



HAL
open science

Drone Detection and Tracking Using RF Identification Signals

Driss Aouladhadj, Ettien Kpre, Virginie Deniau, Aymane Kharchouf,
Christophe Gransart, Christophe Gaquière

► **To cite this version:**

Driss Aouladhadj, Ettien Kpre, Virginie Deniau, Aymane Kharchouf, Christophe Gransart, et al..
Drone Detection and Tracking Using RF Identification Signals. *Sensors*, 2023, 23 (17), pp.7650.
10.3390/s23177650 . hal-04205964

HAL Id: hal-04205964

<https://univ-eiffel.hal.science/hal-04205964v1>







Submitted on 13 Sep 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Article

Drone Detection and Tracking Using RF Identification Signals

Driss Aouladhadj ^{1,2,*}, Ettien Kpre ², Virginie Deniau ¹, Aymane Kharchouf ², Christophe Gransart ¹
and Christophe Gaquière ²

¹ COSYS-LEOST, Université Gustave Eiffel, 20 Rue Élisée Reclus, 59650 Villeneuve-d'Ascq, France; virginie.deniau@univ-eiffel.fr (V.D.); christophe.gransart@univ-eiffel.fr (C.G.)

² MC2 Technologies, 1 Rue Héraclès, 59493 Villeneuve-d'Ascq, France; ekpre@mc2-technologies.com (E.K.); akharchouf@mc2-technologies.com (A.K.); cgaquiere@mc2-technologies.com (C.G.)

* Correspondence: daouladhadj@mc2-technologies.com

Abstract: The market for unmanned aerial systems (UASs) has grown considerably worldwide, but their ability to transmit sensitive information poses a threat to public safety. To counter these threats, authorities, and anti-drone organizations are ensuring that UASs comply with regulations, focusing on strategies to mitigate the risks associated with malicious drones. This study presents a technique for detecting drone models using identification (ID) tags in radio frequency (RF) signals, enabling the extraction of real-time telemetry data through the decoding of Drone ID packets. The system, implemented with a development board, facilitates efficient drone tracking. The results of a measurement campaign performance evaluation include maximum detection distances of 1.3 km for the Mavic Air, 1.5 km for the Mavic 3, and 3.7 km for the Mavic 2 Pro. The system accurately estimates a drone's 2D position, altitude, and speed in real time. Thanks to the decoding of telemetry packets, the system demonstrates promising accuracy, with worst-case distances between estimated and actual drone positions of 35 m for the Mavic 2 Pro, 17 m for the Mavic Air, and 15 m for the Mavic 3. In addition, there is a relative error of 14% for altitude measurements and 7% for speed measurements. The reaction times calculated to secure a vulnerable site within a 200 m radius are 1.83 min (Mavic Air), 1.03 min (Mavic 3), and 2.92 min (Mavic 2 Pro). This system is proving effective in addressing emerging concerns about drone-related threats, helping to improve public safety and security.

Keywords: drone; UAV; C-UAS; RF signal; Drone ID; detection system; tracking system; drone position; distance estimation; reaction time



Citation: Aouladhadj, D.; Kpre, E.; Deniau, V.; Kharchouf, A.; Gransart, C.; Gaquière, C. Drone Detection and Tracking Using RF Identification Signals. *Sensors* **2023**, *23*, 7650. <https://doi.org/10.3390/s23177650>

Academic Editors: Angelo Coluccia, Dimitrios Zarpalas, Anastasios Dimou, Arne Schumann, Lars Sommer and Alessio Fascista

Received: 26 July 2023

Revised: 26 August 2023

Accepted: 1 September 2023

Published: 4 September 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Unmanned aerial vehicles (UAVs) commonly known as drones, are becoming omnipresent in various industries due to their versatility and sophistication. By integrating advanced technologies, such as modular software architecture, and a multitude of sensors (Global Positioning System (GPS), light detection and ranging (LiDAR), radio detection and ranging (RaDaR), and visual sensors), drones can perform a wide range of tasks, from surveillance and videography [1] to agriculture monitoring [2], delivery services [3], and aiding in health emergencies [4,5]. These flying machines offer numerous benefits, including stability, ease of piloting, and autonomous flight [6] with pre-programmed flight data. Another advantage of drones is their ability to fly in large numbers and communicate efficiently [7], taking advantage of swarm intelligence techniques [8] often used in optimization problems. However, the widespread use of drones has also led to their exploitation in malicious activities [9], including drug trafficking [10], smuggling, and bombing [11]. These activities pose a significant threat to public safety. Thus, it is required to detect the presence of unauthorized drones to fight against these malicious activities.

Figure 1 illustrates the multifaceted applications of drones, highlighting both their beneficial and malicious uses. To distinguish between drones used for legitimate or malicious activities, accurate drone detection and tracking systems are required. These systems

can enable countermeasures to be activated in good time. To address these challenges, counter-unmanned aerial systems (C-UASs) [9,12–18] have to be developed. Effective detection, tracking, and recognition solutions [19–21] are essential if any suspicious drone activity is to be neutralized.

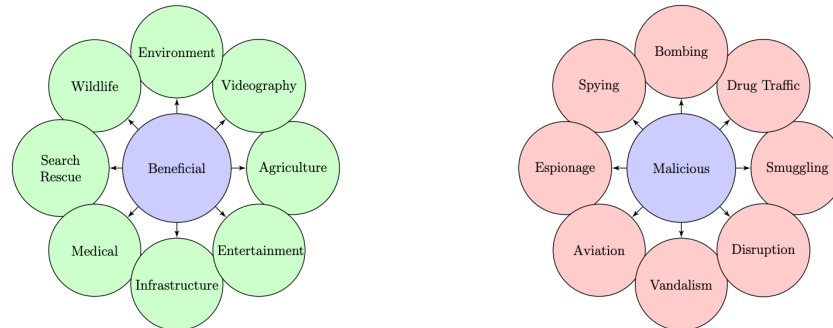


Figure 1. Summary of beneficial and malicious uses of drones.

This article focuses on drone detection through RF spectrum monitoring [22]. It presents a comprehensive and advanced approach to detect and decode Drone ID signals [23]. To assess the effectiveness of the proposed system, a measurement campaign was carried out over a larger area, involving three drones: DJI Mavic Air, DJI Mavic 2 Pro, and DJI Mavic 3, equipped with RF Drone ID signals. These drone models offer insights into the types of drones that may see widespread adoption in the future among both professional and amateur users.

2. Background and Related Work

Different technologies can be exploited for detecting and tracking drones. UAV detection methods, based on imagery and radar sensors, necessarily work in line of sight (LoS) conditions. In urban environments, drones can navigate without being detected by these methods because they can be masked by buildings. In addition, in vast open areas, these methods can have high detection distances but may lead to false detection due to confusion with other flying entities, such as birds. Acoustic technologies, meanwhile, suffer from limited detection range and ambient noise susceptibility. A more exhaustive overview of drone detection methodologies can be found in Table 1.

Table 1. Overview of technologies for drone detection and tracking [17,24].

Type	Definition	Pros	Cons	References
EO/IR Imaging	Visual-based detection using cameras to capture and analyze drone presence, covering the visible and IR spectrum from 3 MHz to 300 GHz.	<ul style="list-style-type: none"> • Use of computer-vision AI algorithms; • Availability of high-resolution cameras; • Real-time tracking. 	<ul style="list-style-type: none"> • Limited range; • Weather-dependent; • LoS is required; • Low-light issues. 	[25,26]
Acoustic	Auditory detection, leveraging microphone arrays to discern drone-produced sounds, covering the spectrum from 20 Hz to 20 kHz.	<ul style="list-style-type: none"> • Passive detection; • LoS is not required; • Low power consumption. 	<ul style="list-style-type: none"> • Sensitive to ambient noise; • Extremely short detection range; • Dependency on drone noise. 	[27,28]
RaDaR	RCS reflection or micro-doppler signature-based detection, with a bandwidth used from 3 MHz to 300 GHz.	<ul style="list-style-type: none"> • Long detection range; • 360-degree coverage; • All-weather operation. 	<ul style="list-style-type: none"> • Large RCS; • Confusion with other flying objects, such as birds; • LoS is required; • Expensive. 	[18,29,30]

Table 1. Cont.

