정 보 보 호 학 회 지
제 30 권 제2호, 2020. 4

무인이동체 드론의 취약점분석 및 대응기술 연구 동향

김 명 수*, 유 일 선*, 임 강 빈*

요 약

군사 등의 특수 목적으로만 사용되었던 무인비행체 드론이 최근 상용 수준의 간결한 구조와 저가화가 가능해지면서 여러 제조업체를 통하여 민간분야의 다양한 응용에 활용 가능함을 증명하고 있다. 그러나 제조업체들 간의 시장 우위 선점을 위한 과열 경쟁으로 인하여 보안 안전성 검증 단계를 거치지 않은 드론과 이에 수반되는 애플리케이션이 시장에 바로 출시되면서 이들이 우리 사회를 향한 공격도구로 활용될 수 있다는 새로운 잠재적 위협이 우려되고 있다, 이와 관련하여 현재 드론과 애플리케이션과의 연결 및 데이터 통신 과정에서 완성도가 낮은 접근제어 기술이나 암호화되지 않은 통신방식을 비롯하여 드론 내부 소프트웨어의 코딩 상의 문제점 등에 의하여 다양한 취약점이 노출되고 있는 상태이다. 이러한 취약점들로 인하여 드론의 인증 해제 및 하이재킹을 통한 불법 영상촬영이나 개인정보의 유출 등을 비롯하여 특정 목표물을 향한 드론의 고의적 추락 등이 발생할 경우 재산 피해뿐만 아니라 인명 피해까지 발생할 수 있다. 특히, 현재의 드론 응용은 초기단계여서 향후 다양한 응용과 유관 기술들이 폭넓게 전개되어야 하는 시점에서 이러한 사고 가능성은 매우 심각하게 인식되어야 할 것이다. 더구나 제4차 산업혁명 시대의 드론은 비상시를 위한 다이나믹 모바일 게이트웨이 역할까지도 수행하여야 하는 환경에서 악의적인 행위는 전체 사회로 확산될 우려도 있으므로 미래 사회의 드론을 위한 안전문제는 매우 시급하고 중대하다고 할 수 있다. 이에 본 고에서는 현재까지 발표된 드론에 대한 다양한 보안위협을 조사하고 이러한 보안위협을 요소별로 분류하여 정리하였다. 본 기고가 간단하게나마 정리한 내용을 통하여 다양한 보안위협에 대한 대응기술을 준비하기 위한 시발점이 되었으면 한다.

Ⅰ. 서 론

드론은 몸체를 구성하는 프레임과 제어기, 통신 모듈, 모터, 프로펠러, 배터리 등으로 구성된 비행체이다. 드론은 형태나 사용 목적 등에 따라 일반 장난감처럼 제작된 소형 드론에서부터 이에 더하여 영상 또는 사진을 촬영할 수 있는 기능을 탑재한 드론 및 기타의 레저용으로 사용되는 드론 등 일반 사용자들이 주로 사용하는 드론과 방송장비를 탑재하고 촬영을 하거나 이를 활용하여 경비, 산불 감지, 재난지원, 해양관찰 등을 수행할 수 있는 전문가용 드론으로 구별될 수 있다[1].

드론을 구성하고 있는 내부 구성요소들을 살펴보면, 드론은 조종사와의 통신을 위하여 일반 무선이나 와이파이, 블루투스, 혹은 장거리 통신을 위하여 셀룰러 모듈 등을 내장할 수 있으며, 현재 위치 확인을 위하여 GPS 모듈이 탑재될 수 있고, 속도 변화 측정을 위한 가속도 센서, 드론의 자세제어를 위한 기울기 측정을 위한 자이로스코프 센서, 지면 상에서의 거리를 확인하기 위한 초음파 센서, 드론이 위치한 현장 상태 확인을 위한 카메라가 탑재될 수 있으며 온도, 습도 등의 측정을 위한 센서뿐만 아니라 고도 확인을 위한 바로미터 센서, 장애물을 피하기 위하여 사물과의 거리를 정할 수 있는 TOF 또는 Lidar 센서 등이 탑재될 수 있다. 또한 드론을 조종하는 조종사는 전용 컨트롤러 외에도 제조업체에서 제작한 모바일용 전용 애플리케이션을 통하여 드론을 조종할 수 있으며, 해당 앱을 통해서 드론의 상태 현황과 카메라를 이용하여 드론에서 촬영하는 영상을 실시간으로 스트리밍 해서 볼 수 있다.

