Radicalization of Airspace Security: Prospects and Botheration of Drone Defense System Technology

Simeon Okechukwu Ajakwe, Kumoh National Institute of Technology
South Korea

Dong-Seong Kim, Kumoh National Institute of Technology
South Korea

Jae-Min Lee, Kumoh National Institute of Technology
South Korea

Abstract

The development of a comprehensive and decisive drone defense integrated control system that can provide maximum security is crucial for maintaining territorial integrity and accelerating smart aerial mobility to sustain the emerging drone transportation system (DTS) for priority-based logistics and mobile communication. This study explores recent developments in the design of robust drone defense control (DDS) systems that can observe and respond not only to drone attacks inside and outside a facility but also to equipment data such as CCTV security control on the ground and security sensors in the facility immediately. Also, it considered DDS strategies, schema, and innovative security setups in different countries. Finally, open research issues in DDS designs are discussed, and useful recommendations are provided. Effective means for drone source authentication, delivery package verification, operator authorization, and dynamic scenario specific engagement are solicited for comprehensive DDS design for maximum security.

Keywords—Authentication, Drone Defense, Network, Radar, Security, UAV.

Introduction

Drones were first developed for military purposes in the early1900s. During World War I in 1910, the first unmanned aerial vehicle in the United States succeeded in flying. This led to countries around the world recognizing the need for unmanned aerial vehicles; thus, leading them to carry out various research initiatives. In 1930, the development of Queen Bee (see Figure 1), the first reciprocating reusable unmanned aerial vehicle in the UK, became the originator of an unmanned aerial vehicle today called Drone (Vintage Wings, 2020). Since then, drones have become a major weapon for carrying out important military missions, such as those throughout World War II and the Vietnam War. Furthermore, since the 2000s drones have been used in various industrial fields for purposes other than military engagement. More recently, in addition to improving the quality of life, the function and control of drones have improved significantly, and it has become a hobby that can be enjoyed by all ages (Industry Policy Analyzer, 2019; Ajakwe et al., 2023).

However, as drone applications continue to cut across all spheres of human endeavor, the number of cases threatening public safety and security, such as terrorist use of drones, is increasing rapidly worldwide. In September 2019, there was an incident in which two refineries of Saudi Arabia's state-run oil company Aramco were damaged by a terrorist attack using drones (Business Standard, 2019). The drone used in the terrorist attack flew not only 1000 kilometers, but was also loaded with bombs to detonate oil facilities. The biggest problem is how the ten attack drones remained undetected as they headed for their destination. Experts believe that it would not have been easy to detect small and fast drones with radars that were tracking existing planes while flying at low altitudes (Plus, 2018; Belwafi et al., 2022). Without a professional system to detect, track, and curtail such advanced drones, their deployment for malicious attacks can be devastating. In Korea, a North Korean drone was found to have crashed into a hill in Inje-gun, Gangwon-do, on its way back to the takeoff point after taking off from Geumgang-gun, North Korea on the morning of May 2017, passing the Military Demarcation Line in the process (Hyo-jeong, 2019). In August 2019, police caught a man in his 40s flying a drone over the sky near the Gori Nuclear Power Plant in Busan, a "first-class national security facility" (Hyo-jeong, 2019). Gori Nuclear Power Plant is an "A" class building with national security facilities, such as ports and airports,—within 3.6 kilometers of such is labelled as a no-fly zone and within 18 kilometers is set as restricted-fly areas. Furthermore, one must have permission from the Ministry of National Defense and local aviation authorities before they can fly drones (Choi, 2019). The investigation by the Korean defense intelligence found that the man had managed to fly drones around the Gori Nuclear Power Plant several times before being caught.

Figure 1

Queen Bee

Source: Vintage Wings, 2020

The first case of drone terrorism in the US was the use of an unmanned aircraft carrying a C-4 bomb to assault the US Department of Defense and Capitol Hill (Daniel, 2017). A recent Federal Aviation Administration (FAA) report indicates that the number off sighted drones and UAV-related violations and attacks in different cities in the US between January 2016 to December 2022 stands at 14178 (Federal Aviation Administration, 2023); indicating an increase in smart city airspace security violations from the previous 4889 cases in 2015 and 8124 cases reported by Castrillo et al. (2022). However, this rise in drone-related violations also implies an increase in drone usage and its technological diffusion into virtually all spheres of life; all of which is subject to subsequent acceptability based on its overall impact on society, as with any other innovative technology. Hence, these violations occurred despite the drone defense security systems and innovations put in place to thwart invasive drone activities for safe airspace operations (Castrillo et al., 2022). Also, the ongoing war between Ukraine and Russia has proven that the use of drones and drone defense system technologies in military warfare is a determinant in quantifying military prowess and tactical intelligence in military combat (Regev, 2023; Ajakwe et al., 2023). The sight of an armed UAV has the potential to overwhelm a civilian area, inflict distress, and cause severe injuries. The combination of modifiable UAVs with attached "ghost guns"[1] to unleash terror is gradually gaining momentum among non-state actors and terrorist groups. The procurement of consumer-grade quad-copters—such as the DJI Phantom, which is modifiable for perpetuating ghost gun terror—by non-state actors raises global security concerns

[1] A 3D-Printed Gun, otherwise called a "Ghost Gun" is any firearm that includes components manufactured with a 3D printer (Grossman, 2018).

(Coghlan, 2020).

With such an increase in disruption and violation of the airspace using drones, frequent illegal drone shootings, and terrorist attacks, the importance of drone defense technology and related industries that neutralize enemy attacks by detecting, identifying, and tracking unidentified drones is growing. In this paper, we examined the types and development status of drone defense and detection technologies. To do this, we explored the recent trends in the development of robust convergence-based DDS and technologies. Also, a cross-examination of the functionalities of different DDS techniques and technologies in providing comprehensive security against malicious and invasive drone usage is considered. Finally, open research issues in the existing surveillance and defense architectures for effective and efficient curtailment of drone invasiveness is discussed. Although, convergence-based DDS designs usually lead to an increase in system complexity and cost, the benefit of guaranteeing maximum security far outweighs the macroeconomic implications of a reprisal attack due to negligence in security architectural designs, especially when that negligence is a result of a desire to minimize cost at the expense of security (Ajakwe et al, 2023b). Therefore, the uniqueness of convergence-based DDS designs lies in the combination of visual, radar, radio frequency, and acoustic features for detecting, localizing, identifying, and neutralizing various drone models at different ranges, heights, speeds, and times upon carrying out comprehensive perceived threat analysis. Threat analysis is conducted based on pattern discoveries and feedback from various sensors and nodes in the security network in a cost-effective manner (Ajakwe et al., 2023).

The paper is broken down into four sections. The first includes a general overview of DDS; the second delves into DDS schema, strategies, and security setups; the third highlights and discusses open research issues in DDS design; and the final concludes the paper and provides recommendations.

