Journal of the Korea Convergence Society
Vol. 9. No. 8, pp. 41-46, 2018

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2018.9.8.041

Vulnerability Case Analysis of Wireless Moving Vehicle

Sangyun Oh, Jinkeun Hong*
Division of Infocom Communication, Baekseok University

무선이동체의 취약점 사례 분석

오상윤, 홍진근*
백석대학교 정보통신학부

Abstract As the industry related to drones has been activated, the public interest in drones has increased explosively, and many cases of drone-using are increasing. In the case of military drones, the security problem is the level of defense of the aircraft or cruise missiles, but commercial small and low cost drones are often released and utilized without security count-measure. This makes it possible for an attacker to easily gain access to the root of the drones, access internal files, or send fake packets. However, this droning problem can lead to another dangerous attack. In this regard, this paper has identified the vulnerabilities inherent in the commercial drones by analyzing the attack cases in the communication process of the specific drones. In this paper, we analyze and test the vulnerability in terms of scanning attack, meson attack, authentication revocation attack, packet stop command attack, packet retransmission attack, signal manipulation and de-compile attack. This study is useful for the analysis of drones attack and vulnerability.

Key Words : Wireless, Drone, Hijacking, Vulnerability, Security

요 약 최근 드론 관련 산업이 활성화되면서 드론에 대한 대중들의 관심이 폭발적으로 증가하였고, 드론을 활용하는 사례가 많이 늘어나고 있다. 군사용 드론의 경우 보안문제는 항공기나 순항미사일의 방어시스템 수준으로 보안이 철저하지만 상용 소형 저가형 드론들은 여전히 보안이 취약하거나 보안을 고려하지 않은 상태에서 출시되고 활용되는 경우가 많다. 이로 인하여 공격자가 쉽게 드론의 루트 권한을 얻고 내부 파일에 접근하거나 fake 패킷을 보내는 등의 드론 탈취 공격이 가능하다. 그런데 이 드론의 탈취 문제는 또 다른 위험한 공격으로 이어질 수 있다. 이런 측면에서 본 논문에서는 특정 드론의 통신과정에서 공격 사례를 중심으로 분석함으로써 상용 드론에 내재된 취약점을 확인하였다. 본 논문에서는 취약점을 스캐닝 공격, 중간자 공격, 인증 철회공격, 패킷 중지 명령 공격, 패킷 재전송 공격, 신호 조작 및 디 컴파일 공격 관점에서 접근하여 분석하고 실험하였다. 본 연구는 드론 공격과 취약점을 분석하는데 참고할 수 있는 유용한 연구로 사료된다.

주제어 : 무선, 드론, 하이재킹, 취약점, 보안

1. Introduction

Recently, the use of drones has been increasing with the development of drones. Drones can be applied to the delivery of goods or the reconnaissance mission of military drones, spraying agricultural drones for agricultural drones, and relaying sports games. However, as the drone technology develops, various problems and accidents have occurred in terms of security. For example, take a photo with a drone in a civilian access control facility or a military facility, or

*This paper is sponsored of Shanhak Project Funding of Baekseok University
*Corresponding Author : Jin-Keun Hong (jkhong@bu.ac.kr)
Received June 15. 2018 Revised July 10, 2018
Accepted August 20, 2018 Published August 28, 2018

use a drones as a hazardous material. As a result, malicious cases such as delivery to the victim increase, and the problem of hijacking of the drones is raised[1-7]. Most of these attacks are known as jamming of radio signals with respect to drones that send and receive RF communication [1]. In this paper, we analyze the attacks based on the communication protocol of drones that communicate based on Wi-Fi rather than jamming RF signals. The security of Wi-Fi-based drones has been constantly studied from previous research to countermeasures including attack cases. However, drones that are still sold for civilian use do not have these security related functions and operate as open APs with no security measures. In this respect, this study has analyzed the security weaknesses, focusing on one case of low cost commercial drones. The composition of this paper is discussed in Chapter 2. In Chapter 3, we focus on the case of drones attack. In Chapter 4, we analyze the weaknesses of drones cases. And concluded with Chapter 5.