상기의 다양한 구성요소와 기능의 추가에 따라 최근 드론을 상용 서비스에 이용하는 사례가 속속 발견되고 있고 그 확산 속도도 점점 더 빨라지고 있다. 이에 따라 드론이 물리적인 이상이 발생하여 사고로 이어질 경우

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00664, IoT가 내재된 가상물리시스템을 위한 규칙 명세 기반의 악의적인 행위 탐지)
* 순천향대학교 정보보호학과 (대학원생, brightprice@sch.ac.kr, 교수, isyou@sch.ac.kr, 교수, yim@sch.ac.kr)

이를 통하여 주변의 환경 구성요소에 미치게 손실의 치명성에 대한 우려가 지속적으로 강조되고 있다. 특히 드론이 공간 상에서 비행을 함으로써 물리적으로 독립되어 있음에도 불구하고 컨트롤러나 네트워크를 통하여 다양한 연결성을 제공하고 있기 때문에 이러한 요소들이 보안 취약점을 가질 경우 이를 통한 잠재적 사이버 위협이 현실화될 것이 매우 우려되는 상황이다. 드론의 내부 구성 요소가 다양한 만큼 이들 모든 요소에 취약점 내포 가능성이 존재하며 이러한 취약점이 악용되어 보안 위협이 현실화될 수 있다. 따라서 드론이 안전하기 위해서는 각 구성 요소가 가질 수 있는 취약점에 대한 전체적인 기술적 검증과 점검이 요구된다. 예로서 드론에 탑재된 GPS 모듈은 위치 정보의 스푸핑을 통해서 공격자가 원하는 곳으로 임의 이동할 가능성이 있다. 자이로스코프 센서 같은 경우에는 특정 음향 또는 초음파의 영향을 받을 경우 내부 값이 임의로 변화되어 드론이 중심을 잃고 추락할 가능성이 있다. 드론이 와이파이를 통해서 연결하는 경우 드론 Wi-Fi가 가진 개방성으로 인하여 같은 애플리케이션을 소유한 다른 사용자가 임의로 드론에 연결할 수도 있다. 또한 사용자가 설치한 드론의 애플리케이션을 살펴보면 앱의 암호화 키 초기 값이 프로그램 내부에 고정적으로 하드코딩되어 있을 수 있어 이를 통하여 보안 채널이 탈취될 수 있고, 극단적으로는 드론과 사용자 간의 통신이 암호화 없이 무방비로 이루어져 패킷 수집기를 통하여 악의적인 사용자에게 노출될 수 있다.

본 고에서는 이러한 보안 위협 가능성과 연계하여 드론에서 발생 가능한 취약점들을 정리하였으며, 이를 센서별, 네트워크별, 공격 유형별로 분류하여 설명하고자 한다.

Ⅱ. 관련 연구

드론은 비행 안전성을 확보하거나 사용자가 요구하는 기능 구현을 위하여 영상을 촬영할 수 있는 카메라, 위치 확인을 위한 GPS 센서, 드론의 기울기 계산을 위한 자이로스코프 센서, 범용 RF 통신뿐만 아니라 블루투스, 와이파이, 셀룰러 등을 지원하는 네트워크, 드론 제어 및 관련 정보 확인과 영상을 스트리밍하는 애플리케이션 컨트롤러 등으로 구성된다. 이러한 드론의 구성요소와 관련된 보안 위협 요소로는 GPS 취약점, 자이로스코프 취약점, 접근 제어 취약점, 하드코딩 취약점, 암호화되지 않은 데이터 전송 취약점, 개방형 Wi-Fi 취약점, 개방된 포트 취약점, 퍼징 공격, DoS 공격, 인증 해제, 중간자 공격 등이 있다. 본 장에서는 드론의 주요 구성 요소와 관련된 취약점을 소개하며 이와 관련된 내용을 표 1에 정리하였다.

〔표 1〕 드론 주요 구성요소와 관련된 취약점 분류

구성요소	취약점	내용	관련연구
GPS	GPS 스푸핑	GPS 좌표 임의 변경을 통한 드론 납치	〔2〕, 〔3〕
자이로 스코프	오프셋 값 추적	자이로스코프의 오프셋 값을 사용하여 드론 추적	〔4〕
	센서 값 불안정	공진 주파수를 사용한 데이터 임의 변동	〔5〕
네트워크	개방형 Wi-Fi 취약점	개방형 Wi-Fi를 사용한 드론 납치	〔3〕, 〔6〕, 〔8〕, 〔10〕
	개방된 포트 취약점	개방된 포트를 통한 루트 접근 권한 획득	〔6〕
	퍼징 공격	데이터 무작위 주입을 통한 드론의 오작동 유도	〔11〕, 〔12〕
	DoS 공격	과도한 패킷 주입을 통한 시스템 과부하 발생	〔6〕, 〔9〕, 〔10〕, 〔11〕
	중간자 공격	위장을 통한 사용자 개인정보 데이터 탈취	〔6〕, 〔13〕
애플리 케이션	하드코딩	주요 데이터 애플리케이션 내부 자체 배치	〔7〕, 〔8〕
	암호화되지 않은 데이터 전송 취약점	평문 데이터 노출을 통한 개인정보 탈취	〔9〕
인증	접근 제어	접근 인증 과정 부재로 인한 공격	〔3〕, 〔6〕, 〔7〕
	인증 해제	암호화 되어 이지 않은 부분을 사용한 인증 해제	〔3〕, 〔6〕, 〔8〕

2.1. GPS(Global Positioning System) 취약점

GPS는 위성에서 출력되는 전파를 기반으로 현재의 위치를 확인하는 시스템이다. 드론에 GPS 모듈을 장착하여 위치 확인을 하거나 사용자가 설정한 장소(예: 집 또는 특정 구역)로 이동하는 기능을 제공할 수 있다. GPS 스푸핑은 GPS를 공격하는 방법 중 하나로, GPS 위성신호보다 더 높은 신호를 드론에 송신하여 드론에 장착된 GPS 센서가 악의적인 사용자가 설정한 좌표를

인식하게 하여 해당 좌표로 이동하도록 유도하는 공격 방법이다. 군용 GPS는 암호화가 되어 있어 스푸핑이 쉽지 않지만 민간 GPS는 암호화가 되어 있지 않아 이러한 공격에 그대로 노출될 수 있다[2, 3].

