The Secure UAV Communication Link Based on OTP Encryption Technique

Sukhrob Atoev[1], Oh-Jun Kwon[2], Chee-Yong Kim[3], Suk-Hwan Lee[4], Young-Rak Choi[5], Ki-Ryong Kwon[1]

[1]Dept. of IT Convergence and Application Engineering, Pukyong National University

[2]Dept. of Computer Software Engineering, [3]Major of Game Animation Engineering, Dongeui University

[4]Dept. of Information Security, Tongmyong University, [5]A&C Company

sukhrob.reus@gmail.com, krkwon@pknu.ac.kr, skylee@tu.ac.kr

Abstract- The demand on the security and reliability of the communication and data link of unmanned aerial vehicle (UAV) is much higher since the environment of the modern battlefield is becoming more and more complex. Since the UAV communication link and its reliability evaluation represent an arduous field, we have concentrated our work on this topic. A UAV communication channel is a key factor that can affect the performance of the data link in terms of high data rate and reliable transmission of information. Moreover, the wireless communication channel opens up the door for several types of remote attacks. Therefore, the communication channel between the vehicle and ground control station (GCS) should be secure and has to provide an efficient data link. For this purpose, we have investigated the one-time pad (OTP) encryption technique for a UAV communication system. The comparative results present that OTP has better performance in terms of accuracy and execution time than other encryption algorithms.

Keywords— UAV(unmanned aerial vehicle), OTP(one-time pad), GCS(ground control station), encryption algorithms

1. Introduction

In recent years, providing a secure communication link for unmanned aerial vehicles (UAVs), widely known as drones, has become a crucial task, since most of these vehicles are used for military tasks, delivery services, search and rescue operations. These vehicles can be controlled either under remote control (RC) by a pilot operator or autonomously by onboard computers. The data link between the vehicle and ground control station (GCS) is established by a wireless communication link that would allow an attacker to hijack and steal the UAV or interface with its operation in a way that forces it to crash into the ground. Therefore, securing the communication link using encryption methods plays an important role in the UAV communication system.

In [1], the authors developed an efficient and secure mechanism that minimizes overhead using RC5 encryption on the MAVLink communication protocol for unmanned aircraft system (UAS). In [2], the encryption scheme chosen to realize a secure communication link for information transfer between a MAV and its GCS. The scheme involves AES-128 in CTR mode for encryption, SHA-256 for key hashing and Diffie Hellman algorithm for key exchange. This scheme was developed both on the MAV autopilot and the GCS and integrated with the MAVLink protocol.

Generally, a UAV communication link can both send control commands from the GCS to vehicle and receive data about the flight on downlink, as shown in Figure 1. A bidirectional link can be established in order to provide a communication between the UAV and GCS [3]. A communication link between these two components should

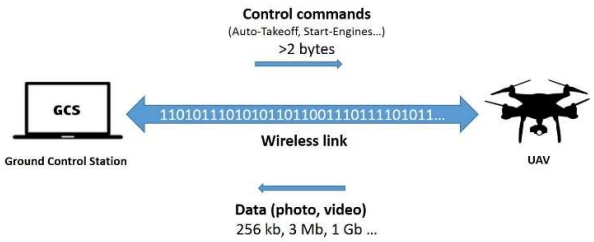

Figure 1. UAV communication link.

be secure and has to provide long range operations as well as a continuous and stable link.

2. One-Time Pad Encryption

The one-time pad (OTP) encryption is the only proven unbreakable encryption method. The OTP encryption algorithm is a binary additive stream cipher, where a stream of truly random keys is generated and then combined with the plaintext for encryption or with the ciphertext for decryption by the XOR addition [4].

The OTP encryption method has the following requirements:

- The key must be truly random;
- The OTP page must only be used once;
- The key length must be as long as the plaintext;
- The used page should be destroyed.

In this encryption method, OTP keys are used in pairs. One copy of the key is kept by each user and the keys are distributed securely prior to encryption. To encrypt the plaintext data, the sender uses a key string equal in length to the plaintext. The key is used by XORing bit by bit, always a bit of the key with a bit of the plaintext to create a bit of ciphertext. Afterwards, this ciphertext is sent to the recipient. On the recipient's side, the encoded message is XORed with the duplicate copy of the OTP key and the plaintext is restored. To ensure the randomness of the keys, both sender's and recipient's keys are automatically destroyed after use.

Let L be the number of bits in the plaintext string, then i ranges from 1 to L. A system can be called

unconditionally secure, when the probability of observing any particular OTP key bit is equals to the probability of observing any other OTP key bit, as expressed by the following equation:

$$c_i = p_i \ XOR \ k_i \quad \Leftrightarrow \quad P(p_i) = P(p_i|c_i) \qquad (1)$$

where p_i is the i^{th} bit in the plaintext string, c_i is the i^{th} bit in the ciphertext string, k_i is the i^{th} bit in the key string, $P(p_i)$ represents the probability that p_i was sent, $P(p_i|c_i)$ represents the probability that p_i was sent given that c_i was observed.

3. Methodology

The secure UAV communication system, as shown in Figure 2, consists of the GCS, the UAV, an attacker, MAVLink protocol [5], and the data link used to facilitate communication. The GCS transmits commands to the UAV at a fixed interval to perform the legitimate command and control. The MAVLink protocol maintains a connection between the UAV and GCS. After establishing a successful connection, payload data can be represented as signals when they are carried by the MAVLink through a wireless link.