Origin and Overview of DDS Approaches

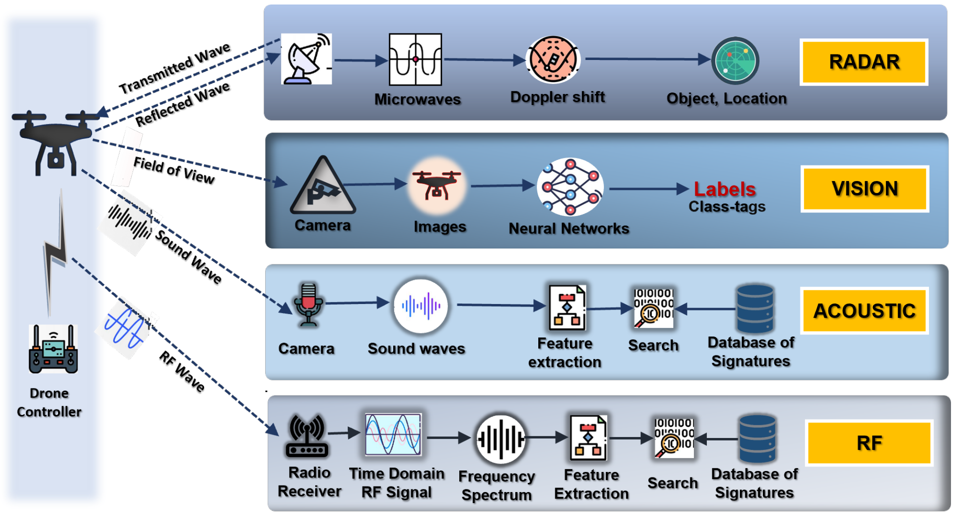
Drone defense systems (DDS) are hard real-time cyber- physical systems (CPS) that run on fault-tolerant networks (FTN) to monitor and supervise the activities and operations of drones from invasive and malicious usage, such as spying, network jamming, reprisal attacks, espionage, etc. The importance of developing DDS technologies cannot be overemphasized as it has become an essential technology for society, from the need to protect major key facilities to the purpose of protecting individual privacy and property. Hence, a convergence-based design approach that guarantees maximum security is a value-added innovation. According to Ajakwe et al. (2023), drone defense is divided into three stages: detection, identification, and incapacitation.

Drone Detection & Identification Technologies

As indicated above, there are three stages to drone defense: detection, identification, and incapacitation. Detection entails spotting an aerial object, while identification entails providing vivid information for distinct definitions and elicitation of the detected object. Incapacitation (otherwise called neutralization) refers to sending an appropriate and timely response based on retrieved sensor information over the communication network in order to control and curtail the identified object (Ajakwe et al., 2022b). No matter how good the identification and incapacitation technologies are, they are useless if the detection is not done properly.

Figure 2

DDS Techniques



Note. DDS Detection Techniques and their underlying Technologies and Characteristics. From Drone Transportation System: Systematic review of security dynamics for Smart Mobility (Ajakwe et al, 2023b).

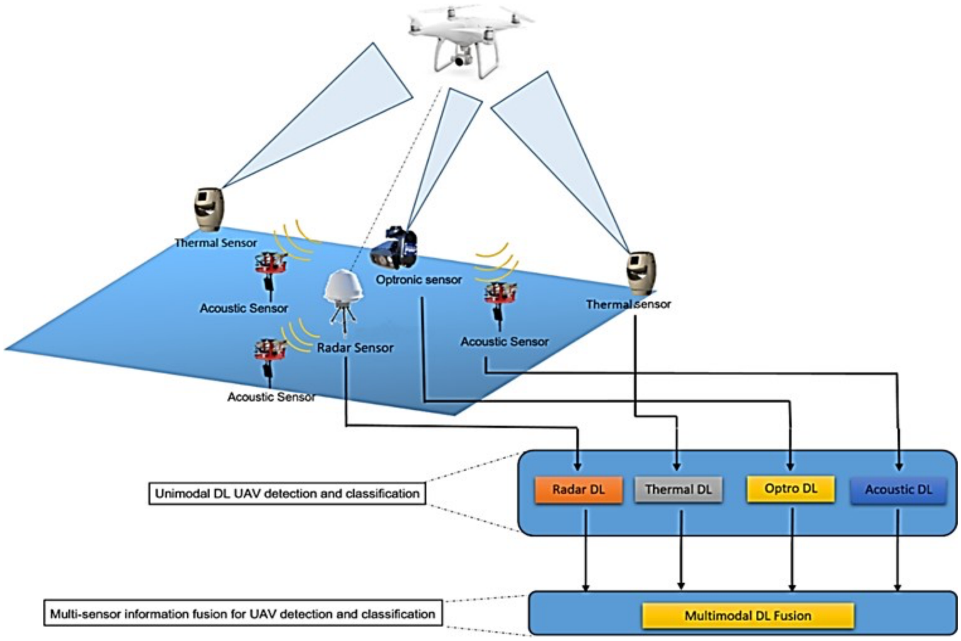
As seen in Figure 2, there are four main techniques for drone detection: radar, radio frequency (RF), optical (video), and acoustic, with each having its peculiarities and potentials. For instance, the RF technique, the most popular, hacks the 2.4GHz and 5.8 GHz wireless communication control signals used by drones to snoop and spoof the network. The purpose behind this is to obtain accurate information such as the location and speed of the drone in the control signal band. With this information, the authority to control the drone can be hijacked and other commands can be issued for a forced landing and return to base. However, deploying a single-modal detection technique in a DDS limits the overall security capabilities of a DDS. The RF technique is deficient in detecting a swarm of drones (Basak et al., 2021); whereas the radar technique creates difficulty in differentiating UAVs from gliding birds (Dini et al., 2022). The acoustic and optical techniques suffer from limitations as well. The acoustic technique has limited range and is encumbered with noise interference (Shi et al., 2020); whereas the optical technique is not weather resilient (Shi et al., 2020; Shi et al., 2018a), amongst other limitations.

To accentuate the importance of maximum security, the recent approach to DDS design and technologies focuses on hybrid-based detection techniques that combine more than one technique to enhance detection range, scope, and speed as shown in Figure 3. These hybrid convergence-based techniques include multiple combinations such as, RF/RFID (Basak et al., 2021; Shi et al., 2018b), vision/acoustic (Syanstrom et al., 2021; Chang et al., 2018), vision/radar (Part et al., 2021; Xie et al., 2019), vision/laser (Ajakwe et al., 2023; Rangwala, 2022; and Kim et al., 2018), and vision/RF (Aledhari et al., 2021) to alleviate the weaknesses of single-modal techniques and enhance detection range, identification capacity, and neutralization functionalities for scenario-specific responses.

To address the swarm of drone detection problems in RF detection technique, Buffi et al. (2017) proposed a multiple RFID detection approach that used a UHF-RFID tag localization to detect a fleet of drones in the air, albeit with limited detection accuracy. Similarly, to address the weakness in acoustic technique, Syanstrom et al. (2021) and Chang et al, (2018) proposed an optical- acoustic detection technique that leverages weather resilience and exact object identification. However, the design is flawed with sensor fusion issues and signal interference. Park et al. (2021) and Xie et al. (2019) developed a radar-optics DDS framework for wide omnidirectional scanning of targeted drones in a complex noisy landscape. Unfortunately, the high computational complexity and deployment cost makes the design impracticable. Lastly,to provide a forensic analysis-friendly and weather-resilientapproach, Aledhari et al. (2021) proposed an RF-optics DDS design that achieved excellent detection and identification accuracy but has limited practical application due to the use of synthetic rather than real data. However, the major drawbacks of these hybrid-convergence-based DDS designs include incomprehensible counter-defense capacity, high system computational complexity, high maintenance and deployment cost, and limited application space, amongst others (Ajakwe et al., 2022a).

