드론 환경에서의 GPS 스푸핑 취약점 분석 및 실증: G 제품을 대상으로

홍세준[O], 고수완[*], 이경률[*]
[O]목포대학교 정보보호학과,
[*]목포대학교 정보보호학과
e-mail: {s193828[O], gpffh123[*]}@mokpo.ac.kr, carpedm@mnu.ac.kr[*]

Vulnerability Analysis and Demonstration of a GPS Spoofing Attack in Drone Environment: Based on Product G

Sejun Hong[O], Suwan Ko[*], Kyungroul Lee[*]
[O]Dept. of Information Security Engineering, Mokpo National University,
[*]Dept. of Information Security Engineering, Mokpo National University

● 요 약 ●

군사 목적으로 사용되던 드론이 일반 사용자를 위한 범용 드론으로 활용 분야가 확장됨에 따라, 국방 및 운송, 물류, 농업과 같은 다양한 분야에서 활용되는 실정이며, 이와 관련된 산업의 발전에 기여하고 있다. 그러나 급격한 발전으로 인하여, 드론의 안전성은 고려하지 못한 한계점이 존재하였고, 이는 드론에서의 다양한 보안위협으로 나타났다. 본 논문에서는 4차 산업 혁명 시대의 핵심 기술인 드론의 안전성을 향상시키기 위한 목적으로, 드론의 신규 취약점을 발굴하고 실증하였다. 실험을 위하여, 최근 출시된 G 제품을 대상으로, 드론에서 발생 가능한 다양한 취약점 중 하나인 GPS 스푸핑 공격을 시도하였으며, 실험 결과, GPS 좌표를 변조함으로써, 비행이 가능한 구역에서 비행 금지 구역으로 인식하도록 좌표를 조작하였으며, 비행 금지 구역으로 인식한 드론은 준비된 동작에 따라, 강제로 착륙시키거나 다른 장소로 이동시키는 것이 가능하다. 본 논문의 결과는 드론의 안전성을 향상시키기 위한 참고 자료로 활용될 것으로 사료된다.

키워드: 드론(drone), GPS 스푸핑(GPS spoofing), 취약점 분석(vulnerability analysis)

I. 서론

드론은 4차 산업 혁명 시대의 핵심 기술로 선정됨에 따라, 다양한 산업적 측면에서의 발전을 위한 연구가 지속적으로 진행되는 실정이다. 드론의 활용 분야를 살펴보면, 최근 러시아-우크라이나 전쟁에서 공격과 정찰을 위한 목적으로 드론이 활용되었으며[1], 국토교통부의 도심항공교통 산업의 일환으로 드론 택시[2]를 상용화할 계획이다. 이와 같이, 드론은 국방 및 운송, 물류, 농업과 같은 다양한 분야에서 활용되고 있으며, 기술적인 발전을 위한 많은 연구가 진행되고 있다.

그러나 이러한 드론의 급격한 발전에도 불구하고, 초기 드론 및 현재 개발되는 드론에 대한 안전성을 고려하지 못한 한계점이 존재하며, 이러한 한계점은 드론에서의 다양한 보안위협으로 나타났다. 따라서 본 논문에서는 4차 산업 혁명 시대의 핵심 기술인 드론의 안전성을 향상시키기 위한 목적으로, G 제품을 대상으로, 드론에서 발생 가능한 신규 취약점을 발굴하고 실증하였다.

II. GPS 스푸핑 공격 분석 및 실증

1. GPS 스푸핑 공격 분석

최근 발발한 러시아-우크라이나 전쟁의 국방 분야에서 드론의 보안과 관련하여, 사이버 보안에 대한 고려의 중요성이 대두되었으며, 이에 따라, 드론의 구성요소에 따른 보안 고려사항 및 관련 대응기술이 연구되고 있다. 이는 드론을 국방 분야에서 주된 전력으로 활용하기 위하여, 사이버 보안을 유지하여야 하며, 다양한 기술적 및 관리적 노력이 필요한 것으로 나타났다[3]. 그럼에도 불구하고, 드론에 내재된 취약점으로 인하여, 다양한 보안위협이 나타났으며, 본 논문에서는 GPS(Global Positioning System) 스푸핑 공격에 대한 취약점을 분석하였다.

GPS는 Global Positioning System의 약자로, 지구 주위를 회전하는 24개의 위성으로부터 수신하는 신호를 계산하여 좌표를 측정하는 시스템이다. 스푸핑은 "속인다"라는 뜻으로, 드론에서의 GPS 스푸핑 공격은 공격자가 드론에게 허위 GPS 신호를 전달함으로써 좌표를

조작하는 공격으로, 조작된 좌표를 수신한 드론은 자신의 위치를 오인하여 다른 장소로 인식하거나 위치에 따라 준비된 동작을 강제로 수행한다.

