ADS: Study on the Anti-Drone System: Today's Capability and Limitation

Younwoo Ki*, Suhyun Chun*, Jihoon Ryoo

State University of New York, Korea and IDCITI
*Students with equal contribution
{younwoo.ki,suhyun.chun,jihoon.ryoo}@stonybrook.edu

***Abstract*—In this paper, we conduct an industry-leading examination of anti-drone systems specifically for the RCS $0.01m^2$ class, aiming to safeguard civilian establishments from escalating drone threats. Given the constraints of deploying anti-drone systems ubiquitously across all public and private facilities, our attention is directed toward emerging anti-drone technologies, both lethal and non-lethal. We carry out a succinct exploration across different stages of anti-drone defense, including detection, tracking, and soft/hard neutralization. Numerous trials across these sectors are reviewed, utilizing their insights to formulate a hypothetical model of an adaptable, cost-effective, and purpose-driven anti-drone system. Additionally, we explore prospective safety and security measures from the drone side, which may potentially invalidate current anti-drone tactics. It is our hope that this paper will serve as a practical guide for the selection of suitable anti-drone systems.**

***Index Terms*—anti-drone system, counter-drone attack, search and track and neutralization, future challenges**

I. Introduction

With the proliferation of drones for non-military purposes, the potential for drone-related incidents has seen an uptick, leading to a situation where the limitations of deploying military-grade anti-drone systems, both financial and regulatory, necessitate a review of accessible alternatives. This paper provides a condensed analysis of such technologies, categorizing them into detection, tracking, and soft/hard neutralization, and highlights the challenges faced as the drone industry advances, with regulations struggling to keep up, resulting in illegal and destructive uses. Anti-drone technologies are urgently needed for defense against malicious drone activities; however, most anti-drone systems rely on military-grade components, including RF jammers and anti-aircraft weapons, which are not suitable for civilian areas due to legal constraints, collateral damages, and potential interference with legacy telecommunication infrastructure. In response to these challenges, the paper proposes advanced solutions for civilian territories, such as using tuned radar technology, and collateral damage-free methods like hijacking or capturing drones, thereby offering an industry's choice for non-military and military-level anti-drone systems, including the consideration of recent incidents, guidelines for system design, and future technology developments.

Figure 1 displays an overview of the ADS(Anti-Drone System), emphasizing the critical consideration of the time

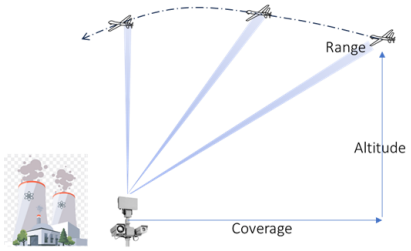

Fig. 1. Overview of the ADS

frame the ADS has from the initial intrusion to the final demolition. Table I illustrates the calculated exposure time from the initial point to the exit moment, underlining the significance of the ADS's range. For example, if the system claims a 4km range for the ADS, it can decide and react to a drone within a maximum of 2 minutes and 22 seconds to a minimum of 16 seconds; this brief window may prevent the ADS from taking proper action. Conversely, if the ADS boasts a 20km range, the system can have a more extended period, ranging from a maximum of 11 minutes and 54 seconds to a minimum of 1 minute and 20 seconds, depending on the drone's speed, providing sufficient time for appropriate response measures.

The rest of the paper is organized as follows: Section II details the first layer of the ADS, focusing on detection and tracking; Section III outlines soft-kill-based non-lethal neutralization methods; Section IV provides information on hard-kill based lethal neutralization techniques; Section V presents state-of-the-art packaged ADS from a leading technological company; Subsequent discussions on the next stage of ADS are covered in Section VI, and the paper is concluded in Section VI-D.

