GOTCHA! Drone: 드론의 무선 신호 취약점 분석을 위한 4단계 프레임워크

허남정*, 최재민*, 장우현[1], 김연재[1], 허재원[1], 박기웅†

*세종대학교 SysCore Lab. (대학원생)

[1]LIG 넥스원 연구원

† 세종대학교 정보보호학과 (교수)

GOTCHA! Drone: A 4-Step Framework for Drone Wireless-Signal Vulnerability Analysis

Nam-Jung Heo*, Jae-Min Choi*, Woo-Hyun Jang[1], Yeon-Jae Kim[1], Jae-Won Huh[1], Ki-Woong Park†

*SysCore Lab., Sejong University(Graduate Student)

[1]LIG NEX1 Researcher

† Dept. of Computer and Information Security, Sejong University (Professor)

요 약

현대 전쟁에서 드론은 서로 다른 형태와 크기를 가지며, 사람이 탑승할 필요가 없이 원격으로 조종할 수 있는 특성으로 인해 테러, 정찰, 암살 등의 다양한 용도로 사용될 수 있다. 이에 대응하여 비행 중인 드론에 변조된 패킷을 전달하여 제어권을 탈취할 수 있는 연구들이 진행되고 있다. 본 논문에서는 실제 드론의 무선 신호를 디코딩하고 분석한다. 이를 통해 드론의 페이로드를 식별하고 TX ID 값만을 변경하여 명령을 전달할 수 있는 4단계 분석 프레임워크 및 대응 전략을 도출한다. 향후 특정 필드 값을 변조하여 다양한 취약점 코드를 생성할 수 있는 기술 고도화를 목표로 한다.

I. 서론

현대 전쟁에서 드론의 사용은 증가하고 있다. 드론은 서로 다른 형태와 크기를 가질 수 있으며, 사람이 탑승할 필요 없이 원격으로 조종할 수 있다. 이러한 특성으로 아마추어 드론이라고 불리는 소형 드론은 테러, 정찰, 암살 등의 용도로 사용되고 있다 [1].

이에 대응하여 사전에 아마추어 드론의 무선 신호를 디코딩하고 주요한 필드를 분석하여 대상 드론의 취약점을 식별하는 연구들이 진행되고 있다 [2-4]. 무선 신호는 브로드캐스트 특성을 가지므로 Software Defined Radio(SDR) 장비와 응용-프로그램을 사용하여 대상 신호를 식별하고 분석할 수 있다.

본 연구에서는 신호의 도청, 위조, 재전송 공격에 취약한 드론을 대상으로 무선 신호 취약점 분석을 위해서 4단계 프레임워크를 사용하여 동일 기종의 새로운 기체에 긴급 제동 명령을 주입할 수 있는 취약점을 식별한다.

본 논문의 구성으로 2장에서는 무선 신호 취약점 식별 연구들을 정리하고 3장에서는 실제 드론을 대상으로 4단계 프레임워크에 따라 무선 신호 취약점을 식별한다. 4장에서는 식별된 취약점에 대한 대응 전략을 도출하고 5장에서 결론 및 향후 연구 방향을 기술한다.

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

이 논문은 2022년 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임 (KRIT-CT-22-051)

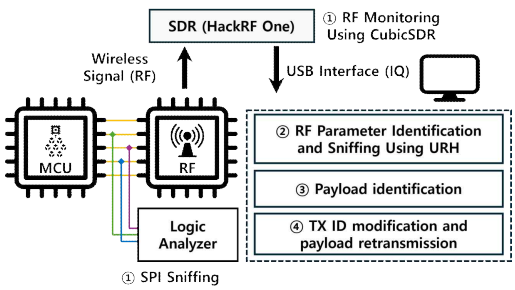
II. 관련 연구

드론의 무선 신호의 취약점을 분석하는 연구들은 DJI 계열 및 DJI 계열이 아닌 드론으로 나뉘어 수행된다. 대표적으로 DJI 계열 드론의 Drone ID 신호를 SDR 장비와 GNU Radio를 사용하여 디코딩하고 드론의 현재 위치 및 조종자 정보를 식별하는 연구가 있다 [2]. 이러한 분석 방식은 Drone ID 신호가 암호화되지 않고 주기적으로 송출되어 신호 분석이 가능하다. 하지만, 암호화가 적용된 명령&제어 신호의 경우에는 신호 분석에 한계가 있다.

