Detecting UAV Attacks through Network Monitoring

Jaemin Yu
ryujm95@dgist.ac.kr
DGIST
Daegue 42988, Republic of Korea

Byeong-Moon Cho
bmcho@dgist.ac.kr
DGIST
Daegue 42988, Republic of Korea

Kyung-Joon Park
kjp@dgist.ac.kr
DGIST
Daegue 42988, Republic of Korea

ABSTRACT

The use of unmanned aerial vehicle (UAV), or so-called drone, is increasing in various fields such as agriculture, commercial, and transportation. UAVs are controlled over the network by ground control system (GCS). However, UAVs controlled by the network are vulnerable to attacks such as DoS attack, GPS spoofing and so on. In this paper, we propose a UAV attack detection method through network monitoring.

INTRODUCTION

In cyber-physical system (CPS), the unmanned aerial vehicle (UAV) system, or so-called drone, is a typical application [1,2]. The uses of drone are increasing in various fields such as agriculture, commercial, and transportation. However, there was an incident in which Iran forces captured the United States drone through GPS spoofing attack in December 2011. Thus, we can see that the drone is vulnerable to attack.

Since drones are vulnerable to security, they are targets of various attacks (ex. GPS spoofing, jamming attack, network attacks, etc.). In order to respond to the attack, detection of the attack must be prioritized. Therefore, the detection mechanism is important in the first step to prevent from UAV attacks.

In this paper, we propose a method to detect UAV attacks through network monitoring and packet analysis. We use various attack characteristics to detect attacks. By our proposed detection method, we can detect various UAV attacks without any physical equipment.

PROPOSED DETECTION MECHANISM

The proposed detection mechanism uses Snort for packet analysis. Snort is an open source intrusion detection system (IDS) that records traffic analysis and packets in real time. Snort can detect attacks by setting various rules [3]. Figure 1 shows how the processing of snort works.

Detecting DoS attack

First, we describe how to detect the DoS attack. DoS attack generates large amounts of traffic at the same time, which causes the system to run out of resources and makes normal operation impossible. Figure 2 shows that the amount of packets exchanged between the drone and the GCS through the experiment. Based on this information,

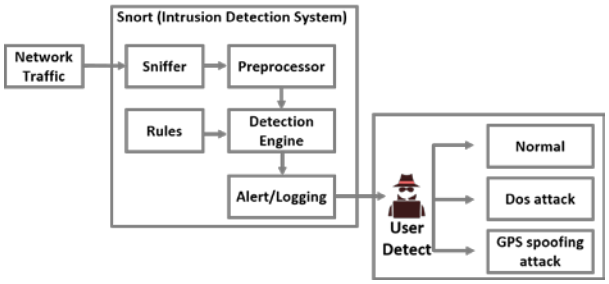

Figure 1. Process of Snort.

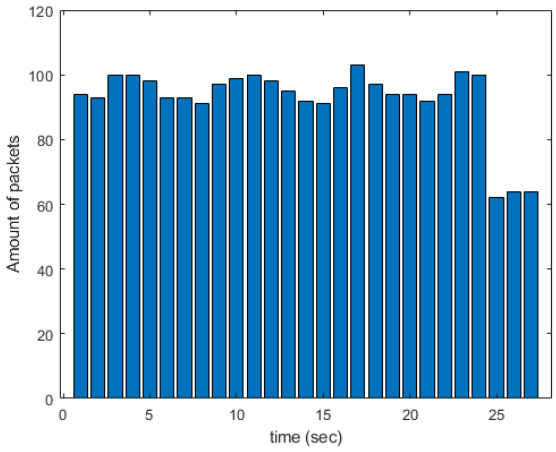

Figure 2. Amounts of packets between Drone and GCS.

we determine the maximum number of packets to detect the DoS attack. The maximum number of traffic is 104. So, we assume that a 20% increase in the number of packets exchanged between drone and GCS is DoS attack. That is, more than 120 packet/seconds can be considered a DoS attack.

Detecting GPS spoofing attack

Presented at the 7th Asian/Australian Rotorcraft Forum, Jeju Island, Korea, Oct. 30 - Nov. 1, 2018.

