International Journal of Internet, Broadcasting and Communication Vol.15 No.4 115-127 (2023)
http://dx.doi.org/10.7236/IJIBC.2023.15.4.115

IJIBC 23-4-13

Anti-Drone Technology for Drone Threat Response: Current Status and Future Directions

Jinwoo Jeong[‡], Isaac Sim[‡], Sangbom Yun, Junghyun Seo

LIG Nex1, Cyber EW R&D Group
Jinwoo.jeong@lignex1.com

Abstract

In this paper, we have undertaken a comprehensive investigation into the current state of anti-drone technology due to the increasing concerns and risks associated with the widespread use of drones. We carefully analyze anti-drone technology, dividing it into three crucial domains: detection, identification, and neutralization methods. This categorization enables us to delve into intricate technical details, highlighting the diverse techniques used to counter evolving drone threats. Additionally, we explore the legal and regulatory aspects of implementing anti-drone technology. Our research also envisions potential directions for advancing and evolving anti-drone tech to ensure its effectiveness in an ever-changing threat environment.

Keywords: *Anti-drone technology, Drone detection, Drone Identification, Drone neutralize*

1. Introduction

Anti-drone technology is a technology whose importance is growing due to the recent increase in the use of drones. Drones are used in a variety of fields, and are especially actively used in various areas such as industry, military, entertainment, and logistics.

First, the increased use of drones has important implications in terms of efficiency and productivity. Drones can automate and simplify tasks that previously required a lot of manpower or cost. Through this, work time and costs can be reduced, and manpower can be devoted to more strategic work. Drones can also perform tasks in potentially hazardous environments. This is very useful in that it allows work to be performed without endangering human life [1]. However, as the use of drones increases, drone-related threats and problems are also increasing. Drones can be difficult to fly and detect, and if used maliciously, they can cause a variety of problems, including invasion of privacy, threats to flight safety, industrial espionage, and military threats [2]. Accordingly, the importance of anti-drone technology is emerging, and it has become necessary to develop countermeasures and technical solutions for the safe operation of drones. Therefore, the latest anti-drone technology has the function of detecting and interfering with the flight of drones, thereby preventing and responding to threats related to drones [3]. The development of such anti-drone technology serves as a foundation for further expanding the usability of drones by strengthening the safety and security of the drone use environment.

This paper covers comprehensive concepts and development directions for the latest anti-drone technology. This paper is structured as follows.

Manuscript received: September. 5, 2023 / Revised: September. 10, 2023 / Accepted: September. 16, 2023
Corresponding Author: jinwoo.jeong@lignex1.com
Tel:+82-31-8038-0186, Fax: +82-70-8233-7007
Chief Research Engineer, Cyber EW R&D Group, LIG Nex1
‡ These authors contributed equally to this work.

Section 2 deals with the classification of anti-drone technology. It introduces major categories such as drone detection and tracking and drone response, and provides an overview of the technologies and algorithms corresponding to each category. Section 3 details drone detection, identification, and neutralization technology. Section 4 also examines the current status of drone-related legislation and future legal and institutional requirements. Finally, Section 5 concludes by looking at the technologies and development directions needed in the future.

2. Classification of Anti-Drone Technologies

Anti-drone technology is largely divided into three types: drone detection technology, identification technology, and neutralization technology [3]. First, drone detection technology is a technology that detects whether a flying object approaching a protected facility is a drone, and includes radar, Radio Frequency (RF) scanning, heat detection, and optical cameras. These technologies are used to detect the presence and determine the location of drones [4]. And drone identification technology is a technology that identifies enemies by identifying the type of aircraft detected as a drone, whether or not it is approved for flight, and the purpose of the flight, by determining whether the detected drone is a threat drone [5]. In order to determine the threat of a drone, the decision on whether or not to fly must be given priority, and the most basic method and procedure is direct identification with the naked eye. This is a method of applying to the relevant agency for approval for flying a drone and filming using a drone, then obtaining a drone registration number and attaching it directly to the drone. This is a method of identifying and post-processing the owner and coordinator in the event of a drone accident, and is not suitable as a preventative drone identification method. Meanwhile, there is a method to remotely identify the identification number of a drone flying within the drone's communication range using an active or passive method. This identification technology corresponds to the step of determining additional response to the detected drone, and determines whether it is a threat drone by checking the shape, size, flight behavior, and communication protocol of the drone. Recently, various technical standardization and legal regulations and devices such as Remote ID are being created overseas to identify drones.

