sensors

MDPI

Review

Drone Detection and Defense Systems: Survey and a Software-Defined Radio-Based Solution

Florin-Lucian Chiper, Alexandru Martian *, Calin Vladeanu, Ion Marghescu, Razvan Craciunescu and Octavian Fratu

Telecommunications Department, University Politehnica of Bucharest, 060042 Bucharest, Romania; florin_lucian.chiper@upb.ro (F.-L.C.); calin.vladeanu@upb.ro (C.V.); ion.marghescu@upb.ro (I.M.); razvan.craciunescu@upb.ro (R.C.); octavian.fratu@upb.ro (O.F.)

* Correspondence: alexandru.martian@upb.ro

Abstract: With the decrease in the cost and size of drones in recent years, their number has also increased exponentially. As such, the concerns regarding security aspects that are raised by their presence are also becoming more serious. The necessity of designing and implementing systems that are able to detect and provide defense actions against such threats has become apparent. In this paper, we perform a survey regarding the different drone detection and defense systems that were proposed in the literature, based on different types of methods (i.e., radio frequency (RF), acoustical, optical, radar, etc.), with an emphasis on RF-based systems implemented using software-defined radio (SDR) platforms. We have followed the preferred reporting items for systematic reviews and meta-analyses (PRISMA) guidelines in order to provide a concise and thorough presentation of the current status of the subject. In the final part, we also describe our own solution that was designed and implemented in the framework of the DronEnd research project. The DronEnd system is based on RF methods and uses SDR platforms as the main hardware elements.

Keywords: drone; UAV; RF methods; software-defined radio; detection system; defense system

check for updates

Citation: Chiper, F.-L.; Martian, A.; Vladeanu, C.; Marghescu, I.; Craciunescu, R.; Fratu, O. Drone Detection and Defense Systems: Survey and a Software-Defined Radio-Based Solution. *Sensors* **2022**, *22*, 1453. https://doi.org/10.3390/s22041453

Academic Editor: Peter Han Joo Chong

Received: 14 January 2022
Accepted: 10 February 2022
Published: 14 February 2022

1. Introduction

Technical innovations continue to manifest at an ever-increasing speed, causing fast and drastic changes to modern society. These changes, driven by the possibilities offered by new technologies, affect citizens, governments, and all public and private industry sectors.

As a result, the development of small, low-cost unmanned aerial vehicles (UAVs), commonly known as drones, has resulted in an ever-increasing number of these devices being utilized in a variety of applications [1]. UAVs have introduced new participants in aviation, quickly evolving beyond their military origin to become powerful business tools [2,3].

Applications of UAVs range from recreation to commercial and military applications, including enjoyment, hobbies, games with drones, homemade entertainment videos, recreational movies [4–6], low altitude flying base stations [7], and the operation of UAVs for military purposes [8–13].

The following research questions were developed for this project:

- What functions should a drone detection and defense system (DDDS) have in order to prove its functionality?
- Which are the most popular methods used in the implementation of DDDSs?
- Which are the main parameters that should be taken into consideration in research?
- What gaps are in the current research of DDDSs?

A widely-used methodology was utilized to conduct a systematic literature review based on preferred reporting items for systematic reviews and meta-analyses (PRISMA) [14] in order to obtain the answers to our study questions. We conducted a literature search in scientific databases that encompass prominent computer science journals and conferences, such as IEEE Xplore, ACM digital library, ScienceDirect, SAGE Journals Online, and Springer Link, to discover key articles on the drone detection and defense systems topic. We used the following search string to discover the relevant publications and papers for our research: ('Drone' OR 'UAV') AND (Counter) in the domains of electrical engineering, applied physics, telecommunications, defense, and computer information systems, for the previous six years (2016–2021). In total, we gathered a set of 7349 potentially relevant publications, excluding grey literature and pre-prints.

We next looked at the titles, keywords, and abstracts of the publications in order to find the papers and articles that described at least one distributed ledger modeling or simulation approach. We chose a total of 99 publications in the process. We examined the references of the selected publications for other papers that were relevant to our inquiry in order to expand our literature collection. Figure 1 shows the overall number of articles produced as a result of this approach.

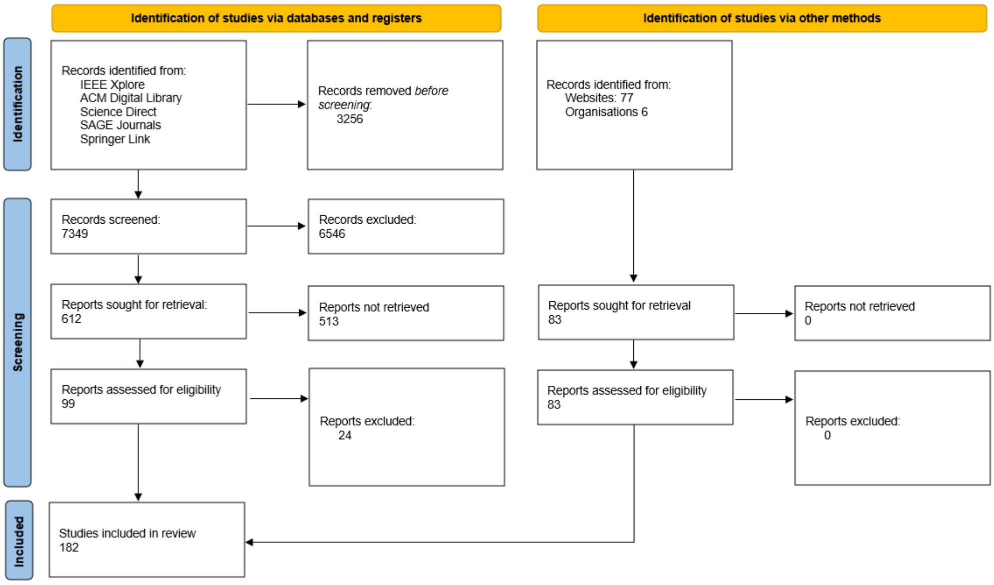


Figure 1. PRISMA 2020 flow diagram for systematic reviews.

The additional references that were identified in the bodies of the selected publications, or referencing those, were added to the literature list. We carefully studied the selected publications once the literature selection procedure was completed in order to determine the described applications and problems. The results of our analysis are reported in the following sections, which represent the core of the topical literature review.

The main contributions of our paper can be summarized as follows:

- We provide a detailed review regarding the drone defense systems based on RF methods, focusing on the solutions that are based on software-defined radio (SDR) platforms. To our best knowledge, other reviews that were performed concerning drone defense systems have not detailed that particular category of solutions;
- We discuss the current worldwide status of the legal issues regarding the jamming function, that enables the systems to annihilate the drones after they are detected;
- We present our own solution for an RF-based drone defense system that was designed and implemented within the framework of the DronEnd research project. The system was developed using several SDR platforms and a custom-made mount for dynamically adjusting the orientation of the jamming antenna, which enables the detection, localization, and annihilation of drones in a given monitored area.

The rest of this article is organized as follows: Section 2 reviews the most recent incidents that involved the reckless flying of UAV systems and the regulations taken by different governments and agencies around the world.

Section 3 describes the system requirements of a drone defense system in correlation with their basic mechanism/sensing technologies, considering their advantages and drawbacks. Also, this section highlights the specific models and architectures used in research for drone detection and defense systems. Section 4 details aspects regarding RF-based DDDSs and the use of SDR platforms in such systems. Section 5 contains a discussion regarding the challenges and the future research directions related to DDDSs. In Section 6, a solution for a drone detection and defense system based on SDR platforms, developed by the authors, is proposed and detailed, also highlighting the novel elements that are brought about, compared to the other existing solutions. The last section concludes the paper and includes the future perspectives of this work.

2. The Necessity of Drone Detection and Defense Systems: Incidents and Regulations

The drone industry's rapid rise has outpaced the rules for safe and secure drone operation, making them a symbol of illegal and destructive terror and crimes [15].

Drones have gained attention as a threat to safety and security since their entrance into civilian technology, which has fueled the development of anti-drone (or counter-drone) technologies. Anti-drone systems are designed to protect against drone accidents or terrorism, but they will need to evolve in order to deal with future drone flight systems [16].

UAVs have been used in a variety of military actions. Non-military UAVs have been accused of endangering airplanes, as well as persons and property on the ground. Due to the potential of an ingested drone to quickly damage an aircraft engine [17], safety concerns have been raised. Multiple near-misses and verified collisions have occurred involving hobbyist UAV pilots operating when violating the aviation safety standards [18].

2.1. Recently Reported Incidents

The necessity of anti-drone defense systems has gained importance, considering the large number of dangerous occurrences that are mentioned in Table 1.

Table 1. List of the recent UAV-related incidents.

Incident Type	Time and Place of the Event	Short Description of the Incident	Aftermaths	References
Aircraft collisions	17 April 2016/UK, London, Heathrow International Airport	An Airbus A320 collided with a Metropolitan Police UAV as it approached landing	There were no serious issues reported.	[19]
	21 September 2017/USA, Staten Island, New York City	A civilian UAV collided with a Black Hawk helicopter	The helicopter was able to continue flying and landed in a safe manner.	[20]
	12 October 2017/Canada, Jean Lesage Airport, Quebec City	A Skyjet Aviation Beech King Air A100 collided with a UAV	The plane landed safely, with only minor damage to its wings.	[21]
	13 December 2018/Mexico, Tijuana International Airport	On a Boeing 737–800 operating as Flight 773, a "quite loud noise" was heard	After a safe landing, the aircraft's nose was discovered to be damaged. The reason for the incident has not been identified; however, it was examined as a drone strike by the airline.	[22]
	10 August 2021/UK, Buttonville Municipal Airport	A Cessna 172 registered C-GKWL collided with a drone operated by the York Regional Police	The Cessna landed safely but with significant damage.	[23]

Table 1. *Cont.*

Incident Type	Time and Place of the Event	Short Description of the Incident	Aftermaths	References
Near-miss incidents	January 2017/P.R. China, Hangzhou Xiaoshan International Airport	A 23-year-old Xiaoshan UAV operator was arrested after taking footage with a drone that flew too close to planes landing	DJI, China's biggest drone manufacturer and the producer of the Mavic Pro drone (which was discovered to have been used in the event), issued a statement expressing its "strong condemnation" of the illegal filming.	[24]
	25 March 2018/New Zeeland, Auckland Airport	A UAV approached within 5 m of an Air New Zealand Boeing 777–200 on final approach to airport	The pilots spotted the UAV as the plane was approaching a position when evasive action was impossible, and they initially worried it would be pulled into an engine.	[25]
	19 December 2018/UK, Gatwick	A repeated deliberate intrusion of UAVs of "industrial standards" occurred	The suspension of all takeoffs and landings began at 9:03 p.m. on 19 December due to UAV sightings over the runway. Flights were briefly restarted the next morning but were banned again after more UAV sightings.	[26]
Other incidents that targeted officials and strategic objectives	April 2015/Japan	A small drone carrying radioactive materials was dropped on the roof of Japan's Prime Minister's mansion	The drone was not only able to fly to the Prime Minister's home, but it was also left unattended for over two weeks. Due to the characteristics of the area, notably privacy, it may have been difficult to deploy intensive detecting technology.	[27]
	October 2016/Syria	ISIL used two ultra-small drones purchased from Amazon to assassinate two Iranians in Syria	The first incidence of commercial drone terrorism, significant since commercial off-the-shelf drones were employed, demonstrating that a wide variety of drone terrorism was achievable because the drones could be cheaply bought without having the expert-level skill to fly.	[28]
	August 2018/Venezuela	Two bomb-carrying drones had a failed attempt to assassinate Venezuelan President Nicolas Maduro during a national outdoor celebration	The first time a drone was used to try to assassinate the country's leader. This incident emphasizes the importance of anti-drone technology for avoiding a traumatic event. Temporary anti-drone systems require rapid installation and deployment.	[29]

In addition to the highlighted incidents, the number of small mishaps caused by unauthorized or illegal drones invading restricted regions is increasing by the day [30]. This is another reason for anti-drone technology becoming increasingly important. As the regulations concerning drone usage are also a significant aspect to be considered when designing a DDDS, we review in the following subsection several aspects in this matter.

2.2. Regulations Regarding the Use of Drones

The most important agencies that regulate the use of drones (e.g., European Union Aviation Safety Agency (EASA), Federal Communication Commission (FCC), Australian Communication and Media Authority (ACMA), Civil Aviation Authority (CAA), etc.) have adopted action plans in order to ensure critical objectives against the illegal usage of UAVs [30–32].

For example, in order to address the hazards and threats posed by drones, European Union members in EASA have endorsed a counter-unmanned aerial systems (counter-UAS) action plan, proposed by the agency in 2019, which has subsequently been included in the European Plan for Aviation Safety (EPAS) [32].

The EASA's EPAS is applicable to all of the national and appropriate agencies, and it has resulted in the effective control of UAV hazards.

Furthermore, the EU has approved EASA's standard European guidelines in order to enable UAV integration and safe operation in the aviation system. The rules that apply to drones are outlined in Regulation (EU) 2019/94735 on the rules and procedures for the operation of unmanned aerial vehicles (UAVs) and Regulation (EU) 2019/945 on unmanned aerial vehicles and third-country operators of unmanned aerial vehicles (UAVs).

