드론 주요 컴포넌트 대상 공격벡터 도출 및 위협 분석

김성경[O1] 백승훈[2] 이상욱[3] 박기웅[4†]
[1]세종대학교 시스템보안연구실, [2]중원대학교 컴퓨터시스템공학과, [3]국가보안기술연구소, [4]세종대학교 정보보호학과
jotun9935@gmail.com, shbaek@.jwu.ac.kr, leesw@nsr.re.kr, woongbak@sejong.ac.kr

Attack Vector Derivation and Threat Analysis of Major Components of Drone

SungKyung Kim[O1] SungHoon Baek[2] SangWook Lee[3] KiWoong Park[4†]
[1]Sejong Univ. SysCore Lab
[2]Jungwon Univ. Dept. of Computer System engineering
[3]National Security Research Institute
[4]Sejong Univ. Dept. of Computer and Information Security

요 약

드론은 조종사가 탑승하지 않고 센서로부터 수집한 데이터와 외부와의 통신을 이용하여 비행한다. 하지만 실시간으로 수집된 센서 데이터와 드론과 조종사간의 통신 링크는 악의적인 사용자에 의해 영향을 받을 수 있다. 따라서 드론이 외부와 상호작용하는 인터페이스에 대한 분석은 중요한 의미를 갖는다. 이를 위해 본 논문은 드론을 구성하는 핵심적인 컴포넌트 중 외부의 데이터를 송/수신하는 요소인 센서와, 무선 통신방식에 대해 조사하였다. 드론이 사용하는 주요 센서들은 자이로스코프, 가속도계, 기압계, 거리계, GPS 센서가 있으며, 외부 통신을 위해 활용할 수 있는 무선통신 방식들은 Bluetooth, Cellular, Wi-Fi, Satellite Communication, Zigbee 등이 있다. 본 논문은 위의 요소를 대상으로 시도되었던 다양한 공격 중, 드론의 보안성에 위협이 될 수 있는 공격 시도들에 대해 설명한다. 이러한 주요 컴포넌트 대상 분석 결과는 향후 안전성을 고려한 드론 플랫폼 설계 및 보안 가이드라인 제작에 활용할 수 있을 것이라고 사료된다.

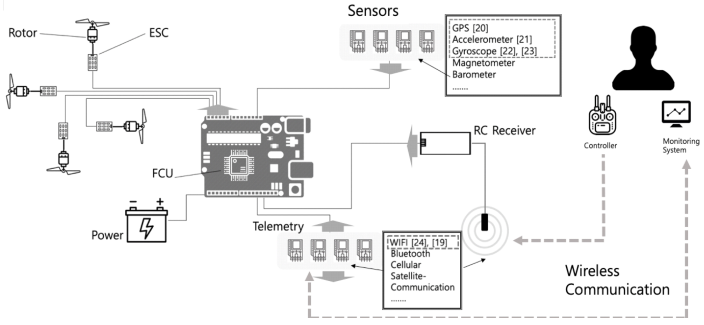
1. 서 론

최근 드론 기술은 농업, 방송, 군사 등의 다양한 산업 전반에 걸쳐서 활용되고 있다[1, 2, 3]. 하지만 드론 기술을 활용한 산업 발달의 이면에는 보안 위협 또한 존재한다[4, 5]. 따라서 안전한 드론 운용을 위해 발생 가능한 보안 취약점을 파악하고 사전에 제거해야 한다. 취약점 분석 방법에서 대상이 사용하는 입력 값으로부터 검증되지 않은 데이터가 대상에 미치는 영향을 검증하는 방법[6, 7, 8]은 높은 중요도를 가지며 현재 상당수의 취약점은 이러한 방법을 이용해 발견되는 경우가 많다. (그림 1)을 보면, 드론 또한 마찬가지로 입력 데이터에 대한 처리를 수행하는 하나의 컴퓨팅 장치의 특징을 가지기 때문에, 대상이 사용하는 입력 값에 대한 검증을 통한 보안 위협 식별은 중요한 의미를[1)] 갖는다. 하지만 드론은 특징과 목적 및 제조사 별로 구성이 상이한 특징을 가지고 있어, 드론 전반에 대한 보안 위협 검증을 위해 일반적인 드론이 공통적으로 사용하는 핵심 컴포넌트의 식별이 선행 되어야한다. 따라서 본 논문에서는 일반적으로 상용화 되어 있는 드론을 구성하고 있는 핵심 컴포넌트를 식별하고 이에 대한 공격벡터 산출 및 보안 위협요소 분석을 수행한다.

본 논문의 구성은 다음과 같다. 2장에서는 드론을 구성하는 핵심적인 컴포넌트와 주요 분석 대상인 센서 및 무선 통신 기술에 대해 소개한다. 이어서 3장에서는 앞서 소개한 센서와 무선 통신 기술을 대상으로 하는 드론 공격 기술에 대해 소개한다. 마지막으로 4장에서는 결론과 향후 연구에 대해 기술한다.

