Buravchenko, K. O. (2024). Analyzing the methods of protection against First-Person View drone. *Actual Issues of Modern Science. European Scientific e-Journal, 31*, __-__. Ostrava: Tuculart Edition, European Institute for Innovation Development.

DOI: 10.47451/inn2024-05-04

The paper is published in Crossref, ICI Copernicus, BASE, Zenodo, OpenAIRE, LORY, Academic Resource Index ResearchBib, J-Gate, ISI International Scientific Indexing, ADL, JournalsPedia, Scilit, EBSCO, Mendeley, and WebArchive databases.

Kostiantyn O. Buravchenko, Candidate in Engineering Sciences (Automation of Control Processes),
Senior Lecturer, Central Ukrainian University. Kropyvnytskyi, Ukraine.
ORCID 0000-0001-6195-7533

Analyzing the methods of protection against First-Person View drone

Abstract: The rapid growth of the drone industry has exceeded regulations for secure and safe drone operation, which makes them representative means of illegal and destructive terrors and crimes. With the introduction of drones into civilian technology, drones are now gaining attention as a threat to safety and security, which leverages the emergence of anti-drone (or counter-drone) technologies. Anti-drone systems are used to defend against drone accidents or terrorism. Currently, anti-drone systems preferably adapt military components to reach the confirmatory destruction of drones. However, several difficulties apply when locating military anti-drone systems in civilian areas. Military counter-drone systems often use jamming systems to attack the target drone control channel. The jammer generates an extremely high amplitude of radio signal in the target frequency band to prevent communication. However, for non-military applications, RF jamming to protect against high-speed drone risks potentially paralyzes existing wireless network systems, such as mobile access or wireless sensor networks. Thus, most national regulations prevent non-military use of jamming systems, and therefore civilian anti-drone systems should investigate other approaches to prevent illegal or unauthorized drones. Previously, radar was considered a less effective method for detecting drones due to the rigid nature of radar cross-sections (RCS). However, advancements in radar technology have now made it possible to detect a wide range of drones with a satisfactory level of accuracy. As a result, radar is increasingly being utilized for long-range drone detection. Despite this progress, the deployment of radar technology is still subject to national regulations, including RF licensing policies. The challenges and significant expenses associated with setting up drone detection radars have led civilian counter-drone initiatives to explore alternative detection techniques, such as optical (vision-based) systems and RF signal detection methods. Civilian approaches to neutralizing drones typically involve non-lethal tactics such as system takeover or net capture. These tactics serve as a technical counterbalance to the drones' inherent safety and stability features, and there is a growing demand for research into both aspects. To make significant progress in this competitive field, it's crucial to systematically enhance anti-drone systems. This involves designing them to counteract drones' defensive maneuvers by adaptively countering their evasion techniques. This requires a thorough assessment of the latest research in drone security and safety, aiming to improve upon traditional drone functionalities. The author conducts an extensive analysis of anti-drone measures. In light of recent drone-related disturbances, we focus on identifying the specific needs of anti-drone systems. The study proposed a new FPV protection method, reducing equipment weight, cost, and autonomy.

Keywords: anti-drone systems, drone detection, jamming technique, software-defined radio drone detection.

Introduction

The rapid growth of the drone industry has exceeded regulations for secure and safe drone operation, which makes them representative means of illegal and destructive terrors and crimes. With the introduction of drones into civilian technology, drones are now gaining attention as a threat to safety and security, which leverages the emergence of anti-drone (or counter-drone) technologies. Anti-drone systems are used to defend against drone accidents or terrorism. Currently, anti-drone systems preferably adapt military components to reach the confirmatory destruction of drones. However, several difficulties apply when locating military anti-drone systems in civilian areas. Military counter-drone systems often use jamming systems to attack the target drone control channel. The jammer generates an extremely high amplitude of radio signal in the target frequency band to prevent communication. However, for non-military applications, RF jamming to protect against high-speed drones potentially paralyzes existing wireless network systems, such as mobile access or wireless sensor networks. Thus, most national regulations prevent non-military use of jamming systems, and therefore civilian anti-drone systems should investigate other approaches to prevent illegal or unauthorized drones. Previously, radar was considered a less effective method for detecting drones due to the rigid nature of radar cross-sections (RCS). However, advancements in radar technology have now made it possible to detect a wide range of drones with a satisfactory level of accuracy. As a result, radar is increasingly being utilized for long-range drone detection. Despite this progress, the deployment of radar technology is still subject to national regulations, including RF licensing policies. The challenges and significant expenses associated with setting up drone detection radars have led civilian counter-drone initiatives to explore alternative detection techniques, such as optical (vision-based) systems and RF signal detection methods. Civilian approaches to neutralizing drones typically involve non-lethal tactics such as system takeover or net capture. These tactics serve as a technical counterbalance to the drones' inherent safety and stability features, and there is a growing demand for research into both aspects. To make significant progress in this competitive field, it is crucial to systematically enhance anti-drone systems. This involves designing them to counteract drones' defensive maneuvers by adaptively countering their evasion techniques. This requires a thorough assessment of the latest research in drone security and safety, aiming to improve upon traditional drone functionalities.