Type	Definition	Pros	Cons	References
Radio Frequency	Monitoring the radio frequency spectrum, identifying drone-specific communication signals.	<ul style="list-style-type: none"> • Passive detection; • LoS is not required; • Low complexity and easy to implement; • Easier to upgrade due to modular implementation; • Possibility of decoding communication signals; • Potential to localize the pilot. 	<ul style="list-style-type: none"> • Requires a large database of RF drone/RC signals; • Confusion with other RF communications, especially in complex environments; • Vulnerable to illegally modified RF hardware drones that exceed receiver capabilities. 	[31–33]

The passive RF detection method relies on spectral surveillance to identify the communications between the drone and its remote control (RC) within the electromagnetic spectrum. These methods do not require LoS. However, passive RF detection faces challenges when the signals emitted by the drone coexist with numerous other signals, such as Wi-Fi or Bluetooth, which share the same frequency band. This presents a challenge in attributing each signal to its respective emitter, especially in complex urban environments. Consequently, it necessitates the collection of RF communication data from each RF source and the construction of a comprehensive database encompassing various scenarios and diverse environments to enhance detection capabilities for more general cases. To address these challenges, recent studies have made notable contributions. In 2019, Al-Sa'd et al. [34] introduced an open-source drone database for RF-based detection and identification, demonstrating the effectiveness of deep neural networks in achieving high accuracy rates. In 2020, Feng et al. [35] proposed an efficient two-step method for detecting drone hijacking using a combination of genetic algorithm-extreme gradient boosting (GA-XGBoost) with GPS and inertial measurement unit (IMU) data, achieving high prediction correctness and time savings. In 2021, the study conducted by Basak et al. [31] introduced a two-stage approach. The detection stage employed goodness-of-fit (GoF) sensing, while the classification stage utilized the deep recurrent neural network (DRNN) framework. They developed a customized you only look once (YOLO)-lite framework from scratch to achieve integrated drone RF signal detection, spectrum localization, and classification. The performance of both techniques was evaluated using a newly created drone dataset, demonstrating favorable results in terms of detection and classification. However, it is important to note that since the classification was conducted in a supervised manner, the performance may vary when encountering unknown or newer drone signals, as highlighted in the limitations. In 2022, Medaiyese et al. [36] employed wavelet transform analytics and machine learning for RF-based UAV detection, achieving 98.9% accuracy with an image-based signature and a pre-trained convolutional neural network (CNN)-based model. Kılıç et al. [37] also focused on drone classification based on RF signals, achieving high accuracy rates using spectral-based audio features and a support vector machine (SVM)-based machine learning algorithm. In the same year, Sazdic-Jotic et al. [38] presented a method for single and multiple drone detection and identification using RF-based deep learning algorithms, achieving high accuracy in both scenarios.

Previous methods used for drone detection and classification exhibit suboptimal performance. First, to integrate new drones into the full database, it is necessary to study and record all potential communication scenarios and take into account different channel and multipath models [32,34,39]. However, this approach can introduce limitations in terms of flexibility and operational efficiency. Moreover, they rely heavily on AI algorithms that operate on large data sets, resulting in a procedure that requires significant training

and consumes considerable memory resources. Furthermore, the previous techniques concentrate only on the processing of the raw modulated signals without the possibility of analyzing the data encoded in the communication protocol. Therefore, they cannot extract crucial information relevant to the defense industry, such as the device manufacturer, the location of the drone, and the purpose and mission of the flight. In this perspective of analyzing the data link layer and the network layer, some recent research has contributed to the development of this idea. Christof [40] reverse-engineered the Wi-Fi protocol of DJI drones. Using deductive and bit-perfect analysis, he was able to determine the structure of the protocol and extract information using specially developed open-source software. This information can be crucial for detecting and locating drones in real time. In addition, Bender [41] and the Department 13 article [42] demonstrated that DJI Drone IDs are not encrypted. This discovery is essential for drone detection, as it allows DJI drones to be spotted and identified using dedicated software-defined radio (SDR). The author proposed a real-time DJI OcuSync Drone ID detection system, using low-cost SDRs with robust packet analysis. This detection system was found to be much cheaper than DJI AeroScope [43], which is priced between USD 20,000 and USD 40,000. In addition, the detection system not only allows model identification but also the retrieval of serial numbers and telemetry information from DJI drones. However, this system's detection range is currently limited to 1.2 km.

The originality of the proposed solution and the work presented in this article is summarized as follows:

- Addressing a method that allows integrating drone detection, classification, and localization solutions into a single module.
- Proposing a complete system integrating both hardware components and software tools and capable of detecting some recent drones.
- Carrying out a long-distance measurement campaign to assess detection performance in terms of distance and altitude.
- Providing real-time estimation of drone localization parameters, including position, velocity, and altitude. The Haversine formulas are used to estimate the remaining distance between the system and the detected drone.
- Providing an estimated remaining reaction time in the context of securing an area with a specified radius.

This research paper delves into drone detection and tracking through RF spectrum monitoring, offering an approach to decode drone identification signals. The proposed system integrates both hardware components and software tools to accomplish detection and tracking tasks. A measurement campaign involving three drones has been executed to evaluate the system's efficacy in terms of range detection, estimating the altitude and velocity of each drone, their trajectory, and finally, their remaining time to penetrate a secured zone protected by this system.

The rest of the paper is organized as follows: We present the RF communication protocols commonly used by drones in Section 3, including details about Drone ID packets. The general methodology underlying our implemented drone detection and tracking algorithms is presented in Section 4. We then describe the hardware components and software tools used for monitoring, signal processing, and analysis in Sections 5 and 6, respectively. For the experimental setup involving three drones, we elaborate on the configuration in Section 7. The methodology for conducting measurements and evaluating the system's performance is detailed in Section 8. In Section 9, we provide a comprehensive analysis and interpretation of the obtained results. Finally, we conclude the paper in Section 10, highlighting the strengths and limitations of our detection solution and providing suggestions for future improvements.

3. Drone Communication Protocols

Most UASs utilize RF transmissions for communication between the UAV and its associated RC [44]. This bi-directional communication involves both uplink and downlink

signals, allowing for seamless information exchange. It enables the transfer of precise control commands, encompassing throttle, pitch, yaw, and roll, to ensure accurate maneuvering of the UAV. Furthermore, it facilitates the exchange of crucial information with the pilot, including UAV position, remaining flight time, distance to target and pilot, payload specifics, speed, altitude, and video imagery. Additionally, it supports the transmission of flight missions, acknowledgments, and protocol-dependent data, expanding the scope of control commands beyond the drone's speed coordinates.

The drone transmission system typically operates in the industrial, scientific, and medical (ISM) bands, and the frequency choice depends on the geographical location of the drone. For example, in France, the 2.4 GHz band offers a wide coverage area but a slower data transmission speed, while the 5.8 GHz band provides a faster data speed but a more limited coverage area.

Several communication protocols can be used to establish the RF link between the drone and its RC, including Wi-Fi, enhanced Wi-Fi, Lightbridge, and OcuSync. The drone's range, video transmission quality, latency, available control frequencies, and other related parameters all depend heavily on the communication protocol employed.

3.1. Wi-Fi and Enhanced Wi-Fi Communication Protocols

The use of standard Wi-Fi in drones offers an efficient and cost-effective control method for many manufacturers. This standard utilizes the conventional IEEE Wi-Fi 802.11 network to connect the drone and a control device. The drone creates a private Wi-Fi network, which users can access by providing a password. This Wi-Fi connection lets users control the possibility of controlling the drone using a dedicated RC, a cell phone, or a tablet.

Some drones on the market, such as DJI's Spark, Mavic Air, DJI Mini, and Mini SE models, employ Wi-Fi technology for connectivity. They support two frequency bands, 2.4 GHz and 5.8 GHz, and the system intelligently switches between them for optimal control. DJI offers two Wi-Fi connectivity options for these drones: standard Wi-Fi for the Spark model and enhanced Wi-Fi for the Mavic Air, Mini, and Mini SE drones. Standard Wi-Fi connectivity provides a transmission range of up to 500 m for the Spark, while enhanced Wi-Fi connectivity enables the Mavic Air, Mini, and Mini SE to achieve a transmission range of up to 2000 m. Both Wi-Fi systems support 720 p video transmission, providing users with a clear view of the drone's camera for surveillance, shooting, and other applications.

Moreover, drone manufacturers have also developed proprietary or enhanced Wi-Fi protocols to optimize performance and enhance the user experience. These protocols offer features such as extended range, reduced latency, and greater resistance to interference, ensuring more robust connectivity for drone operations [45].

3.2. Lightbridge Communication Protocol

In response to the limitations of Wi-Fi for professional drone applications, DJI made a strategic shift towards developing the Lightbridge communication protocol. This move was driven by the need for enhanced performance, reliability, and range in professional and enterprise-level drone operations. Wi-Fi, while suitable for consumer-grade drones, often faces challenges in terms of signal stability, latency, and limited range. By introducing Lightbridge, DJI aimed to address these limitations and provide a robust communication solution for their professional drone lineup.

Lightbridge drones utilize a dual-band transmission system, operating on both the 2.4 GHz and 5.8 GHz frequency bands. This dual-band capability allows for improved signal resilience and flexibility, as the drones can intelligently switch between the two frequency bands based on the environmental conditions and interference levels. The transmission system ensures reliable and low-latency video transmission, providing pilots with a clear and real-time view from the drone's camera.

The Lightbridge communication protocol offers two main versions: Lightbridge HD and Lightbridge HD 2 [46]. These versions are implemented in various DJI drone models, including the Phantom 4 Pro, Phantom 4 Advanced, Inspire 2, Matrice 200 Series, and

Matrice 600 Pro. Lightbridge-equipped drones are capable of transmitting signals over an extended range, reaching up to 3.6 km in countries subject to CE regulations.

