드론 환경에서의 GPS 스푸핑 공격 취약점 분석 및 실증: A 드론을 대상으로

이영재[O], 김진욱[*], 정원빈[*], 이경률[*]
[O]목포대학교 정보보호학과,
[*]목포대학교 정보보호학과
e-mail: {kronosyuki[O], wlsdnr0816[*], goblebin[*]}@mokpo.ac.kr, carpedm@mnu.ac.kr[*]

Vulnerability Analysis and Demonstration of a GPS Spoofing Attack: Based on Product A

Youngjae Lee[O], Jinwook Kim[*], Wonbin Jung[*], Kyungroul Lee[*]
[O]Dept. of Information Security Engineering, Mokpo National University,
[*]Dept. of Information Security Engineering, Mokpo National University

● 요 약 ●

군사 목적으로 개발된 드론은 최근 다양한 산업 및 민간 분야로 확대되고 있으며, 이러한 확대에 따라, 드론이 급격하게 발전하여, 농업이나 무인 드론 택배와 같은 산업 전반적으로 긍정적인 효과를 창출하는 추세이다. 그러나 이러한 발전에 반하여, 드론에 장착된 카메라를 통한 사생활 침해나 테러 목적으로 활용하는 것과 같은 부정적인 측면이 드러나기 시작하였다. 특히, 드론의 위치와 밀접한 연관이 있는 GPS와 관련하여, 무인 이동체의 특성상, GPS 신호에 의존하여 사용자에게 드론의 위치를 전달하지만, 이러한 GPS 신호를 송신하는 위성은 거리가 매우 멀리 위치하고, 이에 따라, 신호 세기가 비교적 약한 문제점을 가진다. 이와 같은 문제점을 악용하는 GPS 스푸핑 공격이 등장하였으며, 이 공격은 만약 공격자가 GPS 신호를 조작하여 송신한다면, 드론에 장착된 GPS 수신기는 조작된 GPS 위치를 수신하며, 이에 따라, 드론의 제어권을 탈취하거나 충돌 유발, 비정상적인 비행 경로 유도와 같은 문제점이 발생한다. 본 논문에서는 최신의 상용화된 드론을 대상으로, GPS 스푸핑 공격의 취약점을 분석하고 실증한다. 이를 위하여, 공격자가 비행 금지 구역에 해당하는 GPS 신호를 조작하는 것으로 공격을 시도하고, 이에 따른 드론에서 준비된 동작인 강제 착륙과 같은 비정상적인 행위를 유발하여, 드론의 임무 수행 능력을 제한하는 취약점을 분석하고 실험을 통하여 실증한다. 본 논문의 결과를 토대로, 최신 드론에서 발생 가능한 보안 위협을 도출함으로써, 드론의 안전성을 향상시키기 위한 자료로 활용될 수 있을 것으로 사료된다.

키워드: 드론(Drone), GPS 스푸핑(GPS Spoofing), 취약점(Vulnerability)

I. 서론

드론 시장이 급성장함에 따라, 군사 분야으로만 활용되었던 드론은 배선 선로 점검, 물류 배달, 기후 관측, 시험 감독과 같은 다양한 분야에서 활용되는 실정이며[1], 사람이 접근하기 어려운 환경인 범죄사고, 테러, 화재, 해양오염과 같은 극한 환경에서도 인적 피해 없이 광범위한 감시를 수행할 수 있다[2]. 이러한 드론의 발전은 산업적으로 매우 긍정적인 영향을 주지만, 드론 시장의 성장에 비하여 드론에 대한 보안 기술은 상대적으로 미흡한 실정이다. 드론에 대한 취약점으로는 GPS 스푸핑, WiFi 취약점, 하드코딩, 인증 해제와 같은 다양한 취약점이 존재하며[3], 특히, 드론의 위치와 밀접한 연관이 있는 GPS(Global Positioning System)와 관련하여, 드론은 기체에 장착된 GPS 수신기를 통하여 위성으로부터 자신의 위치를 파악하지만, 위성에서 송신하는 신호는 드론과의 거리가 멀어 신호 세기가 매우 약하다는 문제점이 존재한다. 이러한 문제점을 악용하는 GPS 스푸핑 공격이 등장하였으며, 이 공격은 공격자가 자신이 원하는 위치로 위조된 GPS 신호를 강하게 송신함으로써, 드론의 위치를 조작하는 것이 가능하다. 이러한 공격으로 인하여, 공격자는 드론에게 비정상적인 비행을 유도하거나 이를 통하여 물리적으로 드론을 탈취하는 것과 같은 취약점이 발생할 수 있다[4].