Currently, the market offers a wide variety of drones for purchase (*Chadwick, 2017*; *Counter drone system, 2017*; *FCC…, 2011*; *Floreano & Wood, 2015*; *Mazar, 2016*; *Nuss, 2017*; *Ritchie et al., 2017*; *Shapir, 2013*; *UK…, 2006*; *Wellig, 2018*). Among these, First-Person View (FPV) drones are sometimes utilized for illicit activities. The subsequent sections will discuss drone detection and various protection mechanisms. An analysis of the pros and cons of numerous strategies will be provided. The primary emphasis will be on personal protection systems, which are expected to be lighter, more cost-effective, and offer greater autonomy compared to their stationary counterparts.

The results of the study

Drone Detection

Drone detection systems (*Aker & Kalkan, 2017*; *Andraši et al., 2017*; *Ding et al., 2018*; *Drone detection systems, 2017*; *Guvenc et al., 2018*; *Saqib et al., 2017*; *Spynel Series, 2020*) utilize a range of characteristics exhibited by drones in flight. Typically, drones generate thermal emissions, acoustic signals, and radio frequency (RF) signals for communication with their controllers. These systems gather data from sensors to verify if drones are present in the vicinity. Based on the collected data, they can pinpoint the probable locations of the drones.

The table in the Appendix presents a classification of drone detection methods according to the type of sensing technology used (*Table 1*). Subsequent subsections delve into each detection approach, examining their fundamental operations and inherent technical constraints.

(A) Thermal Detection

Key drone components like motors, batteries, and electronics emit heat detectable by thermal imaging devices. Research has focused on identifying drones by these thermal footprints. For instance, Andraši et al. (*2017*) suggested a method to spot drones by the heat they emit mid-flight. The Spynel product offers 360° monitoring by detecting infrared radiation from drones.

Thermal detection stands out for its resilience to weather conditions, ability to identify targets, and cost-effectiveness compared to radar systems. However, its effective range is limited to about 51 meters, posing challenges in refining detection detail and improving thermal camera resolution.

(B) RF Scanner

Drones under remote control communicate via RF signals, transmitting sensor data and flight instructions. RF scanners intercept these signals to confirm drone presence. Basic RF detection relies on signal intelligence (SIGINT) and communication intelligence (COMINT). Al-Sa'd et al. developed a deep learning system to classify drone types and flight patterns (*Al-Sa'd et al., 2019*; *RF-300…, 2020*; *The UAS…, 2020*). While more drone types can reduce classification precision, the overall detection rate remains high. DJI's Aeroscope system specializes in capturing control signals from DJI drones.

The primary limitation of RF scanning is its inability to detect drones that do not consistently emit RF signals, such as those on autonomous flights. Additionally, drones with unfamiliar control protocols or operating on different frequency bands pose detection challenges. Despite these drawbacks, RF scanners are widely used for their extended range and affordability, often in conjunction with other detection methods.

(C) Radar-Based Detection

Radar systems identify physical objects and assess their form, distance, velocity, and trajectory by analyzing the radio signals they reflect. Unlike RF scanners, which decode the signal itself, radar systems calculate the object's position by measuring the time it takes for the reflected signal to return. Continuous-wave radar is distinct in its ability to gauge the velocity of a target by utilizing both range data and Doppler shift information.