Lightbridge drones leverage advanced features to deliver high-quality video transmission and responsive control for professional aerial photography, cinematography, and industrial applications. With this protocol, DJI has significantly improved the communication capabilities of their drones compared to the Wi-Fi and the enhanced Wi-Fi protocols, offering professionals a reliable and efficient tool for their work [45].

3.3. OcuSync Communication Protocol

The OcuSync protocol, developed by DJI, is widely employed in the latest consumer and enterprise models of their drones [47]. It offers an extended transmission range compared to both the Wi-Fi and Lightbridge protocols.

OcuSync utilizes a multi-band, multi-service, and multi-channel approach to ensure optimal stability and data throughput. Its multi-service system enables simultaneous transmission of video, control, and telemetry signals. With the implementation of orthogonal frequency division multiplexing (OFDM), the video signal can withstand interference or attenuation, delivering satisfactory performance even over long distances. Furthermore, the protocol incorporates automatic channel switching, seamlessly transitioning to less congested channels when interference surpasses a certain threshold. This ensures uninterrupted video transmission, while the control and telemetry signals utilize frequency hopping spread spectrum (FHSS) modulation. By employing FHSS, packets are sent using random frequencies that regularly change, enhancing resistance to packet loss [40].

DJI has consistently enhanced its OcuSync transmission system over time [48]. It was initially introduced in the Mavic Pro, followed by the improved OcuSync 2.0 [46] in the Mavic 2 Pro/Zoom and Mini 2 drones. The latest advancements include OcuSync 3.0, OcuSync 3.0+, and OcuSync 3.0 Enterprise, featured in drones such as the Mavic 3, Mini 3 Pro, M30 series, and M300 RTK. These drones benefit from OcuSync's advanced capabilities, providing users with reliable, high-quality transmission for a wide range of applications [45].

3.4. Drone Specific Packets

3.4.1. RDID Packet

Remote drone identification (RDID) is now an essential global regulatory framework implemented in regions such as the USA, Europe, France, and Japan, following international standards such as American Society for Testing and Materials (ASTM) and Aerospace and Defence Industries Association of Europe (ASD-STAN). The Federal Aviation Administration (FAA) introduced the RDID rule in April 2021, making real-time identification and tracking of drones, operators, and ground control stations mandatory. Drone manufacturers must comply with the RDID standard by September 2022, and operators have until September 2023 [49].

By broadcasting identification codes, position data, and emergency status, RDID enables effective detection and tracking of drones. This improves safety, security, and regulatory compliance. Drones can achieve RDID compliance through network-based approaches using persistent internet connections or broadcast-based approaches using Wi-Fi or Bluetooth technologies. Specific areas, called FAA-recognized identification areas (FRIA), allow operation without an RDID module. International regulations, such as those of Europe, France, and Japan, address RDID requirements and impose the dissemination of unique identification serial numbers, locations, and operator information. The guidelines provided by ASTM and ASD-STAN focus on the dissemination of drone identity and global navigation satellite systems (GNSS) location using Bluetooth and Wi-Fi technologies [50]. An example of implementing RDID can be found in the repository available in [51].

3.4.2. DJI Drone ID Packets

DJI has launched the transmission of a private drone identifier for several reasons. The use of a localized, unconnected identifier associated with a specific drone enables seamless integration of public safety, security, and drone operator liability while guaranteeing operator privacy and security. To achieve this, DJI uses two exclusive communication protocols, enhanced Wi-Fi and OcuSync, to transmit the DJI Drone ID signal.

On the one hand, the DJI Drone ID enhanced Wi-Fi signal occupies a bandwidth of 5 MHz and uses FHSS modulation on the 2.4 GHz and 5.8 GHz bands. DJI incorporates this identification packet into IEEE 802.11 Wi-Fi beacon management frames, which are designed to announce the presence of vehicles.

On the other hand, the DJI Drone ID OcuSync is transmitted by the drone using the same hardware as its communication. It occupies a bandwidth of 10 MHz and utilizes FHSS modulation on the 2.4 GHz and 5.8 GHz bands. Notably, even if a user forces the DJI OcuSync communication downlink to operate on 2.4 GHz or 5.8 GHz using the DJI smartphone app, the DJI Drone's identification signals continue to be broadcast out-of-band via the communication link [41].

4. Drone Detection and Tracking Methodology

As mentioned previously, the communication protocol varies from one drone to another. This article focuses on drones that use the Wi-Fi standard or enhanced Wi-Fi for communication, as well as drones equipped with Wi-Fi Remote ID or enhanced Wi-Fi DJI Drone ID signals.

Figure 2 illustrates a scenario of malicious use of a drone, with a remote pilot controlling the drone while hovering or flying near a vulnerable site. To ensure effective protection, the detection system has to be in the area to protect. This system has to be able to detect the uplink and downlink signals and relay information about the drone's presence and location to a central server. The range of detection depends on factors such as the RF amplification chain, hardware components, and software processes involved in the system.

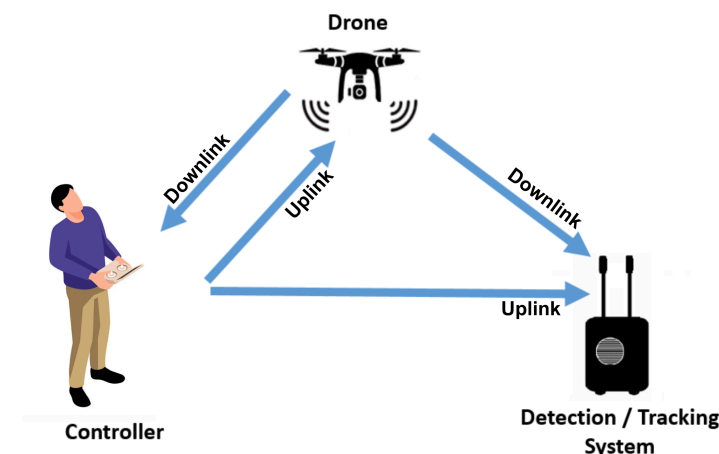


Figure 2. Detection and tracking scenario: downlink (video and telemetry)/uplink (control).

Thus, regardless of whether a drone complies with regulations or not, the system should detect all drones operating within its vicinity. Taking into account these different drones, we break down the problem into three detection cases:

- Drones that communicate using the Wi-Fi standard protocol within the ISM band.
- Drones that transmit a Wi-Fi RDID beacon on channel 6 (at 2437 MHz) within the 2.4 GHz Wi-Fi band.
- DJI drones that transmit the enhanced Wi-Fi DJI Drone ID signal. The specific channel used by these drones is pseudo-random and can be within either the 2.4 GHz or 5.8 GHz ISM band.

This article does not cover DJI drones emitting the OcuSync DJI Drone ID [41], nor drones using communication protocols for which decoding methods are currently undergoing reverse-engineering processes.

5. Detection and Tracking Hardware System

In this section, we present the hardware equipment used to monitor the frequency bands and detect drones with their ID signals. The system comprises various components designed specifically for this purpose.

5.1. Jetson Nano Development Kit

In this study, the Jetson Nano developer kit was selected to constitute the processing unit of the detection system. The Jetson Nano platform hosts all the algorithms and software components necessary for the acquisition, analysis, and decoding of signals. The performance of the Jetson Nano kit may not be essential for the developments described in this article. However, the selection of the Jetson was made with the expectation of the potential utilization of AI algorithms in the future to detect and track drones with unknown protocols.

5.2. Wi-Fi Receiver for RF Monitoring

With the aim of drone detection through Wi-Fi standard and enhanced Wi-Fi protocols, specific receivers are used to detect these signals, as the Jetson card only serves for data processing and not for data acquisition. This prototype features two distinct RF Wi-Fi receivers. The first one is specifically designed to detect frequency hopping DJI Drone ID and standard Wi-Fi communication. The other one is set to detect the RDID fixed at 2437 MHz.

As shown in Figures 3 and 4, both the Intel 8265 [52] and the Panda [53] Wi-Fi boards are capable of detecting Wi-Fi packets. On the one hand, the Intel card has an advantage over other Wi-Fi chips because it can scan a wide range of Wi-Fi channels, from 1 to 177, covering frequencies of 2.4 GHz and 5.8 GHz, with instantaneous bandwidths of 5 MHz, 10 MHz, 20 MHz, and 40 MHz.



Figure 3. Intel wireless chipset.



Figure 4. Panda wireless chipset.

On the other hand, the Panda Wi-Fi card offers a coaxial SMA RF connector for connecting an optimized Rx chain, and supports only 2.4 GHz frequencies, making it ideal for long-range wireless network deployments. Moreover, it offers a throughput of up to 300 MB per second. Both Wi-Fi cards can monitor and intercept Wi-Fi packets, enabling access to the drone's data. Wireless card performance has a significant impact on range and accuracy. Choosing the right Wi-Fi card is, therefore, essential to build an effective drone detection and tracking system.

