GPS-Spoofing을 이용한 Anti-Drone

권준우, 오형석, 서승현
한양대학교 에리카 전자공학부
kjw9628@hanyang.ac.kr, tjrguddh@hanyang.ac.kr, seosh77@hanyang.ac.kr

Anti-Drone System using GPS-Spoofing

Jun-Woo Kwon, Hyeong-Seok Oh, Seung-Hyun Seo
Division of Electrical Engineering, Hanyang University ERICA Campus

요 약

최근 무인이동체 기술과 IoT(사물인터넷)의 발전에 따라 드론에 대한 관심과 사용이 꾸준히 증가하고 있다. 드론은 취미용으로 사람들에게 재미를 주는 것에서 나아가 긴급서비스, 조기경보, 모니터링 등 이용되는 분야가 다양하고 사람들의 편의에 맞게 분야와 활용목적이 점점 늘어나고 있는 추세이다. 하지만 이에 따라 불법몰카나 드론을 사용한 테러 등 악의적으로 드론을 악용하는 사례 역시 빈번하게 발생하고 있다. 이를 예방하고 사전에 차단하기 위하여 본 논문에서는 주파수 송수신기인 Hack-RF One과 라즈베리파이, 안테나를 활용하여 Anti-Drone 시스템 프로토타입을 구현하였다.

1. 서론

드론은 생활속에서 많은 편의와 서비스를 제공하고 있다. 무인이동체 관련 기술과 IoT(사물인터넷)의 발전에 따라 실종자 수색, 고층빌딩 모니터링, 택배서비스, 재난 모니터링 등 드론을 이용한 서비스 역시 많이 증가하고 있다. 정부 역시 드론 산업 육성에 속도를 내면서 공공정책 분야에 드론의 활용도를 높이고 있다. 드론 산업은 항공, 정보통신기술(ICT), 소프트웨어 등 파생되는 관련 산업이 다양해 성장 잠재력이 크며, 드론 관련기술들이 발달함에 따라 2016년 700억원 규모에서 2019년 3천500억원의 시장규모가 형성된 상태이다.

그러나 사생활침해 문제(몰카)와 드론테러 등 드론을 불법적인 목적으로 사용하는 문제가 대두되고 있다. 예를 들면, 실제로 우리나라에서도 드론에 카메라를 장착하여 타인의 건물 내부 주거환경을 몰래 관찰하거나 공용 샤워장을 촬영하는 등 그 악용사례가 빈번하게 적발되고 있다. 뿐만 아니라, 해외에서는 드론을 이용하여 교도서 내부로 마약이나 휴대전화를 전달하거나 테러용으로 드론을 이용하는 등 각종 범죄에 드론이 악용되고 있다. 따라서 승인받지 않은 드론이 특정지역에 들어올 수 없게 하기 위해서 Anti-Drone 기술이 필요하다.

본 논문에서는 허가되지 않은 지역에 드론을 이용한 악의적이고 불법적인 행위나 드론테러 등의 공격에 대응하고자 한다. Rasberry Pi 3B+와 주파수 송수신기인 Hack-RF One, 안테나를 사용하여 불법 침입 드론의 GPS좌표를 교란시키는 기술인 GPS-Spoofing 기술을 구현하고 GPS-Spoofing 기술을 Anti-Drone에 접목시켜 Anti-Drone 시스템의 프로토타입을 구현하고자 하였다.

2. GPS-Spoofing 관련연구

본 논문의 Anti-Drone 시스템은 GPS-Spoofing 기술을 기반으로 한다. Spoofing 이란 승인을 받지 않은 사용자가 승인을 받은 사용자인 것처럼 위장하여 시스템에 접근하거나 네트워크상에서 허가된 주소로 가장하여 접근제어를 우회하는 공격행위이다.

GPS-Spoofing은 공격자가 공격대상의 GPS신호를 임의로 조작하여 원래 가고자 하는 목적지가 아닌, 공격자가 원하는 목적지로 가게 하는 것을 목표로 한다. 아직 GPS Spoofing에 대한 공격 가능성이 명확하지 않고, 경각심이 부족하기 때문에 대부분의 민간 시스템은 방어 메커니즘을 제대로 갖추고 있지 않다. 따라서 대부분의 민간 시스템이나 무인이동체

등은 GPS-Spoofing 공격에 노출되어 있다.