위치에 따른 준비 동작을 살펴보면, 공항과 같이 비행물체에 민감한 장소는 NFZ(No-Fly Zone)라고 불리는 비행 금지 구역으로 설정하고, 해당 위치에 드론이 접근하는 경우에는 강제로 착륙시키는 기능을 수행한다. 따라서, 드론에서 GPS 스푸핑 공격을 시도한다면, 그림 1과 같이, 공격자가 드론을 강제로 착륙시키는 것이 가능하다.

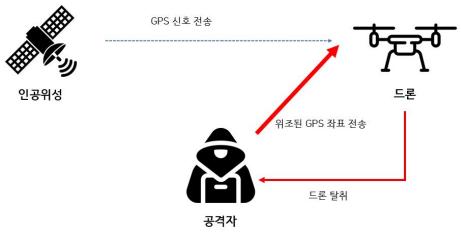

Fig. 1. GPS 스푸핑 공격 과정

2. GPS 스푸핑 공격 실증

상기한 것과 같이, 본 논문에서는 G 제품을 대상으로, 드론에서 발생 가능한 다양한 취약점 중, 본 논문에서 발굴한 신규 취약점인 GPS 스푸핑 공격을 실증하였다. 실험과정을 살펴보면, GPS 신호를 전달하기 위한 HackRF One 장비를 사용하였고, GPS 좌표를 조작하기 위하여 NASA(National Aeronautics and Space Administration)에서 제공하는 GPS 천체력 데이터를 준비하였다.

GPS 스푸핑 공격에 대한 결과를 시각적으로 확인할 수 있도록, No-Fly Zone 중 하나인 무안 국제공항의 위도와 경도에 해당하는 GPS 신호 파일을 생성하였고, 해당 신호를 HackRF One 장비를 통하여 드론으로 전달하였다.

실험 결과, 그림 2와 같이, 실내임에도 불구하고, 조종기의 지도에 표시된 드론의 위치는 No-Fly Zone인 무안 국제공항으로 표시된 것을 확인할 수 있다. 따라서, 비교적 최신에 출시된 G 제품에서 GPS 스푸핑 공격이 가능함을 실증하였고, 이 공격을 통하여 공격자는 의도하지 않은 곳으로 드론을 이동시키거나 착륙을 유도할 수 있을 것으로 판단된다. 만약 이러한 악의적인 행위를 통하여, 공격자가 물리적으로 드론을 탈취한다면, 드론에 저장된 민감한 정보를 탈취하는 추가적인 공격 또한 가능할 것으로 사료된다.

Fig. 2. GPS 스푸핑 공격 실증 결과

Ⅲ. 결론

본 논문은 드론의 다양한 제품들 중 하나인 G 제품을 대상으로, 신규 취약점인 GPS 스푸핑 공격을 분석하고 실증하였다. 실험결과, 실내임에도 불구하고 GPS 좌표가 성공적으로 조작되어 No-Fly Zone 중 하나인 무안 국제공항으로 표시된 것을 확인하였으며, 비교적 최근에 출시된 드론에서도 취약점을 내포한 것으로 나타났다.

본 논문에서 신규로 발굴한 취약점인 GPS 스푸핑 공격에 대응하기 위하여, IMU(Inertial Measurement Unit) 센서를 이용한 GPS 스푸핑 공격 탐지 방안이 연구되는 추세이며[4], 향후 추가적으로 발생 가능한 신규 취약점과 그 대응방안에 대한 연구를 진행할 예정이다.

ACKNOWLEDGEMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2021R1F1A1050542, NRF-2021R1A4A2001810).

REFERENCES

[1] 서강일, 김기원, 김종훈, 조상근, 박상혁, "우크라이나-러시아 전쟁에서 나타난 다영역 대드론체계 연구," 국방로봇학회 논문집, 제2권, 제1호, pp. 25-32, 2023년 1월.

[2] 오연경, 길기남, "드론 택시 비행안전성 확보 방안 연구," 한국항공우주학회 추계학술대회, pp. 929-932, 2019년 11월.

[3] 임준호, 신영아, 정경재, 정익래, "드론 전력화를 위한 필수과제 사이버보안," 한국방위산업진흥회 국방과 기술, 제532호, pp. 106-117, 2023년 6월.

[4] 이준오, 조진성, "드론의 IMU 센서를 이용한 GPS Spoofing 탐지 방안," 한국정보과학회 한국컴퓨터종합학술대회, pp. 2069-2071, 2021년 6월.