the substitution box is achieved using a method based on practitioners preference. The design of the LEOPARD cryptographic primitive was inspired by the novel approaches presented in previous work [15].

VI. Results and Analysis of Experiment

This section discusses the result and analysis of the experiments undertaken. The experiment undertook a direct comparison between the LEOPARD and AES cryptographic primitives. Implementation of LEOPARD and AES was constructed in software. The analysis of the results were conducted using statistical tests on the cipher-text output. The two statistical methods selected to draw comparison between the cryptographic primitives were the arithmetic mean and the serial-correlation test. The arithmetic mean formula and serial correlation formula is presented in Formula 1 and Formula 2.

$$A = \frac{1}{n}\sum_{i=1}^{n} a_i$$

Formula 1: Arithmetic mean formula.

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{(n\sum x^2 - (\sum x)^2)(n\sum y^2 - (\sum y)^2)}}$$

Formula 2: Pearson's correlation co-efficient formula

The arithmetic mean sums the bytes of the cipher-text output and divides by the file length; as the data is packaged into byte values; the ideal arithmetic mean for the cipher-text is 127.5-bits as half the value of a single byte is 127.5-bits. The serial correlation measures the extent to which each byte in the file depends upon the previous byte; the closer the value is to zero the more random the cipher-text output is as it is uncorrelated, correlation closer to positive or negative value of one indicates a non random output. Table I tabulates the comparison of entropy, arithmetic mean and serial correlation between LEOPARD and AES at for a 256 byte message at ten rounds.

Table I
Comparison of LEOPARD and AES for a 256 byte payload at ten rounds

	AES	**LEOPARD**
Entropy value	7.11	7.19
Arithmetic mean	123.9	134.7
Serial-Correlation	0.02	0.07

The LEOPARD cryptographic primitive was 7.2 bits difference from the ideal mean random in contrasts to the AES of bits difference of 3.6. The standard deviation for the arithmetic mean for AES is 5.4 whilst LEOPARD is 14.4. Table 3 tabulates the results of the serial-correlation test between the AES and LEOPARD cryptographic primitives at ten rounds. The entropy score recorded for LEOPARD was 7.19 bit entropy in comparison to 7.11 recorded for AES with a difference of 0.07.

Analysis of the serial correlation co-efficient tests for AES was closer to an ideal serial correlation co-efficient score of 0.00 in comparison to LEOPARD. The standard deviation of the correlation co-efficient scores indicates AES had a standard deviation score of 0.01 whilst the standard deviation for LEOPARD was 0.04. The final test examined the entropy of the cipher-text output for LEOPARD and AES at ten rounds with a 256 byte packet size.

Summary of the experiments undertaken indicate that the LEOPARD cryptographic primitive is just as suited for generating random output as AES from the preliminary statistical analysis undertaken. This suggests that it is feasible to select the LEOPARD cryptographic primitive to obtain a cipher-text output comparable to the AES cryptographic primitive.

VII. Discussion

This discussion relates the results obtained from the experiments undertaken and applies the findings to the problem formulation and problem analysis with priority on the power consumed by the cryptographic primitives and how it affect the context of tactical UAV.

A test was undertaken on a emulated test platform to identify the affect of cryptographic services on the power consumption of a tactical UAV, the investigation focused on the power consumption of a limited battery supply for streamed video data between the base-station and tactical UAV. The Microchip PIC18F45K22 was selected as the microcontroller for the operator and tactical UAV. The Serial Peripheral Interface (SPI) is selected as the physical layer (i.e. OSI model) to transmit and receive messages between each microcontroller. The TinyAEAD construct was the selected AEAD construct due to its flexibility and adaptability of

operating various cryptographic methods [15].

Metrics utilised for the test procedure are milliwatts (mW) for the power consumed and seconds for the time sampled. All timings are taken from the a real-world stopwatch.

Configuration of the components selected are as follows, the crystal frequency selected is 16 MHz to replicate low powered microcontrollers with packet payload sizes of 36, 52 and 84 bytes packet sizes. Table II tabulates the comparison between LEOPARD and AES cryptographic primitives at three rounds with various byte sized messages.

Table II
PACKET COUNT COMPARISON BETWEEN LEOPARD AND AES CRYPTOGRAPHIC PRIMITIVES IN A SIXTY SECOND TIME SAMPLE AT 16 MHZ CRYSTAL FREQUENCY

Payload Size (Bytes)	Number of Packets (AES)	Number of Packets (LEOPARD)
36	3392	3624
52	2462	2638
84	1550	1725

Results obtained show that the LEOPARD cryptographic primitive has an increased number of packets received in comparison to the AES cryptographic primitive; it can be inferred that LEOPARD is better suited for the application of tactical unmanned vehicles with the increased packet throughput represented.

The impact on the operational and performance characteristics of the tactical UAV using the selected approaches indicates that both PSN and SPN design paradigms have an effect on the total number of packets received by the tactical UAV using TinyAEAD at ten rounds. The percentage difference between the two cryptographic primitives is 6.6% for 36 bytes, 6.9% difference for 52 bytes and 10.7% difference for 84 bytes. This suggests that the selection of cryptographic primitive has an influence on the total amount of packets received.

The second test draws comparison of the time required to to encrypt the streamed data from the UAV to the base-station with LEOPARD and AES. Packet sizes of 256 byte and 1024 bytes to represent MAVlink and Ethernet like protocols. Table III tabulates the results of LEOPARD and AES for streamed data.