2. Related Research

Vishal Dey etc have studied the security vulnerabilities and countermeasures of UAV[8]. It present a collection of attack cases, and security vulnerabilities for DJI Phantom 4 and Parrot Bebop 2 drones. Jung Hee Cheon etc present toward a secure drone system[9]. This is proposed an linearly homomorphic authenticated encryption scheme for the ground control center of a multi-rotor drone. Aakash Sehrawat etc reviews surveillance drone for diaster management and military security[10]. This design model is consists of Wi-Fi sensor, infrared camera, GPS for human tracking. Peter Blank etc present about privacy aware restricted areas for unmanned aerial systems[11], and review how privacy issue could be integrated with basic infrastructure to establish a framework for privacy-aware unmanned aerial system. Edwin Vattapparamban etc present drones for smart cities for issues in cybersecurity, privacy, and public safety[12]. Pericle Perazzo etc review path planner for drone based secure location verification[13]. David W. Casbeer etc present optimizing multiple UAV cooperative ground attack missions[14]. Peter T. Jardine etc review that avoidance of enemy defenses is achieved using linear inequality constraints and tested in a ground attack scenario involving a enemy defense system[15]. Stuart etc review cyber secure UAV communications at waveform respect[16]. Jeong Yoonsoo, et al. studied privacy protection model in cloud environment[17] and Moon Hyung Jin studied biometric information and OTP - based authentication using block chain[18]. Chae et al. review the security vulnerabilities and countermeasures in smart farm environment[19]. Choi et. al review security tendency analysis about machine learning algorithm[20].

3. Attack Threats of Drone

The model used in this study is the SYMA X5UW model and is shown in Fig. 1.

Fig. 1. SYMA X5UW Model

The drone has a dedicated controller and supports RF communication, but it supports 802.11 communication using a mobile phone.

Related attacks include middle attacks, certificate revocation attacks, packet retransmission attacks, steered application decompile, and signal analysis attacks.

If you can collect applications that send control commands to the drones, you can analyze the commands through the decompile process in the application. In this process, the attacker can send a fake

packet related to the control. An attacker can land the drones by sending control-related fake packets. You can also attack the drones where you want them. It is also possible to consider how to make the drones ignore the steering signals from the controls for this attack.

4. Vulnerability analysis by drones attack

4.1 Vulnerability Analysis by Scanning Attack

First, a scanning operation was performed on the attack target, which is shown in Fig. 2.

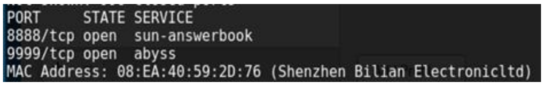

Fig. 2. Scanning Case1 of Drone Communication Protocol

The drones used in the experiment are Shenzhen Bilian company model with camera-equipped Wi-Fi function. The product specification only confirms that arbitrary service is provided in the port, and no other attack method can be found. Fig. 3 shows an attempt to search for a MAC address.

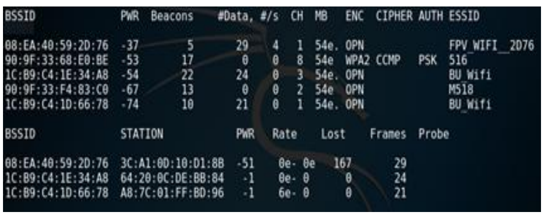

Fig. 3. Scanning Case2 of Drone Communication Protocol

The SSID of the detected drones is FPV_WIFI_2D76 and the MAC address is 08: EA: 40: 59: 2D: 76. The MAC address of the station (cell phone) connected to the drone is C: A1: 0D: 10: D1: 8B. The IP address of the drones can be confirmed to be the default gateway address of 172.16.10.1.

4.2 Vulnerability Analysis by man-in-the-middle attack

Next, Fig. 4 and 5 are examples of the MIM attack.

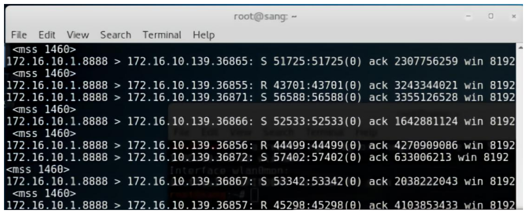

Fig. 4. MIM Attack Case1 of Drone Communication Protocol

The drones receive the APR response message sent by the attacker.

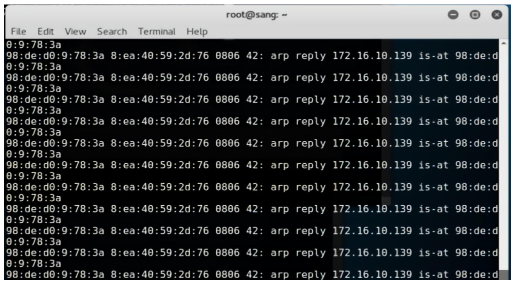

Fig. 5. Middle Attack Case2 of Drone Communication Protocol

The drones can not judge whether the attacker has maliciously sent an ARP packet or not from the mobile phone that is sending the manipulation related packet by the message alone. Therefore, the ARP Cache Poison attack can occur because the drones unconditionally receive all ARP response messages received without any confirmation process.

4.3 Vulnerability Analysis by authentication revocation attack

Next, Fig. 6 is an example of a certificate revocation attack. In the experiment, the wireless LAN card and the channel of the drones were matched and the authentication cancel packet was transmitted.

Fig. 6. DeAuthentication Attack of Drone Communication Protocol

With a revocation attack, disconnection and reconnection occur quickly on a mobile phone.