D. Pratama et al. [3] 연구에서는 DJI Mavic Mini2 드론을 Hack RF One(SDR) 장비를 사용하여 신호 디코딩을 시도한다. 하지만, Hack RF One은 신호 분석 해상도 및 샘플링 능력이 부족하여 디코딩에 실패한다. 대신, 대상 드론이 Wifi 프로토콜을 사용하고 있음을 식별하고 Mikrotik LDF 5 Wifi 공유기를 사용하여 WIFI 링크 하이재킹을 성공한다. 하지만, 최근 DJI 계열 드론은 Wifi 프로토콜 대신 Ocusync 프로토콜 및 ASIC 기반으로 설계된 RF 칩을 사용하기 때문에 현재의 새로운 기종에는 해당 분석 방식이 적용되지 않는 한계점이 있다.

최근 등장한 Universal Radio Hacker(URH) 도구는 기존의 GNU Radio와 달리 디지털 신호 처리 기술의 깊은 이해 없이도 드론의 무선 신호 분석이 가능하다. T. Omar et al. [4] 연구에서는 URH와 SDR 장비만을 사용하여 4D-V2 Mini 드론에 대해서 재전송 공격을 수행하고 이륙과 착륙을 제어하는데 성공한다.

III. 무선 신호 분석 4단계 프레임워크

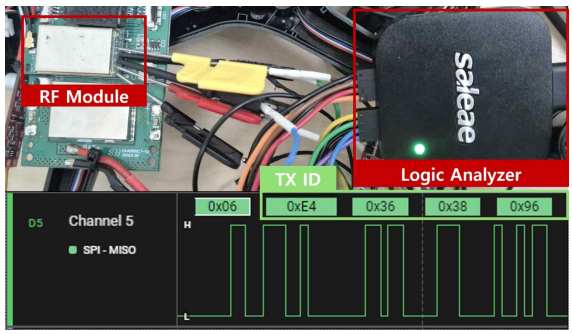


(그림 1) 4단계 무선 신호 분석 프레임워크

본 장에서는 드론의 무선 신호를 분석하기 (그림 1)과 같은 4단계 분석 프레임워크를 사용한다. 본 논문에서 사용된 드론은 재전송 공격에 취약한 기체이다. 무선 신호 분석을 위해서 HackRF One과 SPI 신호 분석을 위해서 Saleae 로직 분석기(Logic Analyzer v2.4.36)를 사용하여 분석을 수행한다.

3.1. SPI Sniffing & RF Monitoring

드론의 전원이 들어오면 마이크로컨트롤러(MCU)가 RF 모듈에 초기 레지스터 정보를 전달한다. 이 과정을 로직 분석기를 사용하여 SPI Bus 태핑을 통해 SPI 신호를 스니핑할 수 있다. (그림 2)은 로직 분석기를 사용해 RF 모듈의 SPI 데이터를 스니핑을 수행하고 TX ID 값을 추출한 결과이다.



(그림 2) RF 모듈의 SPI 스니핑 결과

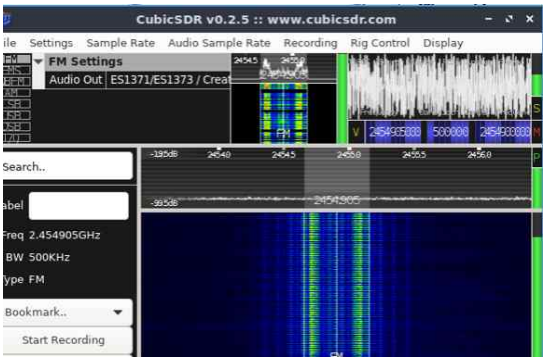
실험에서 수집한 레지스터 정보와 데이터시트를 기반으로 수집된 데이터 필드 내 값을 식별한다. [표 1]은 대상 드론의 RF 모듈 레지스터 정보를 정리한 결과이다.

[표 1] 레지스터 설정 테이블

Reg	Value	Description
0x18	0x62	주파수 대역폭을 500 khz로 고정
0x1F	0x07	TX ID를 4bytes로 고정, 데이터 화이트닝 암호화 및 CRC 비활성화
0x06	0xE4, 0x36, 0x38, 0x96	TX ID 4바이트 설정

SPI 통신 스니핑을 통해 드론 RF 모듈에서 설정된 TX ID 값인 “0xE4, 0x36, 0x38, 0x96”을 식별해낼 수 있다. 데이터시트에 따르면

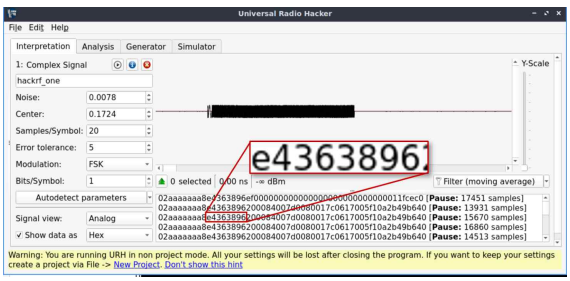
0x1F 주소의 레지스터가 0x07 경우라면, CRC, 암호화 기능은 비활성화되는 것으로 설명되어 있다. 또한 0x18 주소의 레지스터가 0x62일 때는, 주파수 대역폭은 500 khz이다.