Figure 3

Multimodal Convergence-based Drone Detection Framework



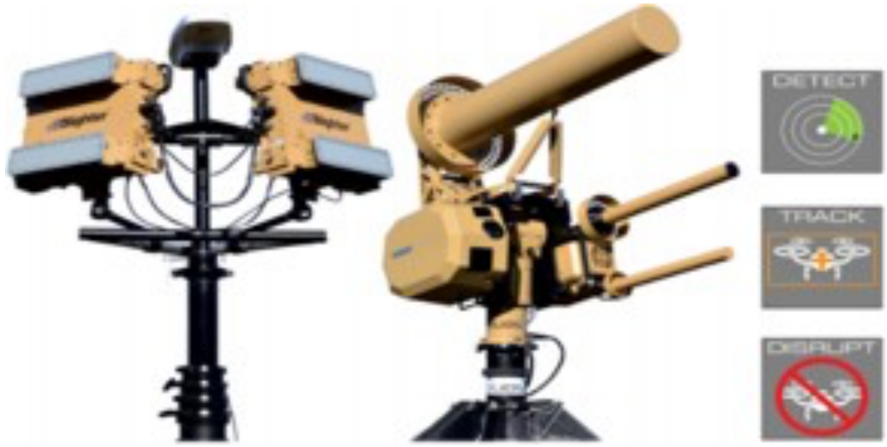
Note. highlighting the sensor fusion of different underlying detection technologies and models From JDR (Source: https://joodrone.tistory.com/14)

Drone Prevention & Neutralization Technologies

The ultimate goal of a DDS is not just to detect and identify a drone, but to prevent and nullify the drone capability to reach its target or objective using either a passive or active neutralization strategy that is dependent on the outcome of the perceived threat analysis, which is based on the metadata from the detection and identification phases. Passive neutralization—otherwise called drone intrusion prevention—is achieved through drone registration, geofencing, and RF propagation. The objective behind these techniques is to disarm or re-direct the drone to a safe zone before deciding to destroy it or otherwise preserve it depending on its harmful status (Ajakwe et al., 2023). With drone registration, the details of each drone operator are utilized to track a target drone; however, it is difficult to expect voluntary registration of drone users due to loopholes in existing laws. Also, it is difficult to grasp the user's intention and continuous management is needed to prevent problems from occurring even after registration, such as information theft (Swinney & Woods, 2022). Geofencing is impracticable for drone defense but can only serve for boundary jurisdiction mapping of the safe and forbidden zone. The challenge with the RF propagation approach is that when detecting and identifying drones, a procedure for taking physical measures by tracking the user's location is necessary, and a neutralization function is accompanied.

Figure 4

Active Drone Defense Jamming



Source: https://dronelife.com/2016/05/31/british-firms-join-faa-airport-anti-drone-project/

On the other hand, active neutralization entails defending a territory from malicious intrusion by destroying a harmful drone after an environmental impact assessment is conducted to minimize the resultant ground effect (Ajakwe et al., 2023). Active neutralization can be either destructive (drone capturing and drone shooting/hitting) or non-destructive (jamming or spoofing) in nature. Jamming is the most effective and widely used non-destructive active neutralization approach, which entails putting out RF signals with higher precision and strength than the targeted signal in order block reception entirely or partially. In meaconing (one of the most effective jamming approaches), genuine global navigation satellite system (GNSS) signals are tuned, recorded, and retransmitted with a delay and higher strength to mislead the receiver (Ferreira et al., 2022). Like jamming, spoofing propagates a fake identical signal with more strength than the satellite signal to force the GNSS receiver to tune to the fake signal rather than the genuine one (Abunada et al., 2020).

Deploying a jammer or spoofer can be very complicated. They can create signal interference and be ineffective for countering a swarm of drones if not properly harnessed and deployed (Ajakwe et al., 2023). Contrariwise, drone capturing, and drone shooting are deployed to destroy a harmful intrusive drone (Ajakwe et al., 2021; Guvenc et al., 2018). However, the negative crash effect of a targeted harmful drone with an attached object that is dangerous—such as a nuclear weapon—toward the immediate environment can be devastating. Also, it creates a disruption of the civil aviation operation during such operations and often requires skilled experts to carry out (Ajakwe et al., 2022b).

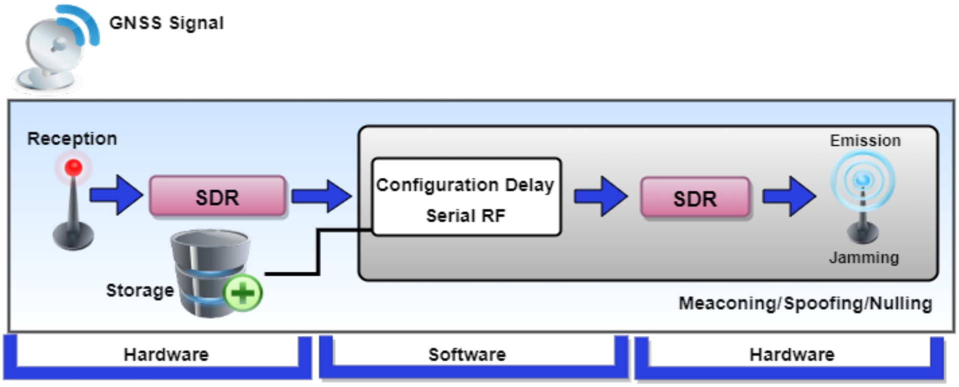
Therefore, in designing and developing an innovative DDS, several factors—such as environmental impact assessment, elicitation of best possible alternatives, choice of cyber-cognito security paradigm, deployment automation dynamics, and other intangibles—must be carefully put into consideration to achieve the objective function of maximum security, albeit at the expense of cost.

Trends in DDS Technologies Across the Globe

The innovative DDS designs incorporate an inclusive and resilient detection and identification protocol, a robust and adaptive neutralization strategy, a defense jurisdiction/mappingschema, and a convergence of drone security gadgets that work in sync to guarantee cost-effective maximum security against all forms of drone intrusion and invasion. Figure 5 highlights the hardware and software components of a typical DDS design.

Figure 5

Hardware- Software Components Integration



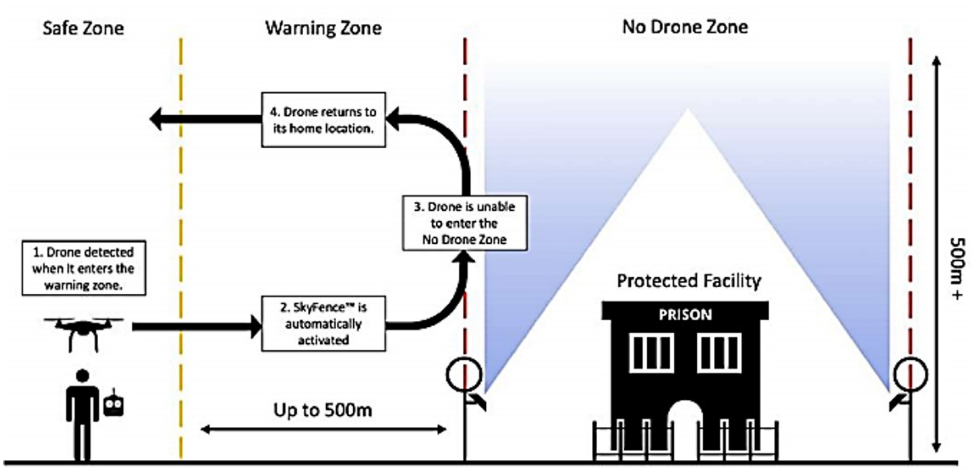
Note. The Hardware-Software Components integration of a typical DDS design highlighting signal receptivity, propagation, and meaconing (Source: Author)

Drone Defense Jurisdiction Schema & Strategy

When a drone in flight is detected via a drone tracker/detector, the drone's control and state information is transmitted for further analysis to determine its harmful status, proximity, authorization, and authentication in readiness for the appropriate neutralization strategy in any given dynamic instance as seen in Figure 6.