Meanwhile, for drones identified as threats, technology is needed to neutralize them when necessary. Drone neutralization technology is largely divided into hard kill and soft kill methods, and uses anti-aircraft weapons or laser beams to intercept drones or block drone communication, thereby rendering the drone incapable of flight or out of control. This is used in situations where drones are clearly threatening [6]. Table 1 below shows the classification of anti-drone technology. This table categorizes Anti-Drone technology into three main domains. Firstly, in the 'Detection' category, various technologies for drone detection are emphasized. Secondly, the 'Identification' category discusses methods for distinguishing and categorizing detected drones. Lastly, the 'Neutralization' category describes technologies used to halt or control drones. This categorization aids in providing a clear understanding of the intricate facets of Anti-Drone technology and facilitates the organization of research findings.

Table 1. Classification of Anti-Drone Technologies

Classification	Main technology	Note
Drone detection	**Radar, RF scan, Heat detection, Optical camera**	Determine whether it is a drone or not
Drone identification	**Direct identification, Drone ID Identification**	Abnormalities identify
Drone neutralization	**Laser, RF gun, Net guns, anti-aircraft weapons, bird of prey**	Hard-Kill
	Jamming, Spoofing, takeover, Geo-fencing	Soft-Kill

In the next section, we look at specific technologies for detecting, identifying, and neutralizing drones.

3. Drone Detection, Identification, and Neutralization Technology

3.1 Drone Detection Technology

3.1.1 Radar

The most basic technique for drone detection is drone detection using radar.

Drones can be detected from a long distance using radar, allowing surveillance of a large area. It also has the advantage of being able to operate in a variety of environments without being affected by weather conditions. Additionally, the location of the drone can be accurately determined, enabling real-time tracking. However, radar visibility may be reduced depending on the size and speed of the drone. Additionally, installing and maintaining radar can be expensive. Additionally, radar has the disadvantage of being limited in distinguishing between types and uses of drones [7, 8]. Therefore, it is necessary to adjust the radar system according to the size, speed, wing structure, etc. of the drone. Recently, research is being conducted on improving accurate detection capabilities for small drones and at low altitudes through improvements in radar technology. Table 2 shows the Radar cross section (RCS) values of representative drone models [9]. As shown in Table 2, the RCS values in square meters represent how detectable or visible each drone model is to radar systems at different frequencies. These values are crucial for assessing the radar signature of drones, which is important for anti-drone technology development and radar-based detection and identification of drones. The table essentially shows how these specific drone models interact with radar signals at different frequencies.

Table 2. RCS Experiment Results

Radar frequency [MHz]	DJI Phantom 2 [m^2]	DJI S900 [m^2]	Octocopter 3DR X8 [m^2]
1500	**/**	**/**	**/**
2400	**0.01**	**0.04**	**0.05**
3600	**0.12**	**0.23**	**0.30**
6000	**0.11**	**0.30**	**0.34**
8500	**0.26**	**0.28**	**0.33**
10700	**0.10**	**0.32**	**0.42**

3.1.2 RF Scan

RF scanning is a technique for detecting drones through RF scanning. It can detect drones non-invasively because it uses the drone's communication signal [10]. In addition, it can detect various wireless communication protocols, so it can detect various types of drones. Figure 1 shows a drone detection system using the RF scanning method for communication specifications such as frequency and output [10]. In (a), the active approach involves emitting RF signals actively from a transmitter. These emitted signals bounce off drones within the detection range, and the system analyzes the return signals to detect and locate drones. Active RF scanning is effective for real-time tracking and precise drone identification. On the other hand, in (b), the passive approach relies on receiving existing RF signals emitted by drones themselves. Drones typically emit RF signals for communication, navigation, and control. The passive detection system intercepts and analyzes these signals to identify and locate drones passively, without emitting its own RF signals. This approach is often used for stealthier detection, as it doesn't reveal the presence of the detection system to potential drone operators.

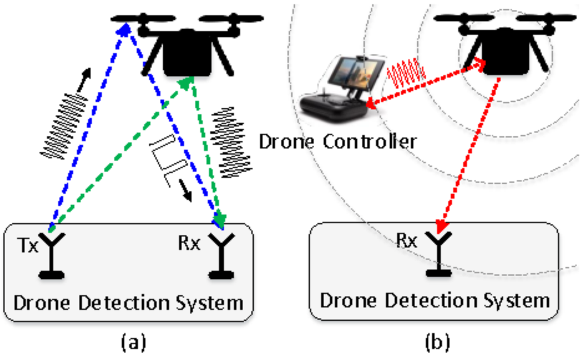

Figure 1. The Overview of Drone Detection System: (a) active and (b) passive approaches.

However, false detections and false alarms may occur due to interference with other wireless communication equipment. In particular, in the case of most commercial drones, the communication protocol is configured using Wi-Fi and LTE systems, so the probability of such interference and false detection is high. In particular, in the case of malicious threat drones, detection of the drone may be difficult if it approaches a restricted flight area in radio silence.