(D) Optical Camera Detection

Optical camera detection, akin to thermal detection, has been extensively researched for its application in anti-drone systems. Researchers like Sapkota et al. (*2016*) have utilized features such as the histogram of oriented gradients to identify drones in images, while Jung et al. (*2018*) have developed real-time video surveillance systems capable of monitoring expansive three-dimensional areas. Optical camera-based drone detection systems are notably cost-effective and subject to fewer regulatory constraints, facilitating the implementation of detailed tracking through widespread deployment. However, they do face limitations such as limited range, dependency on clear weather conditions, and obstruction by physical barriers, necessitating their integration with other sensor systems. Military-grade electro-optical/infrared (EO/IR) systems, which combine optical and infrared sensors, are commonly used for drone detection.

(E) Acoustic Signal Detection

Acoustic signal detection leverages the sound emitted by drone motors, a distinctive characteristic of drones. Innovations by Kim et al. (*2017*) in machine learning using plotted image analysis and k-nearest neighbors algorithms have yielded accuracies of 83% and 61%, respectively. Despite these advancements, challenges such as limited detection range and the complexities of measuring direction and tracking drones persist.

Figure 4 illustrates a comparison of various drone detection components, highlighting their functional capabilities and respective detection ranges. It shows that radar systems boast a significant minimum detection range due to their fundamental operating principles. Many providers are now offering hybrid drone detection systems that combine different technologies to enhance reliability, precision, and ease of installation. Some systems are fully automated, integrating detection and countermeasures like targeting and jamming, although the use of jammers is heavily restricted in most jurisdictions. Consequently, non-military drone countermeasure systems must carefully consider a broad spectrum of factors, including jamming restrictions, compatibility with existing radar setups, and drone neutralization methods.

Drone Neutralization

Drone neutralization is a critical aspect of anti-drone systems, aimed at curtailing the movement of hostile drones. These neutralization techniques are broadly categorized into destructive and non-destructive types. This categorization is significant as it reflects not only the technical challenges involved but also compliance with civil regulations. Given that the destruction of unauthorized drones is outlawed in numerous nations, non-destructive methods are often favored by public institutions. Our focus is primarily on non-destructive strategies to ensure the effective deployment of anti-drone systems even in dire situations.

Typically, definitive methods like jamming are utilized to avert additional emergencies such as unintended landings or crashes and operational malfunctions. While jamming is both definitive and non-destructive, it does induce a temporary halt in communications within the affected vicinity. Consequently, modern tactics are designed to selectively disrupt individual drones based on their operational characteristics. A variety of prevalent drone neutralization solutions are enumerated in Table 2 (*Appendix*), with each method being elaborated upon in subsequent sections.

A) Drone Hijacking

In the realm of anti-drone measures, the terms "hijacking" and "spoofing" are often mistakenly used as synonyms. To enhance clarity, we distinguish between the two in this document. "Hijacking" refers to the act of an anti-drone operator taking over control of a target drone by any means necessary. In contrast, "spoofing" involves creating a false signal to disrupt the intended movement of the drone as directed by its original controller. The key distinction lies in the aftermath of the attack: post-hijacking, the original controller loses all control over the drone, whereas spoofed signals may lead to drone hijacking.

The rationale behind these definitions' centers on the imperative of control deprivation. Seizing control from the original operator may entail tactics like jamming or hacking before the anti-drone system gains actual control. While hijacking presents both technical and regulatory challenges, it offers greater robustness compared to spoofing once control is successfully usurped. Nonetheless, both methods warrant thorough investigation for assured defense.

Drones typically maintain a secure, paired connection with their operator, and hijacking aims to sever this link. Trujano et al. (*2016*) introduced a system that disrupts the pairing with a jamming signal, and then swiftly reconnects the drone to the attacker's controller. Donatti et al. (*2016*) developed a hijacking system that amplifies the RF signal to take control. They explored drone control packet decoding and demonstrated their system with a working model. Hijacking is preferable for safely capturing or landing drones and aids in subsequent inquiries. However, challenges such as expanding coverage and adapting to various measures like autonomous flight and drone communication protocols remain.

(B) Drone Spoofing

Spoofing involves manipulating drone signals to either commandeer the drone or alter its flight path. Drones typically navigate using the operator's RF signal for location and altitude, while relying on sensor data for their current status. GPS signals are crucial for determining a drone's position, whether in manual or autonomous mode. Noh et al. (*2019*) devised a system that emits counterfeit GPS signals, tricking the drone's GPS receiver and causing it to miscalculate its location. This system aims to covertly redirect the drone, particularly when it enters GPS failsafe mode. Simple spoofing methods can exploit various sensor types and may be used in tandem. While deceiving drone sensors is feasible through numerous strategies, the lack of additional safety protocols for certain areas can lead to incidents like crash landings due to loss of control by the drone operator.