TABLE I
Exposed time to the ADS

Speed\Range km/h(m/s)	4km (mm:ss)	8km (mm:ss)	12km (mm:ss)	20km (mm:ss)
100(28)	2:22	4:45	7:09	11:54
200(56)	1:11	2:23	3:34	5:57
300(83)	0:48	0:36	2:25	4:01
500(139)	0:28	0:58	1:26	2:24
900(250)	0:16	0.32	0:48	1:20

TABLE II
RADAR BASED DETECTION

BAND	Frequency	Wavelength	Range(RCS $0.01m^2$)	Advantage	Disadvantage
UHF-Band	0.3∼1GHz	10∼100Cm	not as solo	penetration	low-resolution
L-Band	1∼2GHz	15∼30Cm	not as solo	moisture detection	interfere GPS
X-Band	8∼12GHz	2.5∼3.7Cm	2-5Km	long range	need combination
Ku-band	12∼18GHz	1.6∼2.4Cm	-2Km	high resolution	limited penetration

II. DETECTION - SEARCH AND TRACKING

Detection is the first layer of anti-drone defense. This section reviews various detection methods, from radar systems to camera and RF sensors, and discusses their respective merits and drawbacks.

A. Radar based approach

1) UHF-band: The UHF-band, characterized by a radio frequency range of approximately 0.3-1GHz and corresponding wavelengths of 10-100 $centimeters$, offers certain distinct advantages and challenges. Its ability to penetrate various obstacles such as leaves and buildings makes it useful for detecting drones concealed behind such barriers. However, the inherent low-resolution capabilities of the UHF-band present challenges, particularly in identifying smaller drones, leading to potential inaccuracies in drone detection [1], [2].

2) L-band: The L-band radio frequency encompasses a range from about 1 to 2GHz, with corresponding wavelengths between 30 to 15 $centimeters$. One of the L-band's distinctive characteristics is its capacity to differentiate moisture and leaves based on their contrasting radar images. When the radar encounters wet soil, the moisture absorbs the radar signal, resulting in a dark color representation. Conversely, leaves scatter the radar signals, producing brighter hues in comparison to the moisture. This unique property can be instrumental in various applications. [3]

3) X-band: The X-band radar system operates within the frequency range of 8 to 12 GHz, corresponding to wavelengths between 2.5 to 3 $centimeter$, and offers an effective detection range of up to 5 km. Although this system is proficient in detecting drones at long distances, its low resolution hinders the ability to discern environmental details, which may result in inaccurate target identification. Consequently, the X-band radar system is often integrated with other radar systems, such as the Sea-based X-band radar (SBX-1) [4], to enhance accuracy. The combined capabilities of these systems enable the detection of targets across vast distances, spanning from California to Virginia [5].

4) Ku-band: The Ku-band radio frequency operates within the range of 12 to 18 GHz, with a typical detection range falling within 2 km, although this distance can vary depending on the specific radar system employed. One of the distinguishing characteristics of Ku-band is its higher resolution compared to lower frequency radar bands, enabling more accurate drone detection. However, a notable limitation of the Ku-band lies in its susceptibility to distortions from dense foliage or other obstructions. Such interference can hinder the radar's ability to identify targets concealed behind physical barriers, thereby limiting its penetration and effectiveness in certain environments [6]

Drone radar systems are designed for the tracking, detection, and classification of drones and other aerial objects. These systems are particularly noted for their accuracy in object classification, a feature that significantly reduces false alarms caused by unrelated entities, thereby enhancing tracking precision. Additionally, drone radar systems offer comprehensive 360-degree coverage, achieved by the seamless integration of various radar devices into a cohesive sensor network [7].

Despite these advantages, drone radar systems exhibit certain limitations. Particularly, they may struggle to detect small drones and can face challenges in differentiating between drones and other small objects, such as birds. This aspect underscores the complexity of achieving precise identification in varied and dynamic aerial environments.

B. Camera based approach

1) RGB Camera: RGB cameras detect drones by capturing visual images or videos using the three primary colors in the light spectrum: red, green, and blue. This type of camera can distinguish between drones and background objects based on size, shape, and color. However, in low-light or nighttime conditions, the performance of RGB cameras may suffer significantly, causing them to fail in identifying small drones that appear as mere pixels in images [8].

