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.

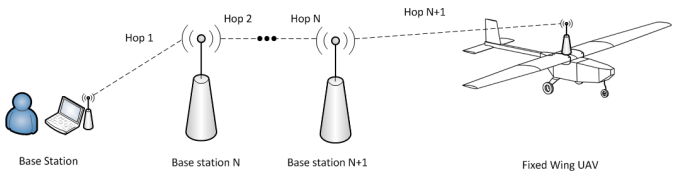

Fig. 1. Wireless open loop control scenario

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).

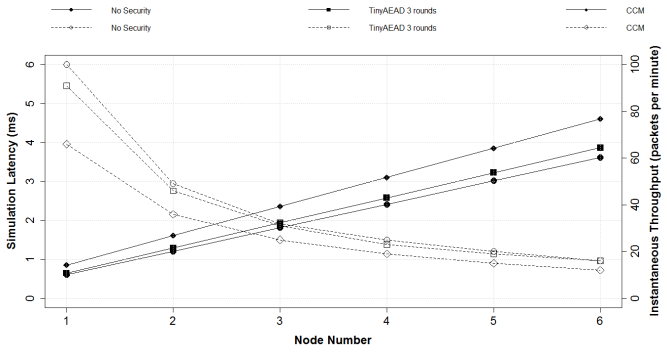

Fig. 2. Simulation results of throughput and latency for a 36 byte packet. Node 1 is the start node, Node 6 is the end node. The first hop is from Node 1 to Node 2

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)

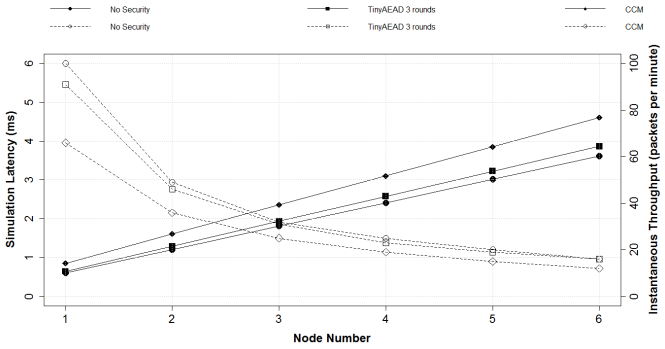

Fig. 3. Simulation results of throughput and latency for a 84 byte packet. Node 1 is the start node, Node 6 is the end node. The first hop is from Node 1 to Node 2

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.

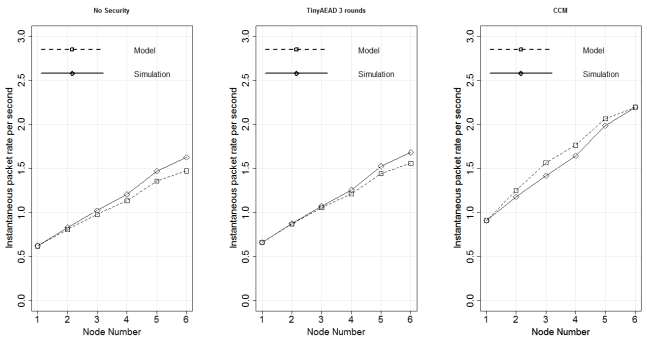

Fig. 4. Simulation versus Model results for throughput for a 36 byte packet

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.

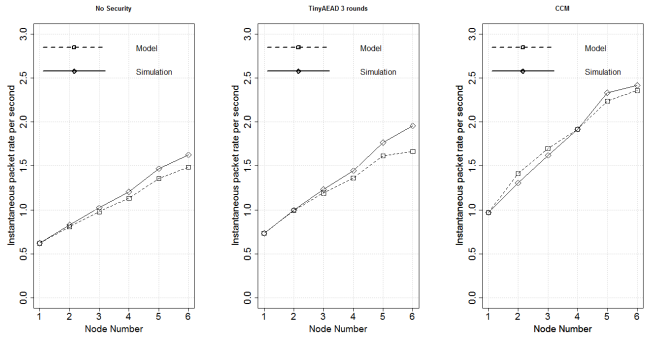

Fig. 5. Simulation versus Model results for throughput for a 84 byte packet

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.