Security Authentication System using Encrypted Channel on UAV Network

Kwanwoong Yoon
Computer Science Engineering
Pusan National University
dbsrhksdnd@gmail.com

Daejun Park
Computer Science Engineering
Hanbat National University
cowzon90@gmail.com

Yujin Yim
Computer Science Engineering
Chungbuk National University
itfgo950@gmail.com

Kyounghee Kim
Computer Science Engineering
Seoul Women's University
maec477@gmail.com

Szu Kai Yang
Computer Information Technology
Purdue University
yang878@purdue.edu

Myles Robinson
Computer Information Technology
Purdue University
robin249@purdue.edu

***Abstract*—Today, UAVs are used in various fields such as monitor, search and rescue missions as well as military. UAVs are useful in various fields, but security has always been a major concern. Additionally, UAV carries sensitive information related to people's privacy and it causes critical problems if the data is exploited by malicious attackers. There were many attempts to solve security problems of UAVs but there is no typical way to protect UAVs from cyber attacks. In this research, we focus on a solution of hijacking network channel or physical hardware by anonymous attackers on commercial UAVs. This paper proposed maintaining control of UAV in hijacking problem with an additional encrypted communication channel, authentication algorithm and DoS attack through Raspberry Pi and shown high applicability on the commercial UAVs.**

I. Introduction

A. Motivation

An unmanned aircraft system(UAS) is an aircraft system without a human pilot. Unmanned aerial vehicle(UAV), also known as a drone, is used in UAS generally. UAVs also have the ability to be remotely controlled or programmed with high efficiency due to lower cost and lightweight features than other aircraft. The advantages of UAVs have gained popularity from many fields such as commercial services, scientific researches, agriculture as well as military missions[1]. They have become pervasive and employed in various fields. In 2013, Amazon announced a new service called Prime Air, a new method of package delivering using UAV, will be available in the future. [2]. However, UAV is very vulnerable to attacks, as they communicate through wireless network. In fact, DoS attack on UAV will be as successful as any Wifi access points[3]. It will be perilous to expose private or personal data that was stored on UAV to attackers. All the valuable and private data should be kept in top security system. Hence, safeguarding UAV from unauthorized access and disruption is vital for UAVs future development.

B. Background

Some attacks on UAVs reveal the vulnerability of UAV security. There are a lot of attacks which are related to wireless networks on UAVs such as,Telnet/FTP attack, DoS, ARP spoofing[4], ad-hoc network[5] and Man in the Middle attack[3]. In other words, UAV wireless connection is an easy point of target when there is no strong protection against malicious hackers[6]. The security researcher, Samy Kamkar, took control of a Parrot AR Drone by deauthenticating the drone and commanding it through his script that was implemented on Raspberry pi[7]. To solve the problem like this in a hijacked environment, this paper propose an advanced idea of encrypted channel[8] to enhance the security of data in UAV system using Raspberry Pi.

C. What was done

The paper is structured as follows: Section 2 proposes a new model to set the UAV operating environment and new algorithm to authorize between the ground station(GS) and the UAV. Section 3 suggests program based on Section 2 in depth. There are included implementation of our system in two cases, synchronizing data before taking-off and authentication processes after taking-off. In Section 4, results of this research are presented.

978-1-5090-6724-4/17 $31.00 © 2017 IEEE
DOI 10.1109/IRC.2017.56

Finally, Section 5 concludes and summarizes this paper, then provides future works.

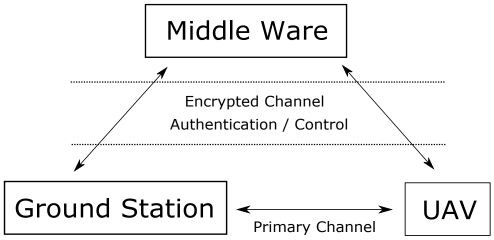

Fig. 1. 3-party model of the system

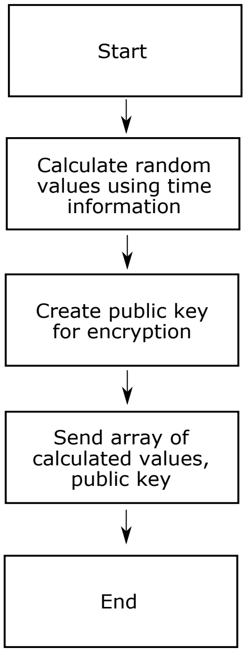
Start
Calculate random values using time information
Create public key for encryption
Send array of calculated values, public key
End