이러한 취약점을 기반으로, 본 논문에서는 드론의 안전성을 향상시키기 위한 목적으로, 공격자의 관점에서 최신의 상용 드론인 A 드론을 대상으로, GPS 스푸핑 공격에 대한 취약점을 분석하고 실증한다.

II. GPS 스푸핑 공격 취약점 분석 및 실증

1. GPS 스푸핑 공격 취약점 분석

본 절에서는 GPS 스푸핑 공격 취약점을 이해하기 위한 배경지식으로 GPS에 대하여 설명하고, GPS 스푸핑 공격의 원리에 대하여 서술한다. 이러한 배경지식을 기반으로, 본 논문의 분석 대상인 A 드론에서 발생하는 GPSS 스푸핑 공격 가능성을 분석한다.

GPS는 위성 수신 안테나를 통하여 3개 이상의 위성으로부터 신호를 수신한 후, 삼각법에 따라 거리를 측정함으로써, 현재의 위치를 파악하는 기술이다[5]. 여기에서 위치 정보를 포함하는 신호는 GPS 위성으로부터 전달받으며, GPS 위성은 지상으로부터 약 2만 km의 거리에 위치한다. 이러한 거리적 제약으로 인하여, 신호 세기가 매우 약하다는 특징을 가지며, GPS 스푸핑 공격은 이러한 특징을 악용함으로써 GPS 수신기에 위치 정보의 혼동을 유발시킨다.

GPS 스푸핑 공격 취약점을 분석하기 위한 공격 시나리오를 살펴보면, 우선, 공격자는 실제 GPS 위성 신호와 동일한 주파수와 프로토콜을 사용하는 거짓 GPS 신호를 생성하며, 생성된 거짓 GPS 신호를 드론으로 송신한다. 이 과정에서 드론은 위성과 공격자 모두로부터 GPS 신호를 수신하지만, 일반적으로 신호 세기가 강력한 신호를 위치로 인식한다. 이러한 특징에 따라, 공격자는 위성의 신호보다 더욱 강력한 거짓 GPS 신호를 송신하여야 하며, 공격자의 거짓 GPS 신호를 수신한 드론은 위치가 혼동되어 작동에 오류를 일으키거나, 위치 정보에 따라 정의된 특정 행동이나 임무를 수행하는 것과 같은 비정상적인 행위를 유발한다.

본 논문에서는 거짓 GPS 신호를 NFZ(No-Fly Zone)의 좌표로 지정함으로써, 위치에 따라 정의된 특정 행동이나 임무를 수행하는 비정상적인 행위를 유발하는 취약점을 분석한다. 여기에서 NFZ는 특정 지역에서의 비행 금지 구역을 의미하며, 이 구역은 보안이나 안전, 환경 보호와 같은 이유로 비행이 금지된 구역이다. 이에 따라, 만약 드론이 NFZ 좌표로 접근한다면, 비행이 금지된 구역으로 인식하여, 강제로 착륙하는 임무를 수행한다. 따라서, 만약 공격자가 드론을 탈취할 목적으로, 사용자와 거리가 멀어진 드론에게 NFZ의 좌표로 조작한 거짓 GPS 신호를 송신한다면, 드론은 강제로 착륙하며, 공격자는 물리적으로 드론을 탈취할 수 있다. 이와 같은 GPS 스푸핑 공격 시나리오를 그림 1에 나타내었다.