(C) Geofencing

Geofencing-based drone neutralization systems prevent drones from entering designated areas. The most common implementation allows drones to autonomously decide whether to land based on their current location (*Hermand et al., 2019*). There are two main types of geofence technology: dynamic geofences, which disseminate information about no-fly zones, and static geofences, which rely on a repository of flight permission data accessible to drones. Most commercial drones equipped with standard flight control stacks, such as PX4 and ArduPilot, feature built-in auto-landing for safety (*ArduPilot Documentation, 2016*; *Meier et al., 2015*). This effectively deters hobby drones from unauthorized areas but is ineffective against drones that have been modified to bypass these systems. Since geofencing depends on the drone's internal navigation, malfunctioning drones could still breach secure zones. Further research into proactive geofencing is needed to overcome these issues, potentially incorporating spoofing and hijacking methods.

(D) Drone Jamming

Drone jamming incapacitates the communication link between a drone and its controller by flooding the frequency range with overpowering RF signals. These signals, often empty packets, disrupt the drone's ability to receive legitimate commands, rendering it uncontrollable. Jamming technologies are diverse, tailored to specific goals and coverage areas, and can be categorized as follows:

- Directional vs. Omnidirectional: Directional jamming targets a specific path, while omnidirectional jamming affects all directions.
- Stationary vs. Mobile: Stationary jamming is fixed to a location like a base station, whereas mobile jamming is deployed from portable units, such as handheld devices or vehicle mounts.
- Narrow vs. Wide Bandwidth: The bandwidth of the jamming signal can be narrow, affecting a specific frequency, or wide, covering a broader spectrum.
- GPS vs. Communication Jamming: GPS jamming disrupts a drone's navigation systems, while communication jamming interrupts the control signals from the operator.

Some jammers target specific network layers, but as drones often use non-standard communication protocols, these methods are not detailed here. Jamming is favored in anti-drone systems for its simplicity, reliability, and broad range. However, due to its potential to interfere with other electromagnetic communications, including TV, telecommunication, and air traffic control, its use is heavily regulated or prohibited in many countries.

(E) Killer Drones

"Killer drones" refer to legal drones designed to pursue and physically disable target drones. Unlike drone capture methods, killer drones aim to make contact and cause damage. They require swift, accurate decision-making, precise path estimation, and high durability. Although still in early development, swarming killer drones with collective intelligence and precise tracking could become an effective multi-target neutralization strategy. Regulatory constraints similar to those on jamming and radar technologies apply, but advancements in drone management systems could ease these restrictions.

(F) Drone Capture

Drone capture methods involve physically restraining a target drone using tools like nets. Capture systems are bifurcated into:

- Terrestrial Capture: Operated by humans or vehicles, these systems offer a variety of net sizes and capacities.
- Aerial Capture: Mounted on defender drones, these systems are limited by the carrying capacity but offer greater precision and speed.

The choice between terrestrial and aerial capture depends on various factors, including device coverage, cost-performance balance, and the drones' load-bearing capacity. Both methods have their merits and should be further explored. As drone neutralization techniques leverage the operational characteristics of drones, they can trigger unintended behaviors. Therefore, a comprehensive approach that combines multiple neutralization strategies is essential to increase success rates. It is also crucial to keep pace with drone safety technologies like anti-spoofing and anti-hijacking. Anti-drone systems must strategically plan neutralizations, taking into account the effective range and anticipated flight paths of target drones.

Summary

Drone Detection: The integration of multiple detection systems has led to a moderate success rate in drone detection. Despite limitations like range and weather dependency, the industry is moving towards hybrid systems for better efficiency. We have provided guidelines for setting up these systems, emphasizing the need for a strategic analysis of the defense area and the importance of a cohesive drone identification network for effective tracking and neutralization.

Drone Identification: Still in its nascent stages, drone identification systems are crucial for regulatory compliance and are expected to become more significant than detection systems alone. The potential for attaching active transponders to drones is being explored, which will be vital for managing airspace, especially with the rise of the Personal Air Vehicle (PAV) industry.

