논문 20-45-04-09 The Journal of Korean Institute of Communications and Information Sciences '20-04 Vol.45 No.04
https://doi.org/10.7840/kics.2020.45.4.686

UAV 시스템에서의 UAV와 GCS 간 Wi-Fi 통신 보안 향상 기법

윤 지 영◆, 이 효 준*, 박 경 준°

UAV System Security Enhancement in Wi-Fi Communication Between UAV and GCS

Jiyoung Yoon◆, Hyojun Lee*, Kyung-Jun Park°

요 약

UAV(Unmanned Aerial Vehicle)는 흔히 드론이라 불리며 최근 활용 범위가 넓어지고 있는 추세이다. 세계 드론 시장은 점차 성장하여 2026년 약 820억 달러에 이를 것으로 예상된다. 이와 함께 UAV 시스템의 취약점에 대한 대안 및 보안 역시 강조되고 있다. UAV는 RC transmitter, Bluetooth, Wi-Fi 등의 무선 통신으로 GCS(Ground Control Station)와 연결되어 GCS로부터 미션을 받아 수행한다. 본 논문에서는 현재 PX4와 Ardupilot에서 제안하는 Wi-Fi 텔레메트리 모듈 펌웨어의 프로세스와 해당 프로세스의 문제점에 대해 서술하고 이 문제점을 해결할 수 있는 UAV와 GCS 간 Wi-Fi 통신의 보안 향상 기법을 제안한다.

Key Words : CPS(Cyber-physical System), UAV(Unmanned Aerial Vehicle), Drone, Network, Security, Network attack, System

ABSTRACT

Unmanned Aerial Vehicles (UAVs), commonly called drones, which have recently become increasingly widespread, are expected to grow bringing the global drone market to about $ 82 billion by 2026. In addition, alternatives against vulnerabilities and security in UAV systems are also emphasized. UAV is connected to the GCS (Ground Control Station) to perform the mission by wireless communication such as RC transmitter, Bluetooth, Wi-Fi, etc. In this paper, we describe the process of firmware operating in the Wi-Fi telemetry module, proposed by PX4 and Ardupilot, and also the problems of the this process. And we propose a method to improve the security of Wi-Fi communication between UAV and GCS to solve this problem.

Ⅰ. 서 론

드론이라 불리는 무인항공기(UAV: Unmanned Aerial Vehicle)는 레저, 미디어 및 엔터테인먼트 군사 등의 목적과 함께 건설, 광업 산업, 생명 구조 활동 등 활용 범위가 점차 넓어지고 있다. 국토부에 따르면 세계 드론 시장은 연 29%씩 성장하여 2026년 약 820억 달러에 이를 것으로 예상되고 있다. 드론은 4차 산업 혁명의 테마인 CPS(Cyber Physical Systems)의 중요한 애플리케이션 중 하나로 대두되고 있다.[1,2]

※ 본 연구는 과학기술정보통신부에서 지원하는 DGIST기관고유사업에 의해 수행되었습니다(20-ST-02).
◆ First Author : Daegu Gyeongbuk Institute of Science & Technology, hailey_yoon@dgist.ac.kr, 학생(석사), 학생회원
° Corresponding Author : Daegu Gyeongbuk Institute of Science & Technology, kjp@dgist.ac.kr, 정교수, 종신회원
* Daegu Gyeongbuk Institute of Science & Technology, hj.lee@dgist.ac.kr, 학생(석사), 학생회원
논문번호 : 201911-265-B-RE, Received October 31, 2019; Revised January 20, 2020; Accepted February 3. 2020

2019년 9월 사우디아라비아의 정유시설과 원유 생산 기지에 대한 드론 공격 사건뿐만 아니라 자폭 드론 공격을 통한 남예멘군 수명 사살 사건 등 UAV를 테러 수단으로 삼은 공격이 빈번해지고 있다. 또한 군사 목적으로 쓰이는 UAV는 임무에 대한 정보 보안 역시 중요하다. 그러나 UAV 네트워크에 대한 취약성은 여러 연구를 통해 실험으로 증명되었고 이러한 취약점을 보완하기 위해 여러 방어 방법이 연구되고 있다.[3-5]

UAV는 RC transmitter, Bluetooth, Wi-Fi 등 다양한 매체를 이용하여 제어할 수 있으며, UAV는 해당 매체를 통해 GCS(Ground Control Station)와 연결되어 비행한다.[6] 우리는 Wi-Fi를 통한 UAV와 GCS의 네트워크 환경을 고려하여 그림 1과 같이 구성하였다. 이렇게 연결된 GCS는 UAV에게 비행 임무와 관련된 명령을 내리고 이에 대한 UAV의 비행 상태 및 여러 센서들의 상태 정보를 모니터링할 수 있다.