2) IR Camera: Infrared (IR) cameras detect drones based on the thermal signatures or infrared radiation they emit. This enables detection even in environments where the drone would be invisible to the naked eye. However, this system may respond to other objects that emit thermal signatures, such as animals or vehicles, potentially leading to false positives in identifying non-threatening objects as illegal drones [9].

3) EO/IR Camera: EO/IR cameras combine two sensors: visible light (electro-optical) and infrared radiation, enabling the identification of drones based on their shape, size, and thermal signatures. Integration with multiple detection systems adds to their accuracy and reliability. However, significant differences in thermal radiation between drones and backgrounds, challenging weather, and low-light environments may hinder the effectiveness of this method [9], [10].

4) Thermal Camera: Thermal cameras identify drones by capturing the heat they emit. They display heat signatures as contrasting black (cold) and white (hot) regions on a screen. Their use of longer infrared wavelengths allows them to remain unaffected by disturbances such as reflective light from headlights, smoke, haze, or dust. While providing a reliable perspective for detecting drones or objects emitting

TABLE III
SOFT-KILL BASED NEUTRALIZATION

	Range(Km)	Collateral damage	Advantage	Disadvantage
RF-Jammer	2-4km	legacy communication infrastructure	mature technology	secondary damage
GNSS-Spoofing	-10km	legacy GNSS infrastructure	long range and hard to defend	complex system
Eagle-Training	-1km	-	effective to small drones	ethical issue & hard to train
Sticky-lime/nets	-1km	-	effective to small drones	have to approach close & limited range
Control take-over	-2km	-	precise targeting	very complex and hard to apply in the field
HP-EMP	-1km	legacy electronic devices	very effective	high-energy required

heat, thermal cameras are limited in their ability to identify drones emitting heat outside their field of vision, leading to potential detection failures [11], [12].

5) Lidar: Lidar (Light Detection and Ranging) is a sensing technology that employs laser pulses to generate three-dimensional maps of its surroundings. By emitting laser light pulses and timing their return, Lidar can create comprehensive 3D images, elevation maps, and valuable data swiftly and precisely. However, Lidar systems consume significantly more power and are more expensive than other drone detection cameras, constituting drawbacks in terms of cost and power efficiency [13], [14].

C. RF-scanner

1) DJI Aeroscope G8: The Aeroscope G8 system functions as a drone detection mechanism that is capable of identifying DJI-manufactured drone communication links, enabling real-time collection of crucial information such as flight status and paths. The system can achieve a monitoring range of up to 50 km and rapidly retrieve essential drone data within 2 seconds.

However, the system faces challenges in specific scenarios. For instance, its detection abilities may be compromised if a DJI-manufactured drone's ID is altered or removed. This includes the feasibility of changing a drone's MAC address using open-source products. Additionally, the system may encounter difficulties detecting older model drones produced before 2014, mainly due to the one-way transmission system utilized in those models [15], [16].

2) edgeDF: The EdgeDF-Drone is a dedicated directional detector crafted specifically for drone detection. It features a linear array antenna with four bands and sectors in a 4x4 configuration. Utilizing a directive antenna, low noise index design, and beamforming technology enables long-range drone detection. Furthermore, it incorporates Full Channel parallel reception technology and AI-based object recognition to precisely detect and identify drone signals, along with their direction.

The system also offers 360-degree multiple drone detection and direction finding, with minimal weather interference compared to other systems. An additional advantage of edgeDF lies in its enhanced privacy and security, as it processes information locally to avoid inadvertent transmission to insecure networks. However, a noted drawback of this system is its lower accuracy in detecting drones at low altitudes or those operating autonomously [17].

III. NEUTRALIZE - SOFT KILL

The second layer of defense is soft neutralization without military weapons. In this section, we survey various soft neutralization techniques - so-called soft kill, discussing their suitability and effectiveness in different scenarios. Minimizing the collateral damage is the main reason why the defender prefers soft-kill-based neutralization.

