

뉴스 기사의 크롤링을 통한 국내 기업의 안티 드론에 사용되는 기술 현황 분석

An Analysis on Anti-Drone Technology Trends of Domestic Companies Using News Crawling on the Web

김 규 석

한국폴리텍대학 분당융합기술교육원 데이터융합SW과

Kyuseok Kim

Professor, Department of Data Convergence SW, Bundang Convergence Technology Campus of Korea Polytechnics, Gyeonggi-do, 13590, Korea

[요 약]

드론은 관련 기술의 발달로 건설, 물류, 과학 연구, 촬영 등을 비롯하여 장난감까지 다양한 목적으로 보편화 되고 있다. 그러나 드론을 범죄나 테러 목적으로 사용하면서 이를 무력화 하는 Anti-drone 관련 기술의 연구, 개발도 활발히 진행되고 있는 상황이다. Anti-drone 기술의 범위는 탐지, 식별, 무력화로 구분할 수 있다. 드론을 무력화를 하는 방식은 전파 방해 등으로 탐지한 드론을 막는 소프트킬 방식이 있고, 물리적으로 파괴하는 하드킬 방식이 있다. 본 연구에서는 Anti-drone과 관련된 Google 및 Naver의 뉴스 기사를 Crawling 하였다. 국내 뉴스 기사를 분석하여 RF, GNSS, Radar 등의 기술을 찾았다. 이와 관련하여 해당 기술의 일반적인 특징과 사용 현황에 대하여 기술하였고, 각 기업 또는 기관의 Anti-drone에서의 적용 현황을 조사, 분석하였다.

[Abstract]

Drones are being spreaded for the purposes such as construction, logistics, scientific research, recording, toy and so on. However, anti-drone related technologies which make the opposite drones neutralized are also widely being researched and developed because some drones are being used for crime or terror. The range of anti-drone related technologies can be divided into detection, identification and neutralization. The drone neutralization methods are divided into Soft-kill one which blocks the detected drones using jamming and Hard-kill one which destroys the detected ones physically. In this paper, Google and Naver domestic news articles related to anti-drone were gathered. Analyzing the domestic news articles, 8 of related technologies using RF, GNSS, Radar and so on were found. Regarding as this, the general features and usage status of those technologies were described and those on anti-drone for each company and agency were gathered and analyzed.

Key word : Anti-drone, Drone, Jamming, Neutralization, News-crawling.

<https://doi.org/10.12673/jant.2020.24.6.458>



This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Received 23 November 2020; Revised 11 December 2020

Accepted (Publication) 21 December 2020 (30 December 2020)

*Corresponding Author, Kyuseok Kim

Tel: +82-31-696-8832

E-mail: kyuseokkim@kopo.ac.kr

I. 개념 및 배경

드론은 본래 군사적 목적으로 개발되었으나 이제는 건설, 물류, 과학 연구, 촬영 등을 비롯하여 장난감으로서도 활용되어 빠르게 보급되고 있다[1],[2]. 또한, 무인공중이동체(UAV : unmanned aerial vehicle)라고도 부르며, 4차 산업혁명 시대에 공공과 민간을 아울러 다양한 시장에서 영향력이 매우 큰 기술로 전망되고 있다[3]. 세계 드론 시장의 70%는 중국의 DJI가 점유하고 있으며, 여러 국가에서 드론의 연구, 개발은 활발히 진행되고 있다[3].

최근 민간 분야에서는 드론을 활용한 물류 서비스 분야에 적용을 준비하고 있다[3]. 2015년 미국의 Amazon은 드론을 활용한 택배 서비스의 시험을 선보였다[3]. 또한, 국내에서도 우정사업본부, CJ대한통운, 롯데택배 등도 드론을 활용한 물류 배송에 대한 연구, 개발을 진행 중이다[4]. 이렇게 드론은 4차 산업혁명 시대의 핵심 기술 중 하나로서 우리의 일상생활에도 긍정적인 효과를 주며 다가오고 있다.

그러나 이런 첨단 기술이 범죄나 테러에도 악용되고 있어 이와 관련된 규제와 기술 연구, 개발이 한창이다[2]. 실제로 드론을 이용한 범죄나 테러가 세계 곳곳에서 발생하고 있으며 뉴스 기사의 키워드 분석을 통해 ‘드론’과 ‘테러’와의 연결 중심성(degree centrality)이 0.8 이상이 될 정도로 높은 관련성이 있음을 알 수 있다[5].