Fig. 2. Process of synchronization for authentication before a UAV takes off

II. Body

A. Model

Fig. 1 shows the 3-party network model that addresses the previously mentioned security problems in UAVs. This model can deal with network and physical security problems. In a network environment, GS can control the movement of UAV and get video/navigation data through both channels. Middleware is directly connected with UAV and processes authentication with GS. Middleware manages two communication channels and detects intrusions of anonymous attackers through the primary channel. When it detects intrusion, it will DoS attack the primary channel to make the attacker lose control of the primary channel. In physical environments, the paper have been designed an electrical circuit to disable UAV hardware for the sake of protecting important data from leaking when it is taken by someone physically. GS can send a destruction signal through an encrypted channel .

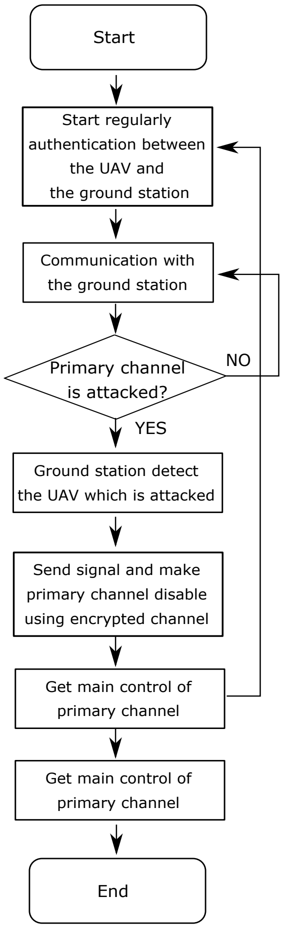
Start
Start regularly authentication between the UAV and the ground station
Communication with the ground station
Primary channel is attacked?
NO
YES
Ground station detect the UAV which is attacked
Send signal and make primary channel disable using encrypted channel
Get main control of primary channel
Get main control of primary channel
End

Fig. 3. Algorithm of entire system

B. Algorithms

In Fig. 2, before UAV takes off, GS calculates random values using the time zones and creates a public key for AES encryption which has high security level[9]. Then GS sends the UAV an array of random values and the public key. UAV is ready to take-off after GS checks that the UAV has received them correctly.

Fig. 3 shows our algorithm of this system. Starting to fly, UAV starts periodically to authenticate between UAV and GS. The primary channel of UAV is monitored