We have categorized neutralization techniques into destructive and non-destructive, noting that non-destructive methods may become obsolete due to advancements in drone security. While jamming is prevalent, its aggressive nature and the development of anti-jamming technologies call for alternative strategies. Geofencing could mitigate risks from authorized drones, but physical defenses may be necessary for deliberate threats.

Anti-drone systems must be multifaceted, incorporating various neutralization techniques to ensure robust defense. Our guidelines provide a framework for assessing drone threats and formulating safe neutralization strategies. As the field evolves, the design of anti-drone systems must adapt to address the challenges posed by sophisticated drones without relying on military-grade weaponry. Our survey aims to contribute to the expansion of drone safety zones and the advancement of anti-drone technologies.

In the study presented, we introduce an innovative approach to enhance the efficiency of anti-drone jamming systems for individual use. The system is composed of two main components: a drone detection subsystem and a jamming subsystem, as illustrated in the accompanying block diagram (*Figure 1*). Traditional non-stationary jamming systems are plagued by significant drawbacks, such as excessive weight and the tendency to jam across broad frequency bands. Our solution to mitigate these issues involves the utilization of a single amplifier in conjunction with multiple antennas, replacing the need for numerous individual amplifier units. This amplifier is designed to accommodate various commonly utilized frequencies and to switch between different narrow-band antennas. The key benefit of this system lies in the employment of a microprocessor to generate a diverse range of frequencies.

For the identification of commonly employed frequencies and amplitudes, we employ the technique of software-defined radio (SDR). The SDR module is tasked with receiving signals across a wide frequency band and pinpointing the peak signals. Upon detection of a drone's control frequency, the microprocessor module is triggered to initiate jamming on that specific frequency.

This proposed methodology significantly boosts the power output of the module while simultaneously reducing the overall weight of the device. The need for multiple amplifiers is eliminated, as we now require only a solitary amplifier capable of adjusting its frequency range to suit various needs.

Discussion

The article in question sets out to conduct a thorough examination of First-Person View (FPV) drone protection systems. It delves into the merits and demerits of various methodologies. The jamming system we propose is designed to address and rectify certain shortcomings present in existing systems. Future research endeavors could potentially explore the operational range, energy efficiency, and economic feasibility of such systems.

Conclusion

It is worth noting that the proliferation of drones, particularly FPV models, presents both opportunities and challenges. While they offer innovative applications, their potential misuse for criminal activities cannot be ignored. The exploration of drone detection and protection mechanisms is therefore crucial. The strategies discussed highlight a range of techniques, each with its own set of advantages and limitations. Emphasizing personal protection, the ideal system would combine reduced weight, lower costs, and enhanced autonomy, distinguishing itself from more cumbersome stationary systems. Such advancements promise to bolster security measures while maintaining accessibility and ease of use for individuals seeking to safeguard their privacy and safety in an increasingly drone-populated airspace.

References:

143 flights cancelled at Frankfurt Airport due to drone sightings. (2019, May). *The Local.* https://www.thelocal.de/20190509/disruption-after-frankfurt-airport-halts-flights-due-to-drone-sighting

Aker, C., & Kalkan, S. (2017). Using deep networks for drone detection. *14th IEEE International Conference on Advanced Video and Signal-Based Surveillance (AVSS)*, 1-6.

Al-Sa'd, M. F. et al. (2019). RF-based drone detection and identification using deep learning approaches: An initiative towards a large open-source drone database. *Future Generation Computer Systems*, *100*, 86-97.

ArduPilot Documentation. (2016). *ArduPilot*. https://ardupilot.org/ardupilot/

Andraši, P. et al. (2017). Night-time detection of UAVs using a thermal infrared camera. *Transportation Research Procedia*, *28*, 183-190.

Chadwick, A. (2017). Micro-drone detection using software-defined 3G passive radar. *Proceedings of the 18th International Radar Symposium (IRS)*, 1-6.

Counter drone system. (2017, September). *Google Patents*. https://patents.google.com/patent/US20170261613A1/en

Ding, G. et al. (2018). An amateur drone surveillance system based on the cognitive Internet of Things. *IEEE Communications Magazine*, *56*(1), 29-35.

Donatti, M. M. et al. (2016). Radiofrequency spoofing system to take over law-breaking drones. *2016 IEEE MTT-S Latin America Microwave Conference (LAMC)*, 1-3.

