GPS 스니핑을 이용한 안티 드론 알고리즘

서진범 · 조한비 · 송영환 · 조영복*

대전대학교 정보보안학과

Anti-Drone Algorithm using GPS Sniffing

Jin-Beom Seo · Han-Bi Jo · Young-Hwan Song · Young-bok Cho*

Daejeon University

E-mail : seojinbeom@naver.com

요 약

최근 드론 기술이 발전함에 따라 드론을 이용한 악의적 공격이 문제가 되고 있고, 악의적 공격을 목적으로 한 공격 드론을 탐지하는 안티 드론 기술(Anti -Drone Technology)이 요구되고 있다. 그러나 현재 사용되는 드론 탐지 시스템은 고가이면서도 운영인력이 많이 필요하다는 문제점이 있다. 따라서 본 논문에서는 공격드론을 감시 정찰 가능한 안티드론에 대한 분석과 알고리즘을 이용한 안티드론 방식을 제안한다. 본 논문에서는 스니핑을 이용해 공격 드론을 파악하고 탐지한 후 현 GPS기반 탐지 시스템을 이용해 스푸핑을 통한 포획 및 탈취 알고리즘을 제안한다.

ABSTRACT

Recently, as the technology of drones develops, a malicious attack using a drones becomes a problem, and an anti-drone technology for detecting an attack dron for a malicious attack is required. However, currently used drone detection systems are expensive and require a lot of manpower. Therefore, in this paper, we propose an anti - drone method using the analysis and algorithms of the anti - drone that can monitor the attack drones. In this paper, we identify and detect attack drones using sniffing, and propose capture and deception algorithm through spoofing using current GPS based detection system.

키워드

안티 드론, 스니핑, 스푸핑, GPS

Ⅰ. 서 론

2000년대부터 무인비행체(드론)가 발전함에 따라 조작의 편의성과 경제성 측면에서 다양한 분야로 드론의 활용도가 높아졌다. 드론은 방송 영화 촬영, 사람의 접근이 어려운 산업 현장의 진단을 위한 촬영, 측량, 재난, 재해, 구호 등 다양한 산업에 활용되고 있다. 드론을 이용한 무분별한 촬영으로 사생활을 침해하는 사건과 개인이나 단체에 의한 특정 인사나 장소를 표적으로 하여 화학물질, 방사선 물질 및 소형폭탄 운반 등 테러에 준하는 위협 등 악용하는 사례도 점점 늘어나고 있다. 특히 드론은 열 발산이 적고, 소음이 낮으며, 반사도가 낮은 재료로 제작되기 때문에 기존의 일반적인 센서 운용만으로는 드론의 탐지, 식별이 어렵다고 알려져 있다[1]. 공격 드론을 방호하는 방법으로는 레이더, 음향, RF탐지 센서가 있는데 레이더 탐지의 경우 극초단파 수준의 전자기파를 물체에 발사시켜 그 물체에서 반사되는 전자기파를 수신해 물체의 거리, 방향 등을 알아내는 무선 감시 장치이며 실시간 목표물이 추적이 불가능한 단점이 있다. 음향 탐지 기법은 공중에 있는 표적에 음파를 방사하여 되돌아오는 정보를 수신, 표적에 대한 방위나 거리 등의 표적 정보를 산출하는 탐지 기법이다. 가격측면에서의 단점과 주변 소음 공해가 있다면 사용하기 어려운 단점이 있다. RF탐지 기법은 통신자와 통신기기 즉 드론간의 통신링크를 가로채 통신사이의 위치, 고도, 위도 정보를 얻어 송신하는 기술이다. 이 기술은 전반적인 부분 즉 국토전

* corresponding author

체를 탐지하기 어려울 뿐만 아니라 탐지 거리의 제한에 따른 단점이 있다[2]. 이에 따라 탐지한 공격 드론들을 무력화하는 기술도 존재하는데, 크게 하드킬(hard kill)과 소프트킬(Soft kill)로 구분된다. 산탄총, 레이저를 통해 드론을 파괴하는 하드킬은 파괴된 드론이 산불피해를 발생 시킬 수도 있다. 최근 강원지방의 산불에 의한 피해가 곳곳에서 발생하고 국민들의 산불예방의식과 안전의식에 대한 경각심이 커져가고 있는 가운데, 물리적 드론의 격추로 낙하하는 드론에 대한 대비책이 없다면 산불, 인명, 재산 피해 등 2차적 손실도 야기하게 된다. 고속으로 비행하는 비행체를 맞추는 단점 또한 제기되었다. 이에 대비되어 목표 드론에 물리적 공격을 가하지 않고 무력화시키는 소프트 킬이 나오게 되었다. 전파교란식 무력화 기술인 드론 제머건(Drone Jemmer Gun)이 개발되었다. 2차 피해를 획기적으로 줄이며 400m밖의 드론도 안정적으로 저격하여 안전하게 착륙 시킬 수 있다는 장점이 있지만, 전 세계적으로 전파교란 시스템은 불법으로, 주변 장비에도 해를 끼칠 수 있다는 단점이 있다. 물리적 기술 중에서도 드론은 격추, 파손 시켜 시스템을 멈추는 기술을 배제한 드론에 장착된 그물망 혹은 지상에서 발사하는 그물망을 이용해 포획하는 기술도 활용되고 있다.