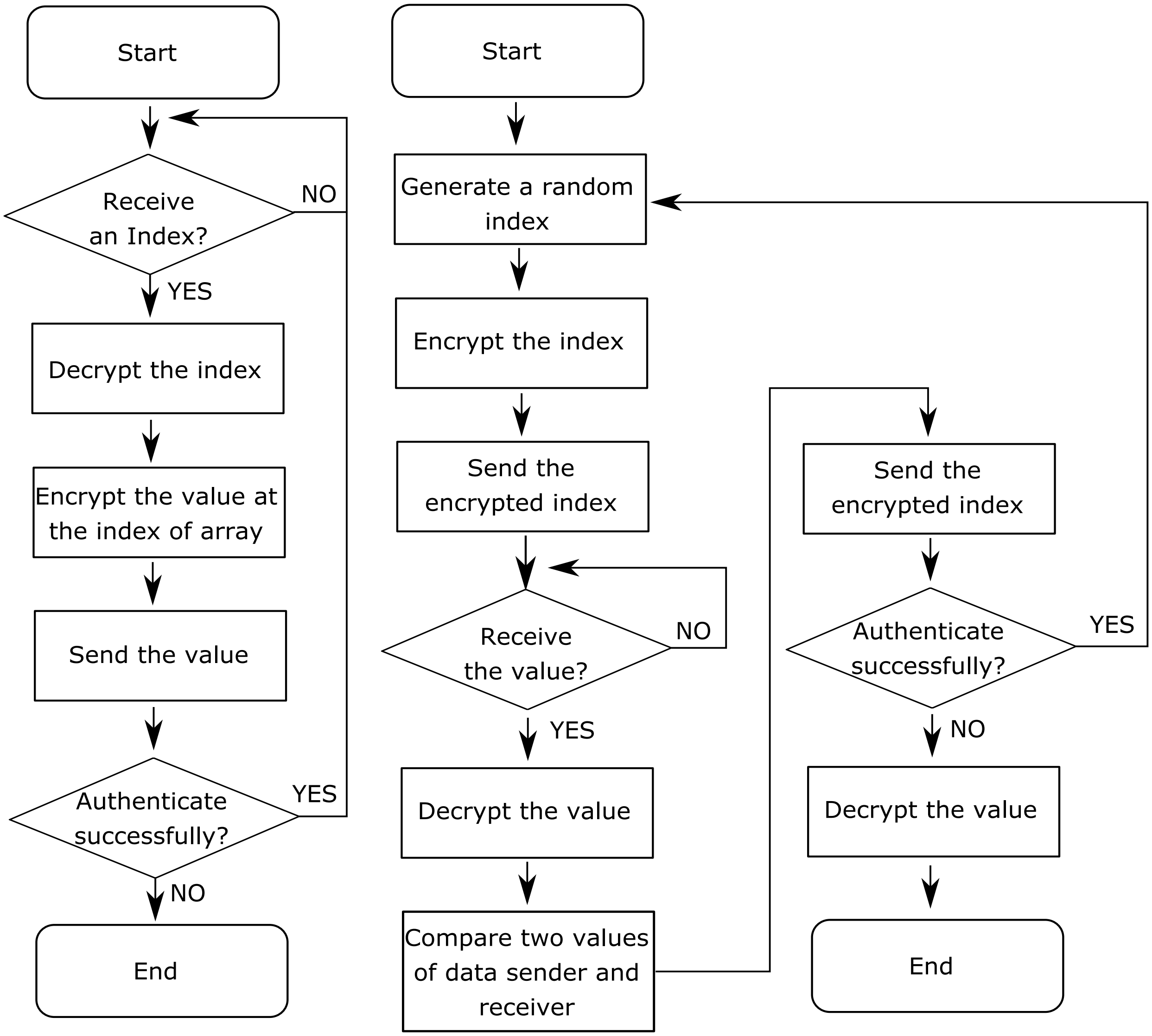

Fig. 4. Algorithm of authentication in data sender(left) and data receiver(right) when UAV is flying

whether it is attacked or not during communication with GS. The GS will detect the UAV which has been attacked from malicious devices in the UAV network. Then GS sends the UAV a signal to disable the primary channel in order to prevent a leakage of data through a hijacked channel. Following, UAV lands, ends or continues to communicate with the GS.

Fig. 4 shows an authentication algorithm when UAV wants to build or maintain a communication channel with other devices during the flight. In many cases, UAV collects a range of data and sends it to GS. Accordingly, data sender is UAV and data receiver is GS. First of all, the data sender generates an encrypted random index to send it to the data receiver. When the data receiver receives the data, it decrypts the index using the public key.

Then, the receiver encrypts the value at the index of array which was synchronized before take-off and sends it to the data sender. Receiving and decrypting the data from data receiver, data sender compares the received value with its own value at the index of array. If both values are correct, authentication succeeds and the authentication process continues while they are having communication. However, if the two values are incorrect, authentication fails . When authentication has failed, the data sender disconnects this channel and returns to the