RF scanning is a method of scanning the RF band and analyzing the drone's signal pattern. It is essential to improve the accuracy of signal identification to reduce interference with other wireless communication equipment and false detections. Additionally, it is essential to improve analysis technology for weak signals to enable detection of drones at a wider range and altitude. These limitations of drone detection through RF scanning can be overcome by developing more effective drone detection and response systems by integrating with other sensors and technologies.

3.1.3 Heat Detection (Infrared Camera)

Drone detection using heat detection works by detecting the heat energy emitted by the drone. Figure 2 shows an image of a hexacopter detected through thermal surveillance [11]. The IR image offers valuable insights into the thermal characteristics of the Hexacopter, highlighting areas of heat generation, such as the motors, battery, and electronic components. This information is instrumental in identifying operational drones, assessing their functionality, and potentially detecting anomalies or malfunctions based on temperature patterns.

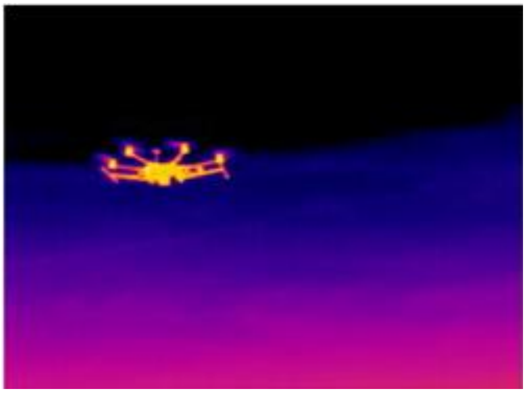

Figure 2. IR Image of the Hexacopter from the FLIR A40M

Detection of drones using a heat detection method takes advantage of the unique thermal energy emitted by drones that makes it easy to distinguish them from other objects. It is easy to distinguish from birds, etc., and the recorded video also has the effect of being evidence. Drone detection using heat detection can detect drones without being affected by time, and can track and detect them in real time. However, heat detection generally only works over a limited range, and detection can be difficult at long distances. Additionally, performance may be affected by weather conditions, and detection accuracy may be low around strong heat sources. This thermal-sensing drone detection technique uses thermal sensors and cameras, such as infrared cameras, to capture and analyze the drone's thermal signals [11]. Recently, research on automatically detecting and tracking drones through artificial intelligence and pattern recognition technology has been active. In addition, research is being actively conducted to minimize environmental impacts and expand the detection range.

3.1.4 Optical Camera

The drone detection technique using an optical camera is a method of accurately detecting and identifying drones through high-resolution images of an optical camera. Real-time detection is possible with a high frame rate and has the advantage of being able to respond quickly. In addition, optical sensors can be used for a variety of purposes, and in addition to drone detection, they can be used for environmental monitoring, security, and video recording [12]. However, even these optical cameras may perform poorly in adverse weather conditions such as fog, rain, or snow, and may have limitations in long-distance detection. Additionally, optical sensors only operate within the visible range, so they have limitations at night or in dark environments.

Optical sensors primarily use cameras and focusers to detect and track drones. Drone detection techniques using optical cameras also utilize image processing and pattern recognition technologies to automatically detect and identify drones. Recently, research has been active on technologies for long-distance detection that are not sensitive to weather conditions. In addition, it is necessary to develop a reliable drone detection system in various environments by integrating with other sensors.

3.2 Drone Identification Technology

As mentioned earlier, drone identification technology, unlike drone detection technology, not only detects the type and operator of the drone. It can be said to be a technology that determines whether a detected drone poses a threat by analyzing whether the drone's flight is approved, its flight intention, and its purpose.

Currently, Korea's anti-drone technology is mainly focused on determining whether a drone is a drone, rather than identifying its identity, such as ID identification, and is moving from focusing on the detection and hard kill of drones and developing drone neutralization technology to focusing on identifying the threat of drones and soft kills.

3.2.1 Direct Drone Identification

The most primitive drone identification method involves direct verification and identification by humans. Many countries, including Korea, that manage drone flights, have established and are operating regulations for prior registration in relation to drone flights. In Korea, depending on whether the use of drones is commercial or non-commercial, it is stipulated that prior notification is required regardless of the weight of the aircraft (for-profit purpose) or to report when the maximum take-off weight exceeds 2kg (non-commercial purpose) [13]. After reporting, the relevant certificate and aircraft unique number are issued and attached to the aircraft. In particular, when taking video using a drone, it is stipulated that military approval must be obtained. Through this, it is possible to identify the drone aircraft and the coordinator, but this method is a method of identifying and post-processing the owner and coordinator in the event of a drone accident, and is far from preventive drone identification technology.

3.2.2 Drone ID-based Drone Identification

Drone ID-based drone identification techniques play an important role in safe drone operation and increasing the efficiency of unmanned aerial systems. DJI's drone ID and America's remote ID are some of the systems developed for this purpose.