이렇게 범죄나 테러에 악용되는 드론을 대응하는 플랫폼 개념의 안티 드론(anti-drone) 기술이 진화하고 그 시장이 폭발적으로 커지고 있다[2]. 안티 드론이 불법적으로 운행되는 상대 드론을 대응하는 과정은 탐지, 식별, 무력화로 나뉠 수 있다. 그 중에서 무력화를 하는 방식은 RF, GNSS 신호 등에 전파 교란(jamming)을 일으켜 불법 드론의 비행을 중지시키거나 작동 불가능시키는 소프트킬(soft-kill) 방식과 해당 드론을 물리적으로 파괴시키는 하드킬(hard-kill) 방식으로 나뉜다.

본 논문에서는 Google과 Naver에서 안티 드론 관련 국내 뉴스 기사를 크롤링하여 국내 기업의 안티 드론에 활용되는 기술과 적용된 제품이나 서비스들을 조사, 분석한다. 이러한 기술들의 일반적인 특징과 사용 현황 그리고 안티 드론에 활용했을 때의 특징들을 분석한다.

2장에서는 기존 논문들을 고찰하고, 3장에서는 안티 드론 기술과 관련된 용어에 대하여 기술하며, 4장에서는 본 연구의 데이터와 수집 방법을 기술하고, 5장에서는 수집된 데이터를 분석하며, 6장에서는 결론 및 추후 연구에 대하여 기술한다.

II. 문헌 고찰

기존 연구들은 안티 드론의 제품과 서비스 그리고 관련 특허들의 국내외 특허 출원 동향을 분석하였다. 또한, 몇 개 선별적인 제품이나 서비스에 관련하여 조사, 분석하는 내용들이었다.

한 연구에서는 드론 무력화 방법으로서 포획망, 전파 교란 관련 기술 등을 중심으로 특허를 조사, 분석하였다[2]. 또한, 다른 연구에서는 국내외 안티 드론 기술을 보유하거나 활용하는 기업, 기관의 제품, 서비스별 기술을 분석을 한 연구를 진행하였다[6].

본 연구에서는 Google과 Naver 뉴스에서 검색되는 안티 드론 관련 국내 뉴스를 크롤링하여 관련 기업, 기관을 나열하고 해당 시스템에 활용된 기술을 중점으로 분석하는데 목적이 있다. 해당 기술의 일반적인 특징과 사용 현황을 기술하며 해당 안티 드론 시스템에 적용된 내용을 조사, 분석하고자 한다.

III. 안티 드론 관련 현황 및 관련 용어 정의

3-1 안티 드론의 현황

2013년 독일의 한 행사에서 메르켈 총리의 몇 미터 앞으로 드론이 접근한 사건을 시작으로 국내에서도 2014년 과주, 백령도 등에서 북한 무인기가 발견되는 등 매년 국내외에서 드론 관련 테러가 발생하고 있다[5].

이와 관련하여 미국의 시장 조사기관인 Markets&Markets에 따르면, 2018년 4억 9900만 달러였던 안티 드론 시장이 2024년에는 22억 7600만 달러로 연평균 28.8% 성장할 것으로 전망하고 있다[7].

3-2 안티 드론의 개념

과거에 군사적 목적의 무인 항공으로 통칭되었던 드론은 UAV, RPAS (remotely piloted aircraft systems) 등 다양한 이름이 혼재했다[1]. 그에 따라 안티 드론이라는 용어도 anti-UAV, anti-UAS (anti-unmanned aircraft system) 등 다양한 용어가 혼재하고 있다[1]. 그러나 다양한 드론의 위협에 대응하는 일종의 공중 방어 플랫폼의 개념으로서 ‘테러나 범죄, 사생활 영역 침입이나 감시, 조작 미수에 의한 사고의 문제 등을 야기하는 나쁜 드론을 무력화하는 드론’으로 설명하는 것으로 ‘안티 드론’이라는 용어를 보편적으로 사용하고 있다[1].

표 1. 안티 드론의 행동 절차

Table 1. Procedures for actions of anti-drone.

	Role	Technology
Detection	Detecting drones in the specified area	Radar, RF, etc
Identification	Identifying a specific model of drones	RF, etc
Neutralization	Hard-kill, Soft-kill	Jamming, Spoofing, Physical destruction, Firing a net, etc

표 2. 안티 드론 관련 용어

Table 2. Terminology for anti-drone.