2.2. 자이로스코프 취약점

자이로스코프는 물리적인 공간정보 추출을 위한 3축을 계산하여 드론의 기울기와 기울어진 방향의 값을 내부 소프트웨어로 전달하는 센서이다. 드론의 움직임은 사용자의 조종과 자이로스코프의 센서 출력을 통해서 내부 소프트웨어로 전달되며, 소프트웨어에서는 입력받은 데이터로 모터의 출력을 조정하여 드론을 움직인다. 이러한 자이로스코프 내부의 데이터 값과 잠재된 취약점을 사용하여 공격할 경우 드론 추적 등의 형태로 악용될 수 있다. 자이로스코프와 관련된 취약점 분석 연구로 자이로스코프의 오프셋 값을 사용하여 드론의 위치를 추적하는 방법[4]과 음향을 사용하여 자이로스코프를 무력화하는 방법[5]이 있다.

2.3. 접근 제어 취약점

접근 제어 취약점은 네트워크 접근 시 인증 절차가 없거나 인증 방법을 우회하여 악의적인 사용자가 네트워크에 제한 없이 접근할 수 있는 취약점이다. 드론에는 사용자 애플리케이션과의 통신을 위하여 고정 IP가 할당될 수 있으며 이를 통하여 드론에 장착된 모듈 제어 및 저장된 데이터 교환을 수행한다. 이러한 통신 과정에서 접근 제어 인증 방법이 없거나 인증 방법을 우회하는 방법이 있을 경우 카메라 제어 및 데이터 탈취 등이 발생할 수 있으며 이와 관련된 취약점 분석 연구로서 [3, 6, 7]가 있다.

2.4. 하드코딩 취약점

하드코딩은 사용자 인증이나 암호화 수행 등의 과정에서 필요한 데이터를 외부 소스에서 데이터를 가져오는 것이 아닌 개발 과정에서 프로그램 소스 코드에 직접 포함하는 것을 말하며 그렇게 함으로써 소프트웨어를 역분석하게 되면 인증이나 암호화 수행 과정에서 사용하는 기밀정보를 임의로 확보하여 이들 절차를 무력

```
private static final int PORT_NUMBER = 2121;
private static final String PWD = "yuneec";
private static File ROOTDIR = new File(Environment
private static final boolean SHOULD_TAKE_FULL_WAKE
private static final String USERNAME = "root";
```

〔그림 1〕 하드코딩 취약점〔7〕

화할 수 있다. 제조업체가 출시한 드론 애플리케이션 중에서는 네트워크 IP를 고정으로 설정하거나 데이터 암호화 등을 위한 키 값을 그대로 하드코딩하여 입력하는 애플리케이션이 존재하며, 악의적인 사용자는 이를 사용하여 고정 IP 주소와 연결된 카메라의 비디오를 캡처하거나 암호 변경 및 복호화를 수행하여 사용자의 데이터를 탈취할 수 있다. [7, 8]에서 하드코딩 취약점 분석과 관련된 연구를 진행하였다.

2.5. 암호화되지 않은 데이터 전송 취약점

드론과 애플리케이션 간의 데이터 통신 과정에서는 악의적인 사용자의 패킷 캡처에 의한 데이터 정보 탈취 방지를 위하여 데이터를 암호화해서 전송해야 한다. 데이터 전송 시 암호화되지 않은 데이터를 그대로 전송할 경우 사용자의 패킷 전송 데이터가 노출되고, 악의적인 사용자가 해당 패킷을 분석하여 악의적인 패킷을 전송하여 드론의 진행을 방해할 수 있다[9].

2.6. 개방형 Wi-Fi 취약점

드론은 사용자 애플리케이션과의 연결을 위하여 개방형 Wi-Fi를 운영하며 사용자는 해당 Wi-Fi에 연결하여 드론 조종 및 영상 등의 관련 데이터를 수신한다. 이러한 개방형 Wi-Fi는 해당 드론의 애플리케이션을 설치하면 누구나 연결할 수 있어 악의적인 사용자에 의하여 드론이 탈취될 수 있다[3, 6, 8, 10].