본 논문에서는 GPS에서 받아오는 데이터를 분류하고 GPS자료를 시각화 하여 구글맵을 이용해 확인하고 위치를 파악한다. 파악된 위치를 기반으로 국지적 방위 시스템에 대한 드론 탐지 및 안티 드론으로 동작할 수 있도록 알고리즘을 제안한다.

II. 관련연구

2.1 드론

드론이란 통상적으로 UAV를 의미하며 20세기 초부터 미국에서 군사적 목적으로 개발 하였다. 크기, 비행 반경, 목적에 따라 드론이 분류되며 대표적으로 민간 부분에서 조난자를 찾기 위한 숲속 자율비행 AI 드론이 있다[3].

그림 1. 숲속 자율비행 AI 드론

드론 무력화 기술로는 소프트킬(Soft kill)과 하드킬(hard kill)로 구분한다. 소프트 킬 방식은가 전자적으로 드론을 무력화 하는 것으로, 드론의 라디오 통신 및 GPS 항행을 교란하는 전파교란(Jamming) 방식과 드론의 항법 소프트웨어에 비행금지구역을 설정하여 특정구역으로 비행하지 못하도록 강제하는 소프트웨어 접근방지 기술(Geo-fencing) 그리고 조종자의 조종신호를 받아 비행중인 드론의 GPS 신호에 허수를 강제하여 실제 GPS위치가 아닌 제3의 지역으로 강제 착륙하게 하는 통제권 강탈(Spoofing)등이 있다. 또한 하드킬의 경우 레이저빔, 무력화용 탄두, 산탄총, 포획용 그물포 등으로 직접적으로 요격 및 포획 하는 방식을 사용하고 있다. 그러나 소프트킬의 경우 법률적 문제나 소프트웨어적 해킹의 위험이 발생할수 있다는 단점을 가지고 있고 하드킬의 경우 타격된 드론의 파손으로 인해 수직 낙하하는 경우 지상에 2차적 피해가 발생할 수 있다는 문제점을 갖는다.

2.2 GPS 기술

미국방부에서 미사일 유도를 위해 1978년경부터 구축한 군사적 목적의 통신체계인 GPS는 모두 24개의 인공위성에서 발신하는 전파(마이크로파)를 수신자의 수신기에서 수신하여 수신기의 위치를 추정한다[4]. GPS의 위치 추정 오차율은 군사용이 3m, 민간용은 15m이다. 오차의 원인은 GPS 위성에서 고의적으로 삽입한 노이즈, 위성에서 지상사이의 전리층, 대기, 기상 상황에 따른 굴절, 지상에서의 반사 및 간섭, 수신기의 노이즈 등이다. 기본적으로 위치 측정 은 GPS 수신기의 삼각 측량법에 의해 이뤄지고, 시각 오차보정 등의 목적으로 보통 네 개 이상의 인공위성이 보내오는 정보를 모아 정확한 시간과 거리를 측정하여 위치를 계산한다. GPS 수신기와 GPS 위성간의 거리에 대한 추정은 식(1)과 같이 표현될 수 있다

$$PS_s = \sqrt{(x_s - x_u)^2 + (y_s - y_u)^2 + (z_s - z_u)^2} + c \times t_{error}$$

여기서 PS는 pseudo range, s는 위성의 위치, u는 사용자 수신기의 위치를 구분하기 위해 사용하였다. t_{error}는 수신기 클럭 오차로 인해 유도된 시간 오차를 나타낸다. 즉, 거리는 위성과 수신기 간의 물리적 거리와 시간 오차 동안 전파가 이동한 거리의 합으로 표현된다. 그러나 GPS는 거리에 따른 신호감쇠 현상이 발생되고 송신전력대비 수신 전력에 따라 로그함수를 취하며 10배를 한 dB값으로 나타내 송신기와 수신기 간의 거리의 함수 관계를 갖는다. [그림2]는 거리에 따른 GPS신호 감쇠 현상을 시뮬레이션 한 결과를 나타내고 있다.