(그림 3) CubicSDR: 주파수 스펙트럼 시각화

(그림 3)는 Cubic SDR을 사용하여 드론의 주파수 스펙트럼을 분석한 결과이다. 드론과 RC가 첫 바인딩 과정에서 주파수 채널을 설정하면, 다시 바인딩을 수행하기 전까지는 한 개의 채널만을 사용하여 통신을 수행한다. 실험에서 식별된 주파수 채널은 2.4549Ghz 대역이다.

3.2. RF 파라미터 식별 및 스니핑



(그림 4) URH(v2.9.8) 버전을 통한 신호 디코딩

아마추어 드론(FC)과 조종기(RC) 사이의 통신은 주로 FSK 변조 방식을 적용한다. 본 연구에서는 URH를 사용하여 RF 신호를 디지털 신호로 디코딩한다.

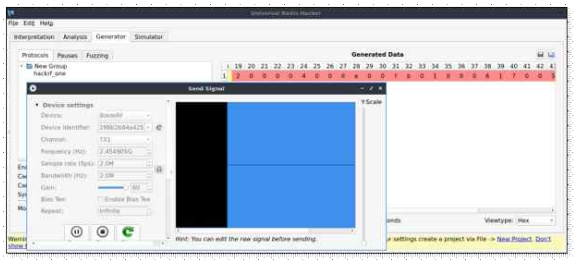
FSK 변조 신호를 정상적으로 디코딩하는 과정에서는 Samples/Symbol 및 Error tolerance과 같은 파라미터가 필요하다.

디코딩 과정에서 SPI 신호에서 추출한 TX ID를 KEY로 사용하여 해당 TX ID가 올바르게 디코딩될 때까지, 파라미터를 변경하였다. 최종적으로, (그림 4)와 같이 SPI 추출 TX ID 값이 디코딩 TX ID인 FSK 파라미터를 식별하였다.

본 연구에서는 (그림 5)와 같이 각각의 프로토콜 구조에 대해서 분석을 수행한다. Preamble 필드는 송신 신호의 시작을 알리는 부분이다. TX ID 값은 송신기 신호를 식별하기 위한 동기화 값이다. Payload는 데이터 전송 시 사용되는 순수한 데이터 부분으로 명령과 응답이 포함된다. 마지막으로 CRC-16 Spi-fujitsu 알고리즘을 적용하여 2바이트의 CRC 코드를 생성하고 있음을 식별할 수 있다.

3.3. 페이로드 식별

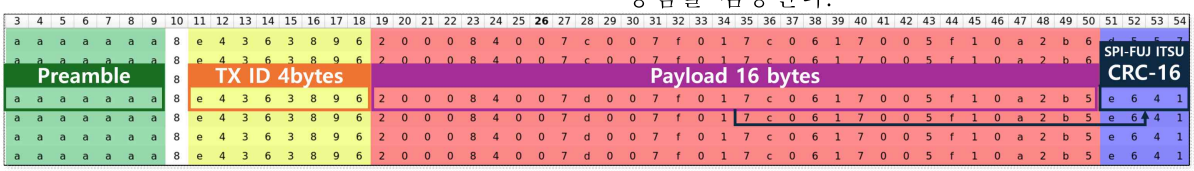
본 절에서 드론의 긴급 제동을 수행하는 페이로드를 식별하기 위해서 드론의 전원이 활성화된 상태에서 중복되지 않는 페이로드를 재전송하여 드론의 동작을 관찰한다.



(그림 6) URH를 통한 디코딩된 신호 재전송

URH는 디코딩된 신호를 다시 RF 신호로 재전송하는 Generator 기능을 제공한다. (그림 6)처럼 Generator 기능 사용하여 각각의 페이로드를 하나씩 전송하고 드론의 동작을 관찰한다.