2.7. 개방된 포트 취약점

드론은 특정 포트를 통해서 사용자의 명령을 전송 받으며, 반대로 특정 포트를 통해서 사용자에게 데이터 또는 스트리밍을 전송한다. NMAP 포트 스캐닝 툴을 사용하여 드론에서 개방된 포트를 확인할 수 있으며 드론에 사용하지 않는 포트가 개방되어 있고 해당 포트에 시스템 접근을 위한 비밀번호가 활성화 되어 있지 않을

경우 악의적인 사용자는 이를 통해서 루트 접근 권한을 획득할 수 있다[6].

2.8. 퍼징 공격

퍼징은 특정 타겟에 정상/비정상 데이터를 무작위로 주입하여 시스템(프로그램과 프로토콜 등을 포함)에서 발생 가능한 모든 취약점과 버그의 발생 여부를 확인하는 방법이다. 드론에 대한 퍼징 공격 수행은 임의의 데이터를 주입함으로써 드론 내부에 버퍼 오버플로우 등의 취약점과 버그가 존재하는지 확인하는 것이며, 공격 수행 방법은 컴퓨터에서 스크립트된 퍼징 도구를 사용하여 드론의 특정 포트에 퍼징 공격을 적용한다. 드론에 전송되는 메시지의 형식은 JSON 또는 MAVLink 등이 사용될 수 있으며 메시지의 길이와 내용은 메시지 전체 길이, ID. 최소/최대값 등의 테스트 케이스를 적용하여 드론에 대한 공격을 수행한다. 본 내용과 관련된 연구로는 컴퓨터의 스크립트를 적용한 방법[11]과 가상 머신 시뮬레이터에서 적용한 방법[12]이 있다.

2.9. DoS 공격

DoS 공격은 시스템에 설계된 기존 트래픽 허용 범위를 초과하는 패킷을 과도하게 전송하여 시스템에 대한 서비스 지연, 오류, 정지 등의 오작동을 유도하는 공격이다. 드론 DoS 공격은 패킷 생성 도구 등을 사용해서 사용자가 조종하는 드론에 과도한 패킷을 전송하여 드론 시스템 정지 또는 사용자의 명령 전송 지연을 유발하며, 이로 인하여 드론의 추락을 유도하는 것을 의미한다. 드론에 DoS 공격이 수행되면 드론 내부 시스템에 과부하가 발생하여 패킷 응답 속도가 평소보다 느려지며 이와 관련된 드론 DoS 공격 연구로는 [6, 9, 10, 11]이 있다.

2.10. 인증 해제

인증 해제는 사용자와 개체 간의 인증된 연결을 발견된 취약점을 사용하여 해제하는 방법으로 드론과 사용자의 연결을 해제하여 드론의 조종을 방해하는 공격 방법이다. 악의적인 사용자는 드론의 암호화가 되어 있지 않은 부분을 악용하거나 네트워크 분석 도구를 사용하여 인증을 해제하며, 이와 관련된 연구로 [3, 6, 8]이 있다.

2.11. 중간자 공격

중간자 공격은 통신하는 사용자 간의 연결 및 전송 과정에서 악의적인 사용자가 중간에 침입하여 사용자가 전송하는 데이터를 탈취하거나 조작하여 다른 사용자에게 전달하는 것을 의미한다. 드론의 중간자 공격은 드론과 사용자 사이에서 전송되는 데이터 탈취를 위하여 사용하는 공격 방법으로, 악의적인 사용자는 중간자 공격을 수행하기 위한 특정 장치(라즈베리파이 등)를 사용해서 주변 드론의 AP를 검색하고 해당 드론의 AP 정보를 모방한다. 이로 인하여 드론 조종 사용자를 자신의 장치에 연결할 수 있으며 이는 사용자의 정보가 악의적인 사용자에게 전송된다는 것을 의미한다. 드론의 중간자 공격과 관련된 연구로 [6]와 [13]이 있다.

Ⅲ. 구성요소별 보안위협에 대한 대응 방안

드론 보안 위협 요소에 대한 대응 방안을 크게 4가지로 분류하면 GPS 스푸핑 된 드론에서 스푸핑 탐지 및 위치를 스푸핑 전 원상태로 복원하는 방법, Wi-Fi 네트워크 연결 과정을 암호화하는 방법, 드론 대상 DoS 공격에 대한 방어 및 복구 방법, 컨트롤러와 드론 사이에 암호화를 적용하여 악의적인 사용자에 대한 중간자 공격을 방지하는 방법 등이 있다. 본 장에서는 상기와 같이 드론의 보안을 위협하는 각 요소에 대한 대응 방안 및 방법을 소개한다.

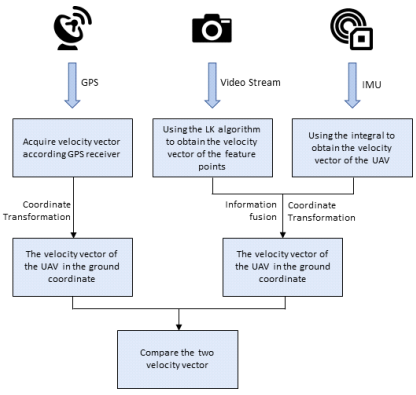
3.1. GPS 스푸핑 탐지 및 복원 방법[14]

GPS 스푸핑 탐지 및 복원을 위하여 드론에 전용의 장치를 내장하는 방법이 있다. 이러한 방법에서는 드론에 내장된 센서 정보와 카메라에서 수집되는 영상 정보를 비교하여 GPS 스푸핑을 탐지한다.