Drone detection systems. (2017, March). *Google Patents*. https://patents.google.com/patent/US20170092138A1/en

Floreano, D., & Wood, R. J. (2015). Science, technology, and the future of small autonomous drones. *Nature*, *521*(7553), 460-466.

FCC Enforcement Advisory Cell jammers GPS jammers and other jamming devices. (2011, February). Washington.

Gatwick Airport drone attack: Police have no lines inquiry. (2019, September). *BBC News*. https://www.bbc.com/news/uk-england-sussex-49846450

Gibbons-Neff, T. (2016, October 11). ISIS used an armed drone to kill two Kurdish fighters and wound French troops report says. *The Washington Post*. https://www.washingtonpost.com/news/checkpoint/wp/2016/10/11/isis-used-an-armed-drone-to-kill-two-kurdish-fighters-and-wound-french-troops-report-says/

Guvenc, I. et al. (2018). Detection tracking and interdiction for amateur drones. *IEEE Communications Magazine*, *56*(4), 75-81.

Hermand, E. et al. (2019). Drone Geofencing in Constrained Environments. *1st ID2Move Belgian Academic Seminar on Autonomous System*.

Hubbard, B., Karasz, P., & Reed, S. (2019, September 14). Two major Saudi oil installations hit by drone strike and US blames Iran. *The New York Times*. https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html

Jung, J. et al. (2018). AVSS: Airborne video surveillance system. *Sensors*, *18*(6), 1939.

Kim, J. et al. (2017). Real-time UAV sound detection and analysis system. *2017 IEEE Sensors Applications Symposium (SAS)*, 1-5.

Mazar, H. (2016). *Radio spectrum management: Policies regulations and techniques*. Hoboken.

Massachusetts man charged with plotting attack on Pentagon and U.S. capitol and Attempting to Provide Material Support to a Foreign Terrorist Organization. (2011). *FBI Archives*. https://archives.fbi.gov/archives/boston/press-releases/2011/massachusetts-man-charged-with-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-material-support-to-a-foreign-terrorist-organization

Meier, L., Honegger, D., & Pollefeys, M. (2015). PX4: A node-based multithreaded open-source robotics framework for deeply embedded platforms. *2015 IEEE International Conference on Robotics and Automation (ICRA)*, 6235-6240.

Nguyen, P. et al. (2016). Investigating cost-effective RF-based detection of drones. *2nd Workshop Micro Aerial Vehicle Network Systems and Applications Civilian Use*, 17-13.

Nuss, B. et al. (2017). MIMO OFDM radar system for drone detection. *Proceedings of the 18th International Radar Symposium (IRS)*, 1-9.

Noh, J. et al. (2019). Tractor beam: Safe-hijacking of consumer drones with adaptive GPS spoofing. *ACM Transactions on Privacy and Security*, *22*(2), 1-26.

RF-300 Data Sheet. (2020). *Dedrone*. https://assets.website-files.com/58fa92311759990d60953cd2/5d1e14bc96a76a015d193225_dedrone-rf-300-data-sheet-en.pdf

Ripley, C. W. (2015, April 22). A drone with radioactive material found on the Japanese Prime Minister's roof. *CNN*. https://edition.cnn.com/2015/04/22/asia/japan-prime-minister-rooftop-drone/index.html

Ritchie, M., Fioranelli, F., & Borrion, H. (2017). Micro UAV crime prevention: Can we help Princess Leia? In *Crime Prevention 21st Century* (pp. 359-376). New York: Springer.

UK Public General Acts Wireless Telegraphy ACT 2006. (2006). London.

Sapkota, K.R. et al. (2016). Vision-based Unmanned Aerial Vehicle detection and tracking for sense and avoid systems. *2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 1556-1561.

Saqib, M. et al. (2017). A study on detecting drones using deep convolutional neural networks. *14th IEEE International Conference on Advanced Video and Signal-Based Surveillance (AVSS)*, 1-5.

Shapir, Y. (2013). Lessons from the Iron Dome. *Military Strategic Affairs*, *5*(1), 81-94.