A. RF-Jammer

RF-jamming is a technique generated through a transmitter that emits RF signals, either of the same or similar frequency to the target signal, creating noise or interference that disrupts the SNR(signal-to-noise ratio) or leads to bit errors [18]. Consequently, drones may activate automatic fail-safe modes, exhibiting responses such as hovering, returning to predefined locations, or immediate landing [19], [20].

RF-jamming is notable for its wide coverage, enabling the disruption of multiple drones simultaneously. The scope of impact varies with design and power output, and limitations include range and line-of-sight requirements [21], [22]. This countermeasure offers flexibility through portable and fixed deployments [23]–[25], but may lead to unintended disruption of legitimate drone operators.

B. GNSS-Spoofing

GNSS-spoofing is a targeted intervention involving the creation of counterfeit GNSS signals that mislead the drone's receiver [26], [27]. Compared to RF-jamming, GNSS-spoofing generally requires less power but more expertise [28]. The key advantage is the potential to safely capture drones without inflicting physical damage. However, resistance to spoofing among high-end drones and the risk of unexpected behavior necessitate caution [29].

C. Eagle-training

Trained eagles or large birds of prey have been employed by military and law enforcement as drone interceptors [30], [31]. While an environmentally friendly and non-destructive approach, considerations include safety, effectiveness under various conditions, and ethical compliance [32], [33].

D. Sticky-lime or nets

The entanglement of drones using nets or sticky limes has been explored as a soft capture technique [34]. These methods, deployable from various platforms, have limitations such as effective range and proximity requirements [35]–[37].

E. Control take-over

Control take-over exploits the radio communication protocol between drones and controllers [38]–[40]. Techniques include reverse-engineering, exploiting protocol weaknesses, and packet sniffing [41]–[43]. This area poses challenges regarding the balance between security and privacy, and it is a domain of hacking.

F. High-power EMP

High-Power EMP, part of Directed Energy Weapons (DEWs), can neutralize drones by inducing currents into their circuitry [44]. Though similar to RF-jamming in some respects, EMP may cause permanent damage and its wide impact raises considerations around collateral damage [45]–[47].

IV. Neutralize - Hard Kill

The ultimate stage of defense involves the robust neutralization of drones using military-grade weaponry. In this segment, we explore an array of such forceful neutralization methods, often termed "hard kill," while discussing their applicability and efficacy under varying circumstances. The dependable outcomes provided by hard-kill-based neutralization fundamentally justify its necessity in a defender's arsenal.

A. Rifle or Short-Range Gun

Utilizing rifles or short-range firearms for counter-drone operations is contingent on various factors, with effectiveness largely hinging on individual shooter expertise and specialized equipment, such as anti-drone ammunition [48]. Despite the inherent challenges in accurately targeting drones, the development of intelligent scopes has augmented tracking and guidance capabilities, thereby enhancing the success rate of this approach [49].

B. Classic Anti-Aircraft Flak

Traditional anti-aircraft flak, characterized by artillery shells that disperse shrapnel over a broad area, may pose serious collateral damage and human endangerment in densely populated regions. Despite these drawbacks, some military contexts may still favor this approach due to its cost-effectiveness and suitability for engaging low-altitude drones. For instance, the Ukraine Army has employed and modified Yugoslavian models, such as the Zastava M75 and M55 cannons, as anti-drone weapons [50], [51].

C. Laser

Directed Energy Weapons (DEWs) like lasers offer a highly precise, long-range solution for drone engagement with minimal collateral damage [19]. This technology affords concealment advantages, particularly in operations requiring discretion. However, challenges include the attenuation of effectiveness in adverse weather conditions and the need for substantial power sources and cooling systems [52]–[55]. The development of laser-based anti-drone systems has expanded across multiple countries and corporations, reflecting diverse deployment options [56].