2. 드론의 주요 컴포넌트 소개

드론 관련 다양한 제조사의 등장[9, 10, 11] 및 다양한 오픈소스와 오픈 하드웨어 프로젝트의 등장[12, 13]에 따라 드론의 구조는 제작에 사용된 보드마다 조금씩 차이가 있으며, 제조사마다 다른 형태를 갖는다. 이러한 상호 운용성으로 인해 다양한 형태의 드론 개발이 유연하게 가능해졌지만, 반대급부로 공격자가 활용할 수 있는 Attack Surface 또한 다양해졌다. 본 논문은 이들 중에서 특정 제조사에서 사용자나 개발상의 편의를 위해 제공하는 특수한 기능에 국한되어 발생하게 되는 취약점[14, 15]이 아닌 일반적인 드론이 필수적으로 갖는 구성 요소에서 발생할 수 있는 취약점을 다루고자 한다. 이를 위해 드



(그림 1) 드론의 주요 구성 요소 및 공격 벡터

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)
* 본 연구는 2019년도 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원(No.2018-0-00420) 및 국가보안기술연구소 위탁과제, "(2019-131)무인이동체 이상행위 식별을 위한 데이터 수집 및 분석 체계 연구"의 지원을 받아 수행된 연구임.

론의 비행에 직접적인 연관이 있는 컴포넌트에 대한 도출이 필요하다. 해당 장에서는 드론의 핵심이 되는 구성 요소에 대해 간략히 소개하고 각각의 컴포넌트들 중에 보안 위협의 가능성이 높은 컴포넌트를 선정한다.

먼저 2017년 Yang, Hyunsoo 등은 일반적인 멀티로터 드론에 대한 핵심 구성 요소를 Frame, Rotor와 ESC(Electronic Speed Controller), Power Source, FCU(Flight Control Unit)와 Onboard PC, Sensor, Wireless Communication의 6가지 항목으로 분류하였다[16].

본 논문에서는 (그림 1)에서 표시한 바와 같이 위에서 소개한 컴포넌트 중 외부의 데이터를 수신하는 주된 컴포넌트인 센서, 그리고 외부와의 데이터 송/수신에 사용되는 무선 통신 기술을 주요 분석 대상으로 선정하였다.

나머지 요소는 다음의 이유로 분석에서 제외하였다. 먼저 Frame과 Power Source는 물리적인 요격 등의 방법을 통해 영향을 받는 부분이기 때문에 분석에서 제외한다. 또한 Rotor와 ESC, FCU와 Onboard PC의 경우는 제조사별로 구성의 차이가 크기 때문에 분석의 대상에서 제외한다.

2.2 드론의 주요 센서

드론은 안정적인 비행을 위해 현재 기체의 고도, 속도, 위치 등의 정보가 필요하다. 이러한 비행 정보 수집을 위해 드론은 센서를 활용하는데, 이 외에도 드론의 사용 목적에 따라 목적에 맞는 센서를 추가로 장착하여 사용하기도 한다. <표 1>은 드론에 장착되는 다양한 센서들 중, 2012년 Lim, Hyon 등이 발표한 논문 내용에서, 8개 오픈소스 드론 프로젝트를 대상으로 하는 주요 컴포넌트 비교 분석[18]에 활용한 센서들로, 자이로스코프, 가속도계, 자력계, 기압계와 GPS 센서에 대해 소개하였다.

2.3 드론의 무선 통신 기술

일반적인 형태의 드론은 기체 내부에 조종사가 탑승하지 않는 방식(UAV, Unmanned Aerial Vehicle)의 형태를 갖기 때문에, 드론의 조종은 드론에 탑재된 통신 모

<표 1> 드론의 주요 센서

센서	설명
3축 자이로스코프 (3-axis Gyroscope)	3축 방향의 각 가속도 측정을 통해 기울기 정보를 도출. 드론의 경우 수평 유지를 위해 사용.
3축 가속도계 (3-axis Accelerometer)	중력에 의한 가속도를 측정하여 물체가 3차원 상에서 이동할 때 각 방향에 대한 각 가속도를 측정하는 센서. 드론의 이동속도 계산 및 비행 시 야기되는 자이로스코프의 오차 보정에 사용.
자력계 (Magnetometer)	방위정보 취득을 위해 사용.
기압계 (Barometer)	대기압 측정을 통해 드론의 고도를 측정하기 위한 센서. 높은 정확도를 만족하지 못하기 때문에 GPS 센서, 초음파센서, 비전 센서 등을 활용해 대체 가능.
GPS 센서 (GPS)	GPS 위성이 발산하는 위성 신호를 수신하기 위한 수신기. 여러 위성으로부터 수신한 신호를 바탕으로 위성간 거리를 계산하여 드론의 현재 위치를 계산하는 용도로 사용.