Fig. 1. GPS 스푸핑 공격 시나리오

2. GPS 스푸핑 공격 취약점 실증

그림 1에서 도출한 시나리오를 기반으로, GPS 스푸핑 공격을 실증하기 위하여, GPS 천체력 데이터를 활용하였고, HackRF One 장비를 사용하여 NFZ 좌표에 해당하는 GPS 신호를 생성하였으며, 생성된 GPS 신호를 송신하는 실험 환경을 구성하였다. 구성한 실험 환경을 토대로, GPS 스푸핑 공격 취약점을 실증한 결과를 그림 2에 나타내었다.

실험 결과, 드론에서 수신한 GPS 신호가 NFZ 구역으로 인식함으로써, “기체 체한 구역 진입”이라는 경고를 출력하며, “60초 내 자동 착륙” 경고 출력과 함께 드론이 강제로 착륙함을 실증하였다. 이러한 결과를 토대로, A 드론에서 GPS 스푸핑 공격이 성공함을 실험을 통하여 검증하였다. 이에 따라, 만약 공격자가 GPS 스푸핑 공격을 악용하여, 공격자가 원하는 위치로 드론을 강제로 이동시키거나 (RTH, Return To Home), 강제로 착륙시키는 것이 가능하며, 탈취한 드론에 저장된 데이터를 탈취하는 추가적인 공격이 가능할 것으로 판단된다.

Fig. 2. GPS 스푸핑 공격 실증 결과

III. 결론

과학 기술이 발전하면서 드론은 군사 목적뿐만 아니라, 다양한 분야에서 긍정적으로 활용되는 실정이다. 이러한 장점에 따라, 드론의 성장을 가속화시키고 있지만, 드론의 보안성을 제공하기 위한 보안 기술은 미흡한 실정이다. 본 논문에서는 드론의 안전성을 향상시키기 위한 목적으로, 공격자의 관점에서 최신의 상용 드론인 A 드론을 대상으로, GPS 스푸핑 공격에 대한 취약점을 분석하고 실증하였다.

취약점 분석 및 실증을 위하여, 정상 GPS 신호보다 강한 세기의 거짓 GPS 신호를 드론에 송신하는 공격 시나리오를 도출하였으며, 실험 결과, GPS 스푸핑 공격에 성공하여, 거짓 GPS 신호인 NFZ의 좌표를 수신한 드론이 강제로 착륙하는 결과를 실증하였다. 향후, 드론뿐만 아니라 GPS를 활용하는 다양한 응용 및 서비스에서의 GPS 스푸핑 공격을 방지하기 위하여, 정상적인 신호와 비정상적인 신호를 수집하여, GPS 스푸핑 공격을 방지하는 방안 및 안전성 평가를 위한 연구를 진행할 예정이다.

ACKNOWLEDGEMENT

이 성과는 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2021R1A4A2001810). 본 과제(결과물)는 2023년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다.(2021RIS-002, 1345370809)

REFERENCES

[1] S. Oh, "A Case Study Civilian Drone" Proceedings of the Korean Society of Broadcast Engineers Conference, pp. 315-318, Jul. 2015.

[2] S. Kim, "The Limitations and Opportunities of Police Activities Using Drones" Security Research, Journal of the Korea Security Science Association, pp. 111-140, 2017.

[3] M. Kim, I. You, and K. Yim, "Trends of Vulnerability Analysis and Countermeasure for Unmanned Aerial Vehicles" Review of the Korea Institute of Information Security and Cryptology, Vol. 30, No. 2, pp. 49-57, Apr. 2020.

[4] C. Choi, Y. Na, and K. Park, "A Study on Drone GPS attack types and countermeasures." Journal of the Korea Society of Information Technology Policy & Management, Vol. 15, No. 2, pp. 3245-3255, Jun. 2023.

[5] Korea Electrical Products Safety Association, "Principles of Global Positioning System(GPS)." Monthly Electrical Products ‘Safety 21’, Product Safety, Iss. 6, No. 150, pp. 62-65, Jun. 2006.