D. Missile

Anti-aircraft missile systems present an opportunity to neutralize distant and sophisticated drone threats, potentially averting damage to sensitive areas. Examples of such systems include South Korea's Cheongung, a long-range surface-to-air missile (SAM) system capable of detecting and tracking various aerial threats [57], and the U.S. Army's Gray Eagle drone, equipped with AGM-114 Hellfire guided missiles [58]. Nevertheless, the use of missiles against drones raises issues related to cost-effectiveness, targeting capabilities for smaller drones, potential collateral damage, and legal constraints.

V. Packaged System

Building upon our assessment of diverse technologies, we turn our attention to a contemporary, state-of-the-art anti-drone system. We undertake an exhaustive and reputation-based evaluation of the system, its prominence in the domain, its potential components, and operational protocols, consistently factoring in considerations of cost and the efficacy of deployment.

A. LIG

LIG's system employs a soft-kill method that disrupts drone control through radio wave jamming. Leveraging radar and RF scanners for initial detection, the system further refines its accuracy by utilizing Electro-Optical/Infrared (EO/IR) technology for visual identification and tracking. Upon confirming a drone as hostile, the system transmits concentrated jamming radio waves to overwhelm the drone's control systems, rendering it inoperative [59], [60].

B. Hanwha

The Hanwha system amalgamates thermal monitoring with Fortem Technologies Inc.'s drone defense system for drone detection and identification. Its thermal sensors facilitate tracking even in challenging environmental conditions. In conjunction with Fortem Technologies' real-time analysis, the system rapidly assesses threat levels and determines the appropriate response, employing physical nets to mitigate potential damage from drone debris [61], [62].

C. Rheinmetall

Rheinmetall's system incorporates diverse technologies, including X-band, S-band radars, passive emitter locators, and ADS-B receivers. By synthesizing data across these frequency bands, the system enhances detection accuracy and minimizes false alarms. A 360° PTZ sensor equipped with infrared and TV cameras ensures continuous drone tracking, further contributing to the system's precision [63].

D. Lockheed Martin

Lockheed Martin's approach employs radar systems such as the Q-53, linked to a battle management system that executes a 'kill chain' process. Upon target identification as hostile, a high-powered laser weapon system is activated, employing a beam combined from multiple fibers to neutralize the threat [64].

E. Rafael Drone Dome

Rafael's Drone Dome system integrates a spectrum of technologies, including RADAR, SIGINT/RF sensors, E/O SPEED ER sensors, a Jammer, and C4I Center, offering both hard and soft kill methods. The system employs EO sensors for long-distance detection and SIGINT/RF sensors for identifying potential threats. Soft kill methods utilize Reactive Jamming (RJ) technology, including Global Navigation Satellite System (GNSS), to disrupt control channels. Hard kill methods leverage Radar for direct target destruction [65], [66].

VI. Discussion

The present study explores various anti-drone technologies, underscoring the importance of evolving countermeasures in the rapidly changing landscape of drone capabilities. This section provides a synthesis of the main findings, linking them with existing literature, and offers insights into potential future directions for both research and practical applications.

A. Overview of Findings

The effectiveness of anti-drone measures, whether they are missile, laser, flak, or gun-based, is intrinsically linked to technological advancement, environmental conditions, and legal or regulatory constraints. Furthermore, the advent of soft-kill methods and advanced detection systems signifies a shift towards more nuanced and adaptable countermeasures. The innovative approaches represented by systems like LIG, Hanwha, Rheinmetal, Lockheed Martin, and Rafael Drone Dome highlight the diversity and complexity of the field.

B. Comparison with Existing Literature

Our findings align with previous research, demonstrating that no single solution is universally applicable to all drone threats. The need for a multifaceted approach, combining different technologies and strategies, resonates with the current trends in the anti-drone industry. The integration of radar, thermal sensors, jammers, lasers, and physical nets in various systems underlines the complexity of modern anti-drone warfare.

C. Challenges and Considerations

The results of our study indicate several challenges facing current anti-drone systems. These include the high cost of certain methods, the risk of collateral damage, and the difficulty in targeting small or low-flying drones. Legal and regulatory hurdles also present a barrier to the deployment of some technologies, particularly in populated areas.