Terminology	Description
Anti-Drone Gun	A portable tool to destroy or immobilize a target drone
Jamming	Disrupting RF or GNSS signals
Spoofing	Sending fake GNSS signals to the target drone to land or return
Anti-Jamming	Cancelling the jamming signal

3-3 안티 드론의 행동 절차

안티 드론은 표 1에 기술된 것과 같이 상대 드론을 탐지 (detection), 식별(identification), 무력화(neutralization) 하는 절차를 거친다[6].

탐지 기술은 불법 드론에 대한 대응의 초기 단계로 특정 구역에 침입한 물체를 탐지하여 드론인지 여부를 판단하는 기술이다[8].

드론이 탐지되면 불법 드론인지의 여부를 식별하는 단계를 거친다. 이 단계에서는 드론의 ID를 무선 통신을 통해 송수신하여 신원을 파악하는 기술로 국내외에서 활발히 연구, 개발되고 있다[8].

마지막으로, 무력화 기술은 타켓팅한 드론에 대해서 침입이나 위협을 제거하는 기술이다[8].

3-4 안티 드론 관련 용어

안티 드론 관련해서 논문, 기사 등에서 자주 등장하는 용어를 표2와 같이 정리하였다.

3-5 안티 드론 시스템의 무력화 유형

안티 드론 시스템의 무력화 방법은 소프트킬(soft-kill) 방식과 하드킬(hard-kill) 방식으로 나눌 수 있다.

소프트킬의 방식은 RF, GNSS 등의 신호를 jamming 또는 spoofing 하여 무력화 시키고, 조종 통제권을 탈취하여 그 자리에 착륙시키거나 이륙 위치로 돌려보내기도 한다. 하드킬의 방식은 불법 드론 상공에 포획 그물망을 발사하여 드론을 무력화 시키기도 한다.

신호를 jamming 또는 spoofing 하는 소프트킬의 방식은 확실한 무력화 수단이 되기에는 기술의 발전이 필요하고, 포획 그물망을 발사하는 하드킬 방식은 사용할 수 있는 거리가 매우 짧고 다수의 비행체를 대응하기 어렵다는 단점이 있다.

IV. 연구 데이터 및 수집 방법

4-1 연구 데이터

본 연구에서 사용된 데이터는 기본적으로 Google에서 ‘안티드론’이라는 키워드로 검색된 국내 뉴스 기사이다. 1차적으로 해당 기사들이 일반 드론 관련 기사인지, 안티 드론 관련 기사인지에 따라 분류하였다. 그 후, 안티 드론 관련 기사에 대해서도 본 연구에서 조사, 분석할 국내 기업, 기관의 제품이나 서비스 관련인지, 일반적인 현황이나 법률과 관련된 것인지 구분하였다.

이렇게 모인 데이터를 정리하여 각 기업, 기관의 안티 드론 시스템에 대한 논문, 기사, 웹페이지 등의 정보를 활용하여 활용 기술 등의 상세 정보가 있는 것들을 조사, 분석하였다.

그 후 Naver에서 ‘안티드론’으로 뉴스 기사를 검색한다. 각 뉴스 기사의 내용에서 Google의 뉴스 기사를 통해 조사, 분석된 기업, 기관이나 관련이 있는 키워드들을 제외한 후 최종적으로 추가된 제품을 추가 조사, 분석하였다.

4-2 연구 데이터 수집 방법

본 연구에서 뉴스 기사를 수집하기 위하여 Python의 Selenium 모듈을 활용하였다[9]. 그림 1과 같이 1차적으로 Google News 검색창에 ‘안티드론’을 입력하여 검색된 뉴스의 URL을 모으는 방식으로 정리하였다.

뉴스 기사 URL을 열어서 국내 기업, 기관의 안티 드론 시스템의 내용을 포함하지 않은 제외하고, 포함된 기사는 논문, 기사, 웹페이지 등을 통해 기술 관련된 좀 더 자세한 내용을 검색한다.

2차적으로 그림 2와 같이 Naver news에서 뉴스 기사를 검색하였다. 앞의 과정과 같이 Python의 Selenium 모듈을 통해 URL을 수집하며 하나씩 접속하여 기사 본문의 내용도 수집을 한다. 기사 본문의 내용에 Google news를 통해 검색된 기업, 기관의 키워드가 포함되어 있거나 특정 관련 없는 내용이 포함되어 있다면 제거하는 방식으로 진행하였다.

마지막으로, Python을 통해 필터링 후 남은 뉴스 기사의 URL을 접속하여 국내 기업, 기관의 이름과 제품을 수집하고 추가 정보를 조사, 분석한다.