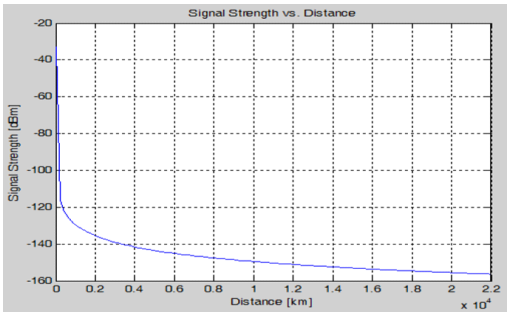

그림 2. 거리에 따른 신호 감쇠 현상

III. GPS기반의 스니핑을 이용한 공격 드론 방어 알고리즘

드론의 탐지 방식 중 RF(Radio Frequency)탐지 기법[5]은 통신자와 통신기기 즉 드론 간의 통신 스니핑, 또는 전파 링크를 가로채 통신 사이의 위치, 고도. 위도 정보를 빼 안테나가 설치되어 있는 기기에 직접 데이터를 송신하는 기술이다. 전반적인 부분을 탐지하기 어려울 뿐만 아니라 안테나의 설치 범위에 다른 탐지 거리의 제한에 따른 단점이 있다.

3.1. RF탐지 기법의 에어로스코프

[그림 4]의 에어로스코프(Aeroscope)는 드론과 조종기의 통신 링크를 가로채어 작동한다. 비행중인 드론의 모델명, 일련번호, 방향, 속도, 고도, 위도뿐만 아니라 조종사의 위치까지 알 수 있어 실시간으로 감시, 관제 할 수 있다. 공항 및 국가의 핵심적인 발전 시설 등 타격 받으면 위험한 장소에 배치하여 위험지역 또는 민감 지역을 비행하는 기체를 발견할시 실시간으로 위치를 표시해 주며 대응할 수 있는 기술이다. 또한 5Km까지 밖에 탐색이 불가능 하지만 어디든 방호지역을 옮길 수도 있다. 단점으로는 20,000$라는 값비싼 금액과 현재 민간에서 판매되는 드론 중 최고속도인 179.3마일(=288.6Km/h)로 주행하는 드론을 일반 승용차량으로는 따라가기 어렵다. 빠른 속도로 이동하는 드론을 추적 하려면 도로, 이동수단, 드론 포획 기술이 추가적으로 필요하다는 단점이 있다.

그림 3. Aeroscope1

3.2. 영상 탐지 기술

영상탐지는 일반·적외선 카메라를 융합하여 사용하며 카메라를 통해 수집된 영상에서 드론 외향이나 패턴을 인식하여 최대 150m의 거리에서 드론을 탐지한다. 장점으로 드론의 종류를 구별하는데 용이하나 단점으로 궂은 날씨에 취약하다. 또한 드론을 식별하기 기술은 주로 FMCW(Frequency Modulated Continuous Wave)를 기반 영상 구현이 만히 사용되고 있는데 움직이는 물체로부터 일정 시간동안 획득한 레이더 신호정보를 이용해 고해상도의 영상을 형성하는 기술로 레이다 영상압축 알고리즘인 RDA(Range Doppler Algorithm)를 기반으로 영상을 획득한다.

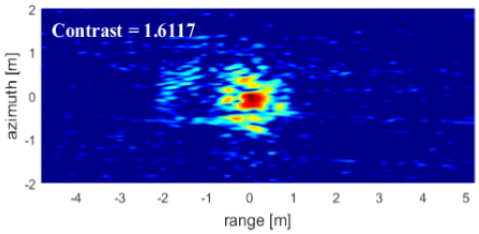

그림 4. 드론 영상획득

3.3 GPS기반의 스니핑을 이용한 공격 드론 방어 알고리즘

본 논문에서는 공격 기법인 스니핑(Sniffing), 스푸핑(Spoofing)을 이용하여 접근해오는 공격 드론을 2차적인 피해 없이 포획하는 방법을 제안 한다. 스니핑(또는 패킷 가로채기 공격)은 네트워크상에 떠돌아다니는 패킷이나 데이터 등을 훔쳐보는 것을 뜻하며, 스푸핑은 드론에게 잘못된 착륙지점의 GPS 신호를 보내어 드론이 해커가 의도한 곳에 착륙하게 해 납치하는 방법(시스템 권한 탈취)을 의미한다. 실제 사례로 2011년 12월 미국의 록히드마틴과 이스라엘이 공동으로 제작한 무인 스텔스 RQ-170는 이란을 영내를 정찰하다가 포획 당한 사건이 발생하기도 하였다.