Furthermore, weather and atmospheric conditions remain a significant challenge, especially for laser-based systems, while the need for extensive power sources and cooling can hinder mobility and deployment.

D. Future Directions

Moving forward, continued research and investment into the development of scalable, cost-effective, and environmentally considerate anti-drone systems will be vital. Cross-disciplinary collaboration, including the integration of artificial intelligence and machine learning, could pave the way for more adaptive and responsive systems.

The ethical implications of anti-drone technologies, particularly concerning privacy and safety, will likely become more prominent as these systems become more widespread. Future research should thus also focus on the societal and legal aspects of these technologies, ensuring that they are deployed responsibly and in line with international standards.

Conclusion

This paper presents a review of the current state of anti-drone technologies, identifying a range of strategies and tools that are both promising and fraught with challenges. It highlights the necessity for a multifaceted approach, one that considers not only the technological aspects but also the legal, ethical, and practical dimensions. In an era where drone usage continues to expand across various sectors, our findings offer valuable insights for policymakers, researchers, and industry professionals, providing a roadmap for future development in the field of anti-drone systems.

Acknowledgement

This work is supported by the Korean National Research Foundation grant NRF-2021R1F1A1052489, the MSIT, ICT CC Program (IITP-2019-2011-1-00783)/ICT start-up fund (RS-2022-00156555), the MOLIT start-up fund (RS-2022-00144171), and the Korea Radio Promotion Association (RAPA) XR-LAB grant. The authors are grateful to the anonymous reviewers for their valued comments and suggestions.

References

[1] A. Mîndroiu and D. Mototolea, "Drone detection," *Journal of Military Technology*, vol. 2, pp. 17–22, 06 2019.

[2] A. Coluccia, G. Parisi, and A. Fascista, "Detection and classification of multirotor drones in radar sensor networks: A review," *Sensors*, vol. 20, p. 4172, 07 2020.

[3] M. Jahangir and C. Baker, "Robust detection of micro-uas drones with l-band 3-d holographic radar," 09 2016, pp. 1–5.

[4] United States Department of Defense Missile Defense Agency, "Sea-based x-band radar (sbx-1)."

[5] D. de Quevedo, F. I. Urzaiz, J. G. Menoyo, and A. A. López, "Drone detection with x-band ubiquitous radar," in *2018 19th International Radar Symposium (IRS)*, 2018, pp. 1–10.

[6] J. Ochodnický, Z. Matousek, M. Babjak, and J. Kurty, "Drone detection by ku-band battlefield radar," in *2017 International Conference on Military Technologies (ICMT)*, 2017, pp. 613–616.

[7] Robin Radar Systems, "Drone-detection-radar." [Online]. Available: https://bit.ly/43VedSZ

[8] P. Kumar, "What are RGBD cameras?: Why RGBD cameras are preferred in some embedded vision applications?" [Online]. Available: https://bit.ly/4576baP

[9] F. Chiper, A. Martian, C. Vladeanu, M. Ion, R. Craciunescu, and O. Fratu, "Drone detection and defense systems: Survey and a software-defined radio-based solution," *Sensors*, vol. 22, p. 1453, 02 2022.

[10] B. Kim, D. Khan, C. Bohak, W. Choi, H. Lee, and M. Kim, "V-RBNN based small drone detection in augmented datasets for 3D ladar system," *Sensors*, vol. 18, p. 3825, 11 2018.

[11] Teledyne FLIR LLC, "What is the difference between active IR and thermal imaging?" [Online]. Available: http://bit.ly/457uENd

[12] P. Andraši, T. Radišić, M. Mustra, and J. Ivošević, "Night-time detection of UAVs using thermal infrared camera," *Transportation Research Procedia*, vol. 28, pp. 183–190, 01 2017.