Second, we describe how to detect the GPS spoofing attack. GPS spoofing attack is to send a wrong GPS signal to prevent the drone from performing its normal mission. Drone periodically sends the GPS packet containing its location information to GCS [4]. At this time, the IDS detects and extracts packets containing the GPS information of the drone. At this time, the IDS detects and extracts packets containing the GPS information of the drone. Using this information, the GPS spoofing attack can be detected if the drone's movement path deviates from the mission.

SIMULATION RESULT

We use the snort IDS in the Windows environment for simulation. It also uses the basic analysis and security engine (BASE), a public analysis tool that can store and analyze snort detection in the database. Drone uses the software-in-the-loop (SITL) simulator [5], and the GCS uses the mission planner [6]. Table 1 shows the packet payload used for DoS attack. Figure 3 shows the log file that records DoS packets detected by Snort. Our proposed method can detect the DoS attack. Figure 4 shows that our proposed method can extract the GPS information. Transmit the extracted GPS information to the drone simulator of IDS. In Figure 5, the yellow line represents the mission path and the purple line represents the movement path of the drone. Figure 5 shows that the movement path of the UAV is off the mission path, we can detect that it has been attacked by a GPS spoofing attack.

CONCLUSIONS

We have proposed the UAV attack detection method through network monitoring and packet analysis. We have detected the DoS attack, GPS spoofing attack by our detection method. Our detection method has the advantage of detecting various attacks at the same time. We have confirmed our proposed detection method through simulation. In future work, we will study a more advanced detection method.

Table 1. Packet used for DoS attack.

Name		Payload	
Packet.1	*Packet.2*	fe:06:82:01:01:7d:88:13:00:00:00:00:48:9c	fe:24:67:01:01:93:b1:0c:00:00:ff:ff:ff:ff:ff:7f:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:f0:0a:00:00:00:01:95:13

Figure 3. DoS attack detection by the snort log file.

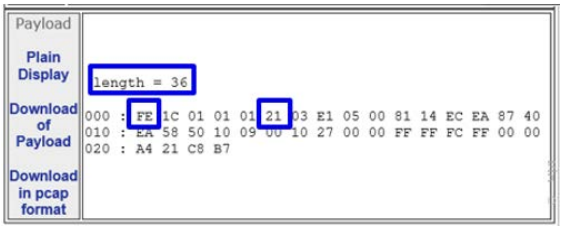

Figure 4. GPS information detected by Snort.

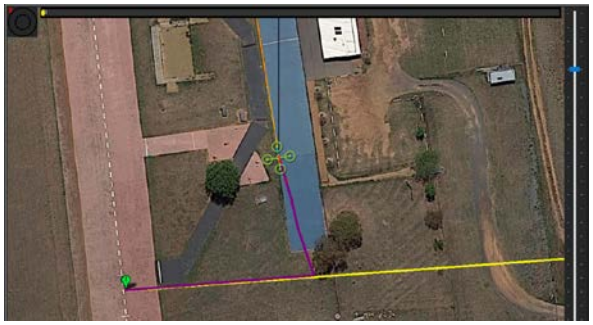

Figure 5. GPS spoofing attack detection by GPS information.

ACKNOWLEDGMENTS

This work was supported by 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 (NRF-2016M1B3A1A01937599) and the DGIST R&D Program of the Ministry of Science and ICT(18-ST-02).

REFERENCES

[1] Park, K. J., Zheng, R., & Liu, X. (2012). Cyber-Physical Systems: Milestones and Research Challenges. *Computer Communications*, *36*(1), 1-7.

[2] Park, K. J., Kim, J., Lim, H., & Eun, Y. (2014). Robust Path Diversity for Network Quality of Service in Cyber-Physical Systems. *IEEE Trans. Industrial Informatics*, *10*(4), 2204-2215.

[3] Snrot. Accessed on: August. 27, 2018. [online] Available: https://www.snort.org/

[4] Yu, J., Cho, B. M., Park, K. J., & Kim, H. (2018, July). Simultaneous Attack on Drone and GCS in UAV Systems. In *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 5-7). IEEE.

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

[6] Mission Planner. Accessed on: August. 27, 2018. [online] Available: http://ardupilot.org/planner/docs/mission-planner-overview.html