기존의 여러 시스템에서는 MavESP8266 펌웨어를 사용하도록 제안하고 있다. 그러나 본 논문에서는 UAV와 GCS 간 Wi-Fi 통신에서의 보안을 강화하기 위해 MavESP8266 펌웨어의 문제점을 찾고 이에 대한 해결방안을 제시한다. MavESP8266 펌웨어는 UAV가 MAVLink 프로토콜을 이용하기 위해 UAV에 장착된 Wi-Fi 모듈에 설치하는 펌웨어이다. MAVLink 프로토콜은 UAV와 GCS, 그리고 UAV에 탑재된 여러 구성 요소들 사이에서 통신하기 위한 프로토콜이며 DJI, Parrot 사의 제품뿐만 아니라 많은 UAV에서 사용하는 대표적인 프로토콜이다.

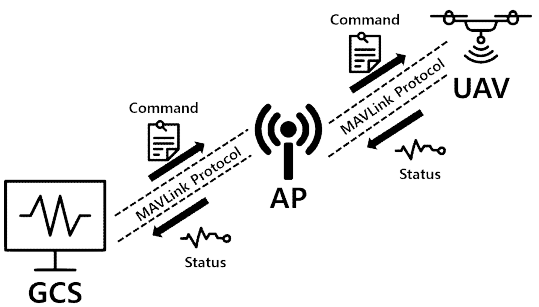

Fig. 1. UAV Network

Ⅱ. 본 론

UAS(Unmanned Aerial System)는 하드웨어, 소프트웨어, 네트워크로 구성되는데 본 논문에서는 Pixhawk2 하드웨어와 ArduCopter V3.6.8 Hexa firmware, ESP8266 Wi-Fi 모듈을 이용하여 네트워크를 구성한다. ESP8266 모듈은 AP의 역할을 하며 GCS에서 Wi-Fi 네트워크에 접속 후 UDP로 UAV와 연결을 맺는다. 주로 UAV 환경 구성을 위해 많이 쓰이는 구성임에도 불구하고 UAV 프로토콜인 MAVLink 프로토콜을 이용하기 위해 MavESP8266 펌웨어를 UAV의 Wi-Fi 모듈에 설치하여 사용할 경우 치명적인 취약점이 있는 것을 발견하였다. 이는 PX4와 Ardupilot 측에서 제안하는 모델로 Pixhawk를 이용한 UAV에서 Wi-Fi 환경을 구성할 때 쓰인다.

정상적인 UAV 네트워크에서의 통신과정을 살펴보면 UAV와 GCS가 연결되는 과정은 그림 2와 같다. 먼저 GCS에서 UAV의 네트워크에 접속을 한 뒤 MAVLink 메시지가 담긴 UDP 패킷을 통해 UAV와 연결을 한다. 연결 초기에 GCS에서 UAV에게 초기 설정과 같은 parameter들을 요청하면 UAV는 자신의 parameter를 전송한다. 이렇게 UAV와 GCS가 연결이 된다면 서로 주기적으로 Heartbeat message를 송수신한다. 또한 UAV는 GCS에게 자신의 상태, 미션 등의 정보를 주기적으로 송신한다. 이러한 연결 과정에서 UAV인 Pixhawk의 펌웨어, ArduCopter V3.6.8 Hexa는 GCS가 원하는 정보만 전송할 뿐 아무런 개입이 없으며 GCS에 대한 네트워크 정보가 없다. 이는 MavESP8266에서 관리된다.