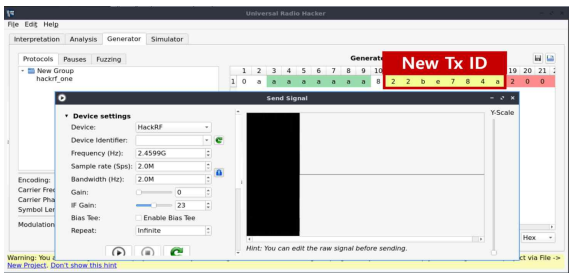
본 연구에서는 특정 페이로드가 드론의 모터를 비활성화 상태로 변경하는 것을 식별하고 해당 페이로드를 저장하는 데에 성공한다. 이를 통해 다음 절에서는 TX ID 값만을 변경하여 동일 기종 새로운 기체에 명령을 전달하여 반응함을 검증한다.



(그림 5) URH를 사용한 신호 디코딩 및 프로토콜 식별

3.4. URH를 통한 TX ID 변경 및 재전송

본 절에서는 동일 기종 새로운 기체에 대해서 식별된 패킷의 TX ID 값만 변경하여 전송할 수 있음을 보여준다. 이전 절에서 수행한 절차를 동일하게 반복하여 새로운 기체의 TX ID 및 주파수 채널을 식별한다. 그 결과 대상 기체의 새로운 TX ID 값은 “0x22 0xBE 0x78 0x4A”이며, 통신 채널은 2.4599Ghz을 사용한다.



(그림 7) URH Generator 기능을 통한 명령 재전송

이전 절에서 식별된 모터의 동작을 긴급 제동하는 페이로드에서 새로운 기체의 TX ID 값으로 교체한 뒤에 명령을 송신한다. (그림 7)은 실제 패킷의 TX ID 값을 교체하여 송신하는 그림이다. 그 결과 대상 드론은 비행 중, 변조된 패킷을 수신하고 긴급 제동하였으며, 대상 드론이 변조된 패킷에 취약함을 식별한다.

IV. 취약점 보호 전략 도출

대상 기체에서 식별된 무선 신호 취약점은 신호 도청, 위조, 재전송 공격 유형에 해당한다. 이러한 취약점은 각각의 보안 전략에 따라 보호 기술이 적용되어야 하며, 어떠한 단일 기법도 모든 문제점을 해결할 수 없다는 점(NO SILVER BULLET)을 인지해야 한다.

신호 도청 공격은 암호화되지 않은 신호의 내용을 가로채서 필드를 식별하고 위조 공격에 사용한다. 대응 전략으로 주파수 호핑 기술을 적용할 수 있다.

신호 위조 공격은 가로챈 신호에서 특정 필드 값을 변조하여 정상 신호인 것처럼 속이는 행위이며, 대응 전략으로 채널의 특성을 지속적으로 파악해 비정상 신호를 식별하는 것이다.

신호 재전송 공격은 녹음한 신호를 재전송하는 것이며, 대응 전략으로 시간 정보 또는 순서 번호를 추가할 수 있다.

본 연구에서 확보한 취약점은 위와 같은 대응 전략을 통하여 보호할 수 있으며, 따라서 본 연구의 연장선상에서는 대응 전략을 확보하는 과정이 포함된다.

V. 결론 및 향후 연구

본 연구에서는 실제 드론을 대상으로 무선 신호에서의 취약점을 식별하기 위한 4단계 프레임워크를 제안하였다. 제안한 프레임워크를 통하여 실제 드론을 대상으로 공격을 성공적으로 수행할 수 있다. 취약한 드론의 긴급 제동 명령을 식별하고 TX ID 값만을 변경하여 대상 드론에 명령을 삽입할 수 있으며, 실험 결과, 본 연구에서 생성한 무선 신호로 인해 드론의 모터 회전이 정지하는 것을 검증하였다. 향후 연구에서는 CRC 값과 페이로드 값을 임의로 변조하여 드론에 퍼징을 구현하고 다양한 취약점을 자동으로 식별하여 데이터베이스로 저장할 수 있는 자동화 프레임워크를 연구할 계획이다.

[참고문헌]

[1] M. Lee et al, “A Study on the Advancement of Intelligent Military Drones: Focusing on Reconnaissance Operations”, in IEEE Access, vol. 12, pp. 55964-55975, 2024.

[2] N. Schiller et al, “Drone Security and the Mysterious Case of DJI’s DroneID”, Network and Distributed System Security Symposium(NDSS), Jan, 2023.

[3] D. Pratama et al, “Behind The Wings: The Case of Reverse Engineering and Drone Hijacking in DJI Enhanced Wi-Fi Protocol”, 2024 International Conference on Platform Technology and Service (PlatCon), pp. 127-132, Aug, 2024.

[4] T. Omar et al, “SDR Based Replay Attack for Drone Intervention”, 2024 Wireless Telecommunications Symposium (WTS), Oakland, CA, USA, pp. 1-5, 2024.