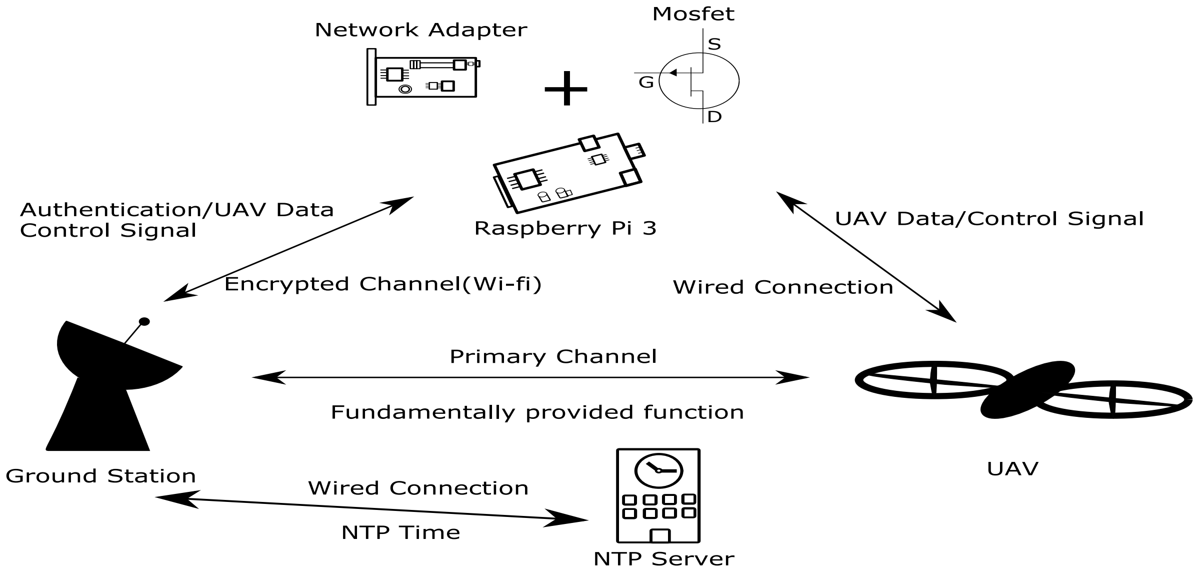

Fig. 5. Overview of the proposed program

first step. In this process, the proposed algorithm can be a solution of the reflection attack[10] which is occurred in bi-directional, challenge-response, mutual authentication protocols. The attackers easily get authentication by reflecting the authenticator's public key. In the contrast, this algorithm can prevent the intrusion from the attacker by processing the authentication with encrypted index value internally.

III. Realization

A. Programs

As shown in Fig. 5, the suggested program according to the model which we mentioned in Section 3. As this paper proposed, the program is a 3-party model. The program uses an online NTP Server pool for NTP Server which is provided for free. Through the encrypted channel, GS can control UAV perfectly. The authentication algorithm is used to build an encrypted channel.

GS can send a destruction signal to close the MOSFET that is wired to short UAV battery when it has been hijacked physically and executing a DoS attack signal when an anonymous attacker breaks into the primary channel. For this function, Raspberry Pi 3 has an additional network adapter to execute the DoS attack and electric circuit to disable the UAV.

The electric circuit that will disable UAV hardware such as memory storage entirely. Lithium cells are burnable in short-circuit[11], hence lithium battery and MOSFET are used in the circuit that will disable UAV. This component is designed to cause short-circuit in the particular condition. Raspberry Pi makes the particular condition by emitting certain voltage level from their electrical I/O port. When Raspberry Pi get a destruction signal from GS, it can disable the UAV using this circuit.

B. Implementation

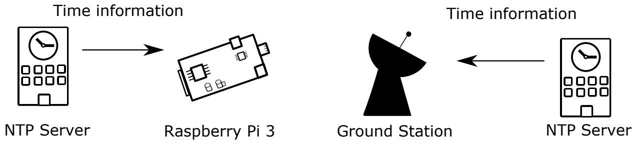

Fig. 6. Generate cipher based time

Stronger authenticated channel needs stall-free transmission for security[12] and proceeds some procedures such as generating the encrypted key, synchronizing before UAVs flight and periodical authentication during the flight .

In Fig. 6, GS and Raspberry Pi create the AES public key and random values based on time information from NTP server which are used for authentication. And then, the created values are stored in a key-table. In this process, the generated key is used for authentication of this channel.

In Fig. 7, system time, the AES public key value must be synchronized between GS and Raspberry Pi. GS and Raspberry Pi will create the key using the time information from each side of NTP server. Like the figure above, each module makes the key separately. If they

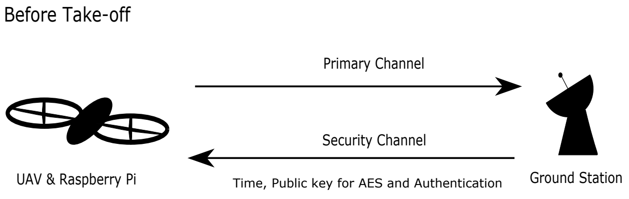

Fig. 7. Time synchronization before take-off

did not synchronize before hovering, each device cannot succeed in authentication after the flight.