5.3. Radio Receiver Architecture

Wi-Fi signals can be strongly attenuated with distance and the presence of obstacles. To ensure drone detection from significant distances, the detection system should detect weak Wi-Fi signals. An RF amplification chain is then required. The implemented RF architecture is tailored to the system's specifications. Indeed, the RDID uses a 10 MHz Wi-Fi channel fixed at 2437 MHz, while the DJI Drone ID uses a 5 MHz bandwidth frequency channel, which is on an unknown hopping channel in the 2.4 GHz or 5.8 GHz frequency bands. The three amplification stages account for these frequencies—the 2437 MHz channel, the full 2.4 GHz, and 5.8 GHz bands. The 2.4 GHz stage is divided into two parts by a two-way RF splitter, whereas the 5.8 GHz stage is transmitted without splitting, as illustrated in Figure 5. A Wi-Fi channel 6 cavity filter is included to capture only RDID packets. In addition, the remaining architecture is used to receive other communication packets, including the DJI Drone ID. Low-noise amplifiers (LNAs) are employed to amplify the RF signals received by the antennas, maximizing the signal-to-noise ratio (SNR). Following amplification, the signal is routed to a filter that eliminates non-useful frequencies according to the channels, making it ready for processing.

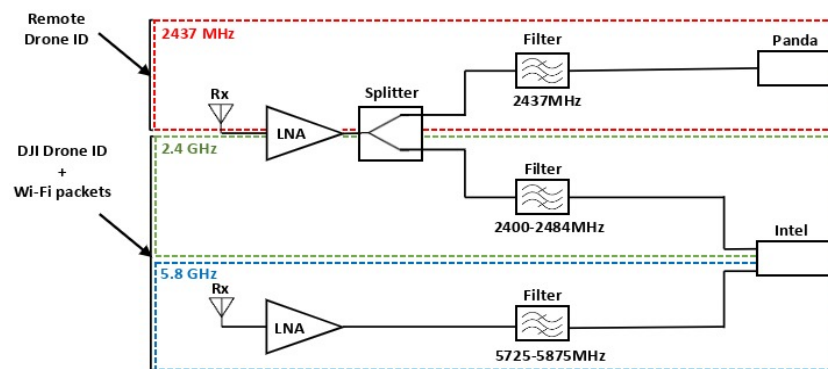


Figure 5. Dual-band RF receiver architecture.

6. Detection and Tracking Software System

In this section, we provide a detailed description of the software tools used for the detection and identification of drone Wi-Fi signals. This section focuses on explaining the different software components and their functionalities in the context of drone detection and tracking.

6.1. Wi-Fi Packet Capture

6.1.1. Aircrack-ng

Aircrack-ng is an open-source wireless network scanner used to detect and address vulnerabilities in wireless networks. It is a comprehensive suite of tools intended to assess the security of Wi-Fi networks, providing various features such as traffic monitoring and packet capture, and export of data for analysis. Aircrack-ng is specifically employed in this work to activate both interfaces (Panda/Intel Wi-Fi wireless chipsets) in monitor mode, allowing them to scan and monitor all the Wi-Fi channels.

6.1.2. Wireshark

Wireshark is an open-source network analysis tool. It decodes captured frames and understands the different structures of communication protocols. In this work, Wireshark is employed to parse and decode the RDID packet at 2437 MHz.

6.1.3. Kismet

Kismet is an open-source wireless network and sniffer that identifies and associates access points with wireless clients without emitting detectable frames. It employs a radio channel hopping algorithm to determine the maximum number of available networks. The

hopping sequence, which can be customized, enables capturing more packets. In this work, Kismet supports the parsing and decoding of enhanced Wi-Fi DJI Drone ID frames due to its frequency hopping modulation capabilities.

6.2. Method for Identifying Wi-Fi Drone Nodes

Another utility of the “aircrack-ng” tool is the use of the “airodump-ng” program to capture raw IEEE Wi-Fi 802.11 frames. It is particularly suitable for collecting initialization vectors or handshakes. Every node has its own extended service set identifier (ESSID) and basic service set identifier (BSSID). The ESSID stands for the identifying name of an 802.11 wireless network, and the BSSID stands for basic service set identifier, and it is the media access control (MAC) physical address of a node. So, it is possible to distinguish drone signals from other node signals using either ESSID or BSSID.

As illustrated in Figure 6, the MAC address is made up of 6 bytes, or 48 bits. Each network card manufacturer is assigned a unique 3-byte identifier code, called the organizationally unique identifier (OUI). The manufacturer then assigns a unique value for the last 3 bytes to ensure that each MAC address is one-of-a-kind worldwide. Therefore, the first three bytes of the MAC address serves as an identifying characteristic of the supplier, which allows us to detect the drone’s presence. To sum up, this technique requires a Wi-Fi drone MAC address database [54] for detection. This method offers several benefits. Firstly, it is independent of the size and the drone material. Secondly, it does not require a LoS between the drone and the sensor. However, this means maintaining an up-to-date database of all MAC addresses for new UAVs.

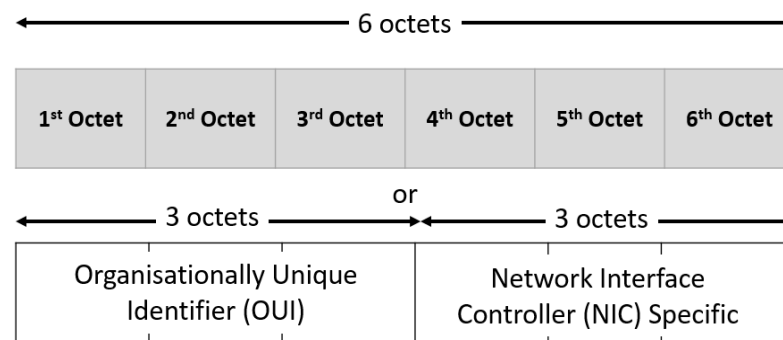


Figure 6. MAC address format [55].

6.3. Decoding Telemetry Packets

This section describes the method for decoding Wi-Fi RDID and enhanced Wi-Fi DJI Drone ID packets. To begin with, we put the Panda and the Intel wireless cards into monitor mode. This is achieved using the “aircrack-ng” tool with the following Linux command: “sudo airmon-ng start \$<name_wireless_card>”. Once in monitor mode, the cards capture all traffic. To focus on analyzing specific packets, a series of filters is applied.

6.3.1. Decoding Wi-Fi RDID Packet

The RDID is broadcast unencrypted via the IEEE 802.11 wireless management flag as a beacon frame with an OUI of “6a:5c:35”. To isolate Wi-Fi beacon frames from the captured traffic, the command “wlan.fc.type_subtype == 0x08” is used. In addition, filtering is achieved with the BSSID command “wlan.bssid[0:3] == 60:60:1F”. To confirm the presence of the RDID, we check whether the OUI tag “6a:5c:35” is present in the decoded packet [56]. For example, Figure 7 displays the Mavic 2 Pro RDID packet capture (PCAP) file after applying these Wireshark commands.

The PCAP contains information about the drone’s location, altitude, speed, heading, and other related parameters. The packet has been decoded and contains various tags that describe the different parameters. The Radiotap header provides information

about the captured packet, such as the interface, ID, and length. The IEEE 802.11 beacon frame indicates that this packet contains wireless management information. The fixed parameters include the timestamp, beacon interval, and capabilities information. The tagged parameters provide additional details about the drone, such as the service set identifier (SSID)(DJI-1581#####), latitude, longitude, altitude above mean sea level (AMSL), altitude above ground level (AGL), latitude takeoff, longitude takeoff, horizontal speed, and heading. Furthermore, there are vendor-specific tags that provide information about the drone manufacturer and serial number.

```

Tag: SSID parameter set: DJI-1581#####
  Tag Number: SSID parameter set (0)
  Tag length: 23
  SSID: DJI-1581#####
Tag: Vendor Specific: Mavic 2 Pro
  Tag Number: Vendor Specific (221)
  Tag length: 67
  OUI: 6a:5c:35
  Vendor Specific OUI Type: 1
Tag: Version: 1
Tag: ID ANSI: 1581 163CGB#####
  Type: ID ANSI (3)
  Length: 19 ICAO Manufacturer
  Code: 1581 Serial number
  length: 14 byte(s)
  Serial number: 163CGB#####
Tag: Latitude: 0,09000
  Type: Latitude (4)
  Length: 4
  GPS Coord: 0
  Tag: Longitude: 0,90000
  Type: Longitude (5)
  Length: 4
  GPS Coord: 0
Tag: Altitude AMSL: 65519 m
  Type: Altitude AMSL (6)
  Length: 2
  Altitude: 65519
Tag: Altitude AGL: 0 m
  Type: Altitude AGL (7)
  Length: 2 Altitude: 0
Tag: Latitude Takeoff: 214##,#####
  Type: Latitude Takeoff (8)
  Length: 4 GPS Coord: 214#####
Tag: Longitude Takeoff: 214##,#####
  Type: Longitude Takeoff (9)
  Length: 4 GPS Coord: 214#####
Tag: Horizontal Speed: 9 m/s Type: Horizontal Speed (10)
  Length: 1
  Speed: 9
Tag: Heading: 168 deg
  Type: Heading (11)
  Length: 2
  Altitude: 168

```

Figure 7. The Output PCAP file from decoding the Mavic 2 Pro RDID packet. Sensitive information was partly replaced by ‘#’ symbol, such as location, MAC address, and serial number.