Figure 6

Drone Defence Jurisdiction mapping


Safe Zone
Warning Zone
No Drone Zone
4. Drone returns to its home location.
3. Drone is unable to enter the No Drone Zone
1. Drone detected when it enters the warning zone.
2. SkyFence™ is automatically activated
Protected Facility
PRISON
500m +
Up to 500m

Note. Highlights the safe zone, warning zone, and forbidden zone based on the distance and altitude from the target facility and the intruding drone. (Source:https://www.dronedefence.co.uk/wp-content/uploads/2019/05/ SkyFence-brochure-2.pdf).

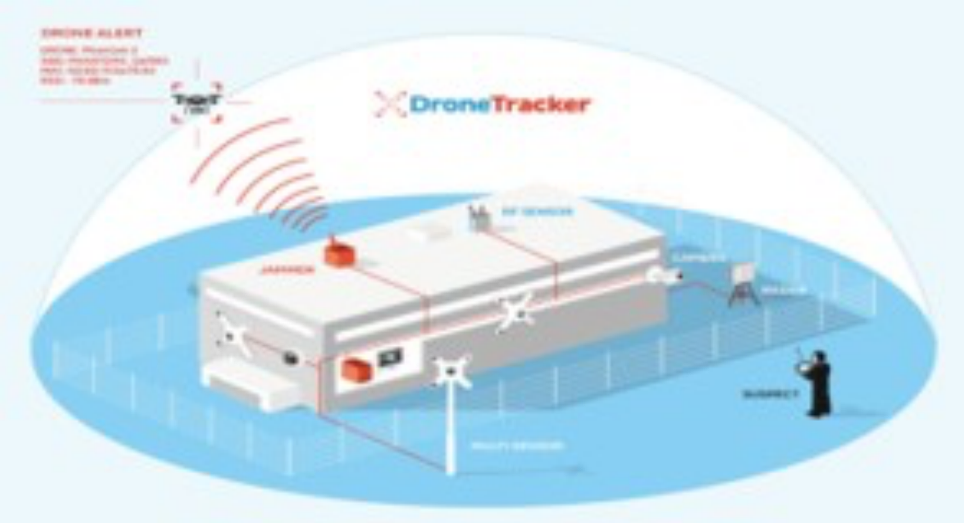
The drone neutralization strategy usually adopts both passive (prevention) and active (defense) neutralization responses,which are carried out in three intertwined stages: environmental impact assessment; attached object status verification; and proximity legality and authentication. This is necessary to determine the appropriate counter-response to deploy in different dynamic scenarios by the DDS.

DDS Technology in Germany

Due to the increase in reprisal attacks and invasions across the globe, different countries and companies have intensified research and development efforts in designing innovative DDS technologies. When approaching a drone, a drone tracker from Germany allows the RF sensor to detect communication in the 2.4-5.8 GHz band of the drone first, and then simultaneously play the image that the drone is filming on the monitoring screen. When the drone approaches closely, secondary detection begins so that multiple sensors can detect multiple appearances, sounds, and Wi-Fi signals of the drone, monitoring them in real time. The location of the detected drone is displayed on the software site map so that the location of the drone can be identified more quickly. In addition, collected frequency and communication information, as well as information on drones such as sound, appearance, and flight pattern were stored in a cloud-based drone identification information database (Castrillo et al., 2022). Figure 7 shows a drone tracker sensing and detecting a target drone in the airspace in readiness for counter-invasion operations.

Figure 7

Drone Tracker



Note. A Drone Tracker sensing and detecting a drone in flight in readiness for counter response (Joo-hye, 2019).

DDS Technology in UK

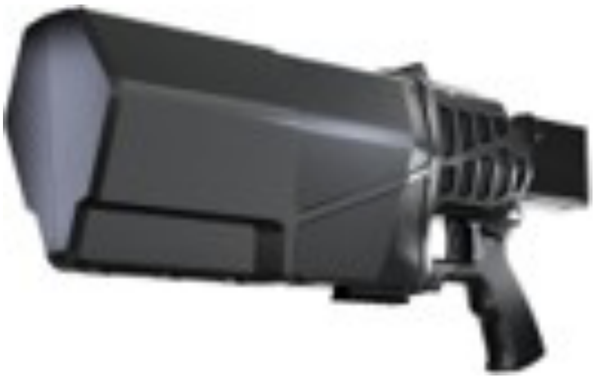
Drone Defence in the UK is a system designed by Drone Innovation Centre in Retford, UK for prison security. Several low-power wireless transmitters (equipped with signal-integrated disruptors) are installed on the existing fence to create an electronic 'wall' up to 500 meters above the ground to disable drones within the range. A transmitter that detects a drone in a control interval and is automatically activated is a method of interfering with the drone's flight control signal and navigation transmission to prevent the operator from controlling and protecting it from threats (Joo-hye, 2019). OpenWorks Engineering, another UK-based anti-drone company, has developed the Sky Wall Patrol system, an anti-tank rocket launcher-shaped jamming gun that physically captures drones by launching a net-mounted projectile at a target. After identifying the target using the built-in Smart Scope, the projectile is fired at the target using compressed air to minimize ambient damage. SkyWall is also available alone, but it is designed to be utilized as a drone defense package in a wide range of regions in combination with SkyLink, a solution for more accurate targeting and capture (Joo-hye, 2019).

DDS Technology in Australia

Australia's DroneShield introduced drone defense technology using jamming guns, a rifle-shaped device that interferes with signals between drones and pilots using radio frequency jamming and GPS jamming. The jamming gun (as seen in Figure 8) is a way to prevent threats from unauthorized drones by disconnecting drones and pilots and activating "FailSaFailSafe" subprogram to send drones back to their origin or interfere with signals (Ajakwe et al., 2021).

Figure 8

Australian jamming gun



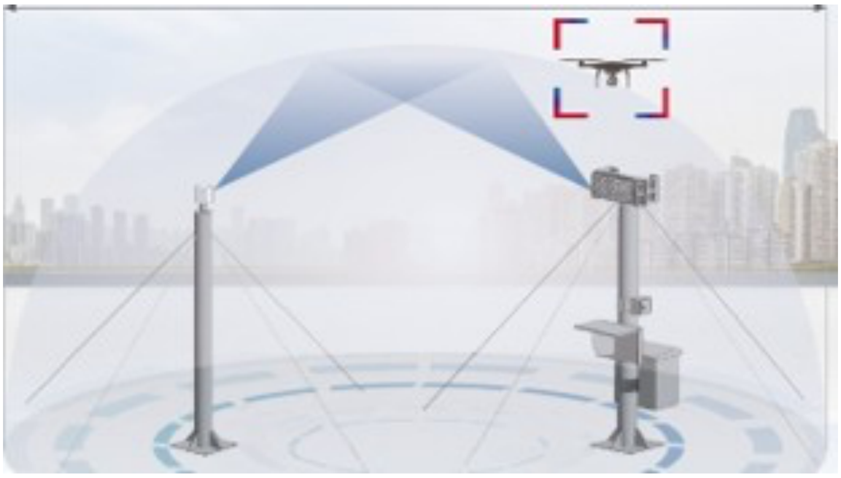
Note. An Australian jamming gun for shooting down an invading drone. (Source: https://openworksengineering.com/skywall-patrol/)

DDS Technology in Korea

In Korea, BM Tech System Co., Ltd. succeeded in the research and development of the first RF Direction Finding drone detection system in Korea. The system has recently completed its first delivery to power generators as shown in Figure 9.