드론에서 GPS 스푸핑을 탐지하기 위해서는 GPS에서 수신된 위치 정보에 해당하는 값과 비교할 수 있는 정보를 드론 내부에서 별도로 생성해야 한다. 이를 위해서 3차원 방향과 속도를 측정할 수 있는 IMU 센서와 드론에 장착된 카메라를 사용하여 해당 정보를 생성한다. GPS 모듈에서 수신한 위치 값과 드론 내부에서 생

성한 값을 비교하는 기준은 NED (North-EastDown) 좌표계를 이용한다. 드론 내부에서의 좌표값 생성은 IMU 센서 정보와 카메라 영상 정보를 활용한다. IMU 센서에서 자체 측정한 가속 값은 NED 좌표계로 변환되며, 카메라에서 촬영되는 영상을 기반으로 LK (Lucas-Kanade) 알고리즘을 사용하여 드론의 속도를 측정하고 해당 값은 마찬가지로 NED 좌표계로 변환된다. 변환된 IMU 센서로부터의 좌표값과 카메라 영상으로부터 얻은 좌표값은 칼만(Kalman) 필터를 사용하여 융합된 정보로 변환된다. 드론의 GPS 모듈로부터의 수신 값도 NED 좌표계로 변환된다. 드론 내부에서 융합 변환된 값인 V와 GPS 수신 정보를 기반으로 변환한 Vg를 비교하여 GPS 스푸핑을 탐지한다. 비교 대상의 두 값에 대한 차분에 임계값을 설정하고 허용한 임계값을 초과할 경우 드론이 GPS 스푸핑이 되었다고 판단한다.

GPS 스푸핑된 드론을 원래 위치로 복원하는 방법은 드론에서 촬영된 카메라의 이미지와 저장된 IMU 센서 값을 사용하여 드론을 원래 위치로 복원하는 방법이다. 이는 드론 내부에 장착된 카메라에서 시간대 별로 이미지를 촬영하고, 촬영된 이미지마다 IMU에서 측정된 순간 속도 및 위치를 저장하여 촬영된 순서대로 드론 내부에 보관하는 것이다. 드론이 GPS 스푸핑되었다고 판단되면 최근에 촬영된 이미지와 저장된 순간 속도 및 위치를 확인하여 해당 위치로 이동하며, 최근 촬영된 이미지에 가까워지면 최근 촬영된 이미지와 현재 카메라의 이미지를 비교한 다음 일치 여부를 확인한다. 일치할 경우 최근 촬영된 이미지의 좌표를 현재 좌표로 대체하며 그다음 촬영된 이미지와 좌표로 이동하며, 이것은 맨 처음 촬영된 이미지와 좌표로 돌아올 때까지 반복한다.



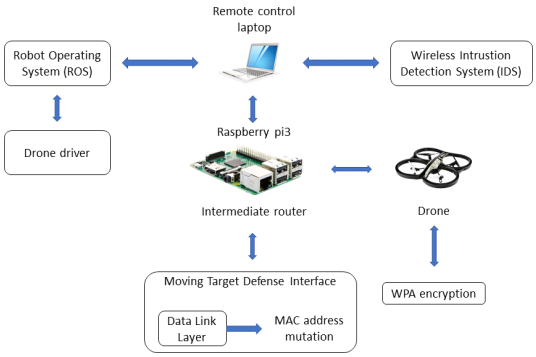
〔그림 2〕 GPS 스푸핑 탐지 방법〔14〕

3.2. 드론 무선 네트워크 암호화 기법 [15]

Wi-Fi 연결 방식 드론의 취약점은 사용자의 드론 연결을 위하여 드론이 AP가 되고 이러한 AP가 암호화 없이 개방되어 있어 악의적인 사용자도 연결이 가능하다는 것이다. 본 방법은 드론과 사용자 사이에 무선 네트워크 암호화를 수행하는 장치를 설치하고 해당 장치에 침입 탐지 및 회피 기술을 추가하여 악의적인 사용자에 대한 공격을 탐지 및 방지한다. 참고문헌에서는 드론과 사용자 간 중간 장치로 라즈베리파이를 사용하며, 드론과 라즈베리파이 무선 암호화 방법은 WPA2를 사용하고, 라즈베리파이 내부에는 공격 여부를 확인하기 위한 Kisnet wireless 침입 탐지 시스템과 공격을 회피하기 위한 이동 표적 방어(Moving Target Defense) 기술을 사용한다.

