드론 임베디드 시스템 및 네트워크 프로토콜 기반 보안위협 동향

박상현[1], 정인수[2], 곽 진[3]
[1]아주대학교 사이버보안학과 정보보호응용및보증연구실 학부생
[2]아주대학교 사이버보안학과 정보보호응용및보증연구실 석박통합과정
[3]아주대학교 사이버보안학과 교수
chipkkang9@ajou.ac.kr, jis0727@ajou.ac.kr, security@ajou.ac.kr

Security Threat Trend based on Drone Embedded System and Network Protocol

Sang-Hyeon Park[1], In-Su Jung[2], Jin Kwak[3]
[1,2]ISSA Lab., Dept. of Cyber Security, Ajou University
[3]Dept. of Cyber Security, Ajou University

요 약

IoT(Internet of Things) 기술을 기반으로 한 드론은 사용자의 요청에 따라 데이터 처리, 수집, 송·수신 등에 고도화된 ICT(Information and Communications Technology) 기술을 활용하고 있다. 또한, 드론은 ICT 기술이 발전함에 따라 문화, 소방, 국방 등 다양한 분야에 적용되어 사용자에게 편의를 제공하고 있다. 그러나, 드론에 적용되는 ICT 기술과 드론에 탑재되는 기술들이 고도화됨에 따라 드론 모듈 내 펌웨어 및 무선 네트워크를 대상으로 한 보안위협이 증가하고 있다. 따라서 본 논문은 드론의 보안위협에 대응하기 위하여 드론 임베디드 시스템 및 네트워크 프로토콜을 대상으로 한 최신 보안위협 동향을 분석한다.

1. 서론

IoT(Internet of Things) 기술을 기반으로 한 무인비행장치 드론은 무선 네트워크 통신, 빅데이터 처리를 위해 ICT 기술이 적용된 모듈을 탑재하여 문화, 소방, 국방 등 다양한 분야에서 사용자에게 편의성을 제공하고 있다[1]. 그러나, 드론에 적용되는 ICT(Information and Communications Technology) 기술과 드론에 탑재되는 기술들이 고도화됨에 따라 드론 모듈을 제어하는 펌웨어와 드론을 제어하는 무선 네트워크를 통해 발생 가능한 보안위협이 증가하고 있다. 드론을 대상으로 한 보안위협은 송·수신 데이터 유출뿐만 아니라, 드론 권한 탈취, 드론 무력화 등이 존재하며, 이에 대응하기 위한 보안위협 분석이 필요하다. 따라서, 본 논문에서는 드론의 보안위협에 대응하기 위하여 드론 임베디드 시스템 및 네트워크 프로토콜을 대상으로 한 최신 보안위협 동향을 분석한다.

본 논문은 2장에서 드론의 정의와 드론 네트워크 프로토콜을 설명한다. 3장에서는 최신 드론 보안위협 동향을 분석하고, 4장에서 결론을 맺는다.

2. 관련 연구

2.1. 드론

드론은 통신부(WiFi, LTE, 비디오 송수신기 등), 제어부(가속도 센서, GPS 센서 등), 구동부(모터, 프로펠러, 배터리 등), 페이로드(비디오 카메라, 적외선 카메라 등)로 구성되어 무선 전파를 통해 조종되는 무인 비행 물체이다. 드론을 조종하는 방법에는 스마트폰을 활용하여 하나의 드론을 조종하는 방법이 있다. 또한, 드론 센서를 통해 수집한 데이터를 기반으로 GCS(Ground Control Station)를 활용하여 다수의 드론을 조종하는 방법이 존재한다[2].

2.2. 드론 무선 네트워크

드론은 WiFi, LTE, 5G를 통해 송·수신 데이터의 종류에 따라 특정 프로토콜을 사용하며, 주로 MAVLink, AeroScope 프로토콜을 활용한다.

❒ MAVLink(Micro Air Vehicle Link) 프로토콜

MAVLink 프로토콜은 UAV(Unmanned Aerial Vehicle)와 GCS 간 양방향 통신에 사용되는 경량 네트워크 프로토콜이다. 이는 특정 주행모드를 통해 운영할 시, GCS로부터 주행모드에 해당하는

페이로드를 받아 드론에게 기능을 요청한다[3].