Spynel Series. (2020, July). *HGH Infrared Systems*. https://www.messe-essen-digitalmedia.de/uploads/E302/pdf/company/hgh-infrared-systems-f9d3f-info.pdf

Syria war: Russia thwarts drone attack on Hmeimim Airbase. (2018, January). *BBC News*. https://www.bbc.com/news/world-europe-42595184

The UAS UAV drone threat vector. (2020, July). *CRFS*. https://pages.crfs.com/hubfs/CR-002800-GD-2-DroneDefense%20Brochure.pdf

Trujano, F. et al. (2016). *Security analysis of DJI phantom 3 standard*. Cambridge.

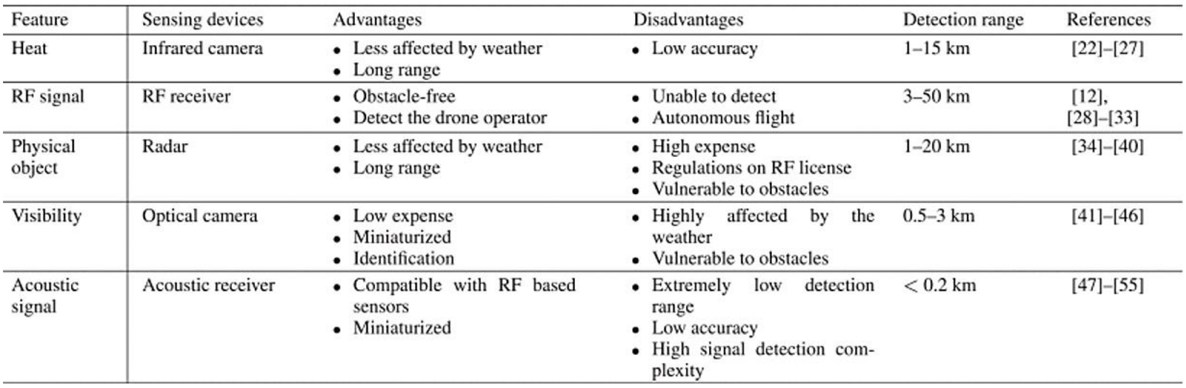
Venezuela President Maduro survives a drone assassination attempt. (2018, August). *BBC News*. https://www.bbc.com/news/world-latin-america-45073385

Wagoner, A. R., Schrader, D. K., & Matson, E. T. (2017). Towards a vision-based targeting system for counter unmanned aerial systems (CUAS). *IEEE International Conference of Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*, 237-242.

Wellig, P. et al. (2018). Radar systems and challenges for C-UAV. *Proceedings of the 19th International Radar Symposium (IRS)*, 1-8.