먼저 드론과 라즈베리파이의 무선 암호화를 위하여 드론 라이브러리에 컴파일된 WPA supplicant 바이너리 파일을 설치한다. 본 파일에는 라즈베리파이의 AP 이름과 비밀번호가 있으며 드론이 수행했던 AP 방식을 중단하고 해당 라즈베리파이에 연결하는 방법이 포함된다. 이후 드론과 라즈베리파이 통신은 WPA2 암호화로 진행된다. 공격자의 공격을 탐지하기 위해서 라즈베리파이 내부에 Kismet wireless IDS를 설치한다. 본 IDS에 경고 목록이 파일로 포함되어 무선 네트워크를 모니터링하며, 이상이 있을 경우 사용자에게 경고 메시지를 전송한다. 공격자의 공격을 회피하기 위해서는 네트워크 시스템 구성 요소가 변동되어야 한다. 이를 위하여 Moving Target Defense 기술을 사용하여 침입 탐지 시 네트워크 구성 요소를 변경한다. 라즈베리파이에 해당 기법을 사용하였으며 MAC 주소를 변경하여 공격자의 공격을 회피한다.

드론과 라즈베리파이가 연결되어 있는 상태에서 공격자가 데이터 수집기로 데이터 캡처를 시도하였으나 무선 네트워크는 암호화가 되어 있어 데이터 분석에 실패한다. 공격자가 라즈베리파이의 MAC 주소에 DoS 공격을 수행하면, Kismet wireless IDS가 모니터링 과정에서 해당 공격을 감지하고 사용자에게 경고 메시지를 전송한다. 그 후 Moving Target Defense 시스템을 사용하여 라즈베리파이 MAC 주소를 변경한다. MAC 주소가 변경된 라즈베리파이로 인하여 공격자는 DoS 공격에 실패한다.

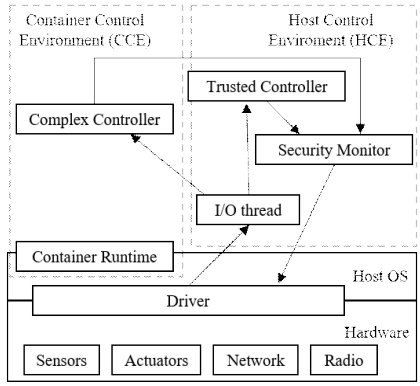


〔그림 3〕 드론 무선 네트워크 암호화 기법〔15〕

3.3. 드론 DoS 공격 방어 및 복구 [16]

본 참고문헌에서의 드론 DoS 공격 방어 및 복구 방법은 드론 운영체제의 주요 리소스인 CPU, 메모리, 통신 채널을 보호하는 컨테이너드론 프레임워크를 구현하고 보안 모니터링과 복구 프로그램을 통하여 공격자의 DoS 공격에 대해서 방어와 복구를 수행하는 방법이다.

컨테이너드론 프레임워크 구현을 위하여 라즈베리파이3 기반의 드론이 사용되며 드론의 DoS 공격에 대비하기 위하여 센서와 드라이버를 시뮬레이션한다. 시뮬레이터에는 컨테이너 및 CCE(Container Control Environment)와 HCE(Host control environment)가 포함된다. 이를 이용하여 드론의 DoS 공격 방어 및 복구를 진행하며 메모리에 대한 DoS 공격 보호 방법은 Memguard를 사용한다. CCE는 컨테이너 환경의 복잡한 컨트롤러를 의미하며, 고급 기능과 최적화된 성능을 가지고 있으나 보안에 취약할 수 있다. HCE의 신뢰된 컨트롤러는 검증은 되었으나 기본적인 기능만 제공한다. CCE와 HCE의 통신은 네트워크 인터페이스를 통하여 수행하며, 컨테이너에는 HCE만 MAVLink 프로토콜로 연결되어 있고 CCE는 HCE에 전용 인터페이스로 연결된다. 드론 내부에서 센서를 기준으로 데이터를 전송하는 방법을 보면 HCE에서 컨테이너에 있는 센서 드라이버의 값을 UDP 소켓을 통해서 CCE의 컨트롤러로 전달하면, CCE의 컨트롤러에서 해당 값에 맞는 액추에이터 출력을 생성하고 UDP 소켓을 통해서 HCE로 전달한다. DoS 공격 방지를 위하여 두 환경의 컨트롤러를 모두 사용하는데, 평소에 기능을 위하여 CCE의 컨트롤러를 사용하다가 비상시에는 HCE의 컨트롤러를 사용한다. DoS 공격을 방지하는 방법은 호스트 제어 환경에서 실행되는 안전 모니터를 통해서 두 컨트롤러를 모니터링하다가 이상 여부가 생기면 안전 모니터에서 CCE의 컨트롤러를 HCE의 컨트롤러로 변경하여 공격에 의한 추가 피해를 방지한다.