When the drones were attacked during the flight, as expected, the Wi-Fi connection on the cell phone was interrupted briefly, and the drones crashed.

4.4 Packet retransmission attack

Fig. 7 is an example of a packet retransmission attack. First, in order to confirm the experiment, the stop command of the dron for retransmission was executed and the experiment contents were captured. The stop command is likely to be at the beginning and end of the packet, and has frequent repeating features. I obtained the following data packet as a result of the specific packet.

```
User Datagram Protocol, Src Port: 6666, Dst Port: 5555
Data (27 bytes)
   Data: 436d6400010012000104040000a0000000808080802020202020...
   Text: Cmd
   [Length: 27]
```

Fig. 7. Stop Command Case of Packet in Drone Communication Protocol

The packet is retransmitted by modulating the MAC address and the IP address of the receiver. This is shown in Fig. 8.

```
root@sang:~# python
Python 2.7.13 (default, Jan 19 2017, 14:48:08)
[GCC 6.3.0 20170118] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from scapy.all import *
>>> from time import sleep
>>> srcIP ='172.16.10.139'
>>> dstIP ='172.16.10.1'
>>> srcPort = 6666
>>> dstPOrt = 5555
>>> srcMAC = '3C:A1:0D:10:D1:8B'
>>> dstMAC = '08:EA:40:59:2D:76'
>>> payload = "436d6400010012000104040000a0000000808080802020202000550f"
>>> print payload
436d6400010012000104040000a0000000808080802020202000550f
>>> spoofed_packet = IP(src=srcIP,dst=dstIP)/UDP(sport=srcPort,dport=dstPort)/pa
yload/Ether(src=srcMAC, dst=dstMAC)
```

Fig. 8. Re-transmission Attack Case of Packet in Drone Communication Protocol

And transmitted a retransmission message to the packet. As a result, we can confirm that the operation of the drones is stopped.

4.5 Vulnerability Analysis based on control application decompile and signal manipulation attack

Fig. 8 is an example of decompile and signal manipulation attacks. If you can get a steered app, you can easily decompile it. The following figure shows the result of analyzing only the data definition part among the decompile sources. The results of the analysis are as follows. The 17th bit is the throttle. The 18th bit is elev (pitch). The 19th bit is rudd (yaw). The 20th bit is a family (roll). The 21st bit is 32 (20 byte conversion). The 22th bit is the bit for the mode type supported by the drones. The 23th bit is the bit for the mode type supported by the drones. The 24th bit is the bit for the mode type supported by the drones. The 25th bit is the bit for the mode type supported by the drones. The default value is 0 when all modes are disabled. The 26th bit is the xor value for the 17th to 25th bit + 85 (85 = 55 in hexadecimal).

From the analysis result in Fig. 8, the attacker can change the steered packet to the intruder's intention and instruct the drone. The drones move in response to commands received from the attacker.

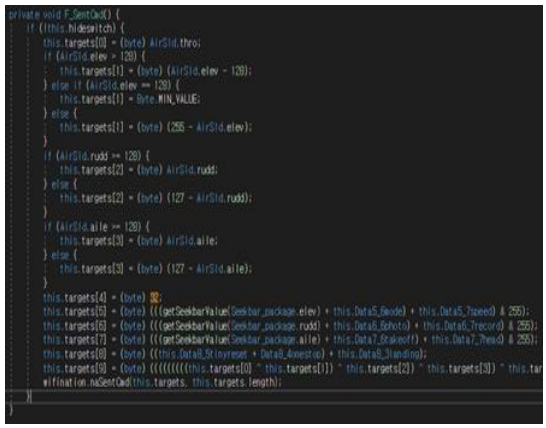

Fig. 8. De-compile Attack and Driving Signal Attack Case of Packet in Drone Communication Protocol

5. Conclusion

In this paper, we analyze the cases of drones attack using Wi - Fi - based communication and present the results of the experiments based on vulnerability of attacks. The basic premise of each attack scenario is that it is an unencrypted environment, so it can be confirmed that the connection to the AP is easy. If you do not use SSID broadcasts or use only basic WPA encryption, you will be able to defend these attacks sufficiently. In this paper, we analyze and test the vulnerability in terms of scanning attack, meson attack, authentication revocation attack, packet stop command attack, packet retransmission attack, signal manipulation and decompile attack. This study is useful for the analysis of drones attack and vulnerability. Future research will be conducted to compare and analyze various types of security vulnerabilities and to suggest solutions

REFERENCES

[1] http://jammers4u.com/drones-jammer

[2] https://www.usnews.com/news/national-news/articles/2017-11-10/homeland-security-warns-of-weaponized-drones-as-terror-threat

[3] http://www.thedrive.com/the-war-zone/17527/russia-is-trying-to-link-the-drone-swarm-attack-in-syria-to-a-us-p-8-patrol-plane

[4] https://warontherocks.com/2017/01/the-drone-threat-to-israeli-national-security/

[5] J. S. Pleban, R. Band & R. Creutzburg. (2014). Hacking and securing the AR.Drone 2.0 quadcopter: investigations for improving the security of a toy, *SPIE 9030, Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2014,* DOI: 10.1117/12.2044868

[6] S. H. Na, J. C. Han & B. J. Ahn. (2014), A Study on the Defence for Deauthentication Attacks in Wi-Fi Network, *Korea Communication Society Conference*, 631-632.