MavESP8266을 플래싱한 UAV의 Wi-Fi 모듈의 경우, UDP 패킷을 받으면 그림 3과 같은 프로세스를 통해 동작한다. UAV가 GCS와 아직 연결되지 않았다면 처음 받은 UDP 패킷의 IP를 Wi-Fi 모듈에서 GCS

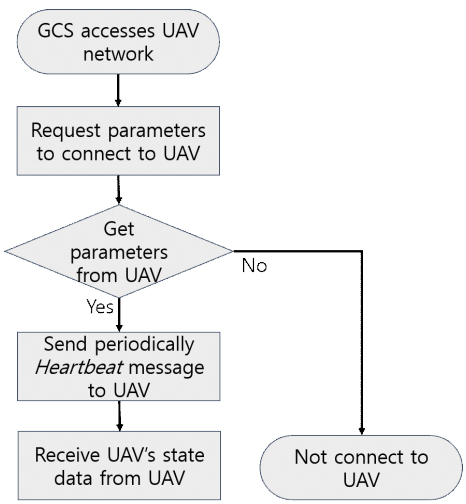

Fig. 2. Initial connection process with UAV in GCS

Algorithm 1. The existing algorithm

```
if UDP packet received
    parse UDP packet to MAVLink message
    if GCS is not connected yet
        _IP ← source IP of UDP packet
    Heartbeat check
    CRC check
    send MAVLink message
```

Fig. 3. The existing MavESP8266 packet processing algorithm

의 IP로 저장한다. 그러나 UAV는 이 프로세스를 거치고 나면 GCS와 연결되었다고 판단 후, UDP 패킷의 Source IP를 검사하지 않고 패킷을 받아들인다. 그림 3은 이 프로세스를 간단하게 나타낸 그림이다.

이 같은 프로세스는 다음과 같은 문제점이 있다. GCS와 연결된 후에는 악의적인 공격자가 Wi-Fi에 접근할 수만 있다면 GCS 인척 UDP 패킷의 Source IP를 바꿀 필요 없이 MAVLink 메시지를 주입시키는 행동만으로 UAV를 쉽게 공격할 수 있다는 점이다. 이와 같은 Wi-Fi는 대부분 펌웨어에서 설정한 Wi-Fi 비밀번호를 그대로 유지하는 경우가 있어 공격이 매우 쉬울 수 있다. 이러한 취약점은 간단하게 임무에 대한 정보를 도청할 수 있을 뿐만 아니라 패킷 인젝션 공격을 통해 UAV를 무력화시키거나 원하는 대로 행동하게 할 수 있어 치명적인 위험을 초래할 수 있다.[7-9]

이 같은 문제점을 해결하기 위해 MavESP8266에서 UDP 패킷을 받고 처리하는 프로세스를 수정할 필요가 있었다. 문제점은 UAV가 GCS와 연결된 후 UDP 패킷을 받을 때 신원을 확인하지 않는 점이기 때문에 우리는 기존의 알고리즘에서 GCS와 연결된 후 UDP 패킷을 받을 때 신원을 확인하는 프로세스를 추가해 주었다. 그림 4와 그림 5는 이를 표현한 것이다. 그림 4에서 표현된 알고리즘으로 수정된다면 그림 5에서처럼 올바른 GCS와 UAV가 연결된 후에는 모르는 시스템이 UAV에게 명령을 보낼 수 없다. 즉 UAV에서 UDP 패킷을 받으면 미리 저장해 둔 GCS의 IP를 수신한 UDP 패킷의 Source IP와 비교한 후 GCS의 IP가 아니라면 패킷을 버리고 해당 IP로부터 오는 UDP 패킷은 받지 않는다.

Algorithm 2. The proposed algorithm

```
if UDP packet received
    parse UDP packet to MAVLink message
    if GCS is not connected yet
        _IP ← source IP of UDP packet
    else
        if _IP != source IP of UDP packet
            exit the process
    Heartbeat check
    CRC check
    send MAVLink message
```

Fig. 4. The proposed MavESP8266 packet processing algorithm

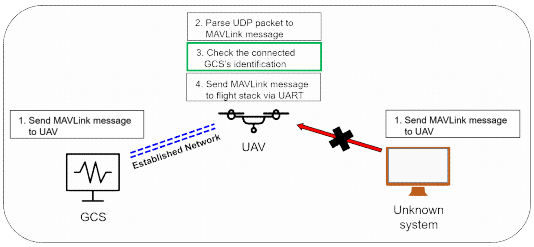

Fig. 5. Network between UAV and GCS with the proposed algorithm

Ⅲ. 실 험

본 논문에서는 그림 6과 같이 Pixhawk2, ArduCopter V3.6.8 Hexa 그리고 Wi-Fi 네트워크 환경을 구성하기 위해 Pixhawk2의 telemetry1 포트에 ESP8266 모듈을 연결한 UAS로 실험을 하였다.