Drone ID has the following features. First, it has identity. Identification uniquely identifies the drone and shares that information with third parties or regulatory authorities. And it has location transparency. It contributes to public safety and air traffic management by providing drone location information in real time. It also has emergency response capabilities. This enables quick response by checking the location and owner information of the drone in an emergency situation. Lastly, it has privacy protection. It discloses necessary drone information while protecting the user's personal information. This drone ID technology is one of the key elements for maintaining regulation and safety in harmony with the growth of the drone industry.

A representative drone ID technology is DJI's Drone ID. DJI uses its own drone communication protocols, especially OcuSync. It is known that the drone's navigation information, status information, location information, and pilot information are transmitted to the ground station by sending a data packet called Drone ID within the protocol through the downlink every 640ms. Additionally, DJI has a drone detection platform called "AeroScope", which allows you to quickly identify the drone's communication link and collect information such as flight status and route. AeroScope is a system that specifically helps national and local safety and security agencies identify and monitor unmanned aerial vehicles from the air. This system identifies the DJI drone's communication link and provides its location, altitude, speed, direction, driver location, flight mode and other information in real time [14].

Meanwhile, remote identification (Remote ID), which is currently underway in the United States, is an important regulation regarding drone operation. Remote ID is a system that enables identification when operating drones through strong legal regulations, allowing other aircraft and ground control authorities to identify and track drones. All domestic and foreign drones sold in the United States must comply with these regulations, and a technical standard for Remote ID has been distributed and has been in effect since September of this year. Figure 3 shows some of the concepts of Remote ID [15]. In the context of Figure 3, Remote ID refers to the ability of a drone to broadcast essential information about itself, such as its unique identification number, its current location, and the location of its operator or pilot. This information is typically transmitted via wireless communication protocols to authorities or other nearby parties who need to monitor and manage drone operations.

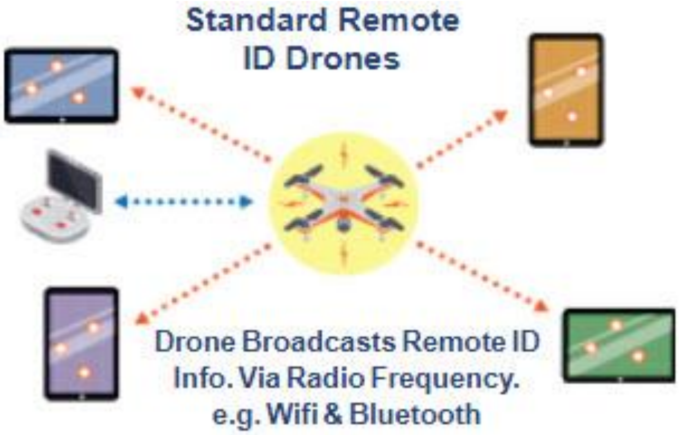

Figure 3. Drone Remote ID

The Remote ID system broadcasts data generated by drones in real time to obtain information from devices or facilities that receive it. This includes the location, altitude, speed, and pilot information of the drone in flight. This information can be provided to other aircraft and ground control systems in the air to monitor and adjust drone operations.

One of the main goals of Remote ID is to facilitate the identification of drones so that drone operators can verify that they are operating legally. This is a strong measure to strengthen public safety and security and prevent illegal operation of drones. In the United States, these regulations are pursuing safe operation of drones and harmony with other means of air transportation.

3.3 Drone Neutralization Technology

Through the drone detection and identification technology mentioned above, drones that are identified as threat drones are neutralized. These drone neutralization technologies are broadly classified into 'Hard Kill' and 'Soft Kill'. Hard kill is a technology that physically destroys the drone, and soft kill is a technology that disrupts or limits the operation of the drone.

Table 3 provides a categorization of methods for neutralizing drones, differentiating between hard-kill and soft-kill approaches. Hard-kill techniques often involve the use of physical force or countermeasures. These methods are typically employed in situations where immediate and decisive action is required to eliminate a drone threat. In contrast, the soft-kill category comprises non-destructive methods aimed at disrupting or mitigating drone operations without causing physical harm. Soft-kill techniques often involve electronic countermeasures like signal jamming, GPS spoofing, or cyber attacks to interfere with a drone's navigation, communication, or control systems. Soft-kill approaches are preferred in scenarios where preserving the integrity of the drone or minimizing collateral damage is a priority.

Table 3. Classification of Drone Neutralization

Classification	Main technology
Hard-Kill	**Laser, RF gun, Net guns, anti-aircraft weapons, bird of prey**
Soft-Kill	**Jamming, spoofing, takeover, geo-fencing**

Details for each drone neutralization technology category are as follows.