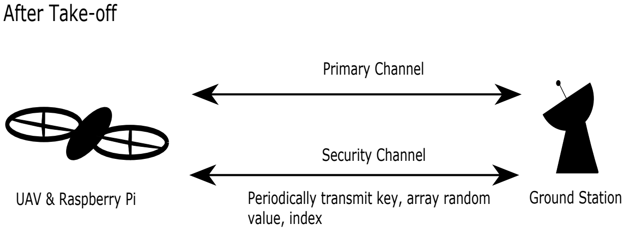

Fig. 8. Authentication when UAV is flying

In Fig. 8, If Raspberry Pi and GS succeed to synchronize the time and take off, they will follow this algorithm. The channel is authenticated periodically every 60 seconds. In authentication process, Raspberry Pi requests the key-table value from GS. After Raspberry Pi receives the value of the key-table, Pi compares its key value with the received packet of the index from GS. If values are the same, then authentication will be done successfully. Otherwise, authentication will fail and the connection of channel will be expired. Through the authenticated channel, Raspberry Pi can send video, GPS and sensor data to GS and GS sends commands to the UAV through Raspberry Pi.

IV. Result

This paper has presented encrypted and secure communication protocol suitable for multi-UAV and Ground Station. A validation test on paralyzing primary channel through DoS attack was carried out by using Wi-Fi penetration testing tool such as Aircrack-ng. The experiment of data communication with WPA2 Wi-fi connection between Raspberry Pi and AR drone shown that there are 10 seconds delay before GS receives data and an over 80 percent growth of CPU usage on Raspberry Pi. A successful connection between UAV on second channel increased the possibility to regain control of UAV if malicious attack such as DoS, on UAV was found. These results shown that higher performance devices to achieve middleware are required for better performance. Furthermore, the proposed algorithm has applicability on commercial UAVs such as AR Drone to make higher security level.

V. Conclusion

This paper has presented a second channel security system design to regain control of UAV if any attack was found on UAV. An analysis of time delay and CPU performance between Raspberry Pi and GS was performed. While a successful communication was established on second channel, a security improvement of the UAV can be done by having self-destroy functions if second channel is compromised. The future work will involve controlling and testing performance of circuits with MOSFET connected to UAV lithium battery on secure channel and shorten time delay between GS and Raspberry Pi.

Acknowledgment

This material is based on work supported by the National program for Excellence in Software of Republic of Korea.

References

[1] 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*. IEEE, 2013, pp. 1–23.

[2] B. Handwerk, "surprising drone uses (besides amazon delivery)," *National Geographic*, Dec. 2013.

[3] N. M. Rodday, R. d. O. Schmidt, and A. Pras, "Exploring security vulnerabilities of unmanned aerial vehicles," in *Network Operations and Management Symposium (NOMS), 2016 IEEE/IFIP*. IEEE, 2016, pp. 993–994.

[4] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson, and W. Alexis, "Securing commercial wifi-based uavs from common security attacks," in *Military Communications Conference, MILCOM 2016-2016 IEEE*. IEEE, 2016, pp. 1213–1218.

[5] J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu, "Adaptive security for multi-layer ad-hoc networks. special issue of wireless communications and mobile computing," *John Wiley InterScience Press*, 2002.

[6] S. Vemi and C. Panchev, "Vulnerability testing of wireless access points using unmanned aerial vehicles(uav)," *European Conference on e-Learning*, 2015.

[7] S. samyk., "Skyjack," https://github.com/samyk/skyjack, Dec. 2013.

[8] J.-S. Pleban, R. Band, and R. Creutzburg, "Hacking and securing the ar. drone 2.0 quadcopter: investigations for improving the security of a toy," in *IS&T/SPIE Electronic Imaging*. International Society for Optics and Photonics, 2014, pp. 90 300L–90 300L.

[9] G. Singh, "A study of encryption algorithms (rsa, des, 3des and aes) for information security," *International Journal of Computer Applications*, vol. 67, no. 19, 2013.

[10] T. Clancy and H. Tschofenig, “Extensible authentication protocol-generalized pre-shared key (eap-gpsk) method,” Tech. Rep., 2009.

[11] Q. Wang, P. Ping, X. Zhao, G. Chu, J. Sun, and C. Chen, “Thermal runaway caused fire and explosion of lithium ion battery,” *Journal of power sources*, vol. 208, pp. 210–224, 2012.

[12] S. Pasini, “Secure communications over insecure channels using an authenticated channel,” mathesis, Swiss Federal Institute of Technology in Lausanne, Sep. 2005.