Figure 9

RF Direction Finding Drone Detection System



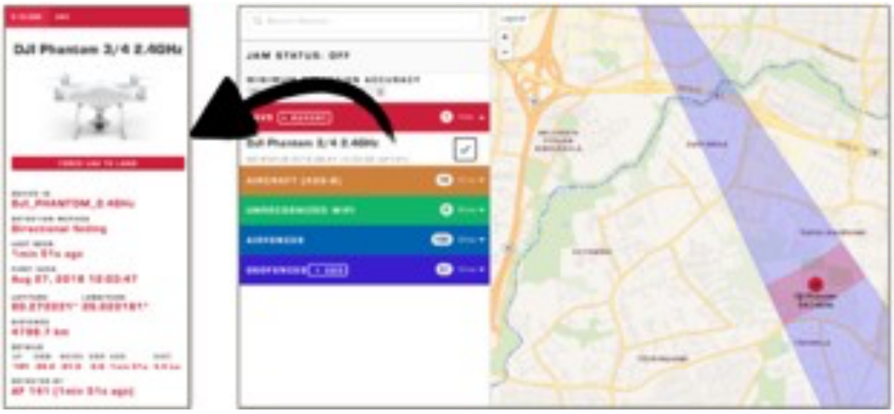
Note. RF Direction Finding Drone Detection System developed by BM Tech. (Source: http://bmtk.co.kr/new/)

When an unauthorized drone enters the detection range, an external RF sensor detects it immediately and displays information that can be called the drone's DNA on the screen—for example, the location of drones and pilots, manufacturers, model names, latitude/longitude, and relative altitude. In addition, it is designed to detect and track alarms (email, SMS, etc.) to related parties within up to 10 seconds when installed in the Open network. In consideration of the user's convenience, the interface is simply designed so that even beginners can easily understand the screen as highlighted in Figure 10.

Voice alarms are automatically set when a drone invades a restricted area in the facility. The limit range setting is the Geofencing function, while the detection range can be set by the user within the range of 3km. Drone detection is carried out based on communication libraries, and it is possible to detect commercial drones such as Parrot, Yuunec, 3DR, and Mavlink Drone as well as DJI, which currently has the highest share in Korea. Through this communication library, accurate information on drones is identified. Therefore, it is possible to frequently identify newly released commercial drones through periodic library DB and firmware updates. Figure 11 shows the information of detected drones within the detection range of BM Tech. DDS design.

Figure 10

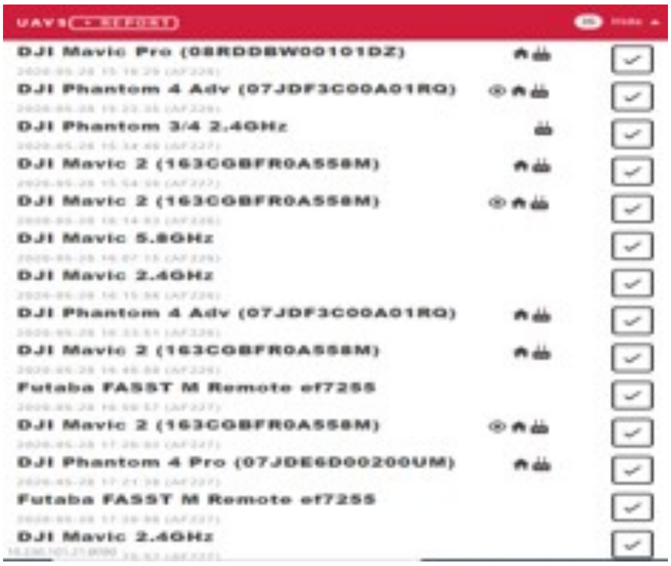
BM Tech and Drone Monitoring Screen



Note. Drone tracking and monitoring screen. (Source: http://bmtk.co.kr/new)

Figure 11

Drone Tracker


UAVS

DJI Mavic Pro (08RDDBW00101DZ)
DJI Phantom 4 Adv (07JDF3C00A01RQ)
DJI Phantom 3/4 2.4GHz
DJI Mavic 2 (163CGBFR0A558M)
DJI Mavic 2 (163CGBFR0A558M)
DJI Mavic 5.8GHz
DJI Mavic 2.4GHz
DJI Phantom 4 Adv (07JDF3C00A01RQ)
DJI Mavic 2 (163CGBFR0A558M)
Futaba FASST M Remote ef7255
DJI Mavic 2 (163CGBFR0A558M)
DJI Phantom 4 Pro (07JDE6D00200UM)
Futaba FASST M Remote ef7255
DJI Mavic 2.4GHz

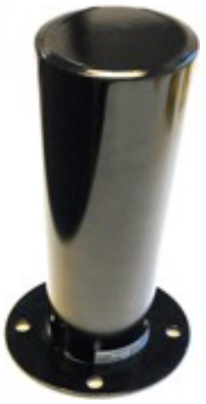
Note. A Drone Tracker sensing and detecting a drone in flight in readiness for counter response. (Source: http://bmtk.co.kr/new)

Another thing to note in this system is that it uses domestically produced security maps rather than open-source ones. This not only satisfies the requirements of public institutions that require a high-level of security from the system, but also passes the security stability test of the national security audit agency so that it can be used safely by important national facilities, counties, or public institutions. In addition, for user convenience, the map zoom-in/out is possible in a web browser user interface (UI) environment, and Geofencing and various function settings can be performed on this map. Maps can be installed by limiting them to the entire Republic of Korea or the area where the system will be installed according to the needs of customers. In addition, it provides statistical functions for customer convenience. The detection time, location, and flight history of the detected drone can be extracted as monthly/annual statistics, and big data can be used as the basis for establishing drone defense plans. The hardware has passed electromagnetic compatibility certification—Korea Certification (KC), according to the domestic use environment—and the highest IP-grade waterproof/dustproof function is recognized, allowing stable use in external environments.

In June 2020, the revision of the Domestic Radio Act opened the way for the use of various defense technologies inevitable for public safety. Therefore, not only monitoring, but also the foundation for immediate response to intrusive drones has been laid. In line with this, BM Tech System Co. Ltd. is speeding up its commercialization following the completion of research on jamming facilities that can effectively respond to intruding drones but minimize damage to the surrounding area.

Figure 12

Commercial Jammer Shape of BM Tech System Co



(Source: http://bmtk.co.kr/new)

The jammer can be used with a drone detection system in conjunction with the revision of the domestic radio law. In addition to jamming that hinders drone pilots and drones, continuous research is being conducted to suit facilities re- quiring high security by allowing them to have full control of intruded drones through GPS jamming and hijacking. At the same time, it is in the process of developing an integrated system that can be linked to a previously developed system by supplying domestic and foreign radar equipment. It is not only to establish a drone defense system with products that have already been developed but also to establish a system that can respond to more diverse situations through linkage with third products. Currently, BM Tech System Co., Ltd. is developing a drone defense integrated control system that can grasp the various drone defense systems mentioned above briefly (BM Tech System, n.d.). This system is a comprehensive control system that can observe and respond not only to drone attacks inside and outside the facility, but also to equipment data such as CCTV security control on the ground, and security sensors in the facility briefly. Although it is still in the early stages of development, it has signed business agreements with leading overseas drone defense and security companies and is now reborn as Korea's best drone defense solution company—in name and in reality.