According to the document, there are three primary types of drone incident offenders that endanger civil aviation, as follows: non-criminal motivation, gross negligence, and criminal/terrorist motivation [30]. They relate to the drone's remote pilot's intention, as described in Table 2.

Table 2. EASA categorization of intention/motivation of pilots of unauthorized drones.

Negligence	Individuals Who Are Oblivious to or Are Unaware of the Appropriate Regulations and Constraints. As a Result, They Fly Their Drones across Sensitive or Forbidden Terrain. They Have a "Clueless" Mentality and Have No Intention of Disrupting Regular Aviation.
Gross negligence	Individuals who are reckless because they are aware of the appropriate regulations and constraints yet choose to break them for personal or professional advantage (e.g., aggressive spotters). Their actions can be described as "reckless", as they disrupt civil aviation while completely ignoring the implications of their conduct.
	Individuals who intentionally strive to use drones to disrupt aerodromes and flight operations, regardless of whether they are aware of the applicable legislation and limits. These individuals may even act as a group to maximize their impact. While their actions may have unexpected repercussions for aviation safety, they do not seek to put human lives in jeopardy.
Criminal/terrorist motivation	Criminals and terrorists are persons who intentionally strive to utilize drones to interfere with the safety and security of civil aviation, regardless of whether they are aware of the applicable legislation and limits. These persons should be considered criminally motivated or even terrorists because their actions are purposeful and show no concern for human lives and property.

3. Drone Detection and Defense Systems: Classification, Sensors, Countermeasures

In this section, we focus on the classification of drone detection and defense systems depending on different criteria, on the comparison of the different sensor types that can be used in order to detect the presence of the drones in the monitored area, on the classification of the countermeasures that can be adopted in order to annihilate the detected drones, and on the regulations regarding the use of jamming as countermeasure.

3.1. Classification of Drone Detection and Defense Systems

Firstly, it is necessary to classify DDDSs in order to understand their capabilities, as it is summarized in Table 3.

Table 3. Classification of DDDSs.

Category	Definition
Ground-based: fixed	Systems designed for usage in fixed locations [33]
Ground-based: mobile	Systems designed to be installed on automobiles and operated while they are in motion [33]
Hand-held	Systems designed to be operated by a single person using their hands; the majority of these systems resemble rifles [34]
UAV-based	Systems designed to be mounted on unmanned aerial vehicles (UAVs) [34]
UAV-swarm-based	Systems designed to use multiple drones [35]

A DDDS implies different available technologies for detection, tracking, and classification, in addition to neutralization techniques. The most essential elements recommended for the DDDS are considered to be detection, tracking, and classification of the target drones [30,34]. The different technologies that are used for allowing drone detection are summarized in Table 4.

Table 4. Technologies used for drone detection in DDDSs.

Technology	Description	References
Acoustic	UAVs are detected and tracked by using an array of microphones	[36–53]
Imaging (EO/IR)	UAVs are detected and tracked by using EO/IR cameras	[54–72]
Radar	UAVs are detected and tracked using their radar signature	[73–102]
Radio frequency (RF)	UAVs are detected, tracked, and identified by monitoring the radio frequencies used for communications; this technology could localize the UAV and the pilot	[103–113]
Hybrid	Combination of two or more of the above-mentioned technologies	[104,114]

3.2. Classification of Detection Sensors

All of the types of sensors that are currently used in DDDS present specific advantages and limitations and, as a direct consequence, such a system must incorporate more sensors of different types in order to achieve a higher detection rate [33].

A brief description of each category of sensors is given below and the different pros and cons for each category are summarized in Table 5.

Table 5. Pros and cons of sensors used in DDDSs.

Type	Pros	Cons	References
Acoustic	• Covers the spectrum of 20 Hz–20 kHz; • Acoustic signature library could be updated easily from flight to flight; • Lightweight and can be easily associated with other types of sensors.	• Limited range; • Vulnerable to ambient noise; • Susceptible to decoys.	[36–53]
Imaging	• Covers all of the visible and IR spectrum (3 MHz–300 GHz); • IR cameras could operate in cloudy weather and in day or night; • Could be assisted by computer-vision technologies.	• Provides 2D images; • Limited performances by weather conditions and background temperature; • Dependent of georeference data • LoS is required.	[54–72]
Radar	• Bandwidth used: 3 MHz–300 GHz; • Could operate in all weather and day/night conditions; • Offers information regarding the velocity of the target; • Can recognize micro-Doppler signatures (MDS) • Offers high coverage; • Good accuracy; • Compact and high mobile, required for tactical applications; • High reliability.	• Large radar cross-section is desired; • Difficult to differentiate UAVs from birds; • Limited performance for low altitudes and speeds (death cone); • Could interfere easily with small objects, especially birds; • LoS is required; • High cost.	[73–102]
RF	• Capturing the communication spectrum and signals UAV and operators; • Low complexity and easy to implement; • Could operate in all weather and day/night conditions; • Easier to improve due to modular implementation of receivers and digital signal processing units used in implementation; • Possibility to localize the pilot.	• Knowledge regarding UAV communication specifications (e.g., frequency bands, modulations, etc.) is required; • Difficult to accurately determine AoA; • Difficult to use in urban areas due to fading and multipath phenomena; • Vulnerable to malicious or illegal modified RF that will exceed receiver capabilities.	[103–113]

3.2.1. Radio Frequency Sensors (RF)

UAV RF detection is a technique that involves the interception and analysis of the signals transmitted (Tx, Rx) between the UAV and the ground station. Usually, these signals consist of uplink (from the ground station) control signals and downlink (from the drone) data signals (position and video data) [103]. A detailed analysis of the DDDSs that are based on RF methods are presented in Section 4.

3.2.2. Radar

The Radar solution for drone defense systems represents an active method to identify and localize a potential UAV threat. In order to determine the range, angle, or velocity of a UAV, radar is widely used as an active sensor in sensing systems in a DDDS. A radar system consists of a transmitter, a receiver, and a processor [73].

3.2.3. Imaging Sensors

This technology involves the use of cameras that take images from a designated area in order to determine the presence of a target drone.

Electro-Optical (EO) Cameras

Some DDDS use imaging sensors (EO/IR), which could be led by other sensors (such as radar and RF) in order to obtain images of the drone and its main characteristics (e.g., payload). These images can be recorded and analyzed by specialists in order to determine the threat level [55].

The main disadvantage of this method is its low performance under dark and foggy conditions. Moreover, the quality of the images depends on the quality of the lenses and the angle of the photography (LoS is mandatory).

Infrared (IR) Cameras/Thermal

This method employs thermal IR cameras that are able to detect the heat produced by a UAV's hardware components, such as the motors, batteries, and processors.

This detection method presents disadvantages related to detection range and environment caused by the sensibility of the sensors that measure the thermal difference between the drone and the background. In consequence, the detection of drone presence depends on the drone's motor temperature, angle (LoS is mandatory), distance, and the temperature of the IR sensors [58].

3.2.4. Acoustic Sensors

This technology involves the use of a microphone array that captures the noise generated by the propellers and rotors of a UAV and compares it with an intern acoustic signature database [42].

Table 5 summarizes the advantages and limitations of each of the different technologies that were mentioned above.

3.3. Classification of Countermeasures

The necessity of DDDS arose for the first time in military applications under special regulations that exceed other governmental or structure capabilities and responsibilities. In consequence, the neutralization techniques are more numerous than the detection techniques [30].

The most important DDDS countermeasures are as follows:

- *Electromagnetic pulse (EMP)*—a beam generated with the goal to damage the internal electronics of the target drone [115–117];
- *Interceptor drone/Collision Drone*—a drone used to force the target drone to land or return home [118–123];
- *Lasers*—directed rays used to destroy the target or blind the camera (dazzler) [124–129];
- *Magnetic*—use powerful magnets in order to create a magnetic field around a protected area [130];
- *Prey birds*—eagles or falcons specially trained to attack the enemy's drone [131];
- *Shooting nets*—a net is launched towards the target drone to prevent the propellers from rotating [132];
- *Projectiles*—large-caliber ammunition used to destroy the target [133];
- *Missiles*—conventional ammunition, could be guided or unguided [133];
- *Guns*—conventional weapons and ammunition [133];
- *Water cannons*—a stream of water is directed towards the target drone [134];
- *RF/GNSS jamming*—disrupt the communication of the target drone with the control station and/or global navigation satellite system (GNSS) [135–139];
- *Spoofing*—decoys the drone by using imitation GNSS and control signals in order to take over the command [140–145];

- *Mixed countermeasure techniques*—use two or more countermeasures in order to maximize the neutralization rate.

The main advantages and drawbacks of each of the different countermeasure technique are presented in Table 6.

Table 6. Characteristics and limitations of countermeasure techniques.

Type	Pros	Cons	References
Electromagnetic pulse (EMP)	• Could burn or interfere with the internal electronics of the drone, disrupting its operation; • Could operate in both narrowband and wideband domains.	• Accurate direction of jamming is necessary; • Difficult to know the effectiveness of jamming.	[115–117]
Interceptor drones	• Searching and tracking capabilities; • Could carry weapons and ammunition.	• Requires a relatively close approach to the target; • Have a considerable delay.	[118–123]
Lasers	• Could operate at low powers (dazzlers) to blind the UAVs cameras or high power, which could burn/destroy the target; • Easy to track the target; • Cheaper and safer than projectiles or another physical countermeasure.	• Sensitive to weather conditions; • It is necessary to have an accurate measurement of the target's position; • High power lasers could interfere with other systems.	[124–129]
Magnetic	• Cost effective; • Could respond to multiple threats.	• Small protected area; • Could interfere with other systems.	[130]
Prey birds	• Does not require complex technology; • Fewer humans are required.	• Applicable only to slower and small UAVs; • Could harm the falcons.	[130]
Projectiles/ shooting nets/ water cannons	• Effective against any type of UAV; • Work in all weather conditions; • Quick reaction method.	• Might cause collateral damage; • High costs; • Requires professional operators.	[131–134]
RF/GNSS jamming	• Could neutralize grouped targets simultaneously, degrading their received signal-to-noise ratio (SNR); • GNSS frequencies and bands are widely known and relatively easy to jam; • The directivity diagram of the jamming signal can be oriented and directed as desired.	• Ineffective against autonomous UAVs; • Ineffective against drones that use inertial navigation systems/sensors (INS); • Ineffective against UAVs that use encrypted communications; • Effective only for short distances; • The jamming could interfere with other sensible equipment.	[135–139]
Spoofing	• DSP and AI algorithms could copy and reproduce the control communication signal with high accuracy in a relatively short time; • Could exploit the vulnerabilities of various systems of UAVs.	• It is necessary to have a consistent analysis of the targeted UAVs regarding their operation frequencies; • Spectrum sensing systems are desirable.	[140–145]

However, as pointed out in [35], destroying the drone does not mean that the problem is solved. Even if a drone is destroyed using one of the methods listed above, it is just half of the answer. It is critical to discover and detain the operator of the illegally flying UAV in order to resolve the problem completely. Without this, a motivated operator will almost certainly return with a newer and better UAV capable of causing even more disruption and damage.

3.4. Regulations Regarding the Use of Jamming in DDDSs

For most of the above-mentioned categories of countermeasures, there are not currently any regulations in force. However, in the case of RF jamming, several existing regulations apply, which will be detailed in the following paragraphs.

The neutralization of drones using jammers is still (in most countries) not legally permitted and is currently the subject of numerous regulatory and legal discussions.

The EU authorities were among the first organizations that took a position regarding the use of jamming devices. The Directive 2014/53/EU prohibits the use of such devices that could cause harmful interferences to the authorized radiocommunications and prevent the normal operation of the communications using radio frequencies [146]. This directive was transposed in all of the member state's legislations.

The Directive 2014/53/EU was transposed into Romanian legislation by Government Decision no.740/2016. According to this decision, the manufacture, importation, possession, advertising, placing on the market, making available on the market, putting into service and/or use of radio equipment or devices designed to cause harmful interference (jammers) are all prohibited and sanctioned with contravention [147].

In the UK, there were a lot of concerns regarding the collateral damage and the safety risks that must be taken into consideration when using jamming, because of the radio signal interference and the impact on other airspace users. However, only a few regulations have stated that such technology should not be used in any circumstances [148].

The FCC (Federal Communications Commission) in the United States does not merely state that the manufacture, sale, importation, and operation of jammers are all forbidden (Communications Act of 1934, Section 301), but that there are some exceptions, such as institutions under the US government. There is always the risk of a drone losing control, crashing, and causing property damage, or personal harm, when a drone jammer is deployed. This means that anyone using a drone jammer, even government-authorized workers, could be held liable. As a result, the deployment of drone jammers by private entities, such as power companies or airports, is still sporadic but strictly regulated. Only the federal government has the ability to approve the use of drone jammers, and this rigorous restriction extends to their manufacture, importation, and sales [149].

In the Russian Federation, flying a drone is legal. However, most Russian cities are equipped with GPS jammers, which create radio interference, preventing electronics, such as drones, from operating normally. As a consequence, drone users have to keep a safe distance from them because all of the major cities have integrated GPS jammers that can interfere with their drone positioning [150]. Also, there are some regulations that prohibit flying a drone within 500 m of a military installation.

In P. R. China, only the local authorities can use jammer "guns" and other RF DDDSs [151].