(그림 1) 은 GPS-Spoofing의 진행 단계이다. 첫 번째 단계는 GPS-Spoofing을 하기 위한 장치인 GPS-Spoofer를 구성하는 것이다. 두 번째 단계는 구성한 GPS-Spoofer를 통하여 공격대상의 GPS신호보다 더 강한 신호를 발생시켜 공격대상의 GPS신호를 takeover 시키는 단계이다. 세 번째 단계는 takeover된 공격대상의 GPS의 좌표를 교란하는 단계이다.

takeover는 앞서 구성한 GPS-Spoofer를 통하여 상대방의 GPS 수신기를 원래의 신호에서 거짓신호인 Spoofing신호로 바꾸는 것으로 시작된다. takeover 단계는 빠르고 강압적인 방법과 천천하고 은밀한 방법으로 나뉜다. 전자의 경우 공격자는 단순히 강한 거짓 신호를 전송해 공격대상이 위성을 추적하지 못하게 하고, 공격대상의 GPS 신호를 더 강한 Spoofing신호에 고정 시킨다. 이와는 대조적으로, 후자의 경우 원초적 신호와 거짓된 신호를 함께 공격대상에 전송하고 그 후에 점차적으로 거짓신호의 세기를 높여 원래의 신호를 Spoofing신호로 천천히 이동 시킨다. 후자방식의 장점은 수신된 신호강도에 비정상적인 점프를 일으키지 않기 때문에 높은 은밀성을 가진다. 그러나 은밀한 takeover를 위해서는 공격대상의 위치에서 원래 신호와 실시간으로 추적하고 동기화하기 위한 전문 하드웨어가 필요하다. 두 번째 단계인 takeover는 한번 수행되고 나면 또 다시 수행해야 할 필요가 없고, 다음 단계에도 영향을 미치지 않는다.

본 시스템에서는 침입 드론을 이용한 공격이나 테러 등을 감안하여 빠르게 침입 드론을 내보내야 하므로 전자의 방법인 빠르고 강압적인 takeover 방식을 사용한다.

(그림 1) GPS-Spoofing 단계.

3. 제안하는 Anti-Drone 시스템

우리가 제안하는 Anti-Drone 시스템은 경찰드론과 GCS(Ground Control System)로 구성되어 있다. 경찰드론은 GPS-Spoofing 장치인 GPS-Spoofer를 직접 장착한 드론을 칭한다. 예를 들어, 허가받지 않은 드론이 특정지역을 침입할 경우 GCS는 침입한 드론의 현재 좌표데이터를 이용하여 침입한 드론을 어디로 내보낼 것인지에 대한 좌표를 계산한다. 계산된 좌표는 GPS-Spoofer에 등록되고 경찰드론이 출격하여 침입한 드론을 특정지역 밖으로 내보내게 된다. (그림 2)는 GCS와 경찰드론의 역할이다.

(그림 2) GCS와 경찰드론의 역할.

3-1. GPS-Spoofer

(그림 3) GPS-Spoofer 구성.

우리는 주파수 송수신기인 Hack-RF One, Rasberry Pi 3B+, 안테나, 무선충전기를 이용하여 (그림3)의 GPS-Spoofer를 제작하였다. Raspberry Pi를 통하여 Hack-RF One을 제어함으로써 GPS 위치 정보를 입력할 수 있다.

3-2. GPS-Spoofing 지도를 통한 좌표파악

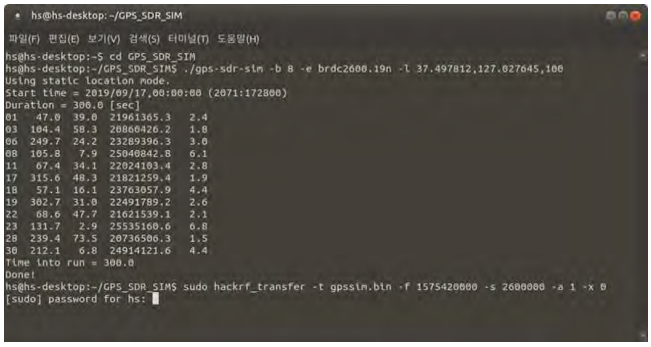
우리는 GCS를 통한 Anti-Drone 시스템 컨트롤을 보다 쉽게 표현하기 위해 Java Eclipse와 Kakao API를 사용하여 GPS-Spoofing 지도를 구현하였다.

(그림4)의 파란색 사각형 부분은 본 시스템의 GCS가 관리하고 있는 영역이다. 만약 허가되지 않은 드론이 파란색 부분의 영역을 침입하게 되면 빨간색 마커로 침입 드론의 경로와 위도, 경도 좌표데이터가 표시된다. 표시된 위도, 경도 좌표데이터를 이용하여 GCS에서는 침입한 드론을 어디로 내보낼 것인지에 대한 Spoofing좌표를 계산한다.

(그림 4) GPS-Spoofing 지도.