Open Issues and Discussion in DDS Design

The challenge of providing maximum security for maintaining territorial integrity and privacy is enormous and daunting. The design of an all-inclusive DDS that will mitigate drone invasion and intrusion is confronted with socio-technological issues that tend to maintain a balance between cost-effectiveness and maximum security. These technological issues cut across airspace security intelligence issues, cybersecurity intelligence design issues, and cognitive intelligence model issues.

Cognitive Intelligence Issues in DDS Design

UAVs with camouflaging characteristics, swift maneuverability, and other advanced technological features make real-time detection and countering difficult, which invariably attracts them to terrorist groups as preferred tools for swift reprisal attacks through breaches of security, privacy, and safety (Yaacoub et al., 2020; Ihekoronye et al., 2022a). Current AI-driven UAV architectures rely on a remote cloud. This solution cannot satisfy the present requirements of the Internet of Things (IOT) and Industrial Internet of Things (IIOT) applications in terms of scalability, cost, coverage, availability, latency, and power consumption. Furthermore, previous research evidence has proven that cloud-based architectures are susceptible to cybersecurity compromise. To address this real-time issue, future research should consider the implementation of enhanced fog/edge computing as well as semi-blockchain architectures that comply with the strict requirements of IOT applications for real-time mission-critical and time-sensitive operations. Furthermore, the flight time of a UAV is directly proportional to the weight of the drone as well as its maximum payload (Ajakwe et al., 2022b). Moreover, a trade-off among cost, payload capacity, and reliability should be achieved when choosing between single and multirotor UAVs (as of this writing, quadrotors are the preferred solution for AI models of UAVs). Also, the computational complexity of the underlying AI model affects the time taken in making decisions. Therefore, developing robust models that ensure better trade-offs between power consumption and high-performance speed will significantly improve the performance of DDS designs in countering such UAVs.

Cybersecurity Intelligence in DDS Design

Currently, existing counter-invasion security models have inadequate features to dynamically differentiate and elicit the harmful status of drones based on the attached object through adaptive neutralization and response strategies (Ajakwe et al., 2023). Further, identifying and preventing various forms of distortions and intrusion into drone networks has remained a pertinent issue. Several recognition issues revolve around the limited counter-invasive recognition capabilities of single-mode security systems compared to the high complexity and cost of hybrid-mode security systems due to multiple sensor fusion for sophisticated security intuitiveness in monitoring drone operations for safety and privacy (Ajakwe et al., 2023; Swinney & Woods, 2022). The integrity of detection, classification, and recognition output is of paramount importance to avoid adversarial samples or inputs that deliberately result in incorrect decision-making (Yaacoub et al., 2020). Also, the recent increase in drone violation incidents is attributed to UAVs with longer flight time (Swinney & Woods, 2022). Therefore, intense research should be directed into developing lightweight, energy-efficient, robust, and scenario-specific hybrid-mode recognition models that not only detect and recognize all types of UAVs in the airspace, but also carry out intuitive and proactive responses against invasive usage with improved detection range and multi-dynamic environmental characteristics to guarantee physical space safety. Finally, visual authentication of drone delivery packages is critical for secured drone smart mobility. Hence, intense research efforts should be directed towards developing resource-efficient convergence of visual identification techniques with other techniques—such as, RF, acoustic, RADAR, LASER, RFID, etc.—as advocated by Ajakwe et al. (2023) to improve recognition accuracy. Also, research geared towards developing a routing strategy, reducing the packet losses, the delivery delays, and the energy-efficient consumption of UAVs (Khabbaz et al., 2019; Dubbati et al., 2019; Hu et al., 2019) will go a long way to address these concerns. Also, the need for mobility optimization (Alzahrani et al., 2020) of DDS designs for fast connectivity and efficient traceability and localization of target destinations in a network-crowded smart city through crowdsensing (Yang et al., 2020), task offloading, and collaborative information sharing with user-privacy preservation demands a critical consideration.

Corporate Airspace Security Intelligence in DDS Design

Currently, there are little concerns about safety issues affecting liability and harm caused, culpability for airspace mishap, and interference (Mabutti, 2009). Also, there is insufficient awareness of government regulations regarding safety practices for airspace usage when it comes to drone-based logistics and priority-based deliveries. Finally, it is worth pointing out that the promulgation of stiffer laws and sanctions for incriminating airspace, cyberspace, and AI-space offenders that engage in drone hijacking, drone identity theft, droneillance—or drone surveillance (Dini et al., 2022)—for cyberwarfare under the guise of drone-based logistics (Ajakwe et al., 2020), and unprovoked drone warfare on civil targets is highly needed to actualize secured smart aerial mobility via drones. Most cyber-physical attacks on drones (for instance, spoofing and signal jamming), as well as authentication issues (for example, identity theft), arise from loopholes in the existing regulatory framework. This remains an open research topic that demands consideration to enhance the development of innovative DDS designs.

Finally, a reliable and robust DDS must therefore incorporate all-inclusive and scalable counter-defense mechanisms that can adapt to scenario-specifics, have amplified detection capacity, precise recognition characterization, and efficient response/feedback in a cost-effective manner at any given instance as shown in Figure 3. Unfortunately, existing DDS designs have inadequate functionalities to cater to the multifarious invasion dynamics created by the polarized and malicious drone usage as witnessed in different cities through reprisal-repugnant airspace security breaches caused by different non-state actors across the globe. The DDS security research community has been bedeviled with pertinent problems, such as how to track a drone user's intention, how to detect/track the user's location before the drone's flight operation, how to efficiently recognize and elicit the harmful status of the drone based on the attached object, how to conduct an environmental impact assessment and effectively jam a drone in a crowded or key facility environment, and how to control drone user-identity theft. A neglect of these critical cyber, physical, and cognitive security needs is a contradiction to innovation, research, and development.

Conclusion

In this paper, we looked at the drone defense technologies available against the recent surge in drone attacks and threats. The drone defense system is a technology that detects and neutralizes illegal drones with threats of attack or terrorism in advance and has a defense system in areas or facilities where damage is expected. In particular, the importance of developing related technologies cannot be overemphasized as drone attacks on major facilities worldwide have increased rapidly. Drone defense has now become an essential technology for society, from the need to protect major national facilities to the purpose of protecting individual privacy and property. In addition, the fact that a solution package can be created by combining various technologies can be said to be a high value-added industry that can promote the development of related industries and create high-quality jobs. If the government's institutional support is combined with technological development, aggressive growth of DDS technology will be possible. Research efforts should be aggressively directed toward effective means for drone authentication, verification, authorization, and dynamic scenario-specific neutralization engagement.

References

Abro, G. E. M., Zulkifli, S. A. B. M., Masood, R. J., Asirvadam, V. S., & Laouti, A. (2022). Comprehensive review of UAV detection, security, and communication advancements to prevent threats. *Drones*, *6*(10), 284.

Abunada, A. H., Osman, A. Y., Khandakar, A., Chowdhury, M. E. H., Khattab, T., & Touati, F. (2020). Design and implementation of a RF-based Anti-Drone System. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 35–42. IEEE.

Airborne object detection using hyperspectral imaging: Deep learning review. (2019,July). International Conference on Computational Science and Its Applications, Saint Petersburg, Russia, 07, 306–321.

Ajakwe, S. O., Ihekoronye, V. U., Kim, D. S., & Lee, J.-M. (2022, June). *Pervasive intrusion detection scheme to mitigate sensor attacks on UAV Networks*. 2022 Korean Institute of Communication and Sciences Summer Conference. Retrieved from https://journal-home.s3.ap-northeast-2.amazonaws.com/site/2022s/abs/0194.pdf

Ajakwe, Simeon Okechukwu, Nwakanma, C. I., Kim, D.-S., & Lee, J.-M. (2022). Key wearable device technologies parameters for innovative healthcare delivery in B5G network: A Review. *IEEE Access*, *10*, 49956–49974. doi:10.1109/ACCESS.2022.3173643

Ajakwe, S. O., Akter, R., Kim, D. S., & Lee, J. M. (2021). Lightweight CNN model for detection of unauthorized UAV in military reconnaissance operations. *Korean Institutes of Communications and Information Sciences Conference*, *1*, 1–3.

