SITL Simulator를 활용한 안티드론 개발

김명주○ 박하늘
경희대학교 컴퓨터공학과
mjoo1106@khu.ac.kr sksm2022@khu.ac.kr

Development of Anti Drone Using SITL Simulator

MyeongJu Kim○ HaNeul Park
School of Computer Science and Enginerring, Kyung Hee University

요 약

안티드론이란 드론으로 인한 불법적인 행위들을 예방하고 처단하기 위해 드론을 탐지하고 식별, 무력화하는 시스템을 일컫는다. 일반적으로 RF 센서나 광학 센서만을 사용하여 드론을 탐지 및 식별한다. 하지만 인공지능을 통해 드론을 식별함으로써 드론의 식별률을 비약적으로 상승시킬 수 있다. 또한, 무력화에 있어, 일반적으로 사용하는 hard kill이나 jamming 방식이 아닌 GPS spoofing을 통해 드론을 원하는 위치에 착륙시킴으로써 드론이 가지고 있는 정보와 제원을 확보할 수 있다 [1]. 본 논문에서는 광학 센서 기반의 드론 탐지 기술, 딥러닝 기반의 드론 식별 기술, 드론 무력화를 위한 GPS Spoofing 기술을 제안한다.

1. 서 론

군사적 훈련을 목적으로 개발되었던 드론이 이제는 다양한 민간분야에서 활용되고 있으며, 정부도 '무인 이동체 기술혁신과 성장 10개년 로드맵', '드론 활성화 지원 로드맵', '드론 산업 발전 기본계획('17~'26)'을 수립하여 추진하는 등 드론 산업 육성을 위하여 각종 지원을 아끼지 않고 있다.

단순한 취미나 레저 활동을 넘어서 방송, 공공행정 분야까지 여러 방면에서 활용이 되고 있으며, 아마존이나 보잉과 같은 세계적 기업은 다양한 영역에 드론을 활용하기 위해 첨단 기술을 동원하여 드론 산업을 육성하고 있다.

그러나 최근 드론의 급격한 확산에 따라 무단비행, 사생활 침해 등 불법적 활용을 통한 드론 범죄가 지속해서 증가하고 있다. 드론의 확산에 따라 미확인 드론을 탐지하고, 무력화하는 안티드론(Anti Drone) 산업의 필요성이 증가하고 있다.

본 논문에서는 실제 드론을 탐지 및 식별하고 무력화시키는 상황을 소프트웨어 환경에서 시뮬레이션해봄으로써 실제 상황에 대비할 수 있도록 한다. 이 논문은 딥러닝을 통해 드론 이미지를 학습하고 학습된 모델을 통하여 드론을 실제로 식별하는 것을 시연한다. 다음으로 드론의 GPS 정보를 임의로 조작한 GPS로 덮어씌워 드론을 원하는 위치에 착륙시킨다. 위 내용을 비바람이 강하거나, 장애물이 많은 환경 등 여러 악조건을 상정하여 gazebo를 통해 구현하고 시뮬레이션해봄으로써 실제 환경에서 이 논문이 가져올 수 있는 기대 효과들을 제시한다.

2. 관련 연구

2.1 ROS

ROS(Robot Operating System)는 오픈소스 기반 로봇 운영체제로 로봇 응용 프로그램을 개발할 때 필요한 하드웨어 추상화, 디바이스 제어, 프로세스 간의 메시지 패싱, 개발환경에 필요한 라이브러리와 다양한 개발 및 디버깅 도구를 제공한다 [2].

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학 사업의 연구결과로 수행되었음" (2017-0-00093)

본 연구는 ROS를 기반으로 안티드론을 개발한다.

2.2 PX4

PX4는 무인항공기의 원격조정 및 자율주행을 위해 설계된 소프트웨어로 NuttX 운영체제와 ROS를 기반으로 동작한다. NuttX는 임베디드 시스템의 플랫폼 중 하나로 RTOS(Real Time Operating System)로 개발되었다.

PX4 프로젝트는 QGroundControl 이라는 지상관제 프로그램과 드론키트라는 원격조정 어플리케이션의 오픈소스를 제공하고 있다.