[7] https://github.com/markszabo/drone-hacking/blob/master/README.md

[8] V. Dey, V. Pudi, A. Chattopadhyay, Y. Elovici. (2018). securing vulnerabilities of unmanned aerial vehicles and countermeasures: an experimental study, *31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID),* 398 - 403.
DOI: 10.1109/VLSID.2018.97

[9] J. H. Cheon, K. Han, S. M. Hong, H. J. Kim, J. S. Kim, S. S. Kim, H. S. Seo, H. B. Shim & Y. S. Song. (2018). Toward a Secure Drone System: Flying With Real-Time Homomorphic Authenticated Encryption, *IEEE Access 6,* 24325-24339.
DOI: 10.1109/ACCESS.2018.2819189

[10] A. Sehrawat, T A. Choudhury & G. Raj. (2017). Surveillance drone for disaster management and military security, *International Conference on Computing, Communication and Automation (ICCCA) 2017,*470 - 475.
DOI: 10.1109/CCAA.2017.8229846

[11] P. Blank, S. Kirrane & S. Spiekermann. (2018). Privacy aware restricted areas for unmanned aerial systems, *Journal of IEEE Security & Privacy*: 16(2), 70-79.
DOI: 10.1109/MSP.2018.1870868

[12] E. Vattapparamban, I. Guvenc, A. I. Yurekli, K. Akkaya, S. Uluagac. (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety, *IWCMC2016*:216-221.
DOI: 10.1109/IWCMC.2016.7577060

[13] P. Perazzo, K. Ariyapala, Z. Conti, G. Dini. (2015). The verifier bee: A path planner for drone based secure location verification, *IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM),*1-9.
DOI: 10.1109/WoWMoM .2015.7158150

[14] S. G. Manyam, D. W. Casbeer, S. Manickam. (2017). Optimizing multiple UAV cooperative ground attack missions, *International conference on Unmanned Aircraft Systems (ICUAS),* 1572-1578.
DOI: 10.1109/ICUAS.2017.7991396

[15] P. T. Jardine, S. Givigi, A. Noureldin. (2015). Incorporating feedback predications for optimized UAV attack mission planning, *23rd Mediterranean Conference on Control and Automation (MED)*;740-746.
DOI: 10.1109/MED.2015.7158834

[16] S. H. Rubin, W. K. Grefe, T. B. Tebibel, S. C. Chen, M. L. Shyu, K. S. Simonsen. (2017). Cyber Secure UAV Communications using heuristically inferred stochastic grammars and hard real time adaptive waveform synthesis and evolution, IEEE Computer society 2017, 9-15, DOI: http://doi.ieeecomputersociety.org/10.1109

/IRI.2017.56

[17] Y. Su. Jung & Y. H. Yon. (2018). User Privacy protection model though enhancing the administrator role in the cloud environment, *Journal of Convergence for Information Technology*: 8(3), 79-84. DOI: https://doi.org/10.22156/CS4SMB.2018.8.3.079

[18] H. J. Mun, (2018). Biometric Information and OTP based on authentiction mechanism using blockchain, Journal of convergence for Information Technology: 8(3), 85-90, DOI: https://doi.org/10.22156/CS4SMB.2018.8.3.085

[19] C. J. Chae, S. K. Han, H. J. Cho, (2016). Security vulnerability and countermeasures in smart farm, *Journal of Digital Convergence*: 14(11), 313-318, DOI: http://dx.doi.org /10. 14400/JDC.2016.14.11.313

[20] D. H. Choi, J. O. Park, (2015), Security tendency analysis techniques through machine learning algorithm applications in big data environments, *Journal of Digital Convergence*: 13(9), 269-276, DOI: http://dx.doi.org/10.14400/JDC.2015.13.9.269

오 상 윤(Oh, Sang Yun) [학생회원]

- 2018년 6월 : 백석대학교 정보통신학부(학부과정)
- 관심분야 : 드론보안
- E-Mail : vmflalvm@naver.com

홍 진 근(Hong, Jin Keun) [정회원]

- 2018년 6월 : 백석대학교 정보통신학부 교수
- 관심분야 : 정보보호, 융합 기술
- E-Mail : jkhong@bu.ac.kr