〔그림 4〕 드론 DoS 공격 방지 아키텍처〔16〕

구현한 결과물에 대한 테스트 방법은 Memguard를 통한 드론 메모리 DoS 공격 방어 방법과 보안 모니터링을 통한 UDP DoS 공격 방어 방법 및 CCE 공격 방어 방법으로 분류된다. Memguard를 통한 드론 메모리 방어 방법을 보면 공격자는 컨테이너 내에서 HCE에 메모리 DoS 공격을 시작하며 메모리 공격은 대역폭 벤치마크 프로그램을 사용하여 공격한다. Memguard가 없을 경우 드론이 추락하지만 Memguard가 활성화되면 드론은 흔들리다가 곧 잠잠해지는 것을 확인할 수 있다. 보안 모니터링을 통한 UDP 방어 방법에서는 공격자가 UDP 채널을 통하여 HCE에 DoS 공격을 수행하며, 이를 위하여 UDP 포트에 지속적으로 패킷을 전송하는 프로그램을 사용한다. 프로그램이 시작되면 드론의 회전 반경이 점차 강해지다가 내부에서 자세 오류 제어를 시작하며, 보안 모니터링에서 평소에 CCE를 감시하다가 출력 수신 중단을 확인하면 안전 컨트롤러로 전환하여 출력하는 것이다.

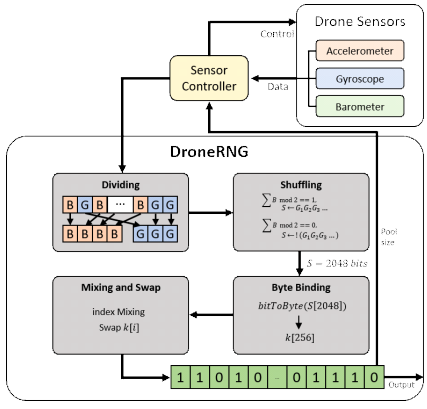
3.4. 센서 데이터 기반 난수 생성기 [17]

센서 데이터 기반의 난수 생성기는 드론에서 프로토콜 암호화 시 일반 난수 생성기를 사용해서 암호화하는 것이 아닌 드론에 장착된 센서의 데이터 값을 사용해서 난수를 생성하는 방법으로, 드론의 가속도계, 자이로스코프, 기압 센서, 기압계 등에서 출력되는 값들을 추출,

수집, 조합하여 시드 값을 생성한 다음, 해당 값을 사용해서 암호화 키를 생성하고 프로토콜 통신 시 해당 키로 암호화하여 통신하는 방법이다.

센서 데이터 기반의 난수 생성을 위하여 드론에는 가속을 계산하는 가속도계와 드론의 기울기를 계산하는 자이로스코프, 기압의 변화를 측정하는 기압계 센서가 있으며 이러한 센서들의 값을 수집하여 드론 난수 생성기로 전달하는 센서 컨트롤러가 있다. 드론 난수 생성기 내부에는 센서에서 들어온 데이터를 랜덤성이 있는 비트와 없는 비트로 분류하는 Dividing, 시드의 임의성 향상을 위한 Shuffing, 비트를 바이트로 변환하는 Byte Binding, RC4 스트림 암호를 기반으로 하는 Mixing과 Swap의 절차가 있으며 Dividing → Shuffing → Byte Binding → Mixing → Swap 5단계에 걸쳐서 난수를 생성한다.

센서 컨트롤러는 드론 센서에서 수집한 데이터를 드론 난수 생성기로 전송한다. 난수 생성기에서는 입력된 데이터를 랜덤성이 있는 비트와 없는 비트로 나누어 구별한 다음 Shuffing 과정을 통해서 해당 비트들을 비트 스트링 S에 저장한다. 비트 스트링이 2048 비트 크기로 채워지면 입력된 비트 스트링 S를 바이트 단위로 처리하여 변환된 256 바이트를 해당 크기의 배열 K에 저장한다. 배열 K는 Mixing과 Swap을 거쳐 난수로 생성된다.



〔그림 5〕 드론 난수 생성기 알고리즘[17]

Ⅳ. 결 론

본 고에서는 무인이동체 드론에 대한 취약점 분석과 대응기술에 대하여 살펴보았다. 드론은 내부 구조와 구성, 위치 확인 등을 위한 센서 정보의 처리, 네트워크에서의 인증 또는 데이터 전송 등에서 설계 또는 구현 과정 등에서 내포되는 잠재적 취약점으로 인하여 하이재킹, 추락, 지연 전송, 데이터 탈취 등의 피해가 발생할 가능성이 존재하며, 이에 대한 대응 방안 연구로 하이재킹을 탐지하고 드론의 위치를 원상 복구하는 방법과 사용자와 무선 네트워크 간의 암호화 방법, DoS 공격 방어 및 복구 방법, 드론의 센싱 데이터를 사용한 난수 생성 방법 등을 소개하였다.

4차 산업혁명 시대에서의 드론은 그 활용의 범위가 크게 확장될 것이고 향후에는 없어서는 안 될 사회의 필수 요소가 될 것이다. 본 고에서 소개하는 위협과 대응방법은 상용의 드론에 적용되어야 최소한의 보안기술이라 생각되며 이 외에도 미시적으로는 펌웨어 변조를 비롯하여 거시적으로는 군집행위 기반 다중 드론의 통합관리 서버에 대한 공격과 이들에 대한 방어기술 등을 포함하여 알려져 있지 않은 다양한 취약점에 대한 대응방안의 마련이 필요하다.

참 고 문 헌

[1] 경상북도, “『4차 산업혁명 기반 드론 산업』 국내외 동향연구 보고서”, November 2019.