[13] FlyGuys, "Advantages and disadvantages of lidar technology." [Online]. Available: https://bit.ly/47uMtra

[14] K. Paschalidis, "Detection of small unmanned aerial systems using a 3D lidar sensor." [Online]. Available: https://bit.ly/3OTWcjn

[15] DJI, "DJI Aeroscope." [Online]. Available: https://www.dji.com/kr/aeroscope

[16] AirSight, "DJI Aeroscope review: Features, specs, and how it's used in layered drone detection." [Online]. Available: https://bit.ly/47sfCTV

[17] HURA, "EdgeDF-Drone." [Online]. Available: http://hura.co.kr/edgeDF

[18] V. U. Castrillo, A. Manco, D. Pascarella, and G. Gigante, "A review of counter-uas technologies for cooperative defensive teams of drones," *Drones*, vol. 6, no. 3, 2022.

[19] D. Pistoia, "Detecting and neutralizing mini-drones: Sensors and effectors against an asymmetric threat," *The Journal of the JAPCC*, no. 25, pp. 81–86, 2018.

[20] Dedrone Marketing, "A primer on drone jamming techniques, spoofing, and electronic interruption of a drone." [Online]. Available: https://bit.ly/45qFZrz

[21] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, "Effective GPS jamming techniques for UAVs using low-cost SDR platforms," *Wireless Personal Communications*, vol. 115, 12 2020.

[22] M. Rutherford, "Can jammers protect airports from drones?" [Online]. Available: https://bit.ly/3YxWfEN

[23] NQDefense, "Handheld anti-drone solution." [Online]. Available: https://bit.ly/3YB1VOE

[24] Battelle Memorial Institute, "Case study: Dronedefender technology." [Online]. Available: https://bit.ly/3s0uRDd

[25] Blighter Surveillance Systems Ltd., "AUDS anti-UAV defence system." [Online]. Available: https://bit.ly/458aAu4

[26] S. Khan, M. Mohsin, and W. Iqbal, "On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions," *PeerJ Computer Science*, vol. 7, p. e507, 05 2021.

[27] H. Kim, J. Park, S. Park, and J. Ryoo, "uGPS: Design and field-tested seamless gnss infrastructure in metro city," in *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, ser. MobiCom '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 636–647. [Online]. Available: https://doi.org/10.1145/3495243.3560520

[28] J. Gaspar, R. Ferreira, P. Sebastião, and N. Souto, "Capture of UAVs through GPS spoofing using low-cost SDR platforms," *Wireless Personal Communications*, vol. 115, 12 2020.

[29] R. N. Charette, "Drones and GPS spoofing redux." [Online]. Available: https://bit.ly/3DXxetn

[30] T. Essary, "These drone-hunting eagles aren't messing around." [Online]. Available: https://bit.ly/3QD8ZIp

[31] E. Ackerman, "Dutch police buy four eagle chicks for anti-drone flying squad." [Online]. Available: https://bit.ly/3QDeE1k

[32] BBC News, "Eagles trained to take down drones." [Online]. Available: https://bbc.in/3YFzuPp

[33] K. D. Atherton, "Can birds be trained to bring down drones?" [Online]. Available: https://bit.ly/3KDRwfe

[34] U.S. Defense Advanced Research Projects Agency (DARPA), "Mobile force protection demonstration." [Online]. Available: https://bit.ly/3QCYhBD

[35] Delft Dynamics, "Dronecatcher: A Delft Dynamics product." [Online]. Available: https://dronecatcher.nl/

[36] OpenWorks Engineering Ltd., "Skywall Auto." [Online]. Available: https://bit.ly/446aWjF

[37] K. D. Atherton, "Drone catcher drone fires nets at lesser drones." [Online]. Available: https://bit.ly/3DSeCLp

[38] K. Domin, E. Marin, and I. Symeonidis, "Security analysis of the drone communication protocol: Fuzzing the mavlink protocol," 2016. [Online]. Available: https://bit.ly/3s7kihQ

[39] TS2 Space, "What are the different types of communication protocols used on drones?" [Online]. Available: https://bit.ly/3Yy6jxG