Despite of the lack of regulations regarding the use of RF jamming signals against drones, and some risks that should be taken into consideration, this method has to be considered to be among the most efficient.

4. Drone Detection and Defense Systems Based on RF Methods

As was mentioned in Section 3, one of the most used methods for drone detection is the identification of the RF signals that are exchanged by the drones with another entity (ground station/operator). Moreover, the annihilation of the detected drones can also be obtained by RF methods, by means of transmitting strong enough jamming signals that can interrupt the communication between the drone and its operator (as mentioned in Section 3.3).

Usually, drones operate on different frequencies, but most commercial drones operate in Industrial, Scientific, and Medical (ISM) frequency bands of 433 MHz and 2.4/5.8 GHz. The simple power detection in these bands will not work due to the presence of other legitimate users in the same geographical area. Therefore, most of the modern RF detection systems provide the detection and identification of the special and unique signals that are generated by the UAV or the data protocols implemented in a UAV.

There are two main functions that are necessary for the detection of the drones, as follows: The *identification* of the presence of the drones by scanning the frequency spectrum and *localization* of the drones. The *annihilation* function, which is necessary in order to allow the defense against the detected drones, can be performed by means of RF jamming, in order to interrupt the communication between the drones and their operators. Table 7 summarizes the main elements regarding the implementation of such systems. In the following paragraphs, each of the below mentioned categories will be detailed.

Table 7. RF-based drone detection and defense systems.

References	Implemented Functions	Methods	SDR Platform Used (Including Manufacturer, City and Country)
[152]	Identification Localization	RF fingerprinting (SFS, WEE, PSE) AoA (MUSIC, RAP MUSIC)	USRP-X310 (Ettus Research, Santa Clara, CA, USA)
[153]	Identification	RF fingerprinting (DRNN)	USRP-X310 (Ettus Research, Santa Clara, CA, USA)
[154]	Identification	RF fingerprinting (CNN)	USRP-X310 (Ettus Research, Santa Clara, CA, USA)
[155]	Identification	RF fingerprinting (KNN)	USRP-B210 (Ettus Research, Santa Clara, CA, USA)
[156]	Identification	RF fingerprinting (KNN, XGBoost)	-
[157]	Identification	RF fingerprinting (Wi-Fi)	-
[158]	Identification	RF fingerprinting	LimeSDR (Lime Microsystems, Guilford, UK)(customized)
[159]	Identification	RF fingerprinting	-
[160]	Localization	Received-signal strength (RSS)	USRP N210 (Ettus Research, Santa Clara, CA, USA)
[161]	Localization	RSS	AD-FMCOMMS5-EBZ Evaluation Board (Analog Devices, Wilmington, DC, USA)
[162–164]	Annihilation	RF jamming	BladeRF (Nuand, San Francisco, CA, USA)
[165]	Annihilation	RF jamming	Great Scott Gadgets HackRF One

Most of the RF-based solutions that are described in the literature focus only on the detection of the drones and do not propose countermeasures for the annihilation of the detected drones. One of the reasons behind this might be the increase in the complexity and price of the system that will be generated by the inclusion of such countermeasures in the designed system. A second reason might be related to the fact that most of the references that will be commented on in this section include academic research, in which the target was not the design of a complete commercial system. A third reason could be the fact that jamming equipment is not legal in many areas worldwide, as discussed in Sections 2 and 3. However, as mentioned previously, the jamming solution can be used in most of the countries if the system that generates it is used for national security or public order purposes.

Almost all of the implementations that were used for validating the solutions that are proposed in the literature are based on SDR platforms because of some of the significant advantages that are offered by this category of platforms, such as the following:

- Low to moderate cost;
- Extended frequency range, which can usually cover all of the frequency bands that are used by commercial drones;
- Scalability, allowing the extension of the platform, depending on the functions that are foreseen, to be implemented;

- Flexibility, allowing the processing of RF signals corresponding to different communication standards.

Only a few of the existing works include aspects that are related to both of the functions that were mentioned previously as necessary for the detection of the drones, *identification* and *localization*. Such an example is [152], where the authors proposed a drone detection system based on multi-dimensional signal feature identification. After identifying the channel on which the drone communicates with the controller, features, such as signal frequency spectrum (SFS), wavelet energy entropy (WEE), and power spectral entropy (PSE), are extracted in order to allow a precise identification of the drone. In a subsequent step, MUSIC and RAP-MUSIC algorithms are used for performing the localization of the drone, by using information, such as azimuth and elevation. The proposed solution is implemented and tested using USRP X310 SDR platforms and a circular antenna array, obtaining an average detection rate of more than 95%.

In most of the papers that are concerned with the *identification* of the drones RF fingerprinting techniques are used, which rely on the unique characteristics of the RF signal waveforms captured from different drones [153–157]. In [153], a classification of the detected drones is made using a deep residual neural network (DRNN), the results being validated using a USRP X310 SDR platform as a receiver and nine different drones as targets. The authors of [154] separate Wi-Fi and Bluetooth signals from UAV transmitted signals based on their bandwidth and modulation features and classify the UAV signals using machine learning (ML) techniques. In [155], the detection of multiple drones is performed using the k-nearest neighbor (KNN) algorithm after performing a short-time Fourier transform (STFT) on the received signal. A real-time testbed based on the USRP B210 SDR platform is also used for evaluating the performance of the proposed method. A combination of RF fingerprints and hierarchical learning is used in [156] for the classification of the detected drone signals. A Wi-Fi statistical fingerprint approach is proposed in [157], which accounts for the particular characteristics of the Wi-Fi control traffic produced by drones and their remote controllers.

In [158], a solution that is based on the low cost LimeSDR platform is developed for detecting the presence of drones in the 2.4–2.5 GHz ISM band. The authors use the LMS7002M RF chip from the LimeSDR module but customize the firmware of the FPGA located on the same SDR platform in order to implement the signal processing steps that are necessary for the identification of the RF signals that are transmitted by different drones.

The authors of [159] apply a STFT on the RF signals that are collected using a spectrum analyzer and calculate the time guards associated with the different hopping sequences using the autocorrelation function (ACF) in order to obtain an accurate differentiation of the different UAV remote control (RC) signals.

The following paragraphs will detail the different approaches that were proposed for the implementation of the *localization* function.

A received-signal strength- (RSS-) based 3D localization system utilizing a software-defined radio is proposed in [160], using the recursive least squares (RLS) algorithm in order to numerically estimate the drone's 3D position.

The authors of [161] propose a localization approach based on the arrays of directional antennas, for obtaining the direction of arrival (DoA) of the NTSC signal that is transmitted by the drones.

Although the articles that were mentioned above only focused on the detection of drones based on RF methods, there are also papers that present implementations of the annihilation function using RF jamming as a countermeasure against drones [163–165].

In [162,163], a low-cost SDR platform, BladeRF X40 (Nuand, San Francisco, CA, USA), was used as hardware to implement a jamming system against unauthorized UAVs. The GNU Radio toolkit was used as a software environment for performing the necessary signal processing tasks. In [162], the communication of the drone with the remote control in the 2.4 GHz ISM band was targeted, whereas in [164] the GPS navigation system was targeted.

The authors of [164] implemented a protocol-aware jammer using the BladeRF SDR platform as hardware. Tests were made to target the Futaba Advanced Spread Spectrum Technology (FASST) and the Advanced Continuous Channel Shifting Technology (ACCST) UAV remote control systems.

In [165], a portable jammer is proposed, based on the HackRF One SDR platform and a Raspberry Pi as a host computer. Multiple tests were made in order to validate the proposed solution, in both the 2.4 GHz and 5.8 GHz ISM bands and in the GPS L1 band.

5. Challenges and Future Perspectives for Drone Detection and Defense Systems

The previous sections contained a review of the different approaches that can be used for implementing a DDDS. In this section, the challenges that currently have to be faced when developing such a system will be detailed, together with a discussion regarding the future perspectives of this domain.

One of the challenges that is faced when implementing a DDDS is the ability to identify and, in a further step, to annihilate not only one, but several different target drones. In recent years, many applications have used multiple drones [166], therefore, such a feature becomes an important characteristic for a DDDS. Depending on the sensors that are used in the system, the possibility of detecting several target drones may or may not exist. A few examples of systems that include such a feature exist in the literature. In [167,168], algorithms are developed in order to allow multi-UAV detection using video streams. In [169], an RF-based deep learning (DL) algorithm is proposed for performing multiple drone detection. The possibility of a simultaneous annihilation of several drones is an even more challenging task. Electromagnetic pulses (EMP) have been proposed as a possible solution for defense against drone swarms [170]. RF jamming performed using antenna arrays could also generate, by means of signal processing methods (beamforming), multiple beams that could be targeted towards multiple target drones.

Another challenge that a DDDS would have to face, especially if the area in which the system is installed is a residential area, and there are several households in the close neighborhood, is to avoid interference or damage to nearby equipment (in the case of RF jamming and EMP) and to respect the privacy of the nearby neighbors (in the case of imaging sensors). In the case of RF jamming, this could be solved if the antennas that are used or the beams, in the case of using a beamforming approach, are very directive and targeted directly towards the target drone(s).

When referring to a DDDSs based on RF methods, one of the main challenges that has to be addressed is related to the legal issues around the use of jamming as a countermeasure, as was also commented on in Section 3.4. For the time being, in most of the regions worldwide, such a countermeasure can only be legally used when it is integrated into a system that is used for the defense of national security or for public order objectives. However, as the number of situations when such a system would be necessary also applies to the defense of private areas that cannot be included in the above mentioned categories, it is to be expected that the legislation in this domain might be modified in the near future in order to include the possibility of private users also legally using such a system, as long as the interference caused to the nearby areas is kept below certain well-defined thresholds.

An important limitation of RF-based DDDSs is related to the impossibility of detecting and annihilating autonomous drones in cases when they have a predefined flying path and do not have any active data communication with an operator located on the ground.

As mentioned in Table 5, each of the different types of sensors (RF, radar, imaging, and acoustic) has its own drawbacks and limitations. As such, the performance of a DDDS that is implemented using a single type of sensor is directly affected by the disadvantages and limitations of that particular category. By combining several different sensor types in a single *hybrid DDDS*, the system could benefit from the advantages of each different category of sensors. A first benefit would be the increase in accuracy that such a hybrid system could achieve, when the information regarding the identification and localization of the drone would be obtained from multiple different sensors. A second benefit would be related to the possibility of detecting the target drone in situations when one of the sensor types would not allow the detection on its own. For example, if we consider a hybrid DSSS that is implemented using both RF and imaging sensors, the imaging sensors could be used for detecting autonomous drones (that cannot be identified using the RF sensors) and the RF sensors could be used for detecting drones in low visibility conditions (when the imaging sensors could not provide the detection). Very few implementations of such hybrid systems are described in the literature (for example those in [105,115]), and we consider that such an approach is a promising future research and development direction for DDDSs.

6. DronEnd Detection and Defense System

In the current section, a drone detection and defense system, designed and implemented by the authors, together with a research team from the cybersecurity company Cyberwall [171], will be presented. The system was developed within the framework of the DronEnd research project [172]. The preliminary details regarding the project were given in [173].

The goal of the DronEnd ground defense system is to secure a certain area against the unauthorized presence of drones. In order to achieve this goal, the DronEnd system scans the RF spectrum in order to detect the presence of the drones in the supervised area, identifies the location of the drone by means of AoA algorithms, and annihilates the drone by using RF jamming methods. The block diagram of the implemented DronEnd ground defense system is presented in Figure 2.

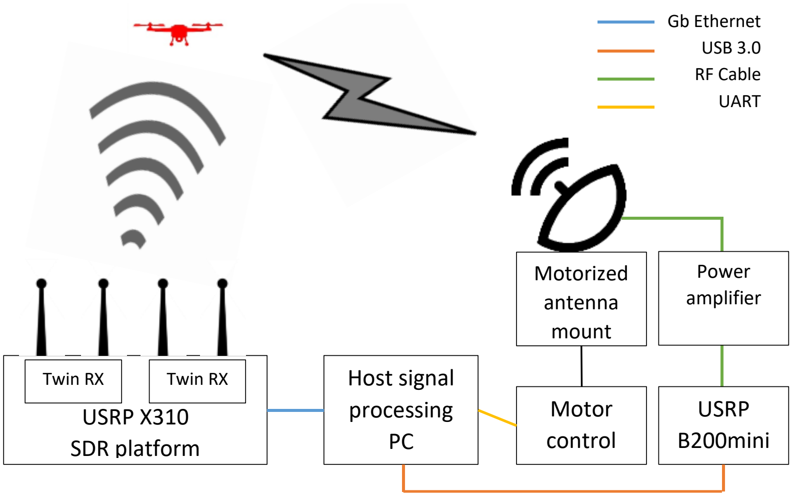


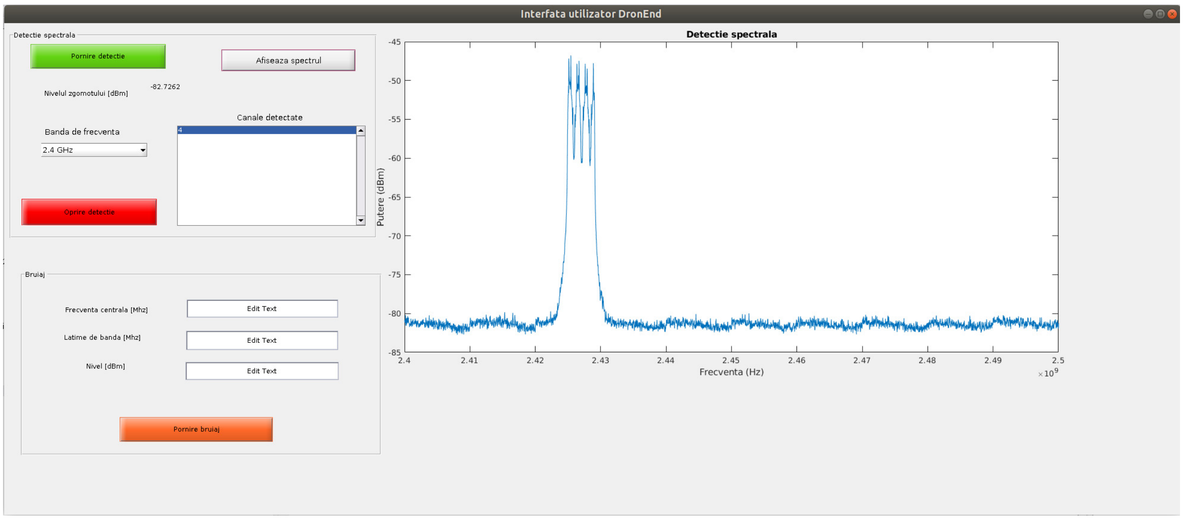
Figure 2. Block diagram of the DronEnd ground defense system.

