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

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.

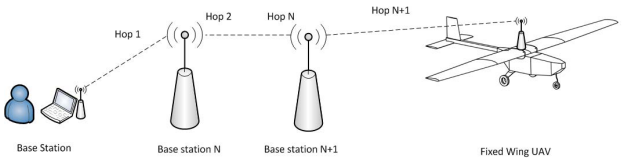

Figure 1. Illustrative concept of a circuit switched linear fixed wing UAV multi-hop topology

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.

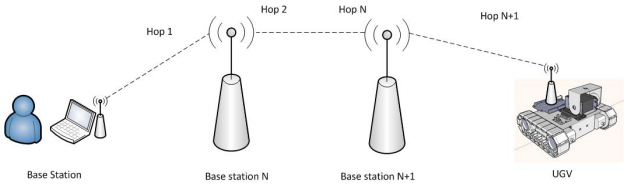

Figure 2. Illustrative concept of a circuit switched linear UGV multi-hop topology

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.

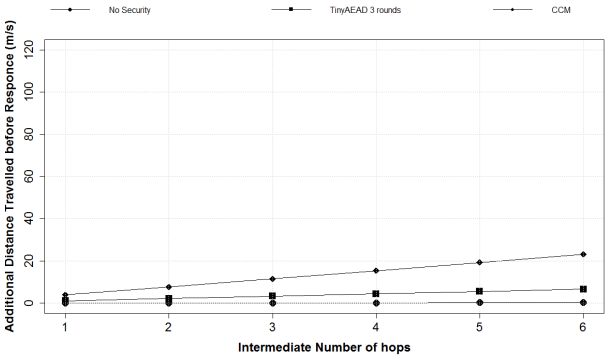

Figure 3. Simulation results of the additional distance incurred by a 30 mph UGV over multiple hops using a 36 byte packet

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.

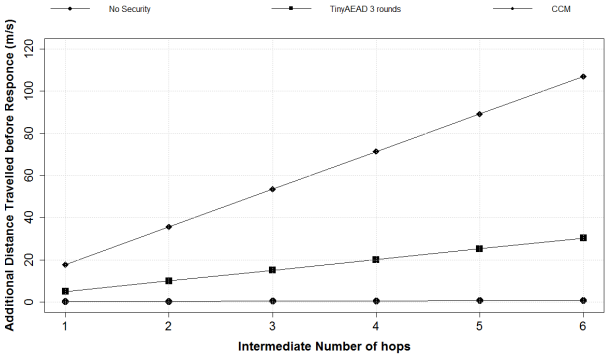

Figure 4. Simulation results of the additional distance incurred by a 135 mph fixed wing UAV over multiple hops using a 36 byte packet

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.

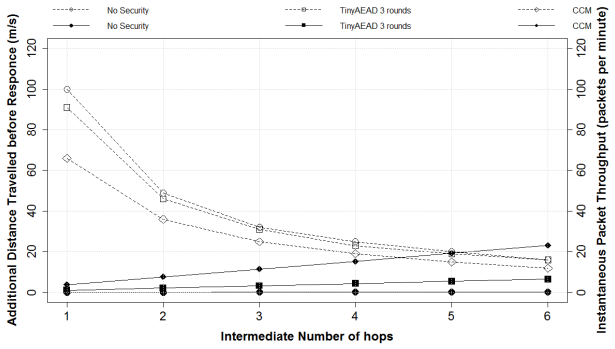

Figure 5. Balance of QoS and QoE of a UGV with and without secure communications. Additional distance travelled by the vehicle is represented by the filled line and the instantaneous throughput is represented by the dashed line

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.

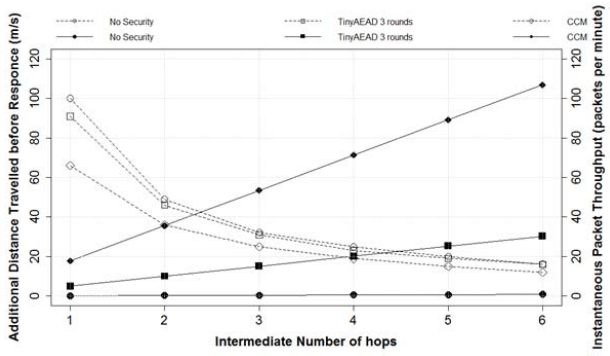

Figure 6. Balance of QoS and QoE of a fixed wing UAV with and without secure communications. Additional distance travelled by the vehicle is represented by the filled line and the instantaneous throughput is represented by the dashed line

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.