6.3.2. Decoding Enhanced Wi-Fi DJI Drone ID Packet

DJI Wi-Fi drones include a standard packet addition known as a DJI Drone ID, which is broadcast through an OUI tag of “26:37:12” in the IEEE 802.11 beacon [57]. Two packet types are used; packets with a subcommand of 0×10 include flight telemetry and location, while packets with a subcommand of 0×11 include user-entered information about the drone and the flight [42]. These packets are alternately sent down the Wi-Fi link every 200 ms. Thanks to the OUI tag and the knowledge of the subcommands, Kismet can detect a DJI Drone ID packet data and classify it as “uav.device”. Kismet allows tracking using a list of drone MAC addresses by retrieving a UAV’s telemetry history. For more details, the DJI enhanced Wi-Fi Drone ID packet structure with the decoding process is explicitly detailed in references [41,42].

Knowing that a DJI enhanced Wi-Fi Drone ID occupies a 5 MHz bandwidth, Wi-Fi channels can be scanned with Kismet from 1 to 177 in the 2.4 GHz and 5.8 GHz frequency bands using the following bash command [41] shown in Figure 8.

```

$ kismet -c wlan0mon:name=channel0, ht_channels=false, vht_channels=false,
  → channels="1W5, 2W5, 3W5, 4W5, 5W5, 6W5, 7W5, 8W5, 9W5, 10W5, 11W5, 12W5, 13W5,
  → 14W5, 140W5, 149W5, 153W5, 157W5, 161W5, 165W5, 169W5, 173W5, 177W5\"

```

Figure 8. Monitor FHSS 5 MHz Wi-Fi signals using Kismet on the 2.4 GHz and 5.8 GHz bands.

By using the Kismet_Rest application programming interface (API) [58] on Python, it is possible to retrieve decoded DJI Drone ID packet data from the Kismet server in the form of a JavaScript object notation (JSON) file as shown in Figure 9.

```
"uav.serialnumber": "OK1U#####\u0000\u0000",
"uav.model": "Unknown (0)",
"uav.manufacturer": "DJI/droneID",
"kismet.device.base.manuf": "SZ DJI,TECHNOLOGY CO.,LTD",
"kismet.device.base.first_time": 1669305679,
"kismet.device.base.macaddr": "60:60:1F:8F:##:##",
"kismet.device.base.freq_khz_map": {"2437000": 19,"2447000": 61,"2442000": 642},
"kismet.device.base.key": "4202770D00000000_###8F1F6060",
"kismet.device.base.packets.crypt": 0,
"kismet.device.base.packets.total": 722,
{
"uav.device":
{
"uav.telemetry_history":
"uav.telemetry.v_north": 85,
"uav.telemetry.timestamp": 1669305681.161549,
"field.unknown.not.registered":
{"kismet.common.location.time_usec": 260621,
"kismet.common.location.alt": -29184,
"kismet.common.location.geopoint": [3.15####, 50.#####],
"kismet.common.location.time_sec": 1669305682,
"kismet.common.location.fix": 3},
"uav.telemetry.airborne": 1,
"uav.telemetry.pitch": 2.145874,
"uav.telemetry.yaw": 0,
"uav.telemetry.motor_on": 1,
"uav.telemetry.v_east": 0,
"uav.telemetry.v_up": -26144,
"uav.telemetry.height": 30441,
"uav.telemetry.roll": 0.022166
},
},
},
```

Figure 9. The Output JSON file from decoding DJI enhanced Wi-Fi Drone ID. Sensitive information was partly replaced by '#' symbol, such as location, MAC address, and serial number.

This packet contains information about a DJI drone, including its serial number, model, and frequency histogram usage. Additionally, telemetry data are included such as the drone's pitch, yaw, and roll, as well as its speed and altitude. It also includes a timestamp indicating when the telemetry data were recorded. This information can be used to track and analyze drone movements and behavior.

The Python code connects to a Kismet server using the `kismet_rest` API to retrieve information about a wireless detected device with a specific MAC address. As shown in the flowchart (Figure 10), the code performs several steps. First, the code imports the required `kismet_rest` module. Then, it creates a `KismetConnector` instance and establishes a connection to the Kismet server. Next, the code defines a list of MAC address masks, stored in the `mac_list` variable, for the devices that need to be detected. If a device is detected, the code retrieves information such as the device name, full MAC address, and manufacturer using the `kismet_rest.Devices.by_mac` function and providing the MAC list. Additionally, the code employs the `kismet.device.base.seenby` function to access multiple dictionary attributes.

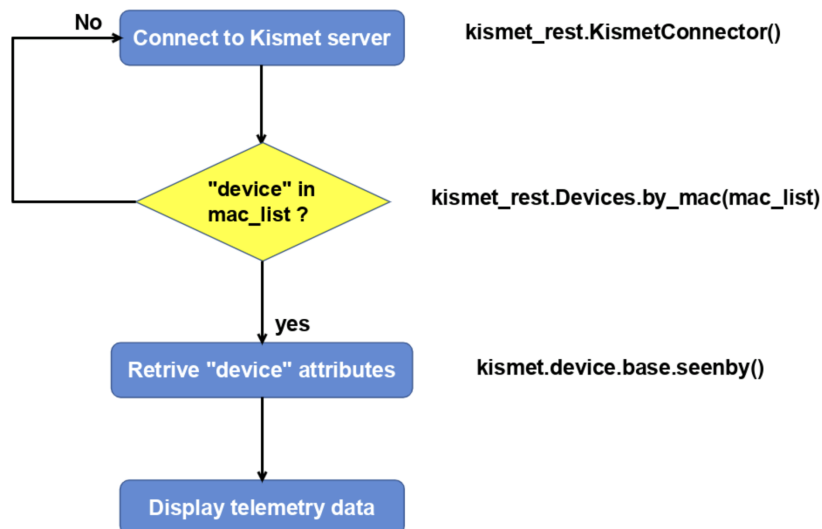


Figure 10. Flowchart of the Kismet REST Python code.

7. Experimental Setup

In this section, we present the experimental setup employed to examine the detection and tracking capabilities of drones. As illustrated in Figure 11, the system incorporates both active and passive components within its RF chains. The specifications of the setup RF components are detailed in Table 2. The receiver chain is linked to the Jetson device for processing.

Figure 12 illustrates the drones tested in the experiments. These drones are the DJI Mavic Air, which is a Wi-Fi drone equipped with the enhanced Wi-Fi DJI Drone ID, and the DJI Mavic 2 Pro and DJI Mavic 3, which are OcuSync drones equipped with an RDID. Each drone selected employs a specific RF protocol and then represents a different category of drone. Their specific characteristics are outlined in Table 3. The drones chosen for the study are representative of many popular drones on the market due to their use of the recent RF protocols (Wi-Fi, enhanced Wi-Fi, and OcuSync). By focusing on these RF protocols, rather than on several specific drone models, our results can be extrapolated to a wide variety of drone models that share the same communication standards.

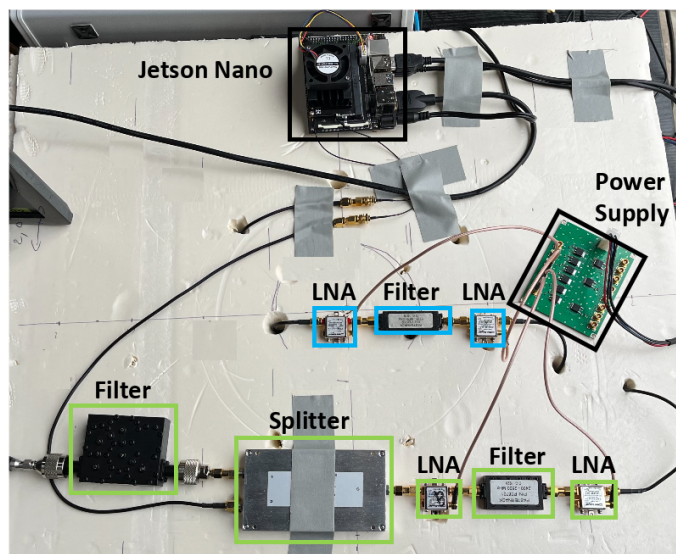


Figure 11. Illustration of the experimental setup.

Table 2. RF component specifications.

Component	Frequency Range	Specifications
Dual-Band Antennas	2.4 GHz/5 GHz	Omnidirectional; Gain at 2.4 GHz: 5 dBi; Gain at 5 GHz: 9 dBi
Low-Noise Amplifier	0.5–8 GHz	Low noise: 1.4 dB @ 2 GHz; High IP3: +34 dBm; Gain flatness: ± 0.9 dB over 0.5 to 7 GHz @6V
Cavity Bandpass Filter	2.4 GHz	Center frequency: 2437 MHz; Bandwidth: 25 MHz; Maximum insertion loss: 1.5 dBm
Bandpass Filter	2.4–2.5 GHz	Bandwidth: 400 MHz; Insertion Loss: 1 dB; Power capacity: 5 W; Voltage standing wave ratio (VSWR): 1.50:1
Bandpass Filter	5.725–5.875 GHz	Bandwidth: 150 MHz; Maximum insertion loss: 1 dB; Maximum power: 5 W
Power Splitter/Combiner	350–6000 MHz	Power capacity (as splitter): 25 W; Insertion loss: 0.9 dB



(a) DJI Mavic Air



(b) DJI Mavic 2 Pro



(c) DJI Mavic 3

Figure 12. Drone models used in the experiments.**Table 3.** Drone Specifications.