<표 2> 드론의 무선통신 기술

센서	설명
Bluetooth	3ISM 대역으로 지정된 주파수 대역인 2,400 ~ 2,483MHz에서 79개 채널을 사용. 주파수 간섭 문제 해결을 위해 Frequency Hopping 기법을 사용.
Cellular	전체 서비스 영역을 셀로 나누고 해당 영역을 담당하는 기지국을 통해 통신을 하는 방식.
Wi-Fi	로컬 네트워크 방식인 LAN을 무선화한 통신 기술. ISM 대역을 사용하는 방식이기 때문에 통신 범위가 확장될 경우 기기 간 간섭이 발생 가능.
Satellite Communication	통신의 중계소를 인공위성이 담당하는 방식의 통신 기법.

듈을 통해 원격에서 이루어지게 된다. <표 2>는 드론에 활용되는 다양한 무선 통신기술[17, 19]에 대한 간략한 소개이다.

3. 드론 주요 컴포넌트 대상 공격

일반적으로 대부분의 보안 취약점은 검증되지 않은 입력 값의 부적절한 사용 통해 발생한다. 따라서 취약점 분석에 있어 대상이 사용하는 입력 값을 통한 취약점 분석[6, 7 ,8]을 비롯해 외부와 상호 작용하는 부분에 대한 중점적인 검증은 높은 중요도를 갖는 분석 방법이다. 해당 장에서는 2장에서 살펴본 드론의 주요 센서와 무선 통신 기술을 대상으로 하는 공격 시도에 대해 살펴본다.

3.1 드론 주요 센서 대상 공격

드론은 안정적인 비행을 위해 다양한 센서를 사용하고, 이들 센서에서 수집한 정보를 바탕으로 이동, 방향전환, 호버링 등의 비행 기능을 구현한다. 해당 장에서는 드론에 사용되는 주요 센서들을 대상으로 이루어진 공격 기법에 대해 소개한다.

- GPS 센서 (GPS Sensor) - GPS 센서를 대상으로 하는 대표적인 공격으로는 GPS 센서가 GPS 신호를 정상적으로 수신하는데 방해를 하기 위해 위성 신호보다 강한 잡음 신호를 방출하는 GPS Jamming 공격과, 위성 신호 정보를 임의의 값으로 조작하여 재전송하는 방식인 GPS Spoofing 공격을 꼽을 수 있으며, 이에 대한 접근 방법을 다룬 다양한 논문이 존재한다.

  UAV를 대상으로 하는 GPS Spoofing을 다룬 대표적인 논문으로는 2014년 Kerns, Andrew J 등에 의해 발표된 논문[20]이 있다. 해당 논문은 GPS Spoofing을 통해 UAV 기체의 위치와 속도를 임의로 제어하는 실험을 시연하여 원격 공격을 통해 드론 포획이 가능하다는 것을 보여준다.
- 3축 가속도 센서 (3-axis Accelerometer) - 가속도 센서를 대상으로 한 대표적인 공격 시도로 Resonant acoustic injection을 활용한 공격이 있다. 대표적인 예로 2017년 IEEE/S&P에 발표된 논문[21]에 따르면 Timothy, 외 4명은 Resonant acoustic injection 공격을 통해 증폭기와 시그널 컨디셔닝을 위한 회로에 존재하는 보안 결함을 이용하여 MEMS 기반 가속도 센서의 무결성을 손상시키는 방법에 대하여 설명한다.
- 3축 자이로스코프 센서 (3-axis Gyroscope) - 자이로

스코프 센서를 대상으로 하는 대표적인 공격 시도로는 2015년 Son. Yunmok 등이 발표한 논문[22]을 꼽을 수 있다. 해당 논문은 의도적로 주입된 잡음에 의해 조작된 자이로스코프의 출력 값이 실제로 드론에 영향을 미칠 수 있는지에 대해 실험을 통해 보여준다.

이 외에도 2017년 Blackhat USA에서 Alibaba Security 연구진의 발표[23]도 드론을 비롯해 MEMS 자이로스코프를 사용하는 다양한 기기를 대상으로 시도한 공격에 대해 설명한다. 하지만 발표 내용에 따르면 실험이 실내에서 이루어졌고, 대상 기기를 분해한 상태에서 실험을 진행하였기 때문에, 외부 환경에서 공격 시, 외부 소리, 거리, 안개 등에 영향을 받을 수 있고, 드론의 플라스틱 기체 프레임과, MEMS의 알루미늄 케이스를 통과하여 주파수를 주입할 수 있어야 한다는 한계를 가지고 있다고 한다.