3-3. 공격대상의 GPS 좌표 교란

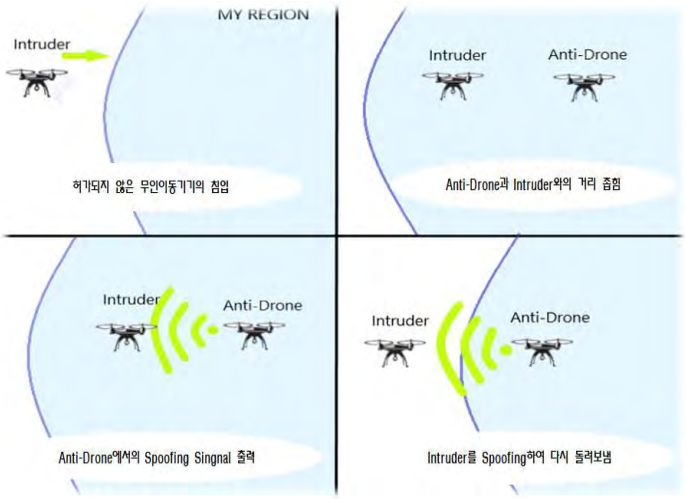
3-2 과정에서 계산된 Spoofing 좌표는 경찰드론이 장착한 GPS-Spoofer의 주파수 송수신기인 Hack-RF One에 등록된다. GPS-Spoofer를 장착한 경찰드론은 침입한 드론에게 다가가 거짓 GPS좌표 데이터 신호를 발사하여 침입한 드론을 특정지역 밖으로 내보낸다. (그림 5)는 Hack-RF One에서 거짓 신호가 발사되는 것을 라즈베리 파이를 통하여 받아보고 있는 것이다.



(그림 5) GPS-Spoofing 신호.

4. Anti-Drone 시스템 작동 시나리오

특정지역으로 허가받지 않은 드론이 침입하게 되면 GCS는 침입한 드론의 경도, 위도 좌표데이터를 수집하게 된다. 앞서 수집된 좌표데이터를 바탕으로 GCS는 침입한 드론을 어디로 내보낼 것인지에 대한 좌표를 계산하게 된다. 계산된 좌표데이터는 경찰드론이 장착한 GPS-Spoofer의 Hack-RF One에 등록이 된다. 출동한 경찰드론은 침입드론에게 다가가 거짓 좌표데이터 신호를 발사시켜 침입한 드론을 takeover 시킨다. takeover 된 침입드론은 특정지역을 벗어나 거짓 좌표데이터의 지역으로 이동하게 된다.



(그림 6) Anti-Drone 과정.

5. 결론 및 향후연구

본 논문에서는 최근 대두되고 있는 문제인 드론을 이용한 불법촬영(몰카)이나 테러공격 등 악의적으로 사용되는 드론을 사전에 차단하고 예방하고자 GPS신호를 교란시키는 기술인 GPS-Spoofing 기술을 이용하여 Anti-Drone 시스템 프로토타입을 제안하고 있다.

본 프로토타입은 크게 경찰드론과 GCS(Ground Control System)로 이루어져 있다. GCS가 관리하는 특정지역에 허가받지 않은 드론이 침입할 경우 GCS에게 침입한 드론의 현재 좌표데이터들이 전송되고, GCS는 이것을 바탕으로 침입한 드론을 어디로 내보낼 것인지에 대한 거짓 좌표를 계산한다. 계산된 거짓좌표를 경찰드론에게 전송된다. 경찰드론은 침입한 드론에게 거짓 GPS신호를 발사하여 침입한 드론을 특정지역 밖으로 내보낸다.

본 시스템은 비교적 쉽게 기본 하드웨어 장비들을 구입하여 구현해 볼 수 있다는 장점을 가지고 있다. 나아가 본 시스템을 실제 사람들이 사용하는 네비게이션이나 무인이동 자동차 등에도 적용해 볼 수 있을 것이라 예상된다.

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음" (IITP-2020-2018-0-01417)

참고문헌

[1] Zeng, K.1 et. al. “All Your GPS Are Belong To Us : Towards Stealthy Manipulation of Road Navigation Systems.” Proceedings of the 27th USENIX Security Symposium, pp1527-pp1544, 2018

[2] Eldosouky, AbdelRahman et. al. “Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing” I E E E Internet of Things Journal, 7권, 4호, pp2840~pp2854, 2020

[3] N Shijith, Prabaharan Poornachandran, V G Sujadevi, Meher Madhu Dharmana, “Spoofing technique to counterfeit the GPS receiver on a drone”, 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy), Kollam(India), 2017

[4] 공현철 외 3명, 픽스호크 드론의 정석, 한국, 성안당, 2019년