[40] F. Trujano, B. Y. Q. Chan, and R. R. May, "Security analysis of DJI Phantom 3 standard," 2016. [Online]. Available: https://bit.ly/3sbBYJj

[41] S. Walters, "How can drones be hacked?: The updated list of vulnerable drones attack tools." [Online]. Available: https://bit.ly/3qvrYtL

[42] N. Nelson, "Hack allows drone takeover via 'ExpressLRS' protocol." [Online]. Available: https://bit.ly/3qCGPm9

[43] A. Luo, "Drones hijacking: multi-dimensional attack vectors and countermeasures." [Online]. Available: https://bit.ly/3KG25OW

[44] S.-G. Kim, E. Lee, I.-P. Hong, and J.-G. Yook, "Review of intentional electromagnetic interference on UAV sensor modules and experimental study," *Sensors*, vol. 22, no. 6, p. 2384, 2022.

[45] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, pp. 100–218, 2020.

[46] J. Gabay, "Jamming and anti-jamming technologies for RF links." [Online]. Available: https://bit.ly/4583hm7

[47] B. P. Routray, "Chinese EMP test to counter unmanned aerial systems: Analysis." [Online]. Available: https://bit.ly/3s9fclf

[48] Ministry of Defense, "Game-changing anti-drone weapon sight for army's close combat soldiers." [Online]. Available: https://bit.ly/3s9NjcO

[49] Smart Shooter Inc., "Our systems: Smart-shooter." [Online]. Available: https://bit.ly/45pWC6z

[50] S. Roblin, "America is slapping cannons on trucks to help Ukraine stop Russia's killer drones." [Online]. Available: https://bit.ly/459KWp4

[51] ——, "To stop killer drones, Ukraine upgrades ancient flak guns with consumer cameras and tablets." [Online]. Available: https://bit.ly/3s9xxi0

[52] J. Hecht, "Lasers versus drones: Can lasers be a solution for the drone problem?" [Online]. Available: https://bit.ly/3KDSh84

[53] D. Halan, "Counter-drone techniques to detect and neutralise hostile drones." [Online]. Available: https://bit.ly/44aFyR7

[54] EchoBlue Ltd., "Anti drone technology and CUAS systems." [Online]. Available: https://bit.ly/447mxio

[55] Y. Lim, Y. W. Choi, and J. Ryoo, "Study on laser-powered aerial vehicle: Prolong flying time using 976nm laser source," in *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, 2021, pp. 1220–1225.

[56] Boeing, "Laser-focused battlefield defense." [Online]. Available: https://bit.ly/3OS5MDA

[57] Agency for Defense Development (ADD), "Missile systems." [Online]. Available: https://bit.ly/3YNY157

[58] General Atomics, "Gray eagle." [Online]. Available: https://bit.ly/3qvswzP

[59] LIG Nex1, "Anti-drone protection system towards national major facilities." [Online]. Available: https://bit.ly/3YwBKZk

[60] L. Chang-won, "LIG Nex1 leads military project to develop jammer capable of neutralzing N. Korean drones." [Online]. Available: https://bit.ly/3s4NVjH

[61] Y. Young-sil, "Hanwha systems completes successful demonstration of anti-drone system." [Online]. Available: https://bit.ly/3OTXuLf

[62] K. Lee, "Hanwha systems demonstrates anti-drone system using physical nets." [Online]. Available: https://bit.ly/45K9wNd

[63] Rheinmetall AG, "Drone defense toolbox: Protection for civilian and military infrastructure." [Online]. Available: https://bit.ly/3OXlWM8

[64] Lockheed Martin Corporation, "Technology that counters drone swarms," 06 2016. [Online]. Available: https://lmt.co/3EdU549

[65] Rafael Advanced Defense Systems Ltd., "Drone Dome™ – C-UAS." [Online]. Available: https://bit.ly/3QDaQNn

[66] "Drone Dome™ – C-UAS, drone detection, neutralization and interception system." [Online]. Available: https://bit.ly/3Yy7qgQ