UAV와 GCS를 Ardupilot Wi-Fi에 연결한 후 비행을 하는 환경에서 공격자가 Wi-Fi 통신에 침입한 후, UAV에게 모터의 동작을 즉각적으로 종료시키는 명령인 disarm_command 패킷을 주입시킴으로써 UAV를 바로 추락시키는 시나리오의 실험을 실행하였다.

그림 7은 실제 실험에서 패킷을 캡처한 그림이다.

Fig. 6. UAV and GCS flight environment

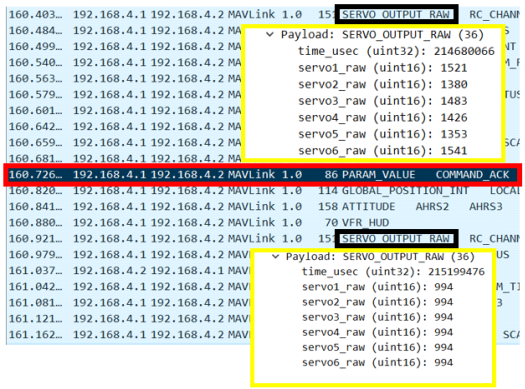

Fig. 7. Packet capture between UAV and GCS in the experiment

그림 7은 IP가 192.168.4.2인 GCS에서 패킷을 캡처한 그림으로 IP가 192.168.4.1인 UAV와의 통신을 보여준다. 빨간 상자는 UAV의 공격에 대한 반응으로, 이를 중심으로 공격전의 상황에서 해당 GCS가 command 관련 패킷을 보낸 적이 없음에도 불구하고 UAV가 GCS에게 명령에 대한 대답인 COMMAND_ACK 메시지를 갑자기 보내는 것을 빨간 상자를 통해 확인할 수 있다. 이는 해당 패킷 캡처가 GCS 입장에서의 패킷 캡처이기 때문에 다른 Sorce IP가 보낸 메시지는 보이지 않지만 올바른 GCS가 명령이 담긴 패킷을 보내지 않았음에도 불구하고 다른 Source IP를 가진 시스템을 GCS로 받아들인 후 올바른 GCS에게 ACK를 보내는 것을 나타낸다. 또한 그림 8은 그림 7에서의 패킷에서 UAV의 비행 임무 중 모터 출력값(SERVO_OUTPUT)을 이용해 그린 그래프로 공격전에는 정상적인 모터 출력을 보이나 공격 후, SERVO_OUTPUT이 초깃값인 994로 떨어진 것을 확인할 수 있으며 이 값을 통해 UAV가 비행 임무 중 추락함을 확인할 수 있다.