Drone	OUI ID	RF Protocol	Linear Maximum Velocity	RDID	DJI Drone ID
DJI Mavic Air	60:60:1F	Enhanced Wi-Fi	10 m/s	×	✓ (Enhanced Wi-Fi)
DJI Mavic 2 Pro	60:60:1F	OcuSync 2.0	20 m/s	✓ (Wi-Fi)	×
DJI Mavic 3	60:60:1F	OcuSync 3.0+	21 m/s	✓ (Wi-Fi)	✓ (OcuSync)

8. Detection and Tracking Assessment

Our objective is to evaluate the performance of the drone detection and tracking system across long distances. We aim to determine the maximum detection and tracking ranges for various drone models. These measurements provide insights into the system's capabilities and limitations. These tests were conducted under different weather conditions and at various times of the day.

8.1. Methodology for Conducting the Measurement Campaign

This section describes the methodology for measuring distances of detecting and tracking the UAVs. An outdoor test site where drone flights are permitted was selected. It is located in a village in the north of France. There were a few sources of radio frequencies in the vicinity, such as cellular network base stations and Wi-Fi access points located in homes close to the test site. The detection system was approximately 1 km away from a small forest. This forest, composed of trees ranging from 20 to 30 m in height, was located in the intended flight path of the drones. Despite the proximity of these potential sources of interference, the site was deemed suitable for accommodating various flight scenarios. We also obtained authorization to fly drones in the unrestricted airspace shown in Figure 13.



Figure 13. Outdoor mapping for long-distance drone experiments: system location (yellow spot) and pilot/drone positions (white spots).

We positioned the reference point at the location of the detection system, which is denoted by a yellow spot in Figure 13. The detection system is equipped with two omnidirectional receiving antennas and placed in an open-field environment. These antennas were mounted on 2.6 m tripods. The test bed perspective is shown in Figure 14.

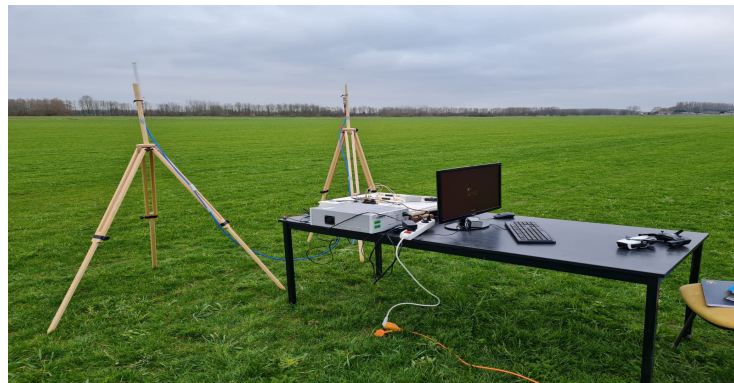


Figure 14. The outdoor test bed perspective.

Each time, the drone and the RC were positioned at different locations, indicated by white spots on the map in Figure 13. For some drones, we added between the white spots other positions for more measurements.

8.2. Performance of the Drone Detection and Tracking System

We gradually increased the drone's altitude from the ground at each position. At the same time, we monitored the system's ability to detect and retrieve telemetry information. This systematic approach allowed us to determine the minimum and maximum altitudes required for successful drone detection and tracking, depending on the distance from the reference point. In this section, we study the drone's trajectory and measure the distances between the detected drones and the system. To assess the system's accuracy, we calculate the errors between the actual and estimated trajectories, as well as the relative errors for the estimated altitude and speed of each drone. Additionally, for every identified drone, we calculated the remaining time to react to secure a designated area, given a specified protection radius.

8.2.1. Measuring Detection Maximum Range and Altitude Interval

Figure 15 presents the results for the Mavic Air, Mavic 3, and Mavic 2 Pro drones, respectively. In each figure, the blue curve represents the minimum altitude for detection at different distances from the reference, while the red curve represents the maximum altitude. The maximum altitude curve remains flat because the drones have altitude restrictions. The Mavic Air is limited to a maximum altitude of 50 m, while the Mavic 3 and Mavic 2 Pro have a maximum altitude of 120 m. The maximum detection distances achieved are 1.3 km for the Mavic Air, 1.5 km for the Mavic 3, and 3.7 km for the Mavic 2 Pro.

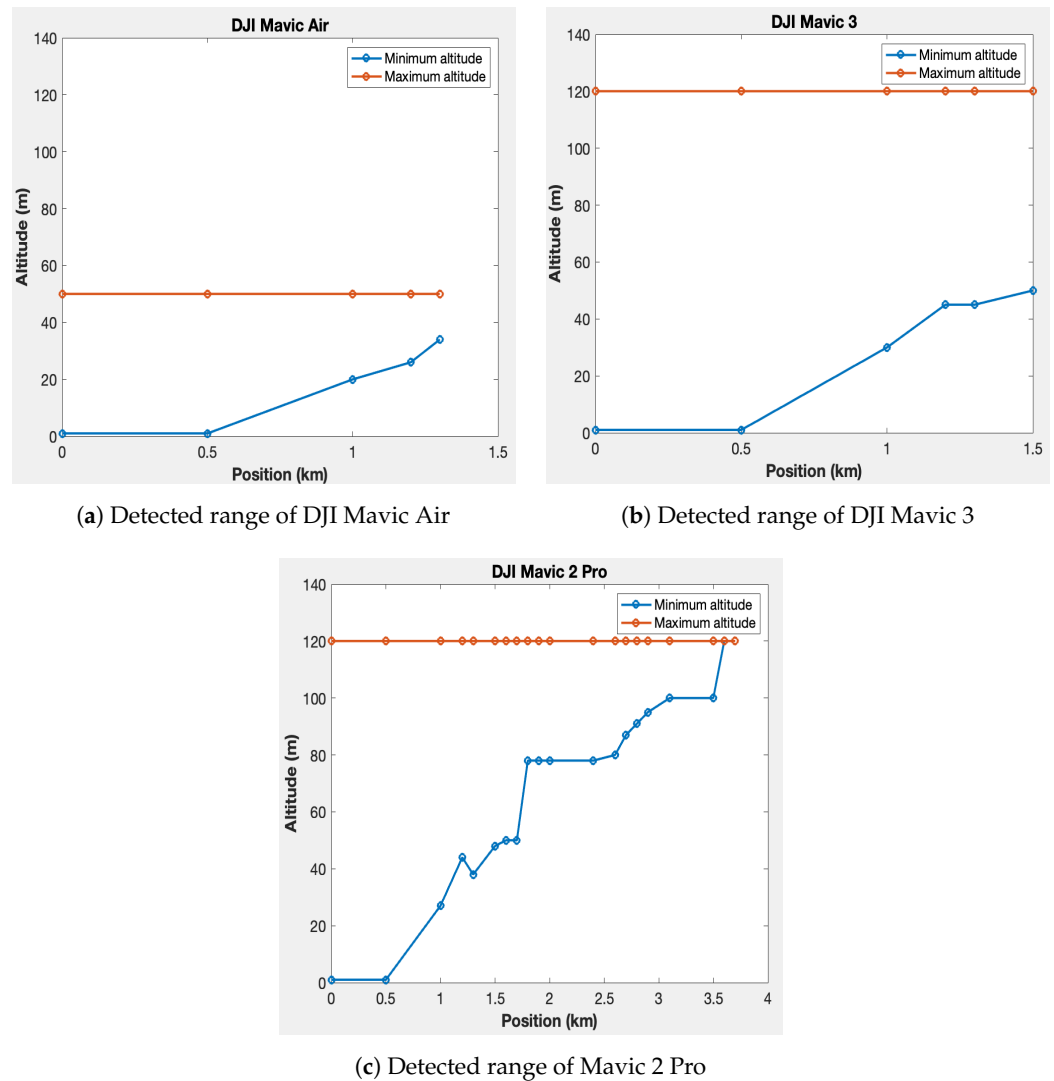


Figure 15. Measured detection ranges and interval altitudes of each drone.