미확인된 드론이 중요 지점에 들어오는 것은 드론에 내장된 비행불가지역 GPS를 받지 않고 오는 것이므로 공격 드론으로 가정하며 접근하는 공격 드론에 대해 스니핑 기법을 이용해서 공격 드론의 위치 정보(GPS 정보), 통신 정보를 취득한다. 이후 공격 기법중 하나인 스푸핑을 이용하여 공격 드론의 시스템 권한을 탈취한 후 특정 지역의 GPS를 주입하여 그 지역에 착륙을 유도하여 포획하고자 한다. [그림 5]는 드론 포획을 위한 순서도이다.

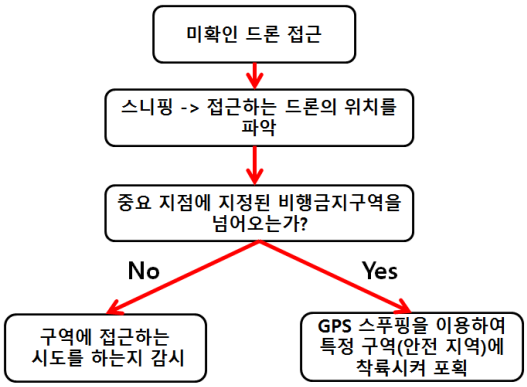

그림 5. 제안 개요도

[그림 5]와 같이 미확인 드론을 GPS를 이용해 접근 유무를 판단하고 경계지역을 넘어오는지 GPS 정보를 이용해 판별한다.

GPS Spoofing 공격을 위해 공유기 취약점을 탐색한다. 공유기 취약점 탐색을 위해 특정 코드를

Ⅳ. 결 론

드론 기술이 발전함에 따라 민간요소에도 다양한 분야로 원활하게 운용되고 있으나 드론의 무분별한 사용으로 악용하는 사례가 늘고 있다. 이를 보안하고자 안티 드론 기술이 전 세계적으로 중요시 되고 있으며 지속적으로 개발되고 있다. 이 시점에서 기존에는 값이 비싸고 복잡한 복합적인 레이더 탐지 시스템 및 거대한 탐지 안테나를 이용한 탐지가 주로 사용되었으나 본 논문은 공격 기법인 스니핑(Sniffing)과 스푸핑(Spoofing)을 이용하여 주요 지점에서 접근하는 드론을 탐지한다. 공격의 목적인 드론의 경우 스니핑 기법으로 접근 경로를 파악하고, 스푸핑을 이용하여 시스템 권한을 탈취한 후 특정 지역(안전 지역)의 GPS를 주입하여 그 지역에 착륙을 유도하여 착륙지점에 강제로 착륙시켜 포획 하는 알고리즘을 제시한다. 이에 따라 강제로 포획한 후 안전지대에서 파괴함으로써 2차적 피해를 방지하고 안전하게 공격 드론을 포획하여 공격 드론의 부가적인 정보(사용자 정보, 드론 기체 정보 등)를 얻을 수 있도록 한다.

References

[1] Edwin Vattapparamban, "Drones for smart cities : Issues in cybersecurity, privacy, and publsafety", International Wireless Communications and Movile Computing Conference(IWCMC), Sep. 2016.

[2] S.H Choi, J.S chae, J.H Cha, J.Y Ahn, "Recent R&D Trends of Anti-Drone Technologies", *Electronics and Telecommunications Trends*. Vol. 33, No. 3, pp. 78-88, June. 2018.

[3] S.C Jung, “A Study on the Security Control and the Image Tracking of a Drone to Apply Element Technologies of the 4th Industrial Revolution”, *PH.D Seoul National University of Science and Technology*, pp. 78-91, Aug. 2017.

[4] N. J. Heo, “근거리 GPS 재밍 공격 탐지 및 영향권 축소 기법”, *제어로봇시스템합동학술대회 논문집,* pp. 510-514, Jul. 2012

[5] H.R Choi, W.H Jeong, K.S Kim, "Efficient Drone Detection method using a Radio-Frequency", *Journal of Satellite, Information and Communications,* Vol.12, No.4, pp. 26-33, Dec. 2017.