In the following subsections, all of the elements of the system will be detailed, highlighting the steps that are necessary in order to perform the functions of detection, localization, and annihilation of the drone through jamming.

6.1. Detecting the Presence of the Drone Using Spectrum Sensing Algorithms

A first step required for detecting the presence of a drone in the case of RF-based drone defense systems is to monitor the radio spectrum through a spectrum sensing process in order to identify the signals that are transmitted by the drone. For the implementation of the spectrum sensing process in the DronEnd system, spectrum sensing algorithms based on the energy detection method have been used. Algorithms, such as 3EED [174] and 3EED with an adaptive threshold [175], that were previously developed, provide improved performance compared to the classical energy detection (CED) [176] algorithm and were used to identify the presence of the drones in the monitored area. The above-mentioned algorithms were implemented on SDR platforms from the USRP family (USRP X310 (Ettus Research, Santa Clara, CA, USA) [177] equipped with Twin-RX RF Daugterboards (Ettus Research, Santa Clara, CA, USA) [178], 10–6000 MHz frequency range). The frequency bands that are used by the drones that were used to test the DronEnd system (DJI Mavic Air (SZ DJI Technology Co., Ltd., Shenzhen, China) [179], DJI Phantom 4 Pro v2.0 (SZ DJI Technology Co., Ltd., Shenzhen, China) [180], and DJI Mini 2 (SZ DJI Technology Co., Ltd., Shenzhen, China) [181]) were the 2.4 GHz (2400–2500 MHz) and the 5 GHz (5730–5830 MHz) ISM bands, which can be covered using the above-mentioned SDR platforms that can receive signals on frequencies up to 6 GHz. Because the position of the target drones was not initially known, omnidirectional antennas were used in this step.

Figure 3 shows the graphical user interface that was implemented in order to view the results of the spectrum sensing. The signal that was transmitted by the DJI Mavic Air drone on channel four of the ISM 2.4 GHz band can be seen as captured using the USRP X310 SDR platform. In the following subsections, the other elements of the DronEnd system will be detailed, highlighting the steps that are necessary in order to perform the functions of localization and annihilation of the drone through jamming. The capture of the RF data was performed using a GNU Radio python script. As the instantaneous bandwidth captured using the Twin-RX RF daughterboard is smaller than 100 MHz, in order to cover the 100 MHz bandwidth of the 2.4 GHz and 5 GHz ISM bands, several sub-bands were concatenated.


Interfata utilizator DronEnd

Detectie spectrala

Nivelul zgomotului [dBm] -82.7262

Banda de frecventa: 2.4 GHz

Canale detectate: 4

Bruiaj

Frecventa centrala [Mhz]: Edit Text

Latime de banda [Mhz]: Edit Text

Nivel [dBm]: Edit Text

Figure 3. Graphical user interface of the spectrum sensing process implemented in the DronEnd system, showing the signal transmitted by the DJI Mavic Air drone in the 4th channel of the 2.4 GHz ISM band.

Once the signal that is transmitted by the target drone is detected, the next step is triggered, which is to localize the angle of arrival of the received signal, as will be discussed in the next subsection.

6.2. Localization of the Drone Using AoA Algorithms

Once the frequency that is used by the drone to communicate has been identified, a second necessary step is to obtain information about the position of the drone. This step was performed using AoA algorithms for detecting the angle of incidence of the detected RF signal. Such algorithms exploit the phase difference of the signals that are received from the drone using a multi-antenna system. The SDR platform that was used as the hardware for providing the RF receive front-end was the USRP X310 [177], on which two Twin-RX RF modules [178] were mounted (covered frequency range of 10–6000 MHz, instantaneous bandwidth 80 MHz). Each of the Twin-RX modules offers two coherent reception channels, and the local oscillator that was used can be shared by the two boards, so that in the end, a total of four coherent reception channels are obtained and are aligned in phase. The antenna system that was used was a linear system of four antennas, spaced at a distance equal to half the wavelength of the minimum frequency that the drones used for testing could transmit (2.4 GHz). In order to estimate the initial phase difference between the four reception channels, a calibration step was required after each system restart, which involves the transmission of a test signal that will be received through the RF cables of equal length on all four of the reception channels. A 5-port RF splitter (Mini-Circuits ZN4PD1-63HP-S+ (Mini-Circuits, New York, USA) [182]) was used in order to distribute the signals. Figure 4 shows both the antenna system that was used and the USRP X310 SDR platform during the calibration stage.

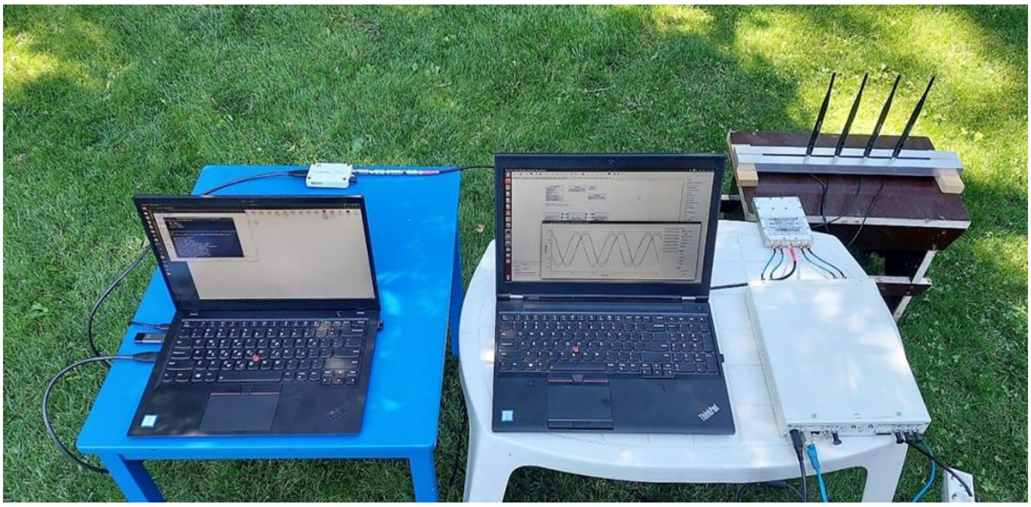


Figure 4. The linear antenna system that was used and the USRP X310 SDR platform during the calibration procedure of the Twin-RX RF modules.

Once the calibration step was completed, the four dipole antennas (VERT2450 [183]) that make up the antenna system were connected to the four receive channels of the USRP X310 SDR platform and, based on the phase difference of the signals that were received, the angle of incidence that corresponds to the drone location could be identified by using AoA algorithms. We used one of the classical AoA algorithms, the MUSIC algorithm, and the result was both displayed on a graphical user interface, as shown in Figure 5, and forwarded as an input to the software module that is responsible for setting the orientation of the jamming antenna, which will be detailed in the next subsection.

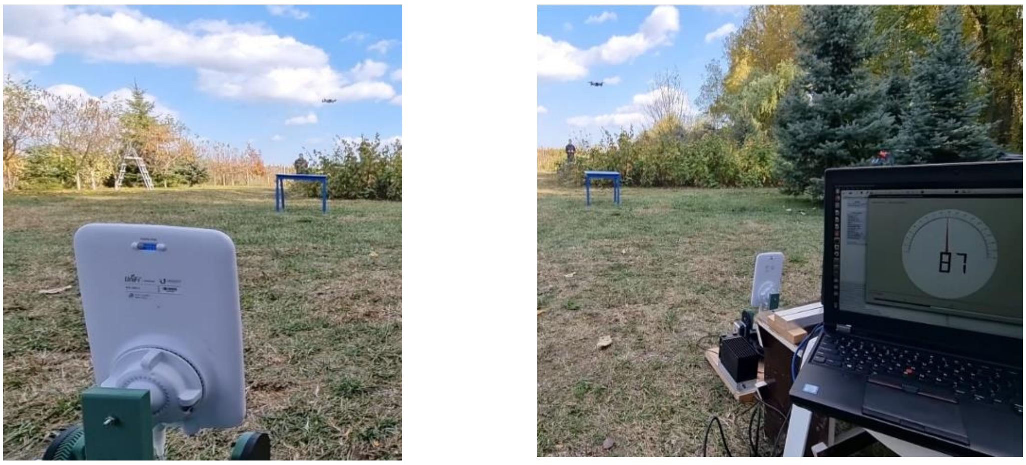


Figure 5. Tests performed using the DronEnd ground system (DJI Mavic AIR target drone). The estimated angle of incidence can be noticed.

The positioning that was thus obtained was one in azimuth, as the antenna system that was used was placed horizontally. By using a second system that was located in a vertical plane, the elevation of the drone could be also estimated.

6.3. Annihilation of the Drone Using RF Jamming

A final step is to transmit a jamming signal to the identified target drone in order to disrupt the communication between the drone and its operator. As the jamming signal should only be transmitted in the direction of the target drone, in order to avoid interference with other equipment in the area, a directional antenna was used for the jamming operation. Figure 6 shows the following components that were used to implement this step: the transmitting antenna, the motorized antenna mount, the stepper motor control module that was used to move the antenna mount, and the power amplifier.

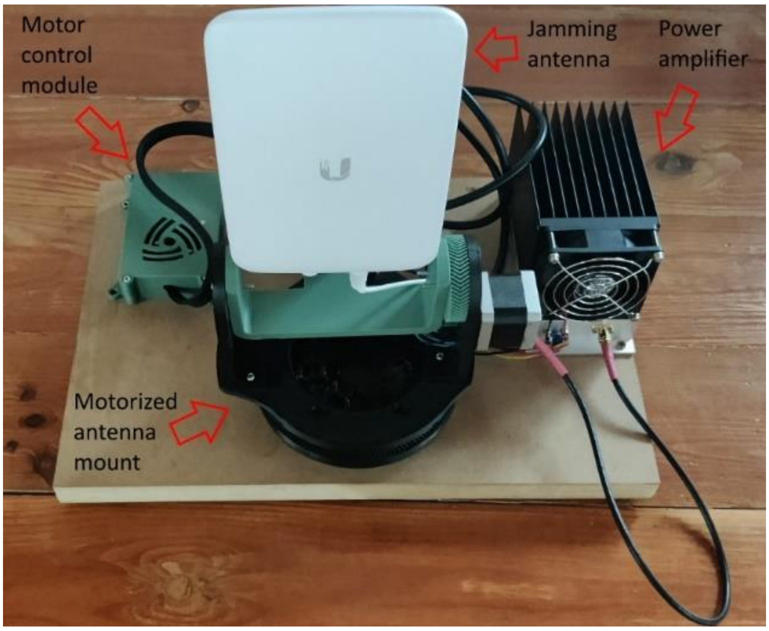
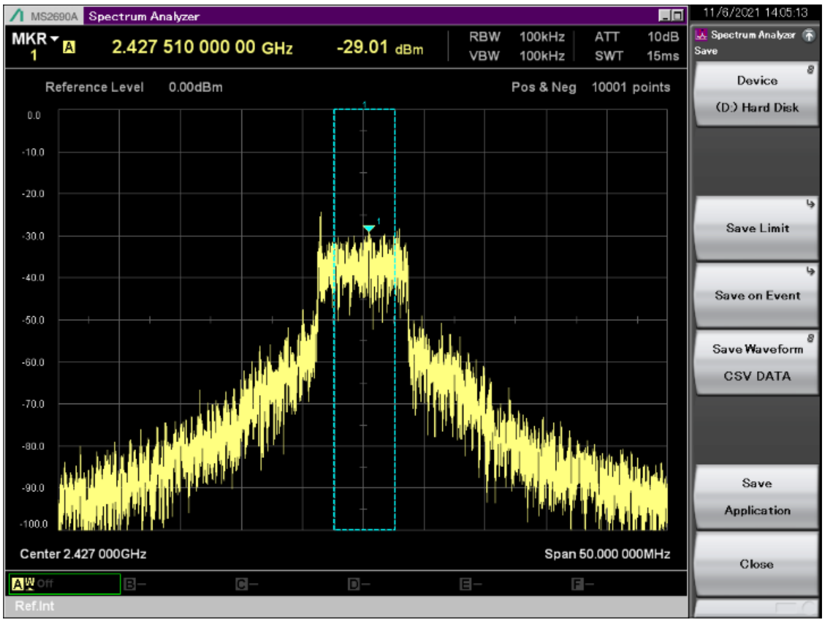


Figure 6. Components used for transmitting the jamming signal.

