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.

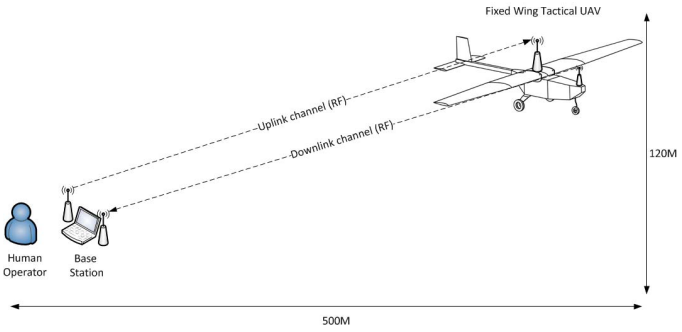

Figure 1. Illustrative concept of a point to point link for fixed wing UAV communication

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:

- 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.

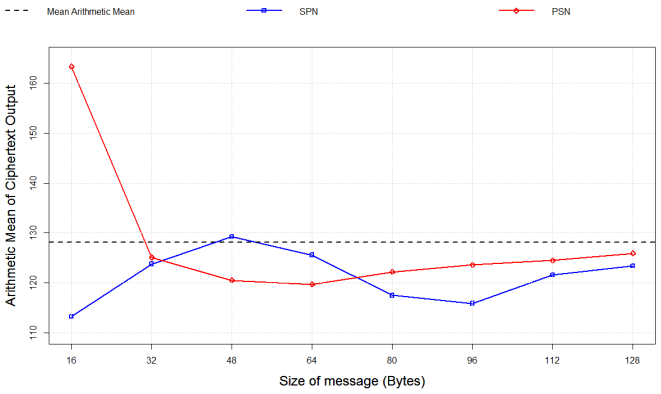

Figure 3. Comparison of the arithmetic mean of SPN and PSN using ten rounds with various byte sized messages

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.