Table III
LATENCY INDUCED BY LEOPARD AND AES FOR VARIOUS STREAMED PACKET LENGTHS AT 16 MHZ CRYSTAL FREQUENCY

Payload Size (Bytes)	Latency AES (ms)	Latency LEOPARD (ms)
128	35.1	31.8
256	65.8	59.5
1024	289.4	261.5

Data presented in Table III show that the latency induced for LEOPARD operating at ten rounds for a 36 byte packet size is reduced by 9.8% in comparison to AES; at 52 bytes the difference in latency between LEOPARD and AES was 10.2% and for 84 bytes the reduction in latency for LEOPARD when compared to AES was 10.1%.

The power consumption of the LEOPARD and AES cryptographic primitives was investigated to determine how the design of the cryptographic primitives contributed towards the power used by the computational device. For this scenario, a unmanned vehicle is selected to represent a mobile platform. Results presented represent the cost of the security measures only. Figure 3 illustrates the power consumption of LEOPARD and AES cryptographic primitives with various crystal frequencies selected.

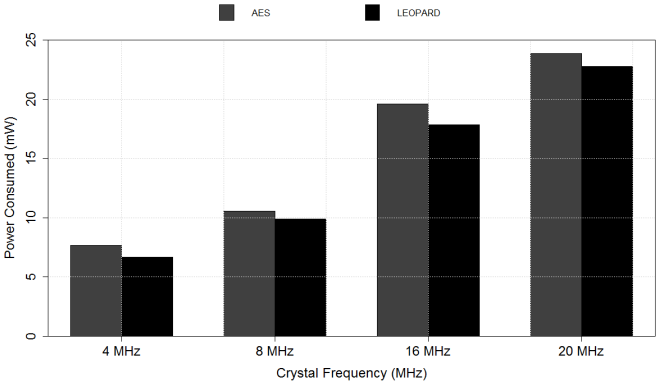


Figure 3. Comparison of power consumed of a mobile real-time system with LEOPARD and AES cryptographic primitives at various crystal frequency

The results of the power consumption of the cryptographic primitives in relation to the power consumed shows that the mobile real-time system using LEOPARD cryptographic primitive has a reduced power consumption in comparison to AES. The difference between the two methods shows that the consumption of the limited power supply of the mobile platform would on average have a 8.5% reduction with LEOPARD cryptographic primitive selected in comparison to AES.

VIII. CONCLUSION

The LEOPARD cryptographic primitive presented in this paper has been proposed; the LEOPARD and AES cryptographic primitives show a strong statistical correlation with a reduction in the processing time required to process LEOPARD. The preliminary cryptanalysis undertaken, the indication is that the LEOPARD cryptographic primitive is a valid methodology for block cipher design as the results obtained are comparable with AES.

The affect of the cryptographic service on the operational and performance of the UAV has also been identified the LEOPARD cryptographic primitives having an improved throughput and reduced power consumption on average of 8% in comparison to AES. This suggests that cryptography has an influence on the operational and performance of the

UAV and may impact on safety, reliability and availability.

Future work is to validate the LEOPARD on a real-world test platform.

REFERENCES

[1] Sonia Waharte and Niki Trigoni. Supporting search and rescue operations with uavs. In *International Symposiom on Robots and Security*, 2010.

[2] K. Mansfield, T. Eveleigh, T.H. Holzer, and S Sarkani. Unmanned aerial vehicle smart device ground control station cyber security threat model. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, pages 722–728, 2013.

[3] R Sparrow, A Adekunle, J Berry, R, and J Farnish, R. Simulating and modelling the impact of security constructs on latency for open loop control. In *Sixth Computer Science and Electronic Engineering Conference 2014 (CEEC'14)*, 2014.

[4] R.D. Sparrow, A.A. Adekunle, R.J. Berry, and R.J. Farnish. Study of two security constructs on throughput for wireless sensor multi-hop networks. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on*, pages 1302–1307, 2015.

[5] A. A. Adekunle. A resourceful symmetric cryptographic construct for securing miniature satellite communications. In *Wireless for Space and Extreme Environments (WiSEE), 2013 IEEE International Conference on*, pages 1–6, Nov 2013.

[6] A. A. Adekunle. A symmetric cryptographic construct for securing wireless sensor network communications. In *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 935–940, August 2015.

[7] R. D. Sparrow, A. A. Adekunle, R. J. Berry, and R. J. Farnish. A novel block cipher design paradigm for secured communication. In *2016 Annual IEEE Systems Conference (SysCon)*, pages 1–6, April 2016.

[8] CAA. Unmanned aircraft system operations in uk airspace guidance, 2015.

[9] R.D. Sparrow, A.A. Adekunle, R.J. Berry, and R.J. Farnish. Balancing throughput and latency for an aerial robot over a wireless secure communication link. In *Cybernetics (CYBCONF), 2015 IEEE 2nd International Conference on*, pages 184–189, 2015.

[10] R.D. Sparrow, A.A. Adekunle, R.J. Berry, and R.J. Farnish. The affect of two cryptographic constructs on qos and qoe for unmanned control vehicles. In *Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on*, 2015.

[11] M. Ramya Priyadharshini, S. Prasanna, and N. Balaji. Energy and mobility based group key management in mobile ad hoc networks. In *Recent Trends in Information Technology (ICRTIT), 2014 International Conference on*, 2014.

[12] Wei Jiang, Ke Jiang, Xia Zhang, and Yue Ma. Energy optimization of security-critical real-time applications with guaranteed security protection. *Journal of Systems Architecture*, 61(7):282 – 292, 2015.

[13] D. Q. Nguyen, M. Toulgoat, and L. Lamont. Impact of trust-based security association and mobility on the delay metric in manet. *Journal of Communications and Networks*, 1:105–111, 2016.

[14] Advanced encryption standard (aes).

[15] A. Adekunle and S. Woodhead. An aead cryptographic framework and tinyaead construct for secure wsn communication. In *Wireless Advanced (WiAd)*, 2012.