Simultaneous Attack on Drone and GCS in UAV Systems

(Invited Paper)

Jaemin Yu, Byeong-Moon Cho, and Kyung-Joon Park
Department of Information & Communication Engineering
DGIST
Daegue 42988, Republic of Korea
{ryujm95, bmcho, kjp}@dgist.ac.kr

Hwangnam Kim
School of Electrical Engineering
Korea University
Seoul, Republic of Korea
hnkim@korea.ac.kr

***Abstract*— Recently, drones are widely used in the commercial fields. Here, we explain how we can neutralize malicious drones and ground control systems (GCSs). The proposed method simultaneously attacks the drone and the GCS. We carry out simulation as well as experimental studies to validate the proposed attack.**

Keywords—UAV, drone, GCS, MAVLink, attack

I. INTRODUCTION

Recently, unmanned aerial vehicles (UAV), or so-called drones, have been widely used in various applications such as delivery service, disaster monitoring, and leisure, which can be considered as a key application of cyber-physical systems [1, 2]. With this trend, crime and terrorism using UAVs are becoming a critical concern. For example, there is an increasing number of malicious-purpose drones such as a drone carrying a bomb. Thus, it is of critical importance how to neutralize malicious drones in an effective manner.

Most malicious UAVs are controlled by the ground control system (GCS) in a network environment. Many UAVs and GCSs use the MAVLink protocol, the de facto standard, as a communication protocol for exchanging control information. Hence, it is possible to neutralize malicious UAVs by properly exploiting the weakness of the MAVLink protocol.

In this paper, in order to neutralize the malicious UAVs, we propose a simultaneous attack methodology on UAV and GCS. We exploit the vulnerability of the MAVLink protocol. Our attack method can effectively make the UAV keep hovering while the GCS cannot detect the attack. Unlike existing neutralizing methods such as jamming and anti-drone, the proposed attack method does not require any physical equipment. In addition, our approach does not cause any secondary damage by preventing crashes.

The rest of the paper is organized as follows. In section II, we describe the vulnerability of the MAVLink protocol and propose the attack method for neutralizing UAV and GCS. We verify the proposed attack method through simulation and experiment in Section III. Finally, our conclusion follows in section IV.

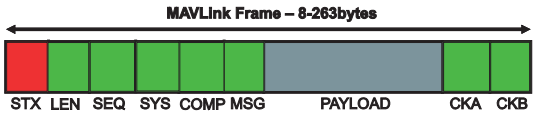

Fig. 1. MAVLink packet structure.

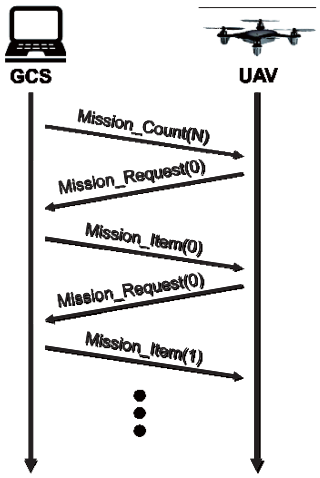

Fig. 2. Waypoint protocol procedure [8].

II. PROPOSED ATTACK USING VULNERABILITY

A. Vulnerability of MAVLink protocol

MAVLink is a very lightweight header-only message marshaling library for micro air vehicles [3]. Fig. 1 shows the MAVLink packet structure. Devices using MAVLink check the STX value, which is the first frame of the data packet to determine whether it is a MAVLink packet. In other words, encrypting the MAVLink packet changes the header value, so that devices using MAVLink cannot recognize it as a MAVLink packet. Hence, encryption is not adopted in MAVLink. Another reason for not using encryption is computational overhead, which is critical for UAV systems. For these reasons, encryption is not adopted in MAVLink, which is a major vulnerability of the protocol.

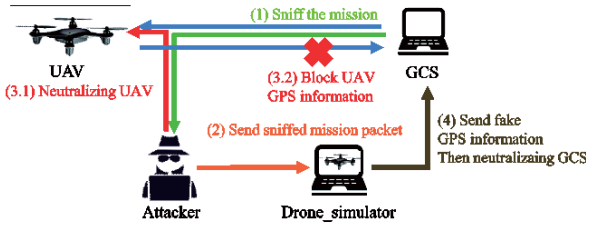

Fig. 3. Overall procedure of simultaneous attack.

B. *Neutralization of UAV*

We describe how to neutralize a UAV. In order to neutralize the UAV, we exploit the vulnerability of the waypoint protocol, which is used to convey the mission to the UAV. Fig. 2 shows the procedure of the waypoint protocol. When the GCS sends a Mission_Count packet in the waypoint protocol, the UAV deletes the stored mission information and gets ready to receive a new mission. Therefore, we can neutralize the malicious UAV by injecting a fake Mission_Count packet. When a UAV receives the fake Mission_Count packet, it keeps hovering, waiting for a new mission. Consequently, we can effectively neutralize the UAV without any crash.

C. *Neutralization of GCS*

Now, we describe how to neutralize GCS. The GCS checks whether the UAV is operating normally through sensor information (e.g. GPS, Altitude) sent from the UAV. The UAV periodically transmits the GLOBAL_POSITION_INT packet containing its GPS information to the GCS. Then, GCS is able to check the position of UAV through GPS information periodically transmitted from the UAV, and to check whether the mission is well performed. When a packet containing fake GPS information is sent to the GCS, the GCS is fooled while the UAV is neutralized. Therefore, the GCS cannot respond appropriately to the neutralization of the UAV.

D. *Proposed simultaneous attack*

We integrate the two methods for neutralizing UAV and GCS simultaneously. Here, we assume that the attacker has penetrated the network in advance. Thus, the attacker can intercept the packets sent and received between the drone and the GCS. Fig. 3 is a description of the simultaneous attack, which can be summarized as follows.