우리는 UAV에 수정된 알고리즘의 펌웨어를

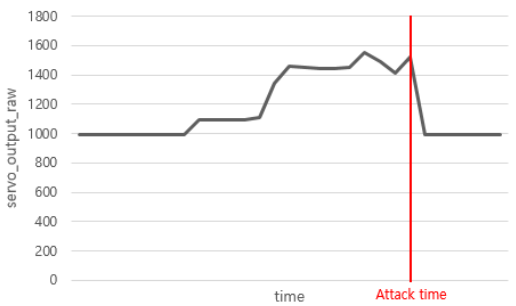

Fig. 8. Motor output graph during UAV's flight mission

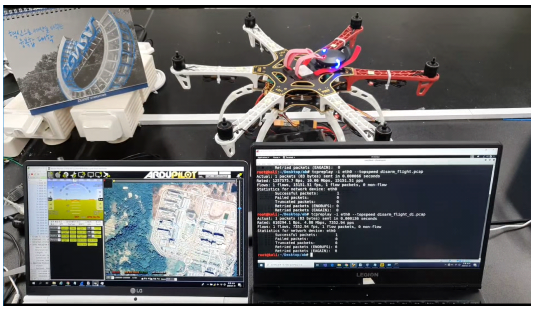

Fig. 9. Experiment using proposed algorithm

ESP8266 모듈에 다시 플래싱한 후 똑같은 시나리오의 실험을 하였다. 이때 기존의 Wi-Fi 모듈에서는 UAV가 추락을 하였고 패킷의 모터 출력값을 통해 UAV의 반응을 확인할 수 있었으나, 수정된 Wi-Fi 모듈을 이용한 실험에서는 UAV가 기존에 설정된 GCS의 비행 임무를 온전히 수행하는 것을 확인하였고 캡처한 패킷들에서도 공격자에 대해 UAV가 반응하지 않았음을 알 수 있었다. 그림 9는 이에 대한 간단한 실험을 실행한 영상을 캡처한 그림이다.[10] 이는 수정된 알고리즘이 저장된 GCS의 신원과 공격자의 신원을 비교하여 공격자의 패킷을 처리하지 않고 버린 것을 알 수 있다.

Ⅳ. 결 론

본 논문에서는 다양한 네트워크 공격에 노출되어 있던 기존의 UAV에 탑재되는 MavESP8266의 문제점을 찾고 UAV와 GCS 간 Wi-Fi 통신에서의 보안을 강화하기 위해 이에 대한 해결방안을 제시하였다. 이는 UDP 패킷을 받은 후 신원을 확인하는 프로세스를 추가함으로써 문제점을 해결할 수 있었다. 그러나 IP 변조를 통한 패킷 주입 공격에는 아직도 취약하므로 향후 이에 대한 해결방안에 대해서도 연구가 진행될 필요가 있다.

References

[1] K.-J. Park, R. Zheng, and X. Liu, "Cyber-physical systems: Milestones and research challenges," *Computer Commun.*, vol. 36, no. 1, pp. 1-7, Dec. 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*

Trans. Ind. Informatics, vol. 10, no. 4, pp. 2204-2215, Nov. 2014.

[3] Y.-M. Kwon, et al., "Empirical analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles," *IEEE Access*, vol. 6, pp. 43203-43212, 2018.

[4] J. Y. Yoon, H. J. Lee, and K. J. Park, "Security enhancement in wi-fi communication between UAV and GCS," in *Proc. KICS ICC 2019*, pp. 400-401, Jun. 2019.

[5] J. M. YU, J. Y. Yoon, and K. J. Park. "Risk analysis of UAV and GCS for network attacks," *J. KIISE*, vol. 37, no. 1, pp. 29-37, Jan. 2019.

[6] A. Y. Javaid, et al., "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," *2012 IEEE Conf. Technol. for Homeland Secur.* (HST), Waltham, MA, USA, Nov. 2012.

[7] S. Deng, et al., "Packet injection attack and its defense in software-defined networks," *IEEE Trans. Inf. Forensics and Secur.*, vol. 13, no. 3, pp. 695-705, 2017.

[8] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, vol. 50, no. 2, pp. 76-79, Feb. 2017.

[9] A. K. Simpson, F. Roesner, and T. Kohno, "Securing vulnerable home IoT devices with an in-hub security manager," *2017 IEEE PerCom Workshops*, Kona, HI, USA, Mar. 2017.

[10] J. Y. Yoon and H. J. Lee, Experiment video, 2020, https://youtu.be/Lgabk9WO5HY

윤 지 영 (Jiyoung Yoon)

2017 : 계명대학교 컴퓨터공학과 학사

2018~현재 : 대구경북과학기술원 정보통신융합전공 석사과정

<관심분야> Cyber-Physical Systems

[ORCID:0000-0003-2504-8476]

이 효 준 (Hyojun Lee)

2017 : 계명대학교 컴퓨터공학과 학사

2019~현재 : 대구경북과학기술원 정보통신융합전공 석사과정

<관심분야> Cyber-Physical Systems

[ORCID:0000-0002-7611-4296]

박 경 준 (Kyung-Jun Park)

1998 : 서울대학교 전기공학부 학사

2000 : 서울대학교 전기공학부 석사

2005 : 서울대학교 전기컴퓨터공학부 박사

2005~2006 : 삼성전자 책임 연구원

2006~2010 : 미국 UIUC 박사 후 연구원

2011~2014 : 대구경북과학기술원 정보통신융합전공 조교수

2014~2019 : 대구경북과학기술원 정보통신융합전공 부교수

2019~현재 : 대구경북과학기술원 정보통신융합전공 교수

<관심분야> Resilient Cyber-Physical Systems

[ORCID:0000-0003-4807-6461]