2.3 QGroundControl

QGroundControl은 MAVLink 프로토콜을 지원하는 드론의 GCS(Ground Control System)이다. GCS는 지상 제어 시스템으로 지상에서 사용자가 드론의 비행 상태를 확인하고 제어할 수 있는 환경을 제공하는 관제 시스템이다 [3]. 이외에도 QGroundControl은 PX4의 펌웨어 업로드, Planning, Flying Missions 기능을 통한 자동 비행, 드론에 장착된 카메라의 실시간 스트리밍 등의 기능을 사용자에게 제공한다.

2.4 Gazebo

Gazebo는 MAVLink 프로토콜을 지원하는 멀티로터 유형의 가상 드론 시뮬레이터이다. 사용자는 드론 기기를 사용하지 않고 작성한 소프트웨어를 안전하게 테스트 및 디버깅할 수 있다. 또한, 다양한 물리 엔진과 센서, 높은 자유도를 제공하며 가상의 환경(World)을 직접 설계할 수 있다.

Gazebo에서 다양한 물건들을 배치하여 현실감 있는 드론 환경을 구축할 수 있다.

2.5 YOLO

객체 탐지란 미디어 내 대상이 되는 객체를 ROI(Region Of Interest)로 검출하고 올바른 클래스로 분류하는 것을 말한다. 널리 알려진 객체 탐지 기법의 하나인 YOLO는 one-shot detection 방식으로 정확도는 상대적으로 two-shot detection에 비해 낮은 모습을 보이지만 실시간으로 객체 검출을 주 목적으로 하는 무인항공기 탐지에는 YOLO가 적합하다는 것을 알 수 있다 [4].

2.6 탐지 및 식별

탐지 및 식별은 주로 센서를 이용한다. 첫 번째로 광학(LIDAR) 센서는 Pulse LASER가 물체에 반사되어 돌아오는 시간을 측정하여 물체의 위치를 측정하는 센서이다. 두 번째로 방향 탐지 센서는 무인 비행체의 조종 신호는 Industrial Scientific and Medical(ISM) 대역인 2.4GHz 대역과 5.8GHz 대역을 주로 사용하고 있다. 이 대역의 RF(Radio Frequency) 신호의 방향과 위치를 방향 탐지 센서로 이용해 조종자와 무인 비행체의 위치 추정이 가능하다. 세 번째로 레이더 센서는 스스로 에너지를 방상하는 센서로 특정 대역의 RF 신호를 송출하고 표적으로부터 반사되어 돌아오는 신호를 수신하여 표적을 탐지한다 [5].

2.7 무력화

무력화는 Hard kill, Soft kill로 구분하는데, Hard kill의 경우 드론을 식별 후 그물을 던지거나 지상에서 레이저빔을 보내는 것으로 무력화하는 방법이다. Soft kill의 경우 전파 교란(Jamming), 가상의 경계 구역(Geo fencing)을 만들어 출입을 제한하는 방법, 공격대상의 GPS 신호를 임의로 조작(GPS spoofing)하여 공격자가 원하는 목적지로 가게 하는 방법이 있다 [6].

3. 시나리오 제안 및 구현

본 장에서는 실제 드론을 탐지 및 식별하고 무력화하는 시나리오를 소개하고자 한다. 전체 시나리오는 LIDAR 센서를 활용하여 물체를 탐지 후 안티드론이 출동하여 식별한다. 만약 무인 비행체로 판단되면 바로 무력화 작업에 착수한다. 탐지의 경우 Simulator에서 제공하는 RF 센서를 활용했고 식별의 경우 딥러닝 기반의 YOLO v5를 활용했다. 그리고 GPS spoofing을 활용하여 무력화를 진행했다.