8.2.2. Estimating Drone Positions

To estimate the drone positions, an automated code distinguishes the telemetry packets for each detected drone thanks to the drone identifier. Then, for each drone, the telemetry packets are sorted by time of reception to trace the trajectory. The latitude and longitude (φ, λ) information are extracted and converted into 2D Cartesian coordinates (x, y) using Equation (1). Figure 16 illustrates the real positions and the estimated positions for each drone.

$$\begin{cases} x = R_{\text{earth}} \cos(\varphi) \cos(\lambda) \\ y = R_{\text{earth}} \cos(\varphi) \sin(\lambda) \end{cases} \quad (1)$$

To perform comparisons between the estimated and the real positions, we calculate the Euclidean distance error. This metric measures the discrepancy between the real positions and the estimated positions of each drone. Denoted by $e(P)$, the Euclidean distance error is obtained using the following formula:

$$e(P) = \sqrt{(x_{\text{estimated}}(P) - x(P))^2 + (y_{\text{estimated}}(P) - y(P))^2} \quad (2)$$

where $(x_{\text{estimated}}(P), y_{\text{estimated}}(P))$ are the estimated coordinates, and $(x(P), y(P))$ are the precise coordinates of the position of the drone P .

Figure 17 shows the Euclidean distance error between the estimated and the real positions.

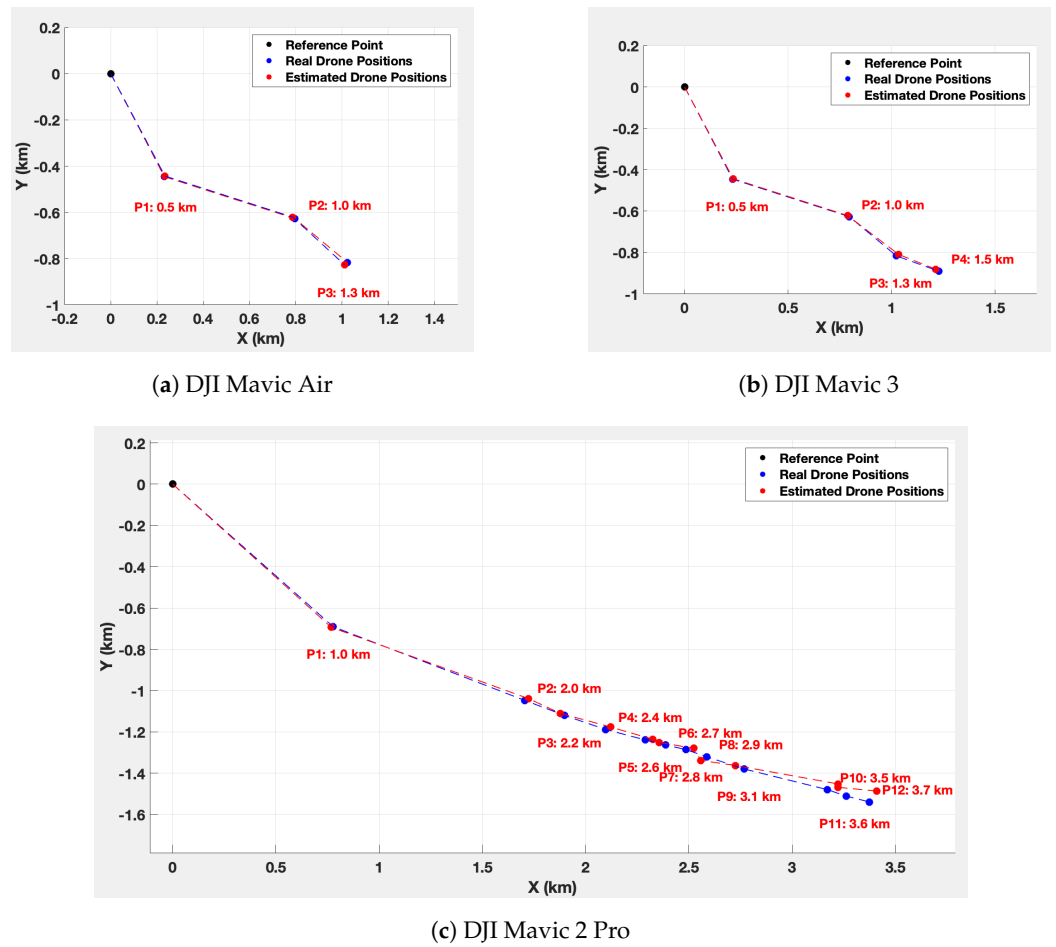


Figure 16. Precise drone positions, estimated drone positions, and the Haversine distances from the system estimation.

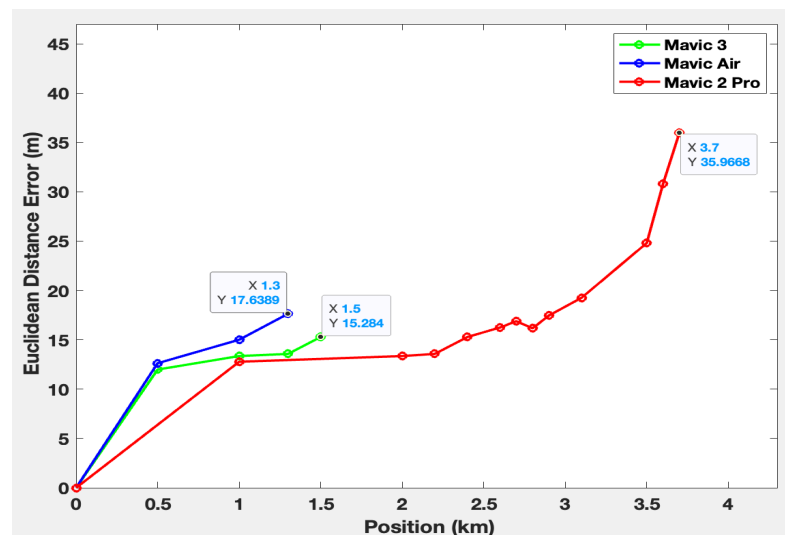


Figure 17. Euclidean distance error between real and estimated positions.

8.2.3. Estimation of Remaining Distance between the Drone and the System

To find out how far the drone is from the system, we use the Haversine equation (Equation (3)) [59]. The calculated distances are shown in Figure 16.

$$\begin{cases} a = \sin^2\left(\frac{\Delta\varphi}{2}\right) + \cos(\varphi_1) \cos(\varphi_2) \sin^2\left(\frac{\Delta\lambda}{2}\right) \\ c = 2 \times \text{atan2}(\sqrt{a}, \sqrt{1-a}) \\ d = R_{\text{earth}} \times c \end{cases} \quad (3)$$

The Haversine equation calculates the distance d between two points on Earth, where φ_1 and φ_2 are the latitudes of the points, and $\Delta\varphi$ and $\Delta\lambda$ represent the differences in latitude and longitude, respectively, and R_{earth} represents the Earth's radius. This formula considers the spherical Earth's shape. Indeed, the traditional Euclidean distance calculations, being based on flat Cartesian coordinates, are not accurate for long distances. By considering Earth's curvature, the Haversine formula provides more accurate distance measurements.

8.2.4. Relative Error for Altitude and Speed Estimation

Let X represent the telemetry measured parameter whose relative error we want to evaluate. The formula for calculating the relative error can be written as follows:

$$\zeta_X(P) = 100 \times \left| \frac{X_{\text{decoded}}(P) - X_{\text{precise}}(P)}{X_{\text{precise}}(P)} \right| \quad (4)$$

Equation (4) represents the relative error $\zeta_X(P)$ for parameter X at position P . Here, $X_{\text{decoded}}(P)$ denotes the decoded value of the parameter X at position P , and $X_{\text{precise}}(P)$ signifies the reference parameter X at position P . As the pilot was in proximity to the drone at each position, we assume that the parameters received by the pilot and recorded in the phone's telemetry history of the pilot represent accurate information about the flight. Thus, $X_{\text{precise}}(P)$ is extracted from the telemetry information in the phone's flight history. On the other hand, the measured parameters represent the decoded values provided by the detection system $X_{\text{decoded}}(P)$.

To assess the errors in altitude and speed, we substitute X with the altitude H and the speed V of the tracked drone, estimated by the system. The formula becomes Equation (5):

$$\begin{cases} \zeta_{\text{altitude}}(P) = 100 \times \left| \frac{H_{\text{decoded}}(P) - H_{\text{precise}}(P)}{H_{\text{precise}}(P)} \right|, \\ \zeta_{\text{speed}}(P) = 100 \times \left| \frac{V_{\text{decoded}}(P) - V_{\text{precise}}(P)}{V_{\text{precise}}(P)} \right|. \end{cases} \quad (5)$$

The relative altitude and speed error curves obtained from this formula, expressed as a percentage for each position, are shown in Figure 18. The blue curve corresponds to the Mavic Air drone, the red curve represents the Mavic 2 Pro drone, and the green curve represents the Mavic 3 drone.

8.2.5. Remaining Time to React

Thanks to the speeds of each drone from Table 3 and the maximum detection distance from Figure 15, we can compute the remaining time to neutralize a potentially dangerous drone, based on the system's location in the protected site.