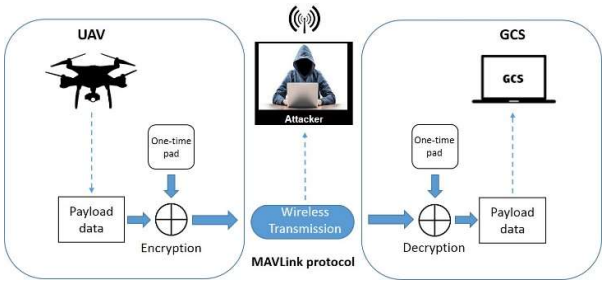

Figure 2. Securing the communication link.

To ensure the transmission of data between the vehicle and GCS, a UAV uses a data link that operates in the frequency range from 150 MHz to 1.5 GHz. On the other hand, a 2.4 GHz frequency band that determines the communication link between the transmitter and receiver is used in order to control the vehicle. During our experiments, we have used two 3DR 915 MHz telemetry radios to communicate over the data link.

In order to secure the communication link between the UAV and GCS, we have divided our work into two parts. In the first part, to secure the MAVLink protocol with OTP encryption technique, GCS source code was modified to include the encryption and decryption functions. In this step, we used the Mission Planner software as the GCS. Secondly, in the same scenario, to secure the communication link between the vehicle and GCS, MAVLink protocol source code was modified to include the encryption and decryption functions.

4. Result Analysis

In this work, the C++ code is performed to encrypt and decrypt the data that can be the control commands, recorded videos and photos, which transmitted between the vehicle and GCS. Actually, there are several commands to control the UAV such as “Start-Engines”, “Auto-Takeoff”, “Enable Autopilot”, etc., in UAV communication system. It should be mentioned that these control commands are represented by hexadecimal numbers.

$$Accuracy = \frac{Number \ of \ encrypted \ bits}{Number \ of \ total \ bits} \qquad (2)$$

Accuracy of the different encryption algorithms is computed by using Equation (2), and shown in Figure 3 and Table 1. It can be observed that OTP encryption technique encrypts and decrypts the data more accurately compare to 3DES, Twofish and AES-128 encryption algorithms.

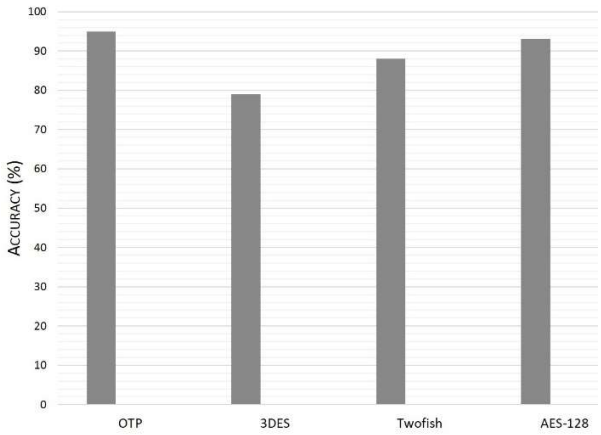

Figure 3. Accuracy comparison of different encryption algorithms

As demonstrated in Figure 4, the execution time for various encryption algorithms depends on the size of the data that can be the control commands, recorded videos and photos.

Table 1. Accuracy of the different encryption algorithms.

Encryption algorithm	Accuracy (%)
OTP	95
3DES	79
Twofish	88
AES-128	93

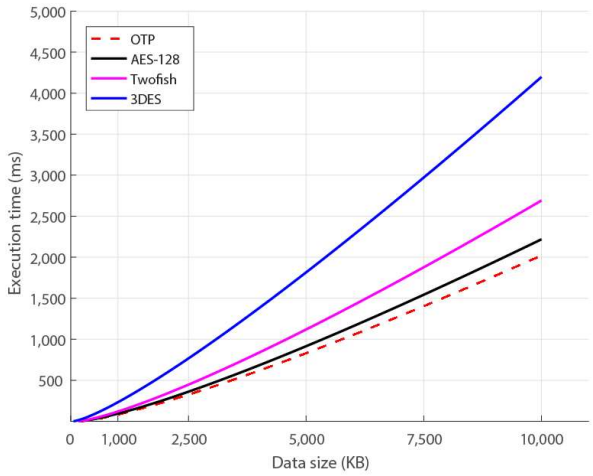

Figure 4. Execution time for different encryption algorithms.

According to the accuracy and execution time performances that are presented in Figures 3 and 4, OTP is more effective than other encryption algorithms to secure the UAV communication link.

5. Conclusion

Since the communication link is an essential part of the UAV, our current work has been carried out in this field. The main purpose of this work was to provide a method for securing the UAV communication link. For this purpose, one-time pad encryption technique was selected because of its security level and speed of encryption. The comparative results obtained from our experiments demonstrate that OTP has better performance than other encryption algorithms.

Acknowledgment

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program (IITP-2019-2016-0-00318) supervised by the IITP (Institute for Information & communications Technology Promotion), Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (No. 2016R1D1A3B03931003, No. 2017R1A2B2012456)

References

[1] N. Butcher, A. Stewart, and S. Biaz, "Securing the MAVLink Communication Protocol for Unmanned Aircraft Systems," *Technical Report #CSSE14-02*.

[2] N. Prapulla, S. Veena, and G. Srinivasalu, "Development of Algorithms for MAV Security," *IEEE International Conference On Recent Trends In Electronics Information Communication Technology*, India, pp. 799-802. 2016.

[3] G. Crespo, G. Glez-de-Rivera, J. Garrido, and R. Ponticelli, "Setup of a communicaton and control systems of a quadrotor type Unmanned Aerial Vehicle," *IEEE Conference on Design of Circuits and Integrated Systems (DCIS)*, Madrid, 2014.

[4] One-Time Pad. Available online: https://www.cryptomuseum.com/crypto/otp/index.htm

[5] MAVLink Protocol Overview. Available online: https://mavlink.io/en/protocol/overview.html