- GCS sends mission packet to UAV. At this time, attacker sniffs the Mission_Item or Mission_Request packet as mission packet. As shown in Fig. 2, these packets contain the mission information of the UAV.
- Attacker sends the sniffing mission packet to the drone_simulator. The drone_simulator then does the same task that GCS sent to the drone.

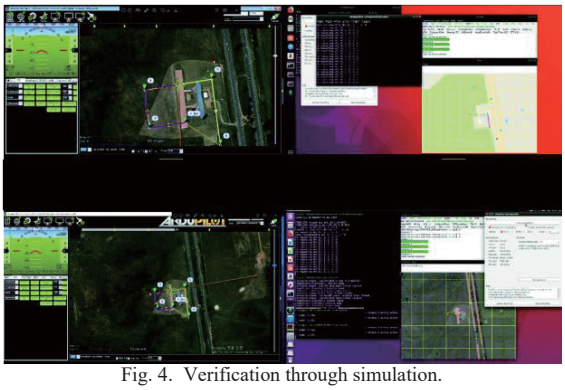
Fig. 4. Verification through simulation.

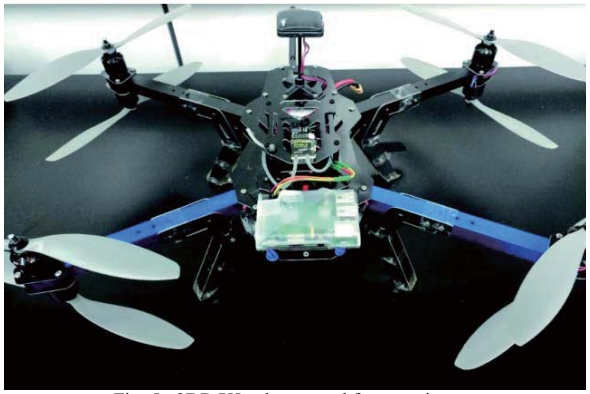
Fig. 5. 3DR X8+ drone used for experiment.

Fig. 6. Mission planner used for experiment.

- Attacker sends the Mission_Count packet to the Drone to neutralize the drone. At this time, the attacker blocks the GPS information that the drone sends to the GCS. Fake GPS information generated by the drone_simulator sends to GCS. We use the Packetsender to send packets [6].
- GCS recognizes that the drone is performing its mission through fake GPS information. Therefore, GCS cannot respond to the neutralization of the drone.

III. Attack implementation

A. Simulation result

We verify our simultaneous attack through simulation. UAV uses the software-in-the-loop (SITL) [4]. In the Fig. 4, the upper left corner of the GCS indicates the upper right, the lower left corner of the drone indicates the attacker drone, and the lower right corner indicates the attacker drone. As shown in Fig. 4, even if the drone is neutralized, the GCS cannot notice it because of the fake GPS information. Thus, the simulation shows that the drone and GCS can be neutralized at the same time.

B. Simulation result

We construct a testbed for further validation. We use the 3DR x8 + drones as shown in the Fig. 5, which uses the MAVLink protocol for experiments. Also, we use the Mission planner [7] as shown in the Fig. 6 for control of the drone. In the simulation, the GPS information cannot transmit to the GCS because the SITL being used as UAV has terminated. However, if we neutralize the UAV in the testbed environment, we should block the GPS information sent to the GCS because the UAV is hovering. So we use Ettercap [5] to block the GPS information of the UAV that is neutralized. As with the simulation, the experiment is conducted according to the proposed simultaneous attack. As shown in Fig. 7(a), we can confirm that the experiment can neutralize the UAV. Furthermore, from Fig. 7(b), we further confirm that the GCS can be neutralized.

IV. Conclusion

In this paper, we have studied the vulnerability of the MAVLink protocol and the neutralization of UAV and GCS. We have devised a simultaneous attack on UAV and GCS where we exploit the unencrypted feature of the MAVLink protocol. We have confirmed through simulation and experiment that the UAV and GCS neutralizing methods are effective.

Acknowledgment

This work was supported by the DGIST R&D Program of the Ministry of Science and ICT(18-ST-02) and Unmanned Vehicles Advanced Core Technology Research and Development Program Through the Unmanned Vehicle Advanced Research Center (UVARC) funded by the Ministry of Science, ICT and Future Planning, the Republic of Korea (NRF2016M1B3A1A01937599).

(a) Drone neutralization experiment.

(b) GCS neutralization experiment.

Fig. 7. Verification through experiment.

References

[1] K.-J. Park, R. Zheng, and X. Liu, "Cyber-physical systems: Milestones and research challenges," Computer Communications, vol. 36, issue 1, pp. 1-7, December 2012.

[2] K.-J. Park, J. Kim, H. Lim, and Y. Eun, "Robust path diversity for network quality of service in cyber-physical systems," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2204-2215, November 2014.

[3] MAVLink protocol. Accessed on: April. 13, 2018. [online]. Available: http://qgroundcontrol.org/mavlink/start

[4] Software in the loop (SITL). Accessed on: April. 13, 2018. [online]. Avalilable: http://ardupilot.org/dev/docs/sitl-simulator-software-in-the-loop.html

[5] Ettercap. Accessed on: April. 13, 2018. [online]. Available: http://www.ettercap-project.org/ettercap/

[6] Packetsender. Accessed on: April. 13, 2018. [online]. Available: https://packetsender.com/

[7] Mission planner. Accessed on: May. 1, 2018. [online]. Available: http://ardupilot.org/planner/docs/mission-planner-overview.html

[8] MAVLink waypoint protoocl. Accessed on: May. 1, 2018. [online]. Available: http://qgroundcontrol.org/mavlink/waypoint_protocol