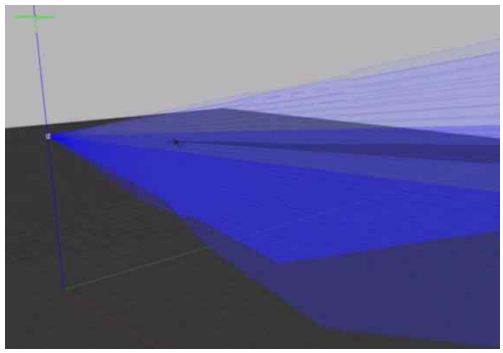
3.1 탐지

LIDAR 탐지는 직진성을 가진 광자로 물체를 탐지하는 기술로 정밀성이 매우 뛰어나다. LIDAR 센서는 물체의 위치를 탐지하는데 오차범위가 mm으로 작은 물체를 정확히 탐지할 수 있는 장점이 있다. 그러므로 비교적 크기가 작은 드론을 정확하게 탐지하는데 적합한 센서이다. RF 센서나 다른 센서들보다 가격이 비싸고 발열을 잡기 힘든 단점이 있지만, Simulator 상에서는 해당 사항이 없으므로 LIDAR 센서를 채택하여 진행했다.

```
<sensor type="ray" name="sensor">

  <!-- Position the ray sensor based on the specification. Also rotate
       it by 90 degrees around the X-axis so that the <horizontal> rays
       become vertical -->
  <pose>0 0 -0.004645 1.5707 0 0</pose>

  <!-- Enable visualization to see the rays in the GUI -->
  <visualize>true</visualize>


  <plugin name="scan" filename="libgazebo_ros_ray_sensor.so">
    <ros>
      <remapping>~/out:=scan</remapping>
    </ros>
    <output_type>sensor_msgs/LaserScan</output_type>
    <frame_name>lidar_link</frame_name>
  </plugin>
```

[그림 1] LIDAR.sdf

[그림 1]은 직접 제작한 LIDAR 센서 모델의 코드 일부이다. Gazebo에서 제공하는 ray 모듈을 사용하여 ray 센서를 구축하고 해당 센서에 ROS libgazebo_ros_ray_sensor 플러그인을 추가하여 탐지된 물체의 정보를 전달받을 수있도록 구현하였다. 해당 모델은 실제 LIDAR를 제작하는 회사인 'Velodyne Lidar' 사의 모델을 모방하여 제작하였다.



[그림 2] LIDAR 센서를 이용한 드론 탐지

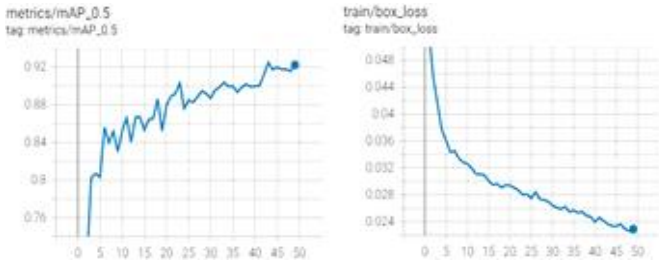
[그림 2]는 제작한 모델을 사용하여 Simulator 상에서 드론을 탐지하는 사진이다

3.2 식별

다양한 비행 물체 중 드론을 정확하게 식별하기 위해 인공지능을 사용하고자 한다. 본 시나리오에서는 'kaggle'을 통해 총 3,600개의 드론 이미지를 수집했고 [그림 3]과 같이 어두운 이미지의 경우 밝기 조절과 외곽선을 강조하는 보정 작업을 수행했다.

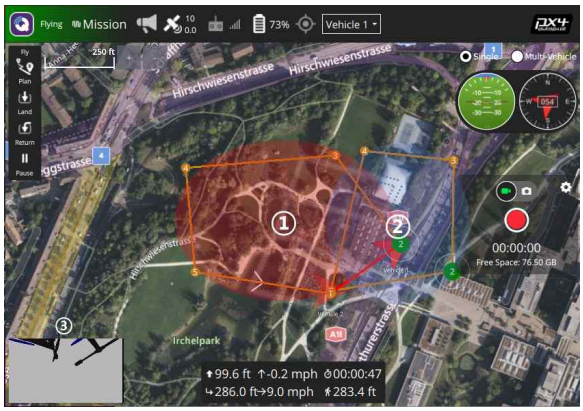
[그림 3] 이미지 작업 전후

YOLO v5로 학습을 진행하기 위해 수집한 이미지의 90%는 Train Set으로 10%는 Validation Set으로 구분했다. 그리고 설정 가능한 image size, batch size, epochs 각각을 416, 16, 50으로 지정하여 이미지 학습을 진행하였으며, 그 결과는 [그림 4]와 같다 [7].



[그림 4] 이미지 학습 결과(mAP, box_loss)

이미지 학습이 끝났으므로 Gazebo 환경에서 카메라가 장착된 안티드론(typhoon h480)을 생성했고 경계 구역을 설정했다. OGroundControl에서 안티드론은 경계 구역을 따라 순찰하도록 경로를 지정했고, 무인 비행체는 경계 구역의 근처로 비행하도록 경로를 설정했다.



