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.

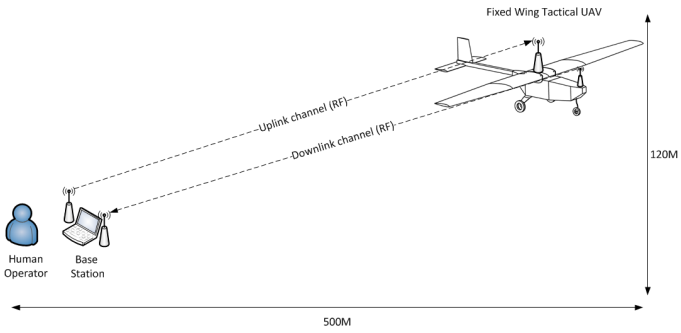

Figure 1. Illustrative concept of a point to point link for fixed wing UAV communication

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.

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.

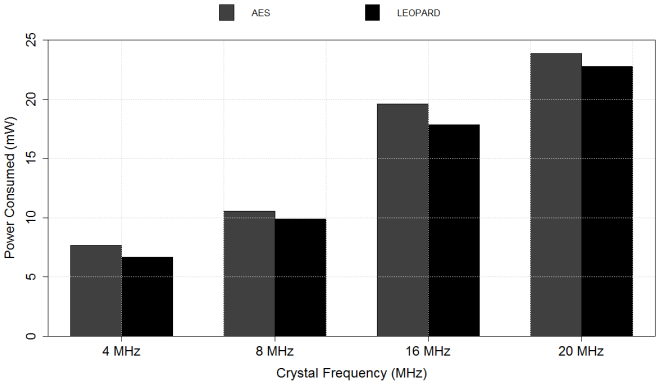

Figure 3. Comparison of power consumed of a mobile real-time system with LEOPARD and AES cryptographic primitives at various crystal frequency

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.