Ajakwe, S. O., Arkter, R., Kim, D., Mohatsin, G., Kim, D. S., & Lee, J.-M. (2021, September). *Anti-Drone systems design: Safeguarding airspace through real-time trustworthy AI paradigm*. The 2nd Korea Artificial Intelligence Conference. Retrieved from http://manuscriptlink-society-file.s3.amazonaws.com/kics/conference/koreaai2021/presentation/G-2-5.pdf

Ajakwe, S. O., Ihekoronye, V. U., Akter, R., Kim, D.-S., & Lee, J. M. (2022). Adaptive drone identification and neutralization scheme for real-time military tactical operations. *2022 International Conference on Information Networking (ICOIN)*, 380–384. doi:10.1109/ICOIN53446.2022.9687268

Ajakwe, S.O., Ihekoronye, V. U., Mohtasin, G., Akter, R., Aouto, A., Kim, D. S., & Lee, J. M. (2022). VisioDECT dataset: An aerial dataset for scenario-based multi-drone detection and identification. *2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 4992–4997. doi:10.21227/n27q-7e06

Ajakwe, Simeon Okechukwu, Ukamaka Ihekoronye, V., Kim, D.-S., & Lee, J.-M. (2022). SimNet: UAV-integrated sensor nodes localization for communication intelligence in 6G networks. *2022 27th Asia Pacific Conference on Communications (APCC)*, 344–347. doi:10.1109/APCC55198.2022.9943785

Ajakwe, Simeon Okechukwu, Ihekoronye, V. U., Kim, D.-S., & Lee, J. M. (2022, November). *AI-trust in intelligent autonomous decision-centric systems: Introspection of security architectures.* 1–2. Retrieved from https://journal-home.s3.ap-northeast-2.amazonaws.com/site/2022f/abs/BXVPP-0383.pdf

Ajakwe, S.O., Ihekoronye, V. U., Kim, D.-S., & Lee, J. M. (2022a). Adaptive drone identification and neutralization scheme for real-time military tactical operations. *2022 International Conference on Information Networking (ICOIN)*, 380–384. doi:10.1109/ICOIN53446.2022.9687268

Ajakwe, S.O., Ihekoronye, V. U., Kim, D.-S., & Lee, J. M. (2022b). DRONET: Multi-tasking framework for real-time industrial facility aerial surveillance and safety. *Drones*, *6*(2). doi:10.3390/drones6020046

Ajakwe, S.O, Ihekoronye, V. U., Kim, D.-S., & Lee, J. M. (2022c). Pervasive Intrusion Detection Scheme to Mitigate Sensor Attacks on UAV Networks. 한국통신학회 학술대회논문집, 1267–1268.Ajakwe, S.O., Ihekoronye, V. U., Kim, D.-S., & Lee, J.-M. (2023). ALIEN: Assisted Learning Invasive Encroachment Neutralization for secured drone transportation System. *Sensors*, *23*(3). doi:10.3390/s23031233

Ajakwe, S.O., Kim, D.S. and Lee, J.M., (2023b). Drone Transportation System: Systematic review of security dynamics for Smart Mobility. *IEEE Internet of Things Journal*. doi: 10.1109/JIOT.2023.3266843.

Akhloufi, M. A., Arola, S., & Bonnet, A. (2019). Drones chasing drones: Reinforcement learning and deep search area proposal. *Drones*, *3*(3), 58.

Alajmi, A. A., Vulpe, A., & Fratu, O. (2017). UAVs for Wi-Fi receiver mapping and packet sniffing with antenna radiation pattern diversity. *Wireless Personal Communications*, 92(01), 297–313.

Aledhari, M., Razzak, R., Parizi, R. M., & Srivastava, G. (2021). Sensor fusion for drone detection. *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, 1–7. IEEE.

Al-Emadi, S., Al-Ali, A., Mohammad, A., & Al-Ali, A. (2019). Audio based drone detection and identification using deep learning. *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 459–464. IEEE.

Allahham, M. S., Al-Sa'd, M. F., Al-Ali, A., Mohamed, A., Khattab, T., & Erbad, A. (2019). DroneRF dataset: A dataset of drones for RF-based detection, classification and identification. *Data in Brief*, *26*, 104313.

Alnuaim, T., Mubashir, A., & Aldowesh, A. (2018). *Low-cost implementation of a multiple-input multiple-output radar prototype for drone detection*. 2019 International Symposium ELMAR, 183–186.

Alwateer, M., & Loke, S. W. (2020). Emerging drone services: Challenges and societal issues. *IEEE Technology and Society Magazine*, *39*(3), 47–51.

Alzahrani, B., Oubbati, O. S., Barnawi, A., Atiquzzaman, M., & Alghazzawi, D. (2020). UAV assistance paradigm: State-of-the-art in applications and challenges. *Journal of Network and Computer Applications*, *166*, 102706.

Analyzer, I. P. (2019, February). Market analysis of anti-drone industry and trends in technology solutions in major countries. Retrieved from https://www.i24news.tv/en/news/ukraine-conflict/1677160351-war-of-the-future-drones-playing-a-significant-role-in-the-ukraine-war

Andraši, P., Radišić, T., Muštra, M., & Ivošević, J. (2017). Night-time detection of UAVs using Thermal Infrared Camera. *Transportation Research Procedia,* 28, 183–190. doi:10.1016/j.trpro.2017.12.184

Basak, S., Rajendran, S., Pollin, S., & Scheers, B. (2021). Combined RF-based drone detection and classification. *IEEE Transactions on Cognitive Communications and Networking*, *8*(1), 111–120.

Belwafi, K., Alkadi, R., Alameri, S. A., Al Hamadi, H., & Shoufan, A. (2022). Unmanned Aerial Vehicles' remote identification: A tutorial and survey. *IEEE Access*, *10*, 87577–87601.

BM Tech System. (n.d.). The first reference of Anti-Drone System in Korea based on RF System. Retrieved February 20, 2023 from https://www.bmtsys.com/en/bbs/content.php?co_id=en_solution08

Buffi, A., Nepa, P., & Cioni, R. (2017). SARFID on drone: Drone-based UHF-RFID tag localization. *2017 IEEE International Conference on RFID Technology & Application (RFID-TA)*, 40–44. IEEE.

Business Standard. (2019, July). *Houthi says it targeted Saudi Arabia's Abha Airport with drone attack*. Business Standard. Retrieved from https://www.business-standard.com/article/news-ani/houthi-says-it-targeted-saudi-arabia-s-abhaairport-with-drone.html.

Castrillo, V. U., Manco, A., Pascarella, D., & Gigante, G. (2022). A review of counter-UAS technologies for cooperative defensive teams of drones. *Drones*, *6*(3).

Chang, X., Yang, C., Wu, J., Shi, X., & Shi, Z. (2018). A surveillance system for drone localization and tracking using acoustic arrays. *2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, 573–577. doi:10.1109/SAM.2018.8448409

Choi, J. S., Son, B. R., Kang, H. K., & Lee, D. H. (2012). Indoor localization of unmanned aerial vehicle based on passive UHF RFID systems. *2012 9th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)*, 188–189. IEEE.