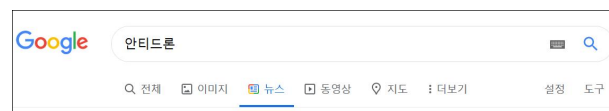


그림 1. 구글 뉴스 기사의 출처
Fig. 1. Source of news articles from Google[10].



그림 2. 네이버 뉴스 기사의 출처
Fig. 2. Source of news articles from Naver[11].

V. 데이터 분석 결과

5-1 Google news 수집 결과

Python을 통해 Google에서 수집된 ‘안티드론’ 관련 국내 뉴스 기사는 195건이었다. 이 중 155건은 그림 3과 같이 일반 드론, 안티 드론의 필요성, 관련 법률의 필요성, 기술 개발 현황 등의 내용이었고, 나머지 40건은 본 연구에서 조사, 분석하는데 필요한 안티 드론 제품 또는 서비스 관련 뉴스 기사였다.

5-2 Naver news 수집 결과

Python을 통해 Naver에서 수집된 ‘안티드론’ 관련 국내 뉴스 기사는 그림 4와 같이 610건이었다.

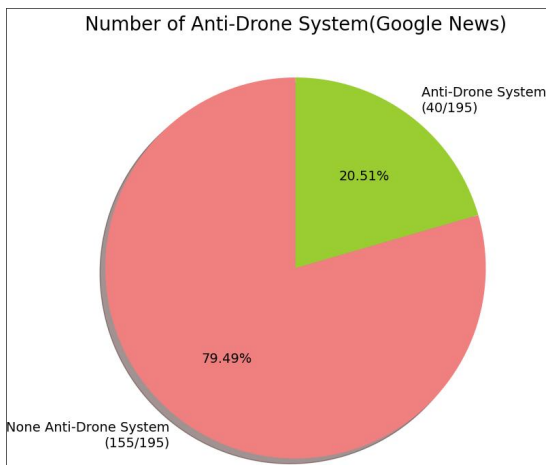


그림 3. 크롤링된 구글 뉴스에서의 안티 드론 시스템의 비율
Fig. 3. Proportion of anti-drone systems in crawled Google news.

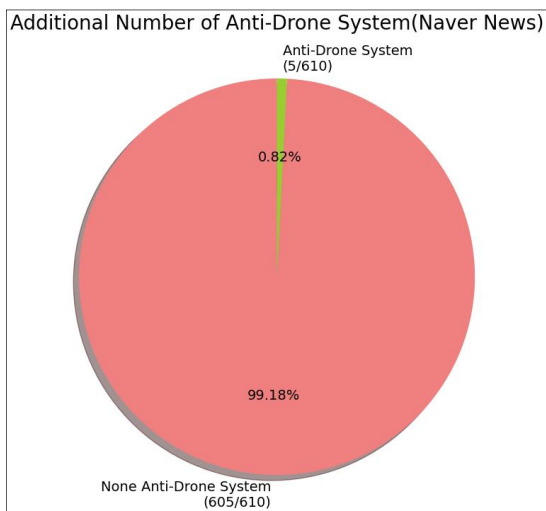


그림 4. 크롤링된 네이버 뉴스에서의 안티 드론 시스템의 비율
Fig. 4. Proportion of anti-drone systems in crawled Naver news.

이 중 Python을 통해 뉴스 기사를 하나씩 접속하여 앞 절에서 얻어진 안티 드론 시스템 그리고 제품에 해당하지 않는 키워드를 1차적으로 필터링 한 결과 173개의 뉴스 기사가 남았다. 추가적으로 하나씩 접속하여 수작업한 결과 그림 4와 같이 최종적으로 5건의 뉴스 기사가 남았다.

5-3 안티 드론 활용 기술

국내 기업, 기관의 안티 드론과 관련된 뉴스 기사 40건에서 언급된 관련 기술에 대하여 논문, 기사, 웹페이지 등을 조사하였다. 그 결과 표 3과 같이 8가지로 정리되었다.

레이다(radar)는 강한 전자파를 활용하여 그것이 물체를 맞고 되돌아오는 반사파를 분석함으로써 목표물과의 거리, 방향, 각도 및 속도를 측정할 수 있는 기술이다. 이는 항공기, 선박, 우주선, 자동차, 지형 등 다양한 물체 및 지형을 탐지하는데 사용되고 있다. 최근에는 기계학습 (machine learning) 기술까지 적용하여 신호에 대한 잡음, 간섭 신호 등을 제거하여 정확도가 높아지고 있다[12],[13]. 또한, 4차 산업혁명 시대에 레이더 기술은 안티 드론 뿐만 아니라 주변 물체를 탐지하는데 필요한 차량 자율주행 등에도 적용되어 활발히 연구, 개발되고 있다.