[그림 5] QGroundControl 경로 설정

[그림 5]는 경계 구역 내에서 안티드론이 무인 비행체를 식별할 수 있는가 실험하기 위한 설정이다. ①은 안티드론의 경계 구역이고 ②는 무인 비행체의 경로이다. 그리고 ③은 video steaming으로, 안티드론의 head 방향의 영상 정보를 실시간으로 송출한다.

[그림 6] 실험 결과

[그림 6]의 결과를 바탕으로 경계 구역 내에서 무인 비행체를 성공적으로 식별하는 것을 확인할 수 있다.

3.3 무력화

GPS spoofing은 드론과 통신 중인 GCS보다 강한 신호를 만들어내 원하는 GPS 정보를 드론에 인식시킬 수 있다. simulator 상에서는 위성을 조작하는 등의 방법은 사용할 수 없어 무인 비행체에 직접 설계한 fake_gps 모듈을 삽입했다.

```
sensor_gps.alt = 0;
sensor_gps.alt_ellipsoid = 0;
sensor_gps.s_variance_m_s = 0.3740f;
sensor_gps.c_variance_rad = 0.6737f;
sensor_gps.heading = NAN;
sensor_gps.heading_offset = 0.0000;
```

[그림 7] fake_gps.cpp

[그림 7]은 직접 설계한 fake_gps 모듈이다. fake_gps의 작동 원리는 기존에 있던 gps 신호를 새로 주입한 fake gps로 변경하는 것이다. 이때 alt는 고도를 의미하고 s_variance_m_s, c_variance_rad은 각각 속도와 각도를 의미한다.

고도와 각도 값을 조정하여 드론을 땅으로 추락시키는데 목적이 있다.

[그림 8] 실험 결과

[그림 8]은 fake_gps 모듈을 삽입한 결과로 드론이 바닥으로 추락하고 관제 시스템과 연결이 종료되는 것을 확인할 수 있다.

4. 결론 및 향후 계획

본 논문에서는 드론 탐지 및 식별 그리고 무력화 시나리오를 제시하고 각 시나리오를 SITL Simulator를 통해 시각화함으로써 실제 상황에서 어떻게 안티드론 시스템이 작동하는지 설명하였다. 또한, 드론의 잠재적 취약성을 시사하고 이에 대응하기 위한 보안 연구의 필요성을 제시할 수 있다.

드론을 생산하는 기업이 다양하고 해마다 드론이 급변하고 있어 드론 외관을 확정하는데 어려움이 있고 컴퓨터 성능상 많은 데이터를 학습시키는 데 어려움이 있었다. 현재 학습모델은 천천히 움직이는 드론 인식률이 34프레임 중 31프레임 정도로 비교적 우수했지만 빠르게 움직이는 드론은 60%에 머물렀다. 더 다양한 기업의 드론 Dataset 을 구해 드론 식별률을 향상할 예정이다.

PX4 드론이 보안에 취약한 Mavlink protocol을 사용한다는 점을 활용하여 GPS spoofing을 구현해보았는데 향후 연구는 Mavlink의 보안 취약점에 대해 연구하고 개선 방안을 도출하고자 한다.

5. 참고문헌

[1] 학술연구정보서비스, ‘Development of ROS Based Indoor Autonomous Robot’, academic journal, 2017

[2] Mordor Intelligence, ‘ANTI-DRONE MARKET-GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS(2022-2027)’, Industry Reports, 2021.

[3] Dardoize Tristan, ‘Implementation of Ground Control System for Autonomous Multi-agents using QGroundControl’, Research, 2019

[4] 한국통신학회, ‘Implementation of Mobility Detection Model in Media using YOLO v3’, academic journal, 2022.

[5] 한국위성정보통신학회, ‘Efficient Drone Detection method using a Radio-Frequency’, K12 4-4, 2017

[6] 한국차세대컴퓨팅학회, ‘Patent Trend Analysis of Anti-Drone : Focusing on the Neutralization Means and Methods’, vol.16, no2, 2020

[7] 한국통신학회, ‘NRP-Sys: Nonlinear Regression Prediction System forYOLO-based Separation Detection of Identical Object’, 9 - 17, 2022.