The angle of incidence that was detected by the AoA algorithm was processed (filtered) using a script implemented in the Matlab environment in order to remove any erroneous indications related to the position of the drone and was subsequently transmitted using a serial interface (UART) to the motor control module (MCM), which controls the stepper motors that are used to move the motorized support for positioning the jamming antenna. The MCM was based on a Microchip ATMega328p processor, which, using the angle information that is obtained using the AoA algorithm, controls the stepper motors. Two Nema 17 stepper motors, controlled using Texas instruments DRV8825 drivers, were used; one to adjust the azimuth and one to adjust the elevation of the jamming signal antenna. In the current configuration, given that the drone's position was estimated only in the azimuth plane, the commands were transmitted only to one of the two motors (the one that was responsible for the azimuth movement).

The SDR platform that was used to generate the jamming signal was a USRP B200mini platform (70–6000 MHz frequency range) (Ettus Research, Santa Clara, CA, USA) [184]. Given that the maximum power that can be obtained at the output of the SDR platform is 10 dBm, a power amplifier (Mini-Circuits ZHL-2W-63-S+ (Mini-Circuits, New York, NY, USA) [185]) was used to amplify the jamming signal in order to extend the range of the system, which offers a 42 dB gain and a maximum output power of 2 W. The antenna that was used to transmit the jamming signal was a Ubiquiti UMA-D (Ubiquiti Inc., New York, NY, USA) directional antenna [186], which covers the 2.4–2.5 GHz and 5.1–5.9 GHz bands and offers a 10 dBi gain in the 2.4 GHz band and a 15 dBi gain in the band of 5.8 GHz. By using a directional antenna that targets the location of the drone for the transmission of the jamming signal, the interferences that are caused to other communication systems that are operating in the neighborhood are minimized. Moreover, the transmit gain can be adjusted depending on the size of the area that has to be protected. Figure 7 shows the jamming signal with a 10 MHz bandwidth emitted in channel four of the 2.4–2.5 GHz ISM band, captured using an Anritsu MS2690A (Anritsu Corporation, Atsugi, Japan) spectrum analyzer.



MKR 1 A 2.427 510 000 00 GHz -29.01 dBm

RBW 100kHz VBW 100kHz ATT 10dB SWT 15ms

Reference Level 0.00dBm

Pos & Neg 10001 points

Center 2.427 000GHz

Span 50.000 000MHz

11/6/2021 14:05:13

Figure 7. Jamming signal transmitted by the DronEnd ground system on channel 4 in the 2.4–2.5 GHz ISM band.

The tests were performed in an outdoor suburban scenario using the DJI Mavic Air, the DJI Phantom 4 Pro v2.0, and the DJI Mini 2 drones as targets and the annihilation of the drone, which resulted in a forced landing on the position where the drone was located when the jamming signal was turned on, was possible for distances of 40 m from the area where the DronEnd ground system was located.

6.4. Conclusion and Future Research Directions

To conclude, the main novel elements that are introduced by the DronEnd system, when compared to other drone detection and defense systems based on RF methods that were mentioned in Section 4, can be summarized as follows:

- Incorporates all of the three functions (identification, localization, and annihilation) that are necessary for a drone detection and defense system in an integrated and scalable platform, which can be reconfigured depending on the requirements of different use cases;
- Includes an agile and accurate identification subsystem, based on improved spectrum sensing algorithms, which performs a real-time identification of the signals that are transmitted by the drone and, moreover, allows a dynamic tracking of the signal transmitted by the drone, even when the transmit frequency is changed;
- Annihilates the detected drone by means of jamming, avoiding at the same time significant interference with nearby devices, as a directional antenna, targeted directly towards the target drone using a motorized antenna mount, is used.

Several aspects are considered as future research directions, in order to improve the performance of the proposed system.

The first direction is related to the possibility of replacing the mechanical motorized antenna mount that was used for targeting the directional jamming antenna with an equivalent static planar antenna array. By using such an approach, the orientation of the resulting antenna beam that was necessary for following the target drone would not involve any moving parts, as the steering would be obtained only by using signal processing methods. The advantages of such an approach would include a smaller delay, the possibility of adjusting the beamwidth by signal processing means, depending on the application necessity, and the absence of aging effects that might affect mechanical parts. However, as the transmit power level that is needed in order to obtain a large enough range for the system might be high, a challenge that would have to be addressed is the design of a power amplification stage for supplying the planar antenna array.

The second direction is related to the addition of a second antenna array, in an orthogonal plane, compared to the one in which the current antenna array is located. By using such a setup, the identification of the target drone could be performed both in azimuth and elevation, allowing for a more precise steering of the directional antenna that is used for transmitting the jamming signal.

The third research direction is related to a subject that was also commented on in Section 5, which is the implementation of a hybrid DDDS in order to improve the overall performance of the system. The addition of imaging sensors is considered, as such an approach would have a twofold contribution; it would improve the accuracy of the detected targets for the situations in which the target drone would be detected by both types of sensors, and it would allow the detection of the target drones also in the situations when only one type of sensor would be able to identify them.

7. Conclusions and Future Work

In this paper, a survey related to the current status of drone detection and defense systems was performed and our own solution for a drone defense system based on SDR platforms (DronEnd) was presented. Different aspects, such as regulatory issues and reported incidents that involved drones, were included in the survey. A classification of the drone detection systems that were based on the type of sensors that are used was performed. A detailed description of the RF-based drone detection and defense systems was made, with an emphasis on the use of SDR platforms for the implementation of such systems. The drone defense system that was developed by the authors within the framework of the DronEnd research project is presented in the final part of the paper. As future work, we intend to conduct a detailed testing of the DronEnd ground system, in order to verify the performance of our solution from the detection, localization, and annihilation points of view and we also plan to develop a flying version of the DronEnd system, by mounting an embedded SDR platform on a support drone and approaching the target drones from the air.

Author Contributions: Conceptualization, F.-L.C., A.M., C.V., I.M., R.C. and O.F.; methodology, F.-L.C. and A.M.; software, A.M.; validation, A.M., C.V., I.M. and O.F.; formal analysis, C.V., I.M. and O.F.; investigation, F.-L.C.; resources, F.-L.C. and A.M.; data curation, F.-L.C. and A.M.; writing—original draft preparation, F.-L.C. and A.M.; writing—review and editing, F.-L.C., A.M., C.V., I.M., R.C. and O.F.; visualization, F.-L.C. and R.C.; supervision, C.V., I.M. and O.F.; project administration, A.M.; funding acquisition, A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by a grant of the Romanian Ministry of Education and Research, CCCDI-UEFISCDI, project number PN-III-P2-2.1-PED-2019-1951, within PNCDI III.

Acknowledgments: The authors would like to acknowledge the editor and the anonymous reviewers for their comments and suggestions that have improved the presentation of this work.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

ACCST	Advanced Continuous Channel Shifting Technology
ACF	Autocorrelation Function
ACMA	Australian Communication and Media Authority
AI	Artificial Intelligence
AoA	Angle of Arrival
CNN	Convolutional Neural Network
DDDS	Drone Detection and Defense Systems
DoA	Direction of Arrival
DRNN	Deep Residual Neural Network
DSP	Digital Signal Processing
DL	Deep Learning
EASA	European Union Aviation Safety
EMP	Electromagnetic Pulses
EO	Electro-optical
FASST	Futaba Advanced Spread Spectrum Technology
FCC	Federal Communications Commission
FPGA	Field-Programmable Gate Array
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
INS	Inertial Navigation Systems/Sensors
IR	Infrared
IS	Islamic State
ISM	Industrial, Scientific, and Medical
KNN	K-Nearest Neighbor
LoS	Line of Sight
MDS	Micro-Doppler Signatures
MCM	Motor Control Module
ML	Machine Learning
MUSIC	MUltiple SIgnal Classification
NTSC	National Television Standards Committee
PSE	Power Spectral Entropy
RC	Remote Control
RF	Radio Frequency
RLS	Recursive Least Squares
RSS	Received-Signal Strength
SDR	Software-Defined Radio
SFS	Signal Frequency Spectrum
SNR	Signal-to-Noise Ratio
STFT	Short-Time Fourier Transform
UAS	Unmanned Aerial Systems
UAV	Unmanned Air Vehicle
WEE	Wavelet Energy Entropy

References

1. Zeng, Y.; Zhang, R.; Lim, T.J. Wireless Communications with Unmanned Aerial Vehicles: Opportunities and Challenges. *IEEE Commun. Mag.* **2016**, *54*, 36–42. [CrossRef]
2. World Economic Forum. Drones and Tomorrow's Airspace. 2020. Available online: https://www.weforum.org/communities/drones-and-tomorrow-s-airspace (accessed on 13 January 2022).
3. Scott, G.; Smith, T. Disruptive Technology: What Is Disruptive Technology? *Investopedia* **2020**. Available online: https://www.investopedia.com/terms/d/disruptive-technology.asp/ (accessed on 13 January 2022).
4. Germen, M. Alternative cityscape visualisation: Drone shooting as a new dimension in urban photography. In Proceedings of the Electronic Visualisation and the Arts (EVA), London, UK, 12–14 July 2016; pp. 150–157.
5. Kaufmann, E.; Gehrig, M.; Foehn, P.; Ranftl, R.; Dosovitskiy, A.; Koltun, V.; Scaramuzza, D. Beauty and the beast: Optimal methods meet learning for drone racing. In Proceedings of the IEEE International Conference on Robotics and Automation, Montreal, QC, Canada, 20–24 May 2019; pp. 690–696.

6. Kaufmann, E.; Loquercio, A.; Ranftl, R.; Dosovitskiy, A.; Koltun, V.; Scaramuzza, D. Deep drone racing: Learning agile flight in dynamic environments. In Proceedings of the Conference on Robot Learning (CoRL), Zürich, Switzerland, 29–31 October 2018; pp. 133–145.
7. Ahmad, A.; Cheema, A.A.; Finlay, D. A survey of radio propagation channel modelling for low altitude flying base stations. *Comput. Netw.* **2020**, *171*, 107122. [CrossRef]
8. Tozer, T.; Grace, D.; Thompson, J.; Baynham, P. UAVs and HAPspotential convergence for military communications. In Proceedings of the IEEE Colloquium on Military Satellite Communications, London, UK, 6 June 2000; pp. 10-1–10-6.
9. Schneiderman, R. Unmanned drones are flying high in the military/aerospace sector. *IEEE Signal Process. Mag.* **2012**, *29*, 8–11. [CrossRef]
10. Chen, J.Y.C. UAV-guided navigation for ground robot tele-operation in a military reconnaissance environment. *Ergonomics* **2010**, *53*, 940–950. [CrossRef]
11. Coffey, T.; Montgomery, J.A. The emergence of mini UAVs for military applications. *Def. Horiz.* **2002**, *22*, 1.
12. Quigley, M.; Goodrich, M.A.; Griffiths, S.; Eldredge, A.; Beard, R.W. Target acquisition, localization, and surveillance using a fixed-wing mini-UAV and gimbaled camera. In Proceedings of the IEEE International Conference on Robotics and Automation, Barcelona, Spain, 18–22 April 2005; pp. 2600–2605.
13. Iscold, P.; Pereira, G.A.S.; Torres, L.A.B. Development of a hand launched small UAV for ground reconnaissance. *IEEE Trans. Aerosp. Electron. Syst.* **2010**, *46*, 335348. [CrossRef]
14. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tezlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. Available online: http://www.prisma-statement.org/ (accessed on 13 January 2022). [CrossRef]
15. Butt, A.; Shah, S.I.A.; Zaheer, Q. Weapon launch system design of anti-terrorist UAV. In Proceedings of the International Conference on Engineering Technology (ICEET), Lahore, Pakistan, 21–22 February 2019; pp. 1–8.
16. EY India. What's the Right Strategy to Counter Rogue Drones? Available online: https://www.ey.com/en_in/emergingtechnologies/whats-the-right-strategy-to-counter-rogue-drones (accessed on 12 January 2022).
17. Ritchie, M.; Fioranelli, F.; Borrion, H. Micro UAV crime prevention: Can we help princess Leia? In *Crime Prevention 21st Century*; Springer: New York, NY, USA, 2017; pp. 359–376.
18. Van Voorst, B.R. Counter Drone System. U.S. Patent 15,443,143, 14 September 2017.
19. Drone Hits Plane at Heathrow Airport, Says Pilot. Available online: https://www.theguardian.com/uk-news/2016/apr/17/drone-plane-heathrow-airport-british-airways (accessed on 12 January 2022).
20. Alex Silverman, Drone Hits Army Helicopter Flying Over Staten Island. Available online: https://newyork.cbslocal.com/2017/09/22/drone-hits-army-helicopter/ (accessed on 12 January 2022).
21. Drone Collides with Commercial Aeroplane in Canada. Available online: https://www.bbc.com/news/technology-41635518 (accessed on 12 January 2022).
22. Boeing 737 Passenger Jet Damaged in Possible Mid-Air Jet. Available online: https://www.bloomberg.com/news/articles/2018-12-13/aeromexico-737-jetliner-damaged-in-possible-midair-drone-strike (accessed on 12 January 2022).
23. Plane Damaged after Being Hit by York Police Drone at Buttonville Airport. Available online: https://toronto.ctvnews.ca/plane-damaged-after-being-hit-by-york-police-drone-at-buttonville-airport-1.5554617 (accessed on 12 January 2022).
24. Drone's Operator Detained for Flying Near Chinese Airplane. Available online: https://edition.cnn.com/2017/01/17/asia/china-drone-passenger-plane-near-miss/ (accessed on 12 January 2022).
25. Air New Zealand Calls for Drone Legislation after Near Miss. Available online: https://www.bbc.com/news/world-asia-43551373.amp (accessed on 12 January 2022).
26. Gatwick Drones: As it Happened. Available online: https://www.bbc.com/news/live/uk-england-sussex-46564814 (accessed on 12 January 2022).
27. Ripley, C.W. Drone with Radioactive Material Found on Japanese Prime Minister's Roof. 2015. Available online: https://edition.cnn.com/2015/04/22/asia/japan-primeminister-rooftop-drone/index.html (accessed on 12 January 2022).
28. Gibbons-Neff, T. ISIS Used an Armed Drone to Kill Two Kurdish Fighters and Wound French Troops, Report Says. 2016. Available online: https://www.washingtonpost.com/news/checkpoint/wp/2016/10/11/isis-used-an-armed-drone-to-kill-twokurdish-ghters-and-wound-french-troops-report-says/ (accessed on 12 January 2022).
29. BBC. Venezuela President Maduro Survives Drone Assassination Attempt. 2018. Available online: https://www.bbc.com/news/world-latin-america-45073385 (accessed on 12 January 2022).
30. Drone Incident Management at Aerodromes. Available online: https://www.easa.europa.eu/sites/default/files/dfu/drone_incident_management_at_aerodromes_part1_website_suitable.pdf (accessed on 12 January 2022).
31. *FCC Enforcement Advisory, Cell Jammers, GPS Jammers, and Other Jamming Devices, document FCC RCD 1329(2)*; FCC: Washington, DC, USA, 2011.
32. Radiocommunications Exemption Arrangements for Drone Jamming Devices. Available online: https://www.acma.gov.au/sites/default/files/2019-08/IFC-4-2019-Consultation%20Paper%20-%20Radiocommunications%20exemption%20arrangements%20for%20drone%20jamming%20devices.docx (accessed on 12 January 2022).
33. Markarian, G.; Staniforth, A. *Countermeasures for Aerial Drones*; ARTECH HOUSE: Norwood, MA, USA, 2021; ISBN 13: 978-1-63081-801-2.