For instance, to protect a site with a 200 m radius, the computed reaction times would be 1.83 min for the Mavic Air, 1.03 min for the Mavic 3, and 2.92 min for the Mavic 2 Pro. This computation is performed using the following formula:

$$T_{\text{to-react}} = \frac{d_{\text{drone}} - r_{\text{site}}}{v_{\text{drone}}} \quad (6)$$

where $T_{\text{to-react}}$ represents the remaining time available to react, d_{drone} is the distance from the drone to the vulnerable site, r_{site} is the fixed radius of the site to protect, and v_{drone} is the maximum linear speed of the drone. This equation provides valuable insights into the time required to take appropriate actions based on the drone's position and maximum linear speed. It offers a simplified representation of the remaining reaction time once the drone is detected.

Equation (6) considers a worst-case scenario in which the drone travels at its maximum speed and approaches the vulnerable site along a direct linear trajectory.

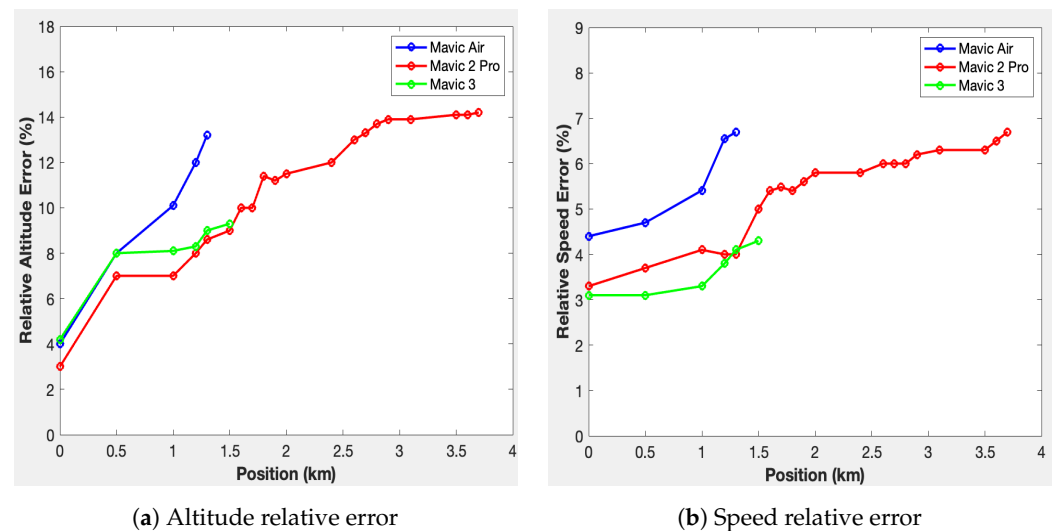
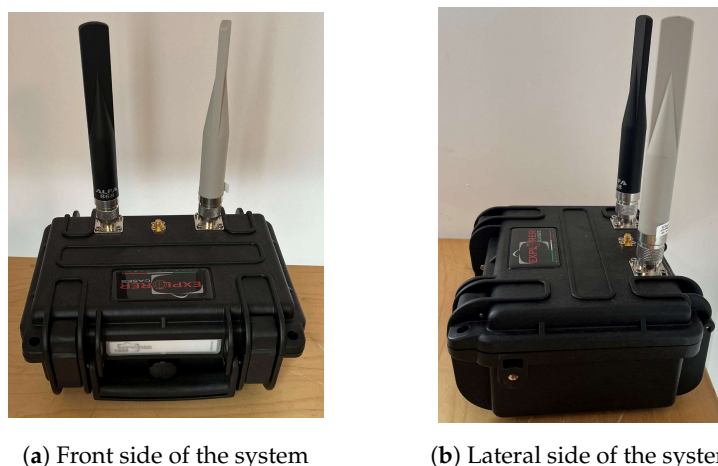


Figure 18. Relative error calculations.

9. Discussion about the Results

The maximum detection ranges for the Mavic Air, Mavic 3, and Mavic 2 Pro are, respectively, 1.3 km, 1.5 km, and 3.7 km. These results highlight the system's enhanced ability to detect the Mavic 2 Pro compared to the others. This can be explained by the fact that signal capture also depends on the signal transmission power specific to each drone. Moreover, the minimum detection altitude of the three drones increases as they move away from the system. This might be attributed to the system's antennas, whose radiation patterns are slightly oriented upwards. In addition, the position estimation error tends to increase as the drones move further away from the detection system. The maximum error is 17 m at 1.3 km for the Mavic Air, 15 m at 1.5 km for the Mavic 3, and 35 m at 3.7 km for the Mavic 2 Pro. The higher error for the Mavic 2 Pro is, therefore, probably due to its greater detection distance. Nevertheless, among the configurations tested, the speed and position estimation errors were no greater than 7% and 14%.

Moreover, the Haversine equation can be used to estimate the remaining distance between the detected UAV and the detection system, using the longitude and latitude data decoded from the frames. Considering the protection of a 200 m radius area with the detection system at its center, the estimated reaction times are 1.83 min for the Mavic Air at a distance of 1.3 km, 1.03 min for the Mavic 3 at 1.5 km, and 2.92 min for the Mavic 2 Pro at 3.7 km. These values, therefore, make it possible to specify the expected performance of the drone interception solution to be implemented. Finally, the detection and tracking system, depicted in Figure 19, can be integrated into a single module offering portability, ease of deployment, and adaptability, making it a relevant tool for organizations and agencies monitoring drone activity in their airspace.



(a) Front side of the system (b) Lateral side of the system
Figure 19. Front and lateral sides of the system.

10. Conclusions and Future Work

In conclusion, the conducted study provides insight into drone detection and tracking systems, focusing particularly on the Mavic Air, Mavic 3, and Mavic 2 Pro drones. The research outlines the detection range for these drones, with maximum detected distances at 1.3 km, 1.5 km, and 3.7 km, respectively. The detection capabilities are influenced by factors such as the drone's transmission power and multipath propagation, contributing to the variation in the observed results. The research notes an increase in position estimation error as drones move further away from the system. The relative error in estimating speed and altitude also increased with distance, though these did not exceed 7% and 14%, respectively. The use of the Haversine equation in estimating the remaining distance between the detected drone and the system yielded promising results. The system was also tested in a hypothetical scenario involving securing an area with a 200 m radius. The remaining reaction times for different drones were computed, providing useful data for applications aiming at the interception of unauthorized drones.

This research presents a system that integrates detection, classification, and localization functionalities in a single module. This study demonstrated the system's capability to differentiate drone signals and track their movements. While the study showcased the system's potential in managing drone activities and its potential contribution to public safety and security, some areas need improvement.

To enhance our solution, we plan future expansions. These include integrating real-time decoding of OcuSync DJI Drone IDs for other DJI drone identification and classification, incorporating AI models for detecting other drones that are not equipped with Drone IDs, improving the RF receiver to extend system coverage, supporting different frequency bands to utilize the system in different geographic regions, and the possibility to connect the system with a jamming device [60,61] for drone interception and man-machine interface (MMI). These planned expansions hold promising prospects for enhancing safety and responsiveness in drone detection and mitigation.

Author Contributions: Conceptualization, D.A. and E.K.; methodology, D.A. and V.D.; software, D.A. and A.K.; validation, D.A., A.K., E.K. and V.D.; formal analysis, D.A.; investigation, D.A., E.K. and A.K.; resources, D.A., E.K. and A.K.; data curation, D.A.; writing—original draft preparation, D.A.; writing—review and editing, V.D. and C.G. (Christophe Gransart); visualization, D.A.; supervision, V.D.; project administration, C.G. (Christophe Gaquière); funding acquisition, C.G. (Christophe Gaquière). All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Association Nationale Recherche Technologie (ANRT) OF FUNDER grant number (No. 2020/0355).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: <https://gist.github.com/aallan/b4bb86db86079509e6159810ae9bd3e4>, accessed on 31 August 2023.

Acknowledgments: We are grateful to the ANRT, MC2 Technologies, and Gustave Eiffel University for financial and material support.

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

Abbreviations

The following abbreviations are used in this context:

UAV	Unmanned aerial vehicle
GPS	Global Positioning System
LiDAR	Light detection and ranging
RaDaR	Radio detection and ranging
C-UAS	Counter-unmanned aerial system
LoS	Line of sight
GA-XGBoost	Genetic algorithm-extreme gradient boosting
IMU	Inertial measurement unit
GoF	Goodness-of-fit
DRNN	Deep recurrent neural network
YOLO	You only look once
CNN	Convolutional neural network
SVM	Support vector machine
AI	Artificial intelligence
SDR	Software-defined radio
RDID	Remote drone identification
UAS	Unmanned aerial system
RC	Remote controller
ISM	Industrial, scientific, and medical
OFDM	Orthogonal frequency division multiplexing
FHSS	Frequency hopping spread spectrum
ASTM	American Society for Testing and Materials
ASD-STAN	Aerospace and Defence Industries Association of Europe
FAA	Federal Aviation Administration
FRIAs	FAA-recognized identification areas
GNSSs	Global navigation satellite systems
LNAs	Low-noise amplifiers
SNR	Signal-to-noise ratio
ESSID	Extended service set identifier
BSSID	Basic service set identifier
MAC	Media access control
OUI	Organizationally unique identifier
PCAP	Packet capture
SSID	Service set identifier
AMSL	Above mean sea level