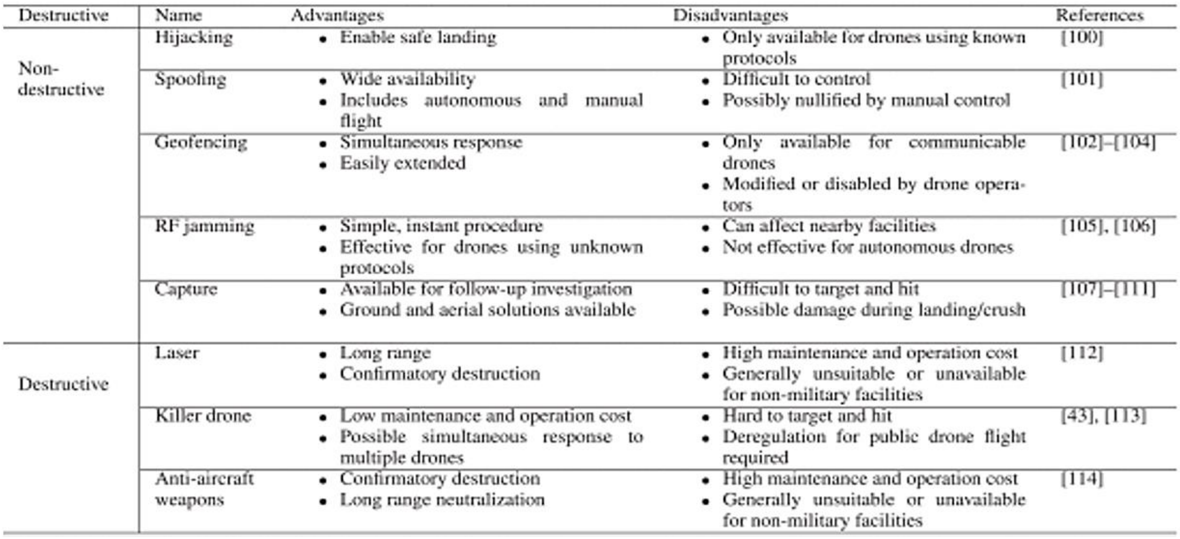
Appendix

Table 1. Drone Detection Technologies



Feature	Sensing devices	Advantages	Disadvantages	Detection range	References
Heat	Infrared camera	• Less affected by weather • Long range	• Low accuracy	1–15 km	[22]–[27]
RF signal	RF receiver	• Obstacle-free • Detect the drone operator	• Unable to detect • Autonomous flight	3–50 km	[12], [28]–[33]
Physical object	Radar	• Less affected by weather • Long range	• High expense • Regulations on RF license • Vulnerable to obstacles	1–20 km	[34]–[40]
Visibility	Optical camera	• Low expense • Miniaturized • Identification	• Highly affected by the weather • Vulnerable to obstacles	0.5–3 km	[41]–[46]
Acoustic signal	Acoustic receiver	• Compatible with RF based sensors • Miniaturized	• Extremely low detection range • Low accuracy • High signal detection complexity	< 0.2 km	[47]–[55]

Table 2. Drone Neutralization Technologies



Destructive	Name	Advantages	Disadvantages	References
Non-destructive	Hijacking	• Enable safe landing	• Only available for drones using known protocols	[100]
	Spoofing	• Wide availability • Includes autonomous and manual flight	• Difficult to control • Possibly nullified by manual control	[101]
	Geofencing	• Simultaneous response • Easily extended	• Only available for communicable drones • Modified or disabled by drone operators	[102]–[104]
	RF jamming	• Simple, instant procedure • Effective for drones using unknown protocols	• Can affect nearby facilities • Not effective for autonomous drones	[105], [106]
	Capture	• Available for follow-up investigation • Ground and aerial solutions available	• Difficult to target and hit • Possible damage during landing/crush	[107]–[111]
Destructive	Laser	• Long range • Confirmatory destruction	• High maintenance and operation cost • Generally unsuitable or unavailable for non-military facilities	[112]
	Killer drone	• Low maintenance and operation cost • Possible simultaneous response to multiple drones	• Hard to target and hit • Deregulation for public drone flight required	[43], [113]
	Anti-aircraft weapons	• Confirmatory destruction • Long range neutralization	• High maintenance and operation cost • Generally unsuitable or unavailable for non-military facilities	[114]

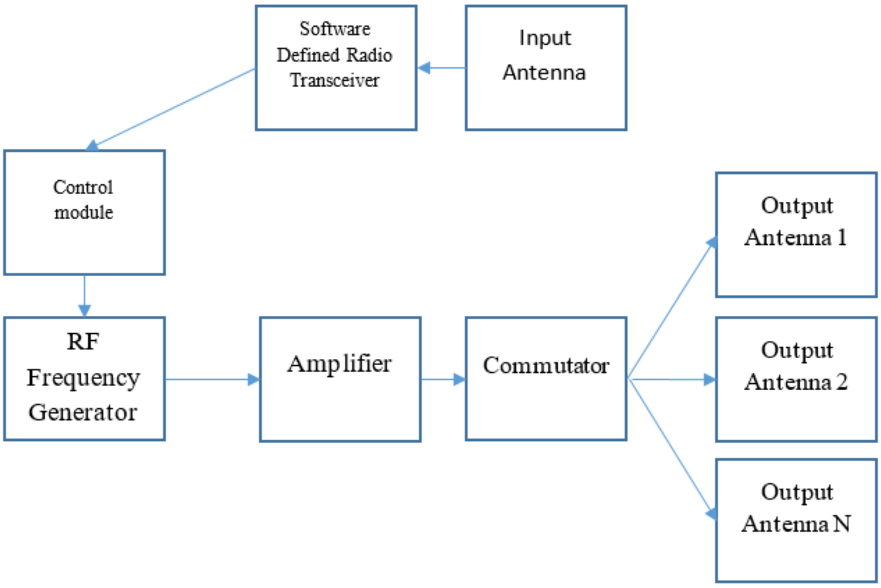


Figure 1. The diagram of the system, composed of two main components: a drone detection subsystem and a jamming subsystem