34. Michel, A.H. *Counter-Drones Systems*, 2nd ed.; Report from the Center of the Study of the Drone at Bard College: Annandale-On-Hudson, NY, USA, 2019; Available online: https://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf (accessed on 13 January 2022).
35. Brust, M.R.; Danoy, G.; Stolfi, D.H.; Pascal, B. Swarm-based counter UAV defense system. *Discov Internet Things* **2021**, *1*, 2. [CrossRef]
36. Alsok. 2020. Available online: https://www.alsok.co.jp/en/ (accessed on 12 January 2022).
37. Ottoy, G.; de Strycker, L. An improved 2D triangulation algorithm for use with linear arrays. *IEEE Sens. J.* **2016**, *16*, 8238–8243. [CrossRef]
38. Shi, Z.; Chang, X.; Yang, C.; Wu, Z.; Wu, J. An Acoustic-Based Surveillance System for Amateur Drones Detection and Localization. *IEEE Trans. Veh. Technol.* **2020**, *69*, 2731–2739. [CrossRef]
39. Mezei, J.; Fiaska, V.; Molnar, A. Drone sound detection. In Proceedings of the 16th IEEE International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, Hungary, 19–21 November 2015; pp. 333–338.
40. Hilal, A.A.; Mismar, T. Drone Positioning System Based on Sound Signals Detection for Tracking and Photography. In Proceedings of the 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 4–7 November 2020; pp. 8–11. [CrossRef]
41. Kim, J.; Kim, D. Neural network based real-time UAV detection and analysis by sound. *J. Adv. Inf. Technol. Converg.* **2018**, *8*, 43–52. [CrossRef]
42. Busset, J.; Perrodin, F.; Wellig, P.; Ott, B.; Heutschi, K.; Rühl, T.; Nussbaumer, T. Detection and tracking of drones using advanced acoustic cameras. *Unmanned/Unattended Sens. Sens. Netw. XI Adv. Free. Space Opt. Commun. Tech. Appl.* **2015**, *9647*, 96470F.
43. Christnacher, F.; Hengy, S.; Laurenzis, M.; Matwyschuk, A.; Naz, P.; Schertzer, S.; Schmitt, G. Optical and acoustical UAV detection. *Electro-Opt. Remote Sens. X* **2016**, *9988*, 99880B.
44. Seo, Y.; Jang, B.; Im, S. Drone detection using convolutional neural networks with acoustic STFT features. In Proceedings of the 15th IEEE International Conference on Advanced Video and Signals-based Surveillance (AVSS), Auckland, New Zealand, 27–30 November 2018; pp. 1–6.
45. Bernardini, A.; Mangiatordi, F.; Pallotti, E.; Capodiferro, L. Drone detection by acoustic signature identication. *Electron. Imaging* **2017**, *2017*, 60–64. [CrossRef]
46. Hauzenberger, L.; Ohlsson, E.H. Drone Detection Using Audio Analysis. Master's Thesis, Department of Electrical and Information Technology, Faculty of Engineering, LTH, Lund University, Lund, Sweden, 2015.
47. Harvey, B.; O'Young, S. Acoustic detection of a xed-wing UAV. *Drones* **2018**, *2*, 4. [CrossRef]
48. Yang, C.; Wu, Z.; Chang, X.; Shi, X.; Wo, J.; Shi, Z. DOA Estimation Using Amateur Drones Harmonic Acoustic Signals. In Proceedings of the 2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM), Sheffield, South Yorkshire, 8–11 July 2018; pp. 587–591. [CrossRef]
49. Kim, J.; Park, C.; Ahn, J.; Ko, Y.; Park, J.; Gallagher, J.C. Real-time UAV sound detection and analysis system. In Proceedings of the 2017 IEEE Sensors Applications Symposium (SAS), Glassboro, NJ, USA, 13–15 March 2017; pp. 1–5.
50. Siriphun, N.; Kashihara, S.; Fall, D.; Khurat, A. Distinguishing Drone Types Based on Acoustic Wave by IoT Device. In Proceedings of the 2018 22nd International Computer Science and Engineering Conference (ICSEC), Chiang Mai, Thailand, 21–24 November 2018; pp. 1–4. [CrossRef]
51. Droneshield. Dronesentry. 2020. Available online: https://www.droneshield.com/sentry (accessed on 13 January 2022).
52. Chang, X.; Yang, C.; Wu, J.; Shi, X.; Shi, Z. A surveillance system for drone localization and tracking using acoustic arrays. In Proceedings of the IEEE 10th Sensor Array Multichannel Signal Process Workshop (SAM), Sheffield, UK, 8–11 July 2018; pp. 573–577.
53. Al-Emadi, S.; Al-Ali, A.; Mohammad, A.; Al-Ali, A. Audio based drone detection and identication using deep learning. In Proceedings of the 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 459–464.
54. Opromolla, R.; Fasano, G.; Accardo, D. A vision-based approach to UAV detection and tracking in cooperative applications. *Sensors* **2018**, *18*, 3391. [CrossRef]
55. Rozantsev, A.; Lepetit, V.; Fua, P. Detecting flying objects using a single moving camera. *IEEE Trans. Pattern Anal. Mach. Intell.* **2017**, *39*, 879–892. [CrossRef]
56. Park, J.; Kim, D.H.; Shin, Y.S.; Lee, S. A comparison of convolutional object detectors for real-time drone tracking using a PTZ camera. In Proceedings of the 2017 17th International Conference on Control, Automation and Systems (ICCAS), Jeju, Korea, 18–21 October 2017; pp. 696–699. [CrossRef]
57. Nalamati, M.; Kapoor, A.; Saqib, M.; Sharma, N.; Blumenstein, M. Drone Detection in Long-Range Surveillance Videos. In Proceedings of the 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Taipei, Taiwan, 18–21 September 2019; pp. 1–6. [CrossRef]
58. Müller, T. Robust drone detection for day/night counter-UAV with static VIS and SWIR cameras. *Proc. SPIE* **2017**, *10190*, 302–313.
59. Magoulianitis, V.; Ataloglou, D.; Dimou, A.; Zarpalas, D.; Daras, P. Does deep super-resolution enhance UAV detection. In Proceedings of the 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Taipei, Taiwan, 18–21 September 2019; pp. 1–6.

60. Birch, G.C.; Woo, B.L. *Counter Unmanned Aerial Systems Testing: Evaluation of VIS SWIR MWIR and LWIR Passive Imagers*; SNL-NM: Albuquerque, NM, USA, 2017; Tech. Rep.; SAND2017-0921 650791.
61. Chen, H.; Wang, Z.; Zhang, L. Collaborative spectrum sensing for illegal drone detection: A deep learning-based image classification perspective. *China Commun.* **2020**, *17*, 81–92. [CrossRef]
62. Ringwald, T.; Sommer, L.; Schumann, A.; Beyerer, J.; Stiefelhagen, R. UAV-Net: A fast aerial vehicle detector for mobile platforms. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, CVPR Workshops, Long Beach, CA, USA, 14–19 June 2019; pp. 1–9.
63. Craye, C.; Ardjoune, S. Spatio-temporal semantic segmentation for drone detection. In Proceedings of the 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Taipei, Taiwan, 18–21 September 2019; pp. 1–5.
64. Sapkota, K.R.; Roelofsen, S.; Rozantsev, A.; Lepetit, V.; Gillet, D.; Fua, P.; Martinoli, A. Vision-based unmanned aerial vehicle detection and tracking for sense and avoid systems. In Proceedings of the 2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2016), Daejeon, Korea, 9–14 October 2016; pp. 1556–1561.
65. Aker, C.; Kalkan, S. Using deep networks for drone detection. In Proceedings of the 14th IEEE International Conference on Advanced Video and Signal based Surveillance (AVSS 2017), Lecce, Italy, 29 August–1 September 2017; pp. 1–6.
66. Zhu, P.; Wen, L.; Du, D.; Bian, X.; Ling, H.; Hu, Q.; Nie, Q.; Cheng, H.; Liu, C.; Chenfeng, L.; et al. VisDrone-DET2018: The vision meets drone object detection in image challenge results. In Proceedings of the 15th European Conference, Munich, Germany, 8–14 September 2018; pp. 1–30.
67. Schumann, A.; Sommer, L.; Klatte, J.; Schuchert, T.; Beyerer, J. Deep cross-domain flying object classification for robust UAV detection. In Proceedings of the 14th IEEE International Conference on Advanced Video and Signal based Surveillance (AVSS 2017), Lecce, Italy, 29 August–1 September 2017; pp. 1–6.
68. Wang, L.; Ai, J.; Zhang, L.; Xing, Z. Design of airport obstacle free zone monitoring UAV system based on computer vision. *Sensors* **2020**, *20*, 2475. [CrossRef]
69. Saqib, M.; Khan, S.D.; Sharma, N.; Blumenstein, M. A study on detecting drones using deep convolutional neural networks. In Proceedings of the 14th IEEE Int. Conf. Adv. Video Signal Based Surveill. (AVSS), Lecce, Italy, 29 August–1 September 2017; pp. 1–5.
70. Cigla, C.; Thakker, R.; Matthies, L. Onboard stereo vision for drone pursuit or sense and avoid. In Proceedings of the 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Salt Lake City, UT, USA, 18–22 June 2018; pp. 738–746.
71. Crivellaro, A.; Rad, M.; Verdie, Y.; Yi, K.M.; Fua, P.; Lepetit, V. A novel representation of parts for accurate 3D object detection and tracking in monocular images. In Proceedings of the IEEE International Conference on Computer Vision (ICCV), Santiago, Chile, 7–13 December 2015; pp. 4391–4399.
72. Liu, H.; Qu, F.; Liu, Y.; Zhao, W.; Chen, Y. A drone detection with aircraft classification based on a camera array. In Proceedings of the 4th International Conference on Structure, Processing and Properties of Materials (SPPM 2018), Dhaka, Bangladesh, 1–3 March 2018; Volume 322. no. 5, Art. no. 052005.
73. Wellig, P.; Speirs, P.; Schupbach, C.; Oeschlin, R.; Renker, M.; Boeniger, U.; Pratisto, H. Radar Systems and Challenges for C-UAV. In Proceedings of the 19th International Radar Symposium IRS 2018, Bonn, Germany, 20–22 June 2018.
74. Torvik, B.; Olsen, K.E.; Griffiths, H. Classification of birds and UAVs based on radar polarimetry. *IEEE Geosci. Remote Sens. Lett.* **2016**, *13*, 13051309. [CrossRef]
75. Ren, J.; Jiang, X. Regularized 2-D complex-log spectral analysis and subspace reliability analysis of micro-Doppler signature for UAV detection. *Pattern Recognit.* **2017**, *69*, 225–237. [CrossRef]
76. Kim, B.K.; Kang, H.-S.; Park, S.-O. Drone classification using convolutional neural networks with merged Doppler images. *IEEE Geosci. Remote Sens. Lett.* **2017**, *14*, 38–42. [CrossRef]
77. Mahafza, B.R. *Radar Systems Analysis and Design Using MATLAB*; CRC Press: Boca Raton, FL, USA, 2013.
78. Li, C.J.; Ling, H. An investigation on the radar signatures of small consumer drones. *IEEE Antennas Wirel. Propag. Lett.* **2017**, *16*, 649–652. [CrossRef]
79. Shin, D.-H.; Jung, D.-H.; Kim, D.-C.; Ham, J.-W.; Park, S.-O. A distributed FMCW radar system based on fiber-optic links for small drone detection. *IEEE Trans. Instrum. Meas.* **2017**, *66*, 340–347. [CrossRef]
80. Mizushima, T.; Nakamura, R.; Hadama, H. Reflection characteristics of ultra-wideband radar echoes from various drones in flight. In Proceedings of the IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNeT), San Antonio, TX, USA, 17–20 January 2020.
81. Torvik, B.; Knapskog, A.; Lie-Svendsen, O.; Olsen, K.E.; Griffiths, H.D. Amplitude modulation on echoes from large birds. In Proceedings of the 11th European Radar Conference, Rome, Italy, 8–10 October 2014; pp. 177–180.
82. Guay, R.; Drolet, G.; Bray, J.R. Measurement and modelling of the dynamic radar cross-section of an unmanned aerial vehicle. *IET Radar Sonar Navigat.* **2017**, *11*, 1155–1160. [CrossRef]
83. Stateczny, A.; Lubczonek, J. FMCW radar implementation in river information services in poland. In Proceedings of the 16th International Radar Symposium (IRS), Dresden, Germany, 24–26 June 2015; pp. 852–857.
84. Farlik, J.; Kratky, M.; Casar, J.; Stary, V. Multispectral detection of commercial unmanned aerial vehicles. *Sensors* **2019**, *19*, 1517. [CrossRef]