이동통신 네트워크인 4G, 5G는 대용량 데이터를 송수신 할 수 있으며, 기술이 발전할수록 지연시간도 매우 짧아지고 있다는 장점이 있다[14]. 이 이동통신 기술들은 휴대폰을 비롯하여 의료, 헬스케어, 물류, 스마트 팩토리 등 다양한 분야에 적용되고 있다. 또한, 최신 기술인 5G 네트워크의 국내 커버리지가 점점 넓어지고 있어 날로 활용 범위가 넓어지고 있다.

컴퓨터 비전(CV; computer vision) 기술은 인간의 시각이 할 수 있는 부분을 컴퓨터가 하는 것이다. 컴퓨터 비전 기술은 자

표 3. 국내 안티 드론에 적용된 기술

Table 3. Technology applied to domestic anti-drones.

	Feature
Radar	Detect an object using radio waves to determine the range, velocity and angle of the object
4G Network	Wide network coverage in Korea
5G Network	Limitedly Available in Korea and Faster than 4G Network
Computer Vision	Enable computers to see, identify and process images as human does
Radio Frequency	A frequency or band frequencies for telecommunications
GNSS (Global Navigation Satellite System)	Location measurement technology such as GPS, GLONASS and GALLIEO
EO/IR (Electro-Optical /Infrared)	Detect objects using both visible and infrared sensors
Sound Sensor	Detect the sound intensity of the object

동차 번호판 인식, 바코드 인식, 얼굴 인식 등 다양한 이미지를 인식, 분석, 처리 하는데 사용되어 왔다. 그리고 최근에는 컴퓨터 비전과 인공지능(AI; artificial intelligence) 기술이 결합되어 비오는 날이나 야간에도 인식이 높아지고 있다. 또한, 이 기술은 문자 인식, 생체 인식, 증강 현실, 제조 공정 등 이미지를 활용한 다양한 분야에서 활용되고 있다[15],[16].

무선 주파수(RF; radio frequency)란 방송, 통신 등 각종 무선기기의 데이터 송수신에 사용되는 기술이다. 주파수 대역에 따라 인가(licensed)/비인가(unlicensed)로 나뉜다. 이동통신 네트워크뿐만 아니라, Bluetooth, Wi-Fi, NFC 등을 비롯해 우리 생활 속에서 사용되고 있는 무선기기는 이 주파수의 범위 내에서 다른 다양한 기술로 사용되고 있다. 또한, 의료 분야에서 치료를 위해 저주파를 사용하고 있다[16].

GNSS(global navigation satellite system)는 일반적으로 GPS(global positioning system)이라고 불리는 기술을 통칭하는 용어이다. 美 국방부에서 개발, 운영하는 GNSS의 종류 중 하나를 GPS라고 부르며, 러시아는 GLONASS, EU는 GALILEO, 중국은 BEIDOU 등 전세계 국가별로 다양한 GNSS의 위성을 개발, 운영하고 있다[15]. GNSS는 항법, 측량, 지도 제작 등의 군용 및 민간용 목적으로 사용되고 있다. 일상 생활에서는 스마트폰, 자동차 네비게이션 등에서 길찾기, 현재 위치 찾기 등을 위해 사용되고 있다. 이러한 GNSS 수신기는 GNSS 위성으로부터 정보를 받으면, 해당 정보에 실린 데이터로부터 신호가 도달하는 시간차를 계산하여 위치를 측정하는 방식이다[16].

전기광학/적외선(EO; electro-optical / IR; infrared) 센서는 가시광선 영역과 적외선 열화상 영역의 영상정보를 활용하며, EO센서와 IR센서로 나뉜다[16]. EO센서는 레이더와 같이 전자기파를 활용하여 물체에 부딪혀 돌아오는 반사파를 탐지해 측정하는 것이다[17]. 레이더와의 차이점은 레이더는 적외선 이상의 전파를 사용하며 EO센서는 근적외선 및 가시광선을 사용한다는 차이점이 있다. IR센서는 적외선을 활용하여 움직임을 감지하는데 사용되는 기술이다[18].