[2] Arteaga, S. P., Hernández, L. A. M., Pérez, G. S., Orozco, A. L. S., and Villalba, L. J. G., “Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo.”, *IEEE Access 7* (2019): 51782-51789.

[3] Dey, V., Pudi, V., Chattopadhyay, A., and Elovici, Y., “Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study.”, *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*. IEEE, pp. 398-403, 2018.

[4] Son, Y., Noh, J., Choi, J., and Kim, Y., “Gyrosfinger: Fingerprinting drones for location tracking based on the outputs of mems gyroscopes.” *ACM Transactions on Privacy and Security (TOPS)* 21.2 (2018): 1-25.

[5] Son, Y., Shin, H., Kim, D., Park, Y., Noh, J.,

Choi, K., ... and Kim, Y., “Rocking drones with intentional sound noise on gyroscopic sensors.”, In *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pp. 881-896., 2015,

[6] Westerlund, O., and Asif, R., “Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things.”, *2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)*. IEEE, pp. 1-10., February 2019.

[7] Kim, D., and Kim, H. K., “Security Requirements of Commercial Drones for Public Authorities by Vulnerability Analysis of Applications.”, *arXiv preprint arXiv*:1909.02786., 2019.

[8] Nunez, J., Tran, V., and Katangur, A., “Protecting the Unmanned Aerial Vehicle from Cyberattacks.”, In *Proceedings of the International Conference on Security and Management (SAM)*, The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). pp. 154-157., 2019.

[9] Kwon, Y. M., Yu, J., Cho, B. M., Eun, Y., and Park, K. J., “Empirical analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles.”, *IEEE Access, 6*, 43203-43212., 2018.

[10] Vasconcelos, G., Carrijo, G., Miani, R., Souza, J., and Guizilini, V., “The impact of DoS attacks on the AR. Drone 2.0.”, In *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR)* IEEE., pp. 127-132., October 2016.

[11] Bonilla, C. A. T., Parra, O. J. S., and Forero, J. H. D., “Common security attacks on drones.”, *International Journal of Applied Engineering Research, 13*(7), 4982-4988., 2018.

[12] Domin, K., Symeonidis, I., and Marin, E. “Security analysis of the drone communication protocol: Fuzzing the MAVLink protocol.”, 2016.

[13] Rodday, N. M., Schmidt, R. D. O., and Pras, A. “Exploring security vulnerabilities of unmanned aerial vehicles.” *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*,, IEEE, pp. 993-994, April 2016.

[14] He, D., Qiao, Y., Chan, S., and Guizani, N., “Flight security and safety of drones in airborne fog computing systems.” *IEEE Communications Magazine, 56*(5), 66-71., 2018.

[15] Gudla, C., Rana, M. S., & Sung, A. H., “Defense Techniques Against Cyber Attacks on Unmanned Aerial Vehicles.” *Proceedings of the International Conference on Embedded Systems, Cyber-physical Systems, and Applications (ESCS)*., The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), p. 110-116., 2018.

[16] Chen, J., Feng, Z., Wen, J. Y., Liu, B., and Sha, L., “A container-based dos attack-resilient control framework for real-time UAV systems.” *In 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, IEEE, pp. 1222-1227, March, 2019.

[17] Cho, S. M., Hong, E., and Seo, S. H., “Random Number Generator Using Sensors for Drone.”, *IEEE Access, 8*, 30343-30354., 2020.

〈저자소개〉

김 명 수 (Myoungsu Kim)

학생회원

2016년 2월 : 순천향대학교 정보보호학과 (공학사)

2016년 3월~현재 : 순천향대학교 정보보호학과 석·박사통합과정

<관심분야> 취약점 분석, 시스템 보안, 하드웨어 보안

유 일 선 (Ilsun You)

종신회원

2002년 2월 : 단국대학교 전산통계학과 박사 졸업
2005년 3월 : 한국성서대학교 정보과학부 전임강사
2008년 3월 : 한국성서대학교 정보과학부 조교수
2012년 3월 : 한국성서대학교 정보과학부 부교수
2015년 9월~현재 : 순천향대학교 정보보호학과 부교수
<관심분야> 인증 및 접근통제, 이동통신보안, 인터넷 보안, 정형화 보안 검증

임 강 빈 (Kangbin Yim)

종신회원

1992년 2월 : 아주대학교 전자공학과 (공학사)
1994년 2월 : 아주대학교 전자공학과 (공학석사)
2001년 2월 : 아주대학교 전자공학과 (공학박사)
1999년 3월~2000년 2월 : (미)아리조나주립대학교 연구원
2003년 3월~현재 : 순천향대학교 정보보호학과 교수
2005년 3월~현재 : 한국정보보호학회 이사
2009년 3월~현재 : 한국인터넷정보학회 이사
2010년 12월~2012년 2월 : (미)퍼듀대학교 객원교수
<관심분야> 취약점 분석, 내부자 공격, 보안 하드웨어 구조, 인증 프로토콜, 홈랜드 시큐리티