85. Eriksson, N. Conceptual Study of a Future Drone Detection System-Countering a Threat Posed by a Disruptive Technology. Master's Thesis, Chalmers University Technology, Gothenburg, Sweden, 2018.
86. Chen, V.C. *The Micro-Doppler Effect in Radar*; Artech House: Boston, MA, USA, 2019.
87. Kim, B.K.; Kang, H.-S.; Park, S.-O. Experimental analysis of small drone polarimetry based on micro-Doppler signature. *IEEE Geosci. Remote Sens. Lett.* **2017**, *14*, 1670–1674. [CrossRef]
88. Fang, G.; Yi, J.; Wan, X.; Liu, Y.; Ke, H. Experimental research of multistatic passive radar with a single antenna for drone detection. *IEEE Access* **2018**, *6*, 33542–33551. [CrossRef]
89. Colorado, J.; Perez, M.; Mondragon, I.; Mendez, D.; Parra, C.; Devia, C.; Martinez-Moritz, J.; Neira, L. An integrated aerial system for landmine detection: SDR-based ground penetrating radar onboard an autonomous drone. *Adv. Robot.* **2017**, *31*, 791–808. [CrossRef]
90. Rahman, S.; Robertson, D.A. Millimeter-wave micro-Doppler measurements of small UAVs. *Proc. SPIE* **2017**, *10188*, 101880T.
91. Drozdowicz, J.; Wielgo, M.; Samczynski, P.; Kulpa, K.; Krzonkalla, J.; Mordzonek, M.; Bryl, M.; Jakielaszek, Z. 35 GHz FMCW drone detection system. In Proceedings of the 17th International Radar Symposium (IRS 2016), Krakow, Poland, 10–12 May 2016; pp. 1–4.
92. Fontana, R.J.; Richley, E.A.; Marzullo, A.J.; Beard, L.C.; Mulloy, R.W.T.; Knight, E.J. An ultra wideband radar for micro air vehicle applications. In Proceedings of the 2002 IEEE Conference on Ultra Wideband Systems and Technologies (IEEE Cat. No.02EX580), Baltimore, MD, USA, 21–23 May 2002; pp. 187–191.
93. Liu, Y.; Wan, X.; Tang, H.; Yi, J.; Cheng, Y.; Zhang, X. Digital television based passive bistatic radar system for drone detection. In Proceedings of the IEEE Radar Conference (RadarConf), 8–12 May 2017; pp. 1493–1497.
94. Aldowesh, A.; BinKhamis, T.; Alnuaim, T.; Alzogaiby, A. Low Power Digital Array Radar for Drone Detection and Micro-Doppler Classification. In Proceedings of the 2019 Signal Processing Symposium (SPSympo), Krakow, Polan, 17–19 September 2019; pp. 203–206. [CrossRef]
95. Jian, M.; Lu, Z.; Chen, V.C. Drone detection and tracking based on phase-interferometric Doppler radar. In Proceedings of the 2018 IEEE Radar Conference (RadarConf18), Oklahoma City, OK, USA, 23–27 April 2018; pp. 1146–1149. [CrossRef]
96. Semkin, V.; Yin, M.; Hu, Y.; Mezzavilla, M.; Rangan, S. Drone Detection and Classification Based on Radar Cross Section Signatures. In Proceedings of the 2020 International Symposium on Antennas and Propagation (ISAP), Osaka, Japan, 25–28 January 2021; pp. 223–224. [CrossRef]
97. Jarabo-Amores, M.P.; Mata-Moya, D.; Hoyo, P.J.G.; Bárcena-Humanes, J.; Rosado-Sanz, J.; Rey-Maestre, N.; Rosa-Zurera, M. Drone detection feasibility with passive radars. In Proceedings of the 15th European Radar Conference (EuRAD), Madrid, Spain, 26–28 September 2018; pp. 313–316.
98. Robin Radar Systems. Elvira. 2020. Available online: https://www.robinradar.com/elvira-anti-drone-system (accessed on 13 January 2022).
99. Björklund, S. Target Detection and Classification of Small Drones by Boosting on Radar Micro-Doppler. In Proceedings of the 2018 15th European Radar Conference (EuRAD), Madrid, Spain, 26–28 September 2018; pp. 182–185. [CrossRef]
100. Güvenç, I.; Ozdemir, O.; Yapici, Y.; Mehrpouyan, H.; Matolak, D. Detection, localization, and tracking of unauthorized UAS and jammers. In Proceedings of the 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St. Petersburg, FL, USA, 17–21 September2017; pp. 1–10.
101. Balleri, A. Measurements of the Radar Cross Section of a nano-drone at K-band. In Proceedings of the 2021 IEEE 8th International Workshop on Metrology for AeroSpace (MetroAeroSpace), Naples, Italy, 23–25 June 2021; pp. 283–287. [CrossRef]
102. Al-Nuaim, T.; Alam, M.; Aldowesh, A. Low-Cost Implementation of a Multiple-Input Multiple-Output Radar Prototype for Drone Detection. In Proceedings of the 2019 International Symposium ELMAR, Zadar, Croatia, 23–25 September 2019; pp. 183–186. [CrossRef]
103. CRFS. Drone Detection: Myths and Reality. 2018. Available online: https://www.crfs.com/blog/drone-detection-myths-and-reality/ (accessed on 13 January 2022).
104. Shi, X.; Yang, C.; Xie, W.; Liang, C.; Shi, Z.; Chen, J. Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges. *IEEE Commun. Mag.* **2018**, *56*, 68–74. [CrossRef]
105. Ezuma, M.; Erden, F.; Anjinappa, C.K.; Ozdemir, O.; Guvenc, I. Micro-UAV detection and classication from RF fingerprints using machine learning techniques. In Proceedings of the 2019 IEEE Aerospace Conference, Big Sky, MT, USA, 2–9 March 2019; pp. 1–13.
106. CRFS. DroneDefense. 2020. Available online: https://pages.crfs.com/hubfs/CR-002800-GD-2-DroneDefense%20Brochure.pdf (accessed on 12 January 2022).
107. Allahham, M.S.; Khattab, T.; Mohamed, A. Deep learning for RFbased drone detection and identication: A multi-channel 1-D convolutional neural networks approach. In Proceedings of the 2020 IEEE International Conference on Information Technology (ICIoT), Doha, Qatar, 2–5 February 2020; pp. 112–117.
108. Al-Sa'd, M.F.; Al-Ali, A.; Mohamed, A.; Khattab, T.; Erbad, A. RF based drone detection and identication using deep learning approaches: An initiative towards a large open source drone database. *Future Gener. Comput. Syst.* **2019**, *100*, 86–97. [CrossRef]
109. Nguyen, P.; Truong, H.; Ravindranathan, M.; Nguyen, A.; Han, R.; Vu, T. Matthan: Drone presence detection by identifying physical signatures in the drone's RF communication. In Proceedings of the 15th ACM International Conference on Mobile Systems, Applications, and Services, Niagara Falls, NY, USA, 19–23 June 2017; pp. 211–224.

110. Rodhe and Schwarz. R&S Ardonis. 2020. Available online: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/ARDRONIS_bro_en_5214-7035-12_v0600.pdf (accessed on 13 January 2022).
111. Nguyen, P.; Ravindranatha, M.; Nguyen, A.; Han, R.; Vu, T. Investigating cost-effective RF-based detection of drones. In Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, Singapore, 26 June 2016; pp. 17–22.
112. DeDrone. RF-300 Data Sheet. 2020. Available online: https://assets.website-files.com/58fa92311759990d60953cd2/5d1e14bc96a76a015d193225_dedrone-rf-300-data-sheet-en.pdf (accessed on 13 January 2022).
113. Medaiyese, O.O.; Syed, A.; Lauf, A.P. Machine Learning Framework for RF-Based Drone Detection and Identication System. *arXiv* **2020**, arXiv:2003.02656. Available online: http://arxiv.org/abs/2003.02656 (accessed on 13 January 2022).
114. Robin Radar Systems. Available online: https://www.robinradar.com/press/blog/9-counter-drone-technologies-to-detect-and-stop-drones-today?fbclid=IwAR2Mnxiqbl1JLYmQJ5FXOe-UCKHfoi9jf8T6HbXW7b-LNzX4YkEphGqigEM (accessed on 13 January 2022).
115. Raytheon. Phaser High-Power Microwave System. 2020. Available online: https://www.raytheon.com/capabilities/products/phaser-highpower-microwave-system (accessed on 12 January 2022).
116. Zohuri, B. High-power microwave energy as weapon. In *Directed-Energy Beam Weapons*; Springer: Cham, Switzerland, 2019; pp. 269–308. [CrossRef]
117. Radasky, W.A.; Baum, C.E.; Wik, M.W. Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI). *IEEE Trans. Electromagn. Compat.* **2004**, *46*, 314–321. [CrossRef]
118. Olivares, G.; Gomez, L.; de los Monteros, J.E.; Baldridge, R.J.; Zinzuwadia, C.; Aldag, T. *Volume II-UAS Airborne Collision Severity Evaluation-Quadcopter*; National Institute for Aviation Research: Wichita, KS, USA, 2017; Tech. Rep.; DOT/FAA/AR xx/xx.
119. RoboTiCan. Goshawk. 2020. Available online: https://robotican.net/goshawk/(2020) (accessed on 12 January 2022).
120. AerialX: DroneBullet. Available online: https://www.aerialx.com/defeat.shtml (accessed on 12 January 2022).
121. Anduril Industries. 2020. Available online: https://www.anduril.com/ (accessed on 12 January 2022).
122. Akhlou, M.A.; Arola, S.; Bonnet, A. Drones chasing drones: Reinforcement learning and deep search area proposal. *Drones* **2019**, *3*, 58. [CrossRef]
123. Ban Lethal. Slaugtherbots. 2020. Available online: https://autonomousweapons.org/ (accessed on 12 January 2022).
124. MBDA Missile Systems. Dragonfire Laser Turret Unveiled at DSEI. 2017. Available online: https://www.mbdasystems.com/press-releases/dragonre-laser-turret-unveiled-dsei-2017/ (accessed on 12 January 2022).
125. India Today. KALI: India'sWeapon to Destroy Any Uninvited Missiles and Aircrafts. 2015. Available online: https://www.indiatoday.in/education-today/gk-current-affairs/story/indias-top-secret-weapon-264111-2015-09-21 (accessed on 12 January 2022).
126. Daily Sabah. Turkey's Laser Weapon ARMOL Passes Acceptance Tests. 2019. Available online: https://www.dailysabah.com/defense/2019/09/30/turkeys-laser-weapon-armol-passesacceptance-tests (accessed on 12 January 2022).
127. Sudakov, D. Russia's Combat Laser Weapons Declassified. 2016. Available online: https://www.pravdareport.com/russia/135198-russia_laser_weapons/ (accessed on 12 January 2022).
128. Zeng, Y.; Lyu, J.; Zhang, R. Cellular-connected UAV: Potential, challenges, and promising technologies. *IEEE Wirel. Commun.* **2019**, *26*, 120–127. [CrossRef]
129. Lin, J.; Singer, P. Drones, Lasers, and Tanks: China Shows Off Its Latest Weapons. 2017. Available online: https://www.popsci.com/china-new-weapons-lasers-drones-tanks/ (accessed on 12 January 2022).
130. Josh Spires, Dubai-Made Magnetic Counter-Drone System to Launch Soon. 2021. Available online: https://dronedj.com/2021/01/04/dubai-made-magnetic-counter-drone-system-to-launch-soon/?fbclid=IwAR3e5Lk5TQZzxU_ovMRYqJ6rDm2XU4_T247rZSH9rJlNotDHMQQQkWQIByU (accessed on 12 January 2022).
131. Atherton, K.D. Trained Police Eagles Attack Drones on Command. 2016. Available online: https://www.popsci.com/eagles-attackdrones-at-police-command/ (accessed on 12 January 2022).
132. This Anti-Drone Net Gun Was Built from Scratch. 2017. Available online: https://www.popularmechanics.com/flight/drones/a27427/anti-drone-net-gun-diy/ (accessed on 12 January 2022).
133. Gettinger, D.; Michel, A.H. A Brief History of Hamas and Hezbollah's Drones. 2014. Available online: https://dronecenter.bard.edu/hezbollah-hamas-drones/ (accessed on 13 January 2022).
134. Taylor, H. Knight, Use of Water for Counter Unmanned Aerial Systems (C-UAS). Available online: https://dsiac.org/wp-content/uploads/2020/10/TI-Response-Report_Use-of-Water-for-C-UAS.pdf (accessed on 12 January 2022).
135. Guvenc, I.; Koohifar, F.; Singh, S.; Sichitiu, M.L.; Matolak, D. Detection, tracking, and interdiction for amateur drones. *IEEE Commun. Mag.* **2018**, *56*, 75–81. [CrossRef]
136. Multerer, T.; Ganis, A.; Prechtel, U.; Miralles, E.; Meusling, A.; Mietzner, J.; Vossiek, M.; Loghi, M.; Ziegler, V. Low-cost jamming system against small drones using a 3DMIMOradar based tracking. In Proceedings of the 14th European Radar Conference (EURAD), Nuremberg, Germany, 11–13 October 2017; pp. 299–302.
137. Li, A.; Wu, Q.; Zhang, R. UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 181184. [CrossRef]