음향센서(sound sensor)는 물체에서 발생하는 소리나 신호를 활용하여 물체를 탐지하는 기술이다[19]. 일반적으로 상대 물체의 특이성을 갖는 소리를 탐지하여 침입 여부를 탐지하는 것이다. 이 센서는 수중, 지상 등 군사용으로 많이 활용되고 있다[16]. 또한, 안티 드론 시스템에서는 드론이 동작할 때 프로펠러의 회전으로 인해 발생하는 특유의 소음을 감지하는데 사용하고 있다[16].

5-4 국내 기업, 기관의 안티 드론 시스템

국내 anti-drone 제품 또는 서비스를 연구, 개발하는 기업, 기관의 내용을 포함하는 Google의 뉴스 기사 40건 및 Naver의 뉴스 기사 5건을 조사, 분석하였다. 뉴스 기사 45건 중 중복된 것을 제외하면 16개의 기업, 기관이 정리되었다. 이 중 논문, 기사, 해당 기업이나 기관의 웹페이지 등을 통해 자세한 내용이 공개되지 않은 것을 제외하면 총 9개의 기업 또는 기관이 표 4

와 같이 정리되었다.

ADE의 'MAESTRO'는 불법 드론에 대해 선별적으로 타겟팅하며 GNSS, RF 기술을 사용하여 포착된 위치에 착륙을 시키거나 이륙 지점으로 돌려보낼 수 있는 안티 드론 건 형태의 휴대용 장비이다[20].

DGIST의 드론 탐지 레이더 시스템은 비지도 학습의 인공지능 기술을 micro Doppler 추출 기술에 접목하였다. 상대적으로 적은 데이터량으로도 3 km가량 떨어진 초소형 드론을 탐지할 수 있는 기술의 장비이다[21].

KAIST의 안티 드론 시스템은 드론의 형태로 감지된 불법 드론에 대해 GNSS 신호를 spoofing 함으로써 움직임 경로에 혼란을 준다[19]. 또한, DJI Phantom 3 Standard, DJI Phantom 4, Parrot Bebop 2, 3DR Solo 등 4가지 드론에 대하여 드론별 Hijacking 전략을 수립하였고 실험에 성공한 장비이다[22].

STX는 안티 드론 관련하여 탐지부터 포획까지 다양한 솔루션의 제품, 서비스를 보유하고 있으며 그 중 국내 제품인 고정 시스템 형태의 전파 교란 장비는 포착된 드론에 대하여 그 자리에 GNSS와 RF 기술을 사용하여 자동 착륙시키거나 이륙 지점으로 돌려보낼 수 있는 장비이다[23].

DABIN Systems의 'Ostrich'는 불법 드론과 드론제어기가 송, 수신하는 RF 신호를 감지하여 드론의 존재 여부를 감지하는 장비이다[24].

DYMSTEC의 'OURANOS'는 안티 드론을 탐지, 식별, 무력화 하는 종합 솔루션을 보유하고 있다. 'OURANOS'는 radar와 RF 기술을 활용하여 불법 드론을 탐지하고, EO/IR 카메라를 통해 식별한다. 또한, '드론 헌터 XR'이라는 장비는 안티 드론 건의 형태로 RF와 GNSS를 사용하여 신호를 jamming시켜 불법 드론을 무력화 시키는 장비이다[25].

표 4. 국내 안티 드론 제품 또는 서비스

Table 4. Domestic anti-drones product or service.

Maker	Role	Name	Applied Technology
ADE	Neutralization	MAESTRO	GNSS, RF
DGIST	Detection, Identification	-	Radar
KAIST	Neutralization	-	GNSS
STX	Neutralization	-	GNSS, RF
DABIN Systems	Detection	Ostrich	RF
DYMSTEC	Detection, Identification	OURANOS	RF, EO/IR, Radar
	Neutralization	HUNTER FD&FO, DRONE HUNTER XR	RF, GNSS
DUTA TECHNOLOGY	Neutralization	Wild CAT I Wild CAT II	GNSS, RF
sanjung solution	Detection, Identification, Neutralization	-	RF, GNSS
KCTS	Detection, Identification, Neutralization	MESMER	RF, GNSS

DUTA TECHNOLOGY의 'Wild CAT I', 'Wild CAT II'는 RF, GNSS 기술을 사용하며 불법 드론에 전파 교란을 일으켜 조종사가 보내는 신호를 잃게 만든다. 그 결과 불법 드론은 비행을 멈추고 그 자리에 착륙시키는 장비이다[26].

Samjung solution은 다양한 드론 탐지부터 포획까지 다양한 장비들을 보유하고 있다. 안티 드론 건 형태의 고정형, 차량형, 드론 탑재형 등 RF, GNSS 기술을 기반으로 한 장비들을 보유하고 있으며, GNSS의 항재밍 (anti-jamming) 성능을 시험할 수 있는 장비도 보유하고 있다[27].