3.3.1 Drone Neutralization Hard-kill Technology

3.3.1.1 Laser

Anti-drone technology using lasers is a defense system against drones or unmanned aerial vehicles, and uses high-energy laser beams to neutralize or destroy targets. The laser fires thousands of pulses per second, causing high heat on the surface of the drone, causing physical damage or damaging electronic equipment, causing it to stop operating [16].

This laser-based drone neutralization technique has a very fast response speed to the target. Additionally, with high precision, only desired targets can be selected and neutralized. And the laser can be fired indefinitely as long as the energy supply continues. However, there are limitations that require high energy and continuous energy supply. Additionally, the effectiveness may be reduced depending on weather conditions such as fog, dust, and rain. Currently, various national organizations, including our military, are developing or introducing laser-based anti-drone systems to protect assets and important facilities from threats from unmanned aerial vehicles. Figure 3 showcases Raytheon's laser-based Counter-Unmanned Aircraft System (C-UAS) High-Energy Laser (HEL). This cutting-edge technology represents a significant advancement in countering unauthorized or hostile drones. Raytheon's C-UAS HEL utilizes high-energy lasers as its primary method of neutralizing drones. These lasers are precisely directed at the target drone to disrupt and damage its critical components. The system is known for its exceptional precision, capable of rapidly targeting and tracking drones, even at extended ranges. This precision minimizes the risk of collateral damage and ensures efficient drone elimination. Raytheon's C-UAS HEL is adaptable and effective against a variety of drone types and sizes, making it a versatile solution for countering evolving drone threats.

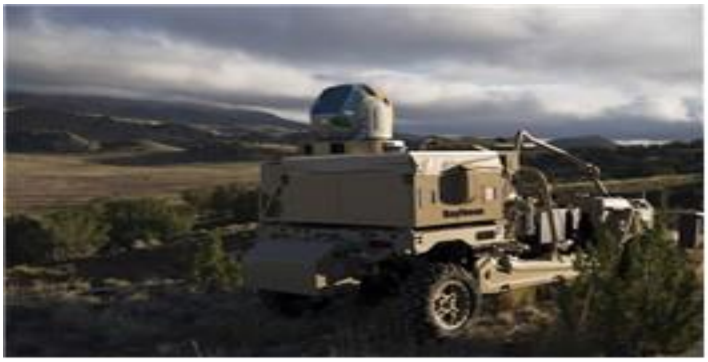

Figure 3. Raytheons' laser-based C-UAS HEL

Drone neutralization technology using lasers is developing rapidly along with the development of drones, and is evaluated as one of the important defense methods that can effectively respond to various threats to unmanned aerial vehicles.

3.3.1.2 RF Gun

Drone neutralization technology using RF guns is a technology that disrupts or neutralizes the functions of a drone by interfering with the wireless communication frequency used to control the drone.

RF guns emit powerful electromagnetic waves in a specific frequency band to disrupt drone control signals. This technology takes advantage of the fact that drones are controlled through transmission and reception, and detects and disrupts the location and activity of the drone along with RF detection technology.

Figure 4 shows Diehl's High-Power Microwave (HPM) technology. Diehl's HPM is a sophisticated and powerful electronic countermeasure system designed for countering drones and other electronic threats. It functions by emitting high-intensity microwave pulses that disrupt and disable the electronic systems of target drones.

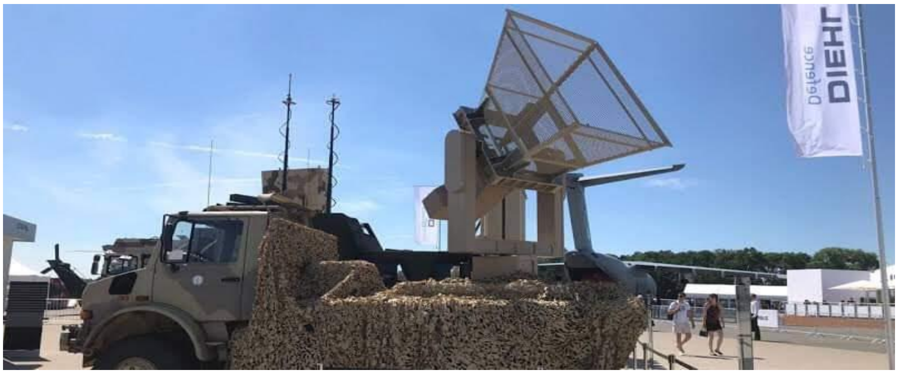

Figure 4. Diehl's HPM

This drone neutralization technology using an RF gun can react quickly and immediately block the drone's control signal, and can stop the drone without physical damage, allowing the drone to be recovered and analyzed. However, the operating range of the RF gun may be limited. Additionally, strong electromagnetic waves can affect other nearby wireless communication equipment in addition to the drone, limiting its use range.