138. Curpen, R.; Balan, T.; Miclos, I.A.; Comanici, I. Assessment of signal jamming efficiency against LTE UAVs. In Proceedings of the International Conferenece on Communications (COMM), Bucharest, Romania, 14–16 June 2018; pp. 367–370.
139. Roh, Y.; Jung, S.; Kang, J. Cooperative UAV jammer for enhancing physical layer security: Robust design for jamming power and trajectory. In Proceedings of the IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, 12–14 November 2019; pp. 464–469.
140. Li, K.; Voicu, R.C.; Kanhere, S.S.; Ni, W.; Tovar, E. Energy efficient legitimate wireless surveillance of UAV communications. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2283–2293. [CrossRef]
141. Noh, J.; Kwon, Y.; Son, Y.; Shin, H.; Kim, D.; Choi, J.; Kim, Y. Tractor beam: Safe-hijacking of consumer drones with adaptive GPS spoofing. *ACM Trans. Priv. Secur.* **2019**, *22*, 12:1–12:26. [CrossRef]
142. Moskvitch, K. Are Drones the Next Target for Hackers? 2014. Available online: https://www.bbc.com/future/article/20140206-candrones-be-hacked (accessed on 13 January 2022).
143. Hooper, M.; Tian, Y.; Zhou, R.; Cao, B.; Lauf, A.P.; Watkins, L.; Robinson, W.H.; Alexis, W. Securing commercial WiFi-based UAVs from common security attacks. In Proceedings of the IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 1–3 November 2016; pp. 1213–1218.
144. Kerns, A.J.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. Unmanned aircraft capture and control via GPS spoofing. *J. Field Robot.* **2014**, *31*, 617–636. [CrossRef]
145. Summers, N. Icarus Machine Can Commandeer a Drone Mid-Flight. 2016. Available online: https://www.engadget.com/2016-10-28-icarus-hijack-dmsx-drones.html (accessed on 12 January 2022).
146. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014. Available online: https://www.ancom.ro/en/uploads/links_files/Directive_RED_2014_53_UE.pdf (accessed on 12 January 2022).
147. Hotărâre Privind Punerea la Dispoziție pe Piață a Echipamentelor Radio. Available online: https://www.ancom.ro/uploads/articles/file/industrie/Echipamente%20radio/HG_740_2016_privind_punerea_la_dispozitie_pe_piata_a_echipamentelor_radio_in_vigoare_din_08_08_2019EN.pdf (accessed on 12 January 2022).
148. Taking Flight: The Future of Drones in the UK Government Response. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/937275/future-of-drones-in-uk-consultation-response-web.pdf (accessed on 12 January 2022).
149. Drone Jammers: How They Work, Why They Exist, and Are They Legal? Available online: https://pilotinstitute.com/drone-jammers/ (accessed on 12 January 2022).
150. Drone Laws in Russia. Available online: https://drone-laws.com/drone-laws-in-russia/ (accessed on 12 January 2022).
151. Here's How China is Battling Drones. Available online: https://www.popsci.com/chinas-new-anti-drone-weapons-jammers-and-lasers/ (accessed on 12 January 2022).
152. Nie, W.; Han, Z.; Li, Y.; He, W.; Xie, L.; Yang, X.; Zhou, M. UAV Detection and Localization Based on Multi-dimensional Signal Features. *IEEE Sens. J.* **2021**. [CrossRef]
153. Basak, S.; Rajendran, S.; Pollin, S.; Scheers, B. Drone classification from RF fingerprints using deep residual nets. In Proceedings of the 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 5–9 January 2021; pp. 548–555. [CrossRef]
154. Ezuma, M.; Erden, F.; Anjinappa, C.K.; Ozdemir, O.; Guvenc, I. Detection and Classification of UAVs Using RF Fingerprints in the Presence of Wi-Fi and Bluetooth Interference. *IEEE Open J. Commun. Soc.* **2020**, *1*, 60–76. [CrossRef]
155. Xu, C.; Chen, B.; Liu, Y.; He, F.; Song, H. RF Fingerprint Measurement for Detecting Multiple Amateur Drones Based on STFT and Feature Reduction. In Proceedings of the 2020 Integrated Communications Navigation and Surveillance Conference (ICNS), Virtual Conference, 8–10 September 2020; pp. 4G1-1–4G1-7. [CrossRef]
156. Nemer, I.; Sheltami, T.; Ahmad, I.; Yasar, A.U.-H.; Abdeen, M.A.R. RF-Based UAV Detection and Identification Using Hierarchical Learning Approach. *Sensors* **2021**, *21*, 1947. [CrossRef]
157. Bisio, I.; Garibotto, C.; Lavagetto, F.; Sciarrone, A.; Zappatore, S. Blind Detection: Advanced Techniques for WiFi-Based Drone Surveillance. *IEEE Trans. Veh. Technol.* **2019**, *68*, 938–946. [CrossRef]
158. Flak, P. Drone Detection Sensor with Continuous 2.4 GHz ISM Band Coverage Based on Cost-Effective SDR Platform. *IEEE Access* **2021**, *9*, 114574–114586. [CrossRef]
159. Kaplan, B.; Kahraman, İ.; Görçin, A.; Çırpan, H.A.; Ekti, A.R. Measurement based FHSS–type Drone Controller Detection at 2.4GHz: An STFT Approach. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Online, 18 November–16 December 2020; pp. 1–6. [CrossRef]
160. IGelman, S.; Loftus, J.P.; Hassan, A.A. *Adversary UAV Localization with Software Defined Radio*; Worcester Polytechnic Institute: Worcester, MA, USA, 2019; Tech. Rep.; E-project-041719-144214.
161. Miranda, R.K.; Ando, D.A.; da Costa, J.P.C.L.; de Oliveira, M.T. Enhanced Direction of Arrival Estimation via Received Signal Strength of Directional Antennas. In Proceedings of the 2018 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Louisville, KY, USA, 6–8 December 2018; pp. 162–167. [CrossRef]
162. Brito, A.; Sebastião, P.; Souto, N. Jamming for Unauthorized UAV Operations-Communications Link. In Proceedings of the 2019 International Young Engineers Forum (YEF-ECE), Costa da Caparica, Portugal, 10 May, 2019; pp. 94–98. [CrossRef]
163. Ferreira, R.; Gaspar, J.; Souto, N.; Sebastião, P. Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms. In Proceedings of the 2018 Global Wireless Summit (GWS), Chiang Rai, Thailand, 25–28 November 2018; pp. 27–32. [CrossRef]

164. Pärlin, K.; Alam, M.M.; le Moullec, Y. Jamming of UAV remote control systems using software defined radio. In Proceedings of the 2018 International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, Poland, 22–23 May 2018; pp. 1–6. [CrossRef]
165. Fang, L.; Wang, X.H.; Zhou, H.L.; Zhang, K. Design of Portable Jammer for UAV Based on SDR. In Proceedings of the 2018 International Conference on Microwave and Millimeter Wave Technology (ICMMT), Chengdu, China, 7–11 May 2018; pp. 1–3. [CrossRef]
166. Skorobogatov, G.; Barrado, C.; Salamí, E. Multiple UAV systems: A survey. *Unmanned Syst.* **2020**, *8*, 149–169. [CrossRef]
167. Yavariabdi, A.; Kusetogullari, H.; Celik, T.; Cicek, H. FastUAV-NET: A Multi-UAV Detection Algorithm for Embedded Platforms. *Electronics* **2021**, *10*, 724. [CrossRef]
168. Li, J.; Ye, D.H.; Chung, T.; Kolsch, M.; Wachs, J.; Bouman, C. Multi-target detection and tracking from a single camera in Unmanned Aerial Vehicles (UAVs). In Proceedings of the 2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Daejon, Korea, 9–14 October 2016; pp. 4992–4997. [CrossRef]
169. Sazdić-Jotić, B.; Pokrajac, I.; Bajčetić, J.; Bondžulić, B.; Obradović, D. Single and multiple drones detection and identification using RF based deep learning algorithm. *Expert Syst. Appl.* **2022**, *187*, 115928. [CrossRef]
170. The Most Promising Defense against Militarized Drone Swarms. Available online: https://mindmatters.ai/2021/06/the-most-promising-defense-against-militarized-drone-swarms/ (accessed on 13 January 2022).
171. Cyberwall. Available online: http://cyberwall.ro (accessed on 12 January 2022).
172. DronEnd Research Project. Available online: http://dronend.ro (accessed on 12 January 2022).
173. Martian, A.; Chiper, F.-L.; Craciunescu, R.; Vladeanu, C.; Fratu, O.; Marghescu, I. RF Based UAV Detection and Defense Systems: Survey and a Novel Solution. In Proceedings of the 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Bucharest, Romania, 16–18 June 2021; pp. 1–4. [CrossRef]
174. Vladeanu, C.; Nastase, C.; Martian, A. Energy Detection Algorithm for Spectrum Sensing Using Three Consecutive Sensing Events. *IEEE Wirel. Commun. Lett.* **2016**, *5*, 284–287. [CrossRef]
175. Martian, A.; Al Sammarraie, M.J.A.; Vlădeanu, C.; Popescu, D.C. Three-Event Energy Detection with Adaptive Threshold for Spectrum Sensing in Cognitive Radio Systems. *Sensors* **2020**, *20*, 3614. [CrossRef] [PubMed]
176. Urkowitz, H. Energy Detection of Unknown Deterministic Signals. *Proc. IEEE* **1967**, *55*, 523–531. [CrossRef]
177. Ettus Research USRP X310. Available online: https://www.ettus.com/all-products/x310-kit/ (accessed on 12 January 2022).
178. Ettus Research Twin-RX RF Daughterboard. Available online: https://www.ettus.com/all-products/twinrx/ (accessed on 12 January 2022).
179. DJI Mavic Air Drone. Available online: https://www.dji.com/mavic-air (accessed on 12 January 2022).
180. DJI Phantom 4 Pro v2.0 Drone. Available online: https://store.dji.com/product/phantom-4-pro-v2/ (accessed on 12 January 2022).
181. DJI Mini 2 Drone. Available online: https://store.dji.com/product/mini-2 (accessed on 12 January 2022).
182. Mini-Circuits ZN4PD1-63HP-S+ 4 Ways DC Pass Power Splitter. Available online: https://www.minicircuits.com/WebStore/dashboard.html?model=ZN4PD1-63HP-S%2B (accessed on 12 January 2022).
183. Ettus Research VERT2450 Antenna. Available online: https://www.ettus.com/all-products/vert2450/ (accessed on 12 January 2022).
184. Ettus Research B200mini SDR Platform. Available online: https://www.ettus.com/all-products/usrp-b200mini/ (accessed on 12 January 2022).
185. Mini-Circuits ZHL-2W-63-S+ Power Amplifier. Available online: https://www.minicircuits.com/WebStore/dashboard.html?model=ZHL-2W-63-S%2B (accessed on 12 January 2022).
186. Ubiquiti UMA-D Antenna. Available online: https://dl.ubnt.com/datasheets/unifi/UMA-D_DS.pdf (accessed on 12 January 2022).