KCTS의 'MESMER'는 RF, GNSS 기술을 활용하여 안티 드론을 탐지, 식별, 무력화 한다. 무력화 시, 드론의 제어권을 탈취하여 지정된 장소의 착륙 또는 강제 착륙을 시킬 수 있다. 또한, 이 시스템의 인터페이스는 안드로이드 기반의 소프트웨어를 통해 현황을 모니터링, 조작할 수 있는 장비이다[28].

VI. 결 론

군사적 목적으로 개발된 드론이 민간에서도 다양한 목적으로 보급되면서 범죄나 테러에도 악용되고 있다. 그에 따라 불법적으로 사용되는 드론을 대응할 안티 드론과 관련된 연구, 개발도 매우 중요한 부분으로 부각되고 있으며 그 시장도 급속히 커지고 있다.

본 연구는 Google과 Naver의 뉴스 크롤링을 통해 국내 기업, 기관에서 연구, 개발하고 있는 안티 드론 제품, 서비스에 대하여 조사, 분석하였다. Python의 Selenium 모듈을 통해 총 805건의 뉴스 기사를 수집하고, 일부는 모듈을 통한 필터링을 하여 정리하였다. 그 중 적용 기술 등의 세부 정보를 논문, 기사, 웹페이지 등에 공개된 기업, 기관은 9개였고, 이와 관련된 기술은 8건이었다.

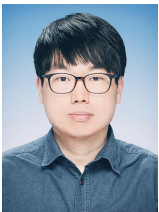
관련된 기술적인 정보를 찾을 수 있었던 KAIST, DGIST 등 2개의 대학과 ADE, STX, DABIN Systems, DYMSTEC, DUTA TECHNOLOGY, samjung solution, KCTS 등 7개의 기업의 안티 드론 시스템의 적용 기술을 조사, 분석하였다. 전반적으로 Jamming을 통한 안티 드론 무력화 시스템이 많았으며, GNSS와 RF 기술을 주로 사용하였다. 또한, 탐지 관련된 기술로는 Radar와 EO/IR 센서를 활용한 시스템들이 있었다.

현재까지의 안티 드론 기술은 다른 기술들에 비해 오래되지 않은 만큼 아직은 성숙단계에 이르지 못했다. 따라서, 관련 기술의 표준이나 정확도 관련 연구, 개발도 필요하다. 추후 안티 드론 관련된 기술의 시장이 점점 커지고 관련 연구, 개발 범위도 더 커지는 만큼 관련 자료들을 바탕으로 각 기술별 장단점과 정확도를 분석하는 연구를 진행할 수 있을 것이다.

References

- [1] D. H. Lee and W. Kang, "A study on the establishment of anti-drone concept and effective response system," *Korean Security Journal*, Vol. 60, pp. 9-31, Sept. 2019.
- [2] C. J. Park and K. Y. Kim, "Patent trend analysis of anti-drone : focusing on the neutralization means and methods," *The Journal of Korean Institute of Next Generation Computing*, Vol. 16, No. 2, pp. 7-17, Apr. 2020.
- [3] K. S. Han and H. Jung, "Trends in logistics delivery services using UAV," *Electronics and Telecommunications Trends*, Vol. 35, No. 1, pp. 71-79, Feb. 2020.
- [4] N. S. Park, [Issue] Drones, deliver mail in mountainous area...expecting commercialization [Internet]. Available: <https://www.koit.co.kr/news/articleView.html?idxno=73746>
- [5] J. Y. Park, "Anti-drone technology for protecting electric power facilities from bad drones," *The Korean Institute of Electrical Engineers*, Vol. 69, No. 4, pp. 15-20, Apr. 2020.
- [5] B. S. Jung, "Case analysis of drone terrorism and Its efficient countermeasures," *The Police Science Journal*, Vol. 14, No. 2, pp. 149-176, May 2019.
- [6] H. J. Lee, "Research of response for drone terrorism on military airfields," *Korean Terrorism Studies Review*, Vol. 13, No. 2, pp. 25-56, June 2020.
- [7] A. Meher, Anti-drone market worth \$2.4 billion by 2025 [Internet]. Available: <https://www.marketsandmarkets.com/PressReleases/anti-drone.asp>
- [8] K. M. Kang, J. C. Park, S. N. Choi, J. H. Oh and S. H. Hwang, "Trends in low altitude small drone identification technology and standardization," *Electronics and Telecommunication Trends*, Vol 34, No. 6, pp. 164-174, Dec. 2019.
- [9] PyPI. Python buildings for Selenium [Internet]. Available : <https://pypi.org/project/selenium/>
- [10] [Internet]. Available: <https://www.google.com>
- [11] [Internet]. Available: <https://www.naver.com>
- [12] S. J. Moon and H. K. Kim, "A precise location tracking systems with smart context-awareness based-on doppler radar sensors," *Journal of Institute of Control, Robotics and Systems*, Vol. 16, No. 12, pp. 1159-1166, Dec. 2010.
- [13] D. H. Kim, C. J. Bang, C. Y. Kim, S. W. Jeon and J. W. Kim, "Recent research trends of machine learning-based radar techniques," *The Journal of Korean Institute of Communication and Information Sciences*, Vol. 43, No. 8, pp. 1382-1385, Aug. 2018.
- [14] J. W. Shin and J. S. Shin, "5G mobile communication technology," *Robot and Human*, Vol. 16, No. 2, pp. 14 - 21, Apr. 2019.
- [15] E. T. Kim, C. W. Park, Y. S. Kim, S. W. Baik and S. B.