Anti-drone technology using RF guns is widely used in the defense and security fields to respond to threats caused by drones, and is recognized as an important tool that can quickly and effectively respond to drone threats in various situations.

3.3.1.3 Net Gun

Drone neutralization technology using a net gun is a technology that captures drones using a net. The principle is to launch a specially designed net to capture a target drone, thereby disrupting the flight of the drone and causing it to fall to the ground.

This drone neutralization technology using a net gun neutralizes the drone through physical methods, so it does not require electromagnetic technology such as electronic interference or jamming. Therefore, the method of capturing a drone using a net gun can physically stop the drone without affecting other wireless communication equipment or other drones nearby [14]. However, drone neutralization technology using a net gun may also have limited neutralization ability depending on the range of the net gun. And in order to capture a drone moving at high speed, the user's precise aiming and quick reaction speed are required. However, drone neutralization technology using net guns is known to be a relatively effective technique.

3.3.1.4 Bird of Prey

Drone neutralization technology using birds of prey is a method of capturing or stopping drones by utilizing the power of nature.

Large birds such as eagles and hawks have high speed and precision, making them very effective in capturing fast-moving drones in the air. Utilizing these birds of prey uses natural methods rather than complex technical approaches such as electromagnetic interference or hacking, so it does not require additional equipment or systems. And trained birds of prey can react quickly and capture the target drone. In fact, the Dutch company 'Guard From Above', together with the Dutch police, conducted tests using birds of prey against hostile drones and showed significant results in neutralizing drones [14]. However, there may be limits to the range of activity or capture ability of birds of prey, and performance may vary depending on environmental factors or weather conditions. Anti-drone technology using birds of prey is particularly useful for preventing or stopping illegal drone activities in the private sector.

3.3.1.5 Anti-Aircraft Weapons

Drone neutralization technology using anti-aircraft weapons is the most intuitive defense technology to respond to the threat of drones. It performs detection and shootdown functions by considering the speed, altitude, and size of the drone. In combination with a short-range radar, it quickly detects the drone and detects its precise location to neutralize the drone through a direct strike.

This drone neutralization technology using anti-aircraft weapons can quickly detect and respond to drone threats through an automated air defense system, and can be used not only in military situations but also in various areas such as aviation safety and protection of important national facilities. However, performance may vary depending on various variables such as the size, speed, and altitude of the drone. Therefore, using a combination of multiple technologies can be effective.

3.3.2 Drone Neutralization Soft-kill Technology

3.3.2.1 RF Jamming

Wireless jamming is a technology that disrupts the communication of certain electronic devices by disrupting radio frequencies. In drone neutralization technology, wireless jamming is used to disrupt or disturb the drone's remote control signal or GPS signal to disrupt the normal flight of the drone or disable its control.

Drones primarily use radio frequencies to communicate with their pilots. Radio jamming disrupts these radio frequencies and blocks communication between the drone and the pilot [4]. Additionally, in the case of drones that receive GPS signals, they generate strong GPS signals, preventing normal GPS signal reception and disabling the drone's flight.

In general, wireless jamming is a retransmission attack technique that stores and retransmits wireless signals for drone control to neutralize the drone, but there are also techniques such as hijacking the session between the drone and the operator and man-in-the-middle attack techniques. Session hijacking is a technique that neutralizes a drone by intercepting session-related information between the drone and the operator and forging and altering data on the network. Additionally, the man-in-the-middle attack technique is a technique that neutralizes drones by disguising them as drones or ground control devices and transmitting altered data to each other when there is no authentication function between the drone and pilot. In addition, there is also a technique that disables the drone by radiating a frequency corresponding to the resonance frequency of the gyro sensor in order to cause errors in the gyro sensor mounted on the drone [14].

This drone neutralization technology through wireless jamming can neutralize drones without physical damage and can effectively limit drone flights in specific areas. However, other wireless communication devices within the jamming range may be affected, and therefore the use of wireless jamming devices may be restricted in certain areas. Currently, drone neutralization technology using wireless jamming is an important technology that can effectively neutralize the threat of drones among soft kill technologies.

3.3.2.2 Spoofing

Drone neutralization technology using spoofing is a technology that neutralizes a drone by forging the GPS signal that the drone receives and deceiving the location information that the drone uses as a standard for flight. Through manipulated GPS signals, the drone's flight path can be changed or moved to an unwanted area. In addition, there are techniques that randomly transmit drone control signals in addition to GPS signals to disrupt the normal flight of the drone and neutralize its control, and there are techniques that transmit worthless signals to neutralize normal drone flight [17]. This allows the flight of drones to be interrupted or disabled without physical damage or destruction, and is effective in restricting drone access to specific areas. Drone neutralization technology using spoofing, along with RF jamming, plays an important role in effectively responding to drone threats and ensuring the safety of important facilities or specific areas.