Coghlan T. (2020). *Hebollah uses of drones to drop bombs on Syrian rebels.* The Times. Retrieved from https://iwww.thetimes.co.uk/article/hezbollah-uses-drone-to-bombs-on-syrian-rebels-675wqcdx2

Dang, Y. (2020). Can we enable the drone to be a filmmaker? *ArXiv Preprint ArXiv:2010. 10706*

Dini, M. A., Ajakwe, S. O., Kim, D.-S., Lee, J. M., & Jun, T. (2022, November). Droneilliance and detection dynamics: A review of radar techniques and trends. *2022 Korean Institute of Communication and Sciences Summer Conference*, 1–2. Retrieved from https://journal-home.s3.ap-northeast-2.amazonaws.com/site/2022f/abs/ZZRYQ-0384.pdf

Federal Aviation Administration (FAA). (2023, January). *UAS Sightings Report*. Federal Aviation Administration. Retrieved from https://www.faa.gov/uas/resources/public_records/uas_sightings_report.

Ferreira, R., Gaspar, J., Sebastião, P., & Souto, N. (2022). A software defined radio based anti-UAV mobile system with jamming and spoofing capabilities. *Sensors*, *22*(4), 1487.

Grossman, N. (2018) *Drones and terrorism: Asymmetirc warfare and the threat to global security*. I.B. Tauris, London, UK

Guvenc, I., Koohifar, F., Singh, S., Sichitiu, M. L., & Matolak, D. (2018). Detection, tracking, and interdiction for amateur drones. *IEEE Communications Magazine*, *56*(4), 75–81.

Haviv, H., & Elbit, E. (2019). Drone threat and CUAS technology: White Paper. *Elbit Sytems*, (01), 1–19. Retrieved fromhttps://www.tweedekamer.nl/downloads/document?id=c6b69754-8a63-4772-a90c-9377aff2e248

Hu, Z., Bai, Z., Yang, Y., Zheng, Z., Bian, K., & Song, L. (2019). UAV aided aerial-ground IoT for air quality sensing in smart city: Architecture, technologies, and implementation. *IEEE Network*, *33*(2), 14–22.

Hyo-jeong, C. (2019, August). *40s were caught flying drones around Kori Nuclear Power Plant, the first-class national security facility*. Chosun Retrieved from https://www.chosun.com/site/data/html_dir/2019/08/20/2019082000433.html

Ihekoronye, V. U., Ajakwe, S. O., Kim, D.-S., & Lee, J. M. (2022a). Aerial supervision of drones and other flying objects using convolutional neural networks. *2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 069–074. doi:10.1109/ICAIIC54071.2022.9722702

Ihekoronye, V. U., Ajakwe, S. O., Kim, D.-S., & Lee, J. M. (2022c). Hierarchical intrusion detection system for secured military drone network: A perspicacious approach. *MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM)*, 336–341.

Joo-hye, Y. (2019, October). *Israel to launch AUDS market*. Kotra. Retrieved from http://news.kotra.or.kr/user/globalAllBbs/kotranews/album/781/globalBbsDataAllView.do?dataIdx=177887&column=&search=&searchAreaCd=&searchNationCd=&searchTradeCd=&searchStartDate=&searchEndDate=&searchCategoryIdxs=&searchIndustryCateIdx=&searchItemNaml

Khabbaz, M., Antoun, J., & Assi, C. (2019). Modeling and performance analysis of UAV-assisted vehicular networks. *IEEE Transactions on Vehicular Technology*, *68*(9), 8384–8396.

Kim, J., Kim, S., Ju, C., & Son, H. I. (2019). Unmanned aerial vehicles in agriculture: A review of perspective of platform, control, and applications. *IEEE Access*, *7*, 105100–105115.

Kim, B. H., Khan, D., Bohak, C., Choi, W., Lee, H. J., & Kim, M. Y. (2018). V-RBNN based small drone detection in augmented datasets for 3D LADAR system. *Sensors*, *18*(11), 3825.

Masutti, A. (2009). Proposals for the regulation of unmanned air vehicle use in common airspace. *Air and Space Law*, *34*(1). *Communications Magazine*, *56*(4), 68–74.

Okechukwu Ajakwe, S., Ifeanyi Nwakanma, C., Lee, J.-M., & Kim, D.-S. (2020). Machine learning algorithm for intelligent prediction for military logistics and planning. *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, 417–419. doi:10.1109/ICTC49870.2020.9289286

Okechukwu Ajakwe, S., Ukamaka Ihekoronye, V., Kim, D.-S., & Lee, J.-M. (2022). Tractable minacious drones aerial recognition and safe-channel neutralization scheme for mission critical operations. *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 1–8. doi:10.1109/ETFA52439.2022.9921494

Oubbati, O. S., Chaib, N., Lakas, A., Lorenz, P., & Rachedi, A. (2019). UAV-assisted supporting services connectivity in urban VANETs. *IEEE Transactions on Vehicular Technology*, *68*(4), 3944–3951.

Park, S., Kim, H. T., Lee, S., Joo, H., & Kim, H. (2021). Survey on Anti-Drone Systems: Components, designs, and challenges. *IEEE Access*, *9*, 42635–42659. doi:10.1109/ACCESS.2021.3065926

Plus, T. (n.d.). Why couldn't you stop the drone terror that flew 1000km?, Retrieved from http://www.vintagewings.ca/VintageNews/Stories/tabid/116/articleType/ArticleView/articleId/484/The-Mother-of-All-Drones.aspx.

Rangwala, S. (2022). *The LiDAR range wars - Mine is longer than yours*. Forbes Magazine. Retrieved from https://www.forbes.com/sites/sabbirrangwala/2021/05/27/the-lidar-range-wars-mine-is-longer-than-yours/?sh=27d80ebb3141.

Regev, J. (2023, February). War of the future: Drones playing an essential role in the Ukraine war. Retrieved from https://www.i24news.tv/en/news/ukraine-conflict/1677160351-war-of-the-future-drones-playing-a-significant-role-in-the-ukraine-war

Shi, X., Yang, C., Xie, W., Liang, C., Shi, Z., & Chen, J. (2018a). Anti-Drone System with multiple surveillance technologies: Architecture, implementation, and challenges. *IEEE Communications Magazine*, *56*(4), 68–74. doi:10.1109/MCOM.2018.1700430

Swinney, C. J., & Woods, J. C. (2022). A review of security incidents and defence techniques relating to the malicious use of small unmanned aerial systems. *IEEE Aerospace and Electronic Systems Magazine*, vol. 37, no. 5, pp. 14-28, 1 May 2022, doi: 10.1109/MAES.2022.3151308.

Svanström, F., Alonso-Fernandez, F., & Englund, C. (2021). A dataset for multi-sensor drone detection. *Data in Brief*, *39*, 107521.

Shi, Z., Chang, X., Yang, C., Wu, Z., & Wu, J. (2020). An acoustic-based surveillance system for amateur drones detection and localization. *IEEE Transactions on Vehicular Technology*, *69*(3), 2731–2739.

Vintage Wings (2020, February). The Mother of All Drones. Retrieved February 20, 0223, from http://www.vintagewings.ca/VintageNews/Stories/tabid/116/articleType/ArticleView/articleId/484/The-Mother-of-All-Drones.aspx

Xie, W., Wang, L., Bai, B., Peng, B., & Feng, Z. (2019). An mproved algorithm based on particle filter for 3D UAV target tracking. *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 1–6. doi:10.1109/ICC.2019.8762028

Yaacoub, J.-P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, *11*, 100218.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/