❒ AeroScope 프로토콜

AeroScope는 'A'사의 RF(Radio Frequency) 신호 감지 시스템이다. 이는 드론에서 발생하는 RF 신호를 캡처하고 분석하여, 드론의 ID, 위치, 속도, 고도 등의 정보를 실시간으로 제공한다[4].

3. 드론 대상 최신 보안위협 분석

3.1. 드론 임베디드 시스템 대상 보안위협

❒ Buffer Overflow 취약점 악용 권한 상승 공격

본 공격은 드론 통신부의 lewei_cam 카메라 모듈 제어 프로세스 취약점을 대상으로 한 공격이다[5]. 공격자는 실시간으로 영상을 촬영하고 전송하는 과정에서 lewei_cam_execute() 함수의 버퍼를 대상으로 한 Buffer Overflow 공격이 가능하다. 이로 인해, 공격자는 원격 환경에서 악성 코드를 실행하여 카메라 모듈의 권한을 탈취하고, 송·수신 영상을 감청할 수 있다.

❒ 드론 펌웨어 취약점을 활용한 서비스 거부 공격

본 공격은 'A'사의 드론의 제어부 및 구동부를 관리하는 펌웨어를 대상으로 한 공격이다[6]. 공격자는 'A'사의 드론 제어 상태와 관련된 데이터 송·수신 과정에서 전용 데이터 패킷을 무작위로 대입하여 Buffer Overflow 공격 수행이 가능하다. 이를 통해, 공격자는 악성 데이터 패킷을 생성 및 전송하여 RCE(Remote Code Execution) 공격이 가능하고, 서비스 거부 공격까지 수행할 수 있다.

3.2. 드론 네트워크 프로토콜 대상 보안위협

❒ 패킷 검증 취약점 악용 서비스 거부 공격

본 공격은 MAVLink 프로토콜의 인증 취약점을 악용한 공격이다[7]. 공격자는 드론 상태 정보를 설정하는 패킷의 송·수신 과정에서 악성 패킷을 정상 패킷으로 받아들이도록 하는 Flooding 공격을 수행한다. 이를 통해, 공격자는 드론 기기를 무력화하거나 탈취할 수 있다.

❒ 암호화 취약점 악용 사용자 정보 탈취 공격

본 공격은 'A'사 드론에서 사용하는 AeroScope 프로토콜의 취약점을 악용한 공격이다[8]. 'A'사의 드론(2017~2022년 모델)은 패킷을 전송하는 과정에서 정상적인 패킷 암호화를 수행하지 않는다. 이로 인해, 공격자는 사용자의 물리적 위치 등 민감정보가 포함된 평문 데이터를 탈취할 수 있다.

<표 1> 드론 보안위협 동향

Attack Vector	Target	Details
Embedded System	lewei_cam	Hijacking Video through theft of authority
	Drive and Control Firmware	Denial of Service through RCE
Network Protocols	MAVLink	Disabling drone by Packet Flooding
	AeroScope	Exposure of Sensitive Information through stealing plain text data

4. 결론

본 논문에서는 드론 보안위협에 대응하기 위하여 드론 임베디드 시스템 및 네트워크 프로토콜을 대상으로 한 최근 보안위협 동향을 분석했다. 이를 통해, 추후 임베디드 시스템 및 네트워크 프로토콜에 대하여 발생 가능한 보안위협 대응방안 도출에 기여할 수 있다.

사사문구

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2021R1A2C2011391)

참고문헌

[1] Ed Alvarado, "Drone Market Analysis 2022-2030", Drone Industry Insights, Sep. 2022.

[2] KISA, "드론 사이버보안 가이드", Dec. 2020.

[3] Yassine Mekdad, "A Survey on Security and Privacy Issues of UAVs", Elsevier, Computer Networks, Vol 224, Sep. 2021.

[4] DJI, "DJI AEROSCOPE", https://www.dji.com/kr/aeroscope

[5] CVE, "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40918", Sep. 2022.

[6] Nico Schiller, "Drone Security and the Mysterious Case of DJI's DroneID", NDSS Symposium 2023, California, USA, Feb. 2023.

[7] CVE, "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10283", Mar. 2020.

[8] CVE, "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29945", Apr. 2022.