3.3.2.3 Take Over

Takeover refers to an anti-drone technology that steals control signals from a drone and takes control away from the original operator. Through this technology, drones can be guided to a safe location or neutralized. The control takeover technique detects the communication link between the drone and its controller and intervenes in the communication link through disruption and spoofing to hijack and obtain control of the drone. Stealing control is a combination of RF jamming and spoofing techniques, and as drone communication protocols have recently become more sophisticated, reverse engineering and fuzzing techniques are being actively researched. The main methods include a method of injecting malicious code into the ground control device to steal information and issue malicious commands to the drone to neutralize it, and a method of modifying the drone's firmware and executing malicious code to leak information and issue commands. There are also techniques to seize control by stealing system privileges through a backdoor.

Drone neutralization technology by seizing control rights also has the advantage of being able to neutralize or control a drone without physical damage, and also safely recovering the drone's payload or data. However, in the case of drones that use highly encrypted communications, it may be difficult to take control.

3.3.2.4 Geo-Fencing

Geo-Fencing is a technology that sets a specific area as a virtual “prohibited zone” or “allowed zone.” In other words, Geo-Fencing sets certain facilities as off-limits areas in the drone's navigation system, and these settings are based on GPS information. When the drone attempts to approach a set restricted area, the navigation system recognizes this and moves to the area. Restrict access to the drone or stop the operation of the drone altogether. Geo-Fencing technology is mainly used in important facilities or sensitive areas such as ports, airports, and military facilities, and can prevent illegal access by drones [18].

Even in areas where Geo-Fencing technology is applied, drones that approach are easily identified as threat drones and have the advantage of being able to respond quickly, so their use is increasing to strengthen the security of national infrastructure, military facilities, and other important facilities.

4. Institutional Supplementary Measures for Anti-Drone Technology

In February 2023, the Korean government reviewed and decided on ‘complementary anti-drone measures for national important facilities’ at the ‘16th National Terrorism Countermeasures Committee’ [19]. The government announced a plan to select priorities based on the importance of facilities for nationally important facilities that require introduction or reinforcement of anti-drone systems, establish and implement a step-by-step introduction plan, and actively promote anti-drone technology research and development and implement related laws and regulations. It was decided to improve the plan to create a foundation for preemptive response to the threat of drone terrorism. In addition, following the infiltration of North Korean drones, the Drone Operations Command was established as a unit under the direct control of the Ministry of Defense in September 2023 under the direction of the President, and systematically and efficiently performs strategic and operational missions using drones in the joint battlefield area and utilizes drone power. It establishes and implements plans for military operations (drone operations), and its main mission is to perform military operations such as detection, tracking, and striking to respond to enemy drones.

Meanwhile, Korea is sparing no effort in supporting anti-drone technology in all directions, such as introducing a legal basis for anti-drone technology through radio wave blocking in accordance with the Radio Waves Act and criminal immunity provisions for secondary damage that may occur from anti-drone operations. It is not happening. However, some laws and systems are restrictions on anti-drone technology, such as the Airport Facilities Act prohibiting actions that may have a negative impact on airport facilities [20].

Anti-drone technology is required across all fields, including national defense, industry, and transportation, and has many overlaps with the work of various government ministries. Therefore, a joint public-private management system is required to maintain consistent policies and legal systems. Through this, standardization of anti-drone technology must be established. Standardization of anti-drone technology is an important step toward coordinating and improving drone threat preparedness and response. Standardization of anti-drone technology ensures compatibility between various manufacturers and organizations and enables efficient response to drones. This provides a variety of benefits in military, industrial and public safety fields. Standardized anti-drone systems help quickly detect and intervene against drone threats. Additionally, standardization of anti-drone systems promotes cooperation between various countries and companies and establishes leadership in research and development. In addition, standardization of anti-drone technology ensures compatibility between various systems, improves efficiency, and promotes multinational cooperation, enabling a better response to drone threats. Currently, many countries and industries, including Korea, are carrying out such standardization efforts [21].

5. Conclusion

Throughout this paper, we have undertaken an extensive exploration of various anti-drone technologies and methodologies. We have meticulously analyzed the technologies employed in countering illicit drones through the stages of detection, identification, and neutralization.

Our investigation has unequivocally illustrated the interconnection between the development of anti-drone technology and the ever-evolving landscape of drone technology itself. As a result, we have outlined the prospective trajectories for the advancement and applicability of anti-drone technology in the future. Furthermore, we have actively sought efficient approaches to address emerging threats like drone-based terrorism, considering both technical and legal responses.

Through the findings presented in this paper, we, as authors, aim to offer valuable guidelines for the future research and development of anti-drone systems.

6. Reference

[1] D. Floreano and R. J.Wood, “Science, technology and the future of small autonomous drones,” *Nature,* Vol. 521, pp. 460-466, May. 2015.