3.2 드론 무선 통신 대상 공격

해당 장에서는 현재까지 드론에서 사용하는 통신을 대상으로 이루어진 공격 기법에 대해 소개한다.

- Wi-Fi – 드론이 사용하는 Wi-Fi 통신을 대상으로 한 대표적인 공격 시도로 AR.Drone 2.0에서 발생했던 취약점을 꼽을 수 있다[24]. AR.Drone 2.0 모델은 전원이 인가되면 자동적으로 부팅 과정을 거쳐 모터 체크를 하고, Wi-Fi 핫스팟으로 동작한다. 이 때, Wi-Fi 통신을 암호화하여 사용하고 있지 않기 때문에 인가되지 않은 사용자도 해당 Wi-Fi에 접속이 가능하다.

  다음으로 2016년 Rodday 등이 발표한 논문[19] 또한 드론의 Wi-Fi 통신을 대상으로 한 공격 시도이다. 해당 취약점의 경우 비행 계획 소프트웨어와 텔레메트리 박스 내의 Wi-Fi 칩셋 간의 Wi-Fi 링크가 비교적 안전하지 않은 암호화 방식인 WEP 방식으로 암호화 되어 key 획득이 가능하기 때문에 발생한다.

4. 결론 및 향후 연구

본 논문은 현재까지 드론에 대해 이루어졌던 다양한 공격들을 센서 대상 공격과, 무선 통신 대상 공격으로 분류를 하여 각각의 컴포넌트를 대상으로 이루어진 공격들에 대해 조사하였다. 앞에서 살펴본 바와 같이 드론의 주요 센서를 대상으로 하는 다양한 공격 기법들의 등장이 의미하는 바는 임베디드 시스템 및 마이크로프로세서가 전달받는 센서의 출력 값에 대한 무결성이 확실히 보장되지 않는다는 사실을 의미한다. 다음으로 드론이 사용하는 주요 무선 통신 기술을 대상으로 한 공격들을 살펴본 결과 해당 공격들은 주로 안전하지 않은 통신 채널을 사용했을 때 야기되는 특징이 있었다. 본 논문을 통한 분석 결과는 향후 안전한 드론 플랫폼 설계 및 드론 보안 가이드라인 제작 시 고려해야 할 내용으로 활용할 수 있을 것이라고 기대한다.

참 고 문 헌

[1] Saha, Arnab Kumar, et al, “IOT-based drone for improvement of crop quality in agricultural field“, 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2018.
[2] Boyle, Michael J, “The costs and consequences of drone warfare“, International Affairs 89.1, 1-29. 2013.
[3] 국토교통부, 한국교통연구원, 한국항공우주연구원 “드론 활성화 지원 로드맵 연구”, 9~65, 2017
[4] https://www.wired.com/2011/12/iran-drone-hack-gps
[5] https://www.wired.com/2013/05/drone-api/
[6] https://www.owasp.org/index.php/Fuzzing
[7] http://www.shell-storm.org/blog/Taint-analysis-and-pattern-matching-with-Pin/
[8] Hsueh, et al, “Fault injection techniques and tools“, Computer 30.4, 75-82, 1997.
[9] https://www.dji.com
[10] https://www.parrot.com
[11] http://www.symatoys.com
[12] https;//github.com/PX4/Hardware
[13] http://ardupilot.org
[14] http://nvd.nist.gov/vuln/detail/CVE-2017-3209
[15] http://research.checkpoint.com/dji-drone-vulnerability
[16] Yang, Hyunsoo, et al, “Multi-rotor drone tutorial: systems, mechanics, control and state estimation.“ Intelligent Service Robotics 10.2, 79-93, 2017.
[17] 손성화, 강진혁, 박경준. “드론 무선통신의 개요 및 이슈”, 한국통신학회지, 33.2, 93-99. 2016.
[18] Lim, Hyon, et al, “Build your own quadrotor: Open-source projects on unmanned aerial vehicles.“ IEEE Robotics & Automation Magazine 19.3, 33-45, 2012.
[19] Rodday, et al, “Exploring security vulnerabilities of unmanned aerial vehicles“, NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2016.
[20] Kerns, Andrew J. et al, “Unmanned Aircraft Capture and Control Via GPS Spoofing.”, J. Field Robotics 31, 617-636, 2014.
[21] Trippel, Timothy, et al, “WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks“, 2017 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2017.
[22] Son, Yunmok, et al, “Rocking drones with intentional sound noise on gyroscopic sensors“, 24th {USENIX} Security Symposium, 2015.
[23] Alibaba Security, “Sonic Gun to Smart Devices”, Blackhat ,USA. 2017.
[24] Pleban, et al, “Hacking and securing the AR. Drone 2.0 quadcopter: investigations for improving the security of a toy“, Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2014. Vol. 9030. International Society for Optics and Photonics, 2014.