- Moon, "Vision based localization methods for indoor robots," *Communications of the Korean Institute of Information Scientists and Engineers*, Vol. 26, No. 4, pp. 12-21, Apr. 2008.
- [16] [Internet]. Available: <https://en.wikipedia.org/>
- [17] S. H. Choi, J. S. Chae, J. H. Cha and J. Y. Ahn, "Recent R&D trends of anti-drone technologies," *Electronics and Telecommunications Trends*, Vol.33, No. 3, pp. 78-88, June 2018.
- [18] J. B. Hong, M. S. Kang, Y. S. Kim, M. S. Kim and G. Y. Hong, "Experiment on automatic detection of airport debris (FOD) using EO/IR cameras and radar," *Journal of Advanced Navigation Technology*, Vol. 22, No. 6, pp. 522-529, Dec. 2018.
- [19] Y. K. Cho, J. Y. Jeong and E. S. Jang, "Development of sound source detection system using double microphones," in *Proceedings of the KISS Winter Conference*, Pyeongchang: Korea, Vol. 2018, No. 12, pp. 2050-2052, 2018.
- [20] Adeinc. Anti-drone [Internet]. Available: <http://www.adeinc.io>
- [21] I. Alnujaim, D. G. Oh and Y. W. Kim, "Generative adversarial networks for classification of micro-doppler signatures of human activity," *IEEE Geoscience and Remote Sensing Letters*, Vol. 17, No. 3, Mar. 2020.
- [22] J. H. Noh, Y. J. Kwon, Y. M. Son, H. C. Shin, D. H. Kim, J. Y. Choi and Y. D. Kim, "Tractor beam: safe-hijacking of consumer drones with adaptive GPS spoofing," *ACM Transactions on Privacy and Security*, Vol. 22, No. 2, pp. 1-26, Apr. 2019.
- [23] STX corporation. Anti drone business [Internet]. Available: <http://www.stx.co.kr/kor/Utility/drone.aspx>
- [24] DABIN systems. Products & services [Internet]. Available: <http://www.dabinsystems.com/pro/dron.htm>
- [25] DYMSTEC. Anti drone system [Internet]. Available: <http://www.dynamicshielding.com/anti-drone-2/anti-drone-system/>
- [26] DUTA technology. Product [Internet]. Available: http://www.duta-rnd.com/ko/duta_sub/products/item.php?it_id=1541492570
- [27] samjung solution. Anti drone equipment [Internet]. Available: <http://www.sjsolution.com/index.php>
- [28] Korea counter terrorism system Inc. Drone technology [Internet]. Available: http://korea-cts.com/web/home.php?go=Cmenu_05_03



김 규 석 (Kyuseok Kim)

2011년 2월 : 한국항공대학교 정보통신공학과 (공학사)
2019년 8월 : 아주대학교 정보통신대학원 정보통신공학과 (공학석사)
2019년 9월~현재 : 서울대학교 환경대학원 환경계획학과 박사과정
2011년 1월~2019년 6월 : LG전자(주) 선임연구원
2019년 7월~2020년 2월 : (주)LG유플러스 책임
2020년 2월~현재 : 한국폴리텍대학 분당융합기술교육원 데이터융합SW과 조교수
*관심분야 : ITS, UTM, 교통공학, IoT, 근거리 무선통신, 데이터 처리