[2] M. Ritchie, F. Fioranelli, and H. Borrion, “Micro UAV crime prevention: Can we help Princess Leia?” in *Proc. Crime Prevention in the 21st Century.* Cham, Switzerland: Springer, pp. 359–376, 2017.

[3] Joon-Young 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, 2020.

[4] Youngbin Go, Minseok Kim, Seohyun Yoo, and Jeongchang Kim, “Study on SDR-Based Drone Detection Using Radio Frequency Signal,” in *Proc. Symposium of the Korean Institute of communications and Information Sciences*, pp. 512-513, Jun. 2023.

[5] Suna Choi and Kyu-min Kang, “Study on analysis of co-existence with wireless devices in the 5.8GHz band for Remote Identification of Drones,” in *Proc. Symposium of the Korean Institute of communications and Information Sciences*, pp. 585-586, Nov. 2022.

[6] Chanjeong Park and Kiyong 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.

[7] Wanjei Cho, Keunwoo Kim, Jeonghoon Park, and Seong-Cheol Kim, “CFAR detection method for detecting small drones using FMCW radar,” in *Proc Symposium of the Korean Institute of communications and Information Sciences*, pp. 183-184, Jun. 2023.

[8] Y.-J. Kong, S.-H. Sohn, J.-S. Hyun, D.-G. Yoo, and I.-C. Cho, “Design Plan of Signal Processing Structure for Real-Time Application in Drone Detection Radar,” *The Journal of The Institute of Internet, Broadcasting and Communication*, vol. 22, no. 3, pp. 31–36, Jun. 2022.

[9] Jarez S. Patel, Francesco Fioranelli, David Anderson, “Review of radar classification and RCS characterisation techniques for small UAVs or drones,” *IET Radar, Sonar & Navigation*, Vol. 12, No. 9, pp. 911-919, Jul. 2018.

[10] Nguyen, Phuc et al. “Investigating Cost-effective RF-based Detection of Drones.,” in *Proc. the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*, pp. 17-22, Jun. 2016.

[11] J. Farlik, M. Kratky, J. Casar, and V. Stary, “Multispectral Detection of Commercial Unmanned Aerial Vehicles,” *Sensors*, Vol. 19, No. 7, pp. 1517, Apr. 2019.

[12] Hunje Lee, Sujeong Han, Jeongil Byeon, and Jihoon Choi, “Detection and Classification of Drones Based on Deep Learning Using Camera, Radar, and Audio Sensors,” in *Proc. Symposium of the Korean Institute of*

communications and Information Sciences, pp. 1116-1117, Feb. 2023.

[13] Heewook Kim, Kunseok Kang, and Daeho Kim, "Analysis of Regulation and Standardization Trends for Drone Remote ID," *Electronics and Telecommunications Research Institute*, Vol. 36, no, 6, pp. 46-54, Dec. 2021.

[14] C. Bender and J. Staggs, "Leveling the Playing Field: Equipping Ukrainian Freedom Fighters with Low-Cost Drone Detection Capabilities," in *Proc. 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, Tallinn, Estonia, pp. 287-312, May. 2023.

[15] R. Raheb, S. James, A. Hudak and A. Lacher, "Impact of Communications Quality of Service (QoS) on Remote ID as an Unmanned Aircraft (UA) Coordination Mechanism," in *Proc. 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)*, San Antonio, TX, USA, pp. 1-8, Oct. 2021.

[16] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim, “Rocking drones with intentional sound noise on gyroscopic sensors,” in *Proc. of the 24th USENIX Conference on Security Symposium(SEC'15)*, pp. 881-896, Aug. 2015.

[17] Juhwan Noh, Yujin Kwon, Yunmok Son, Hocheol Shin, Dohyun Kim, Jaeyeong Choi, and Yongdae 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.

[18] Heeseo Chae, Junho Park, Honam Song, Yonghwan Kim, and Haewook Jeong, "The IoT based automate landing system of a drone for the round-the-clock surveillance solution," in *Proc. the 2015 IEEE International Conference on Advanced Intelligent Mechatronics (AIM)*, pp. 1575-1580, Aug. 2015.

[19] Office for Government Policy Coordination, “2023 national counter-terrorism activity plan and Discussion on supplementary anti-drone measures for nationally important facilities,” *Press release*, Vol. 16, pp.1, Feb. 2023.

[20] Ilseok Oh, “Development plan for anti-drone policy,” *INSS Strategy Report*, Vol. 8, No. 215, Aug. 2023.

[21] Gyumin Kang, Jaecheol Park, Suna Choi, Jinhyeong Oh, and Seonghyeon Hwang, “Trends in Low Altitude Small Drone Identification Technology and Standardization,” *Electronics and Telecommunications Trends*, Vol. 34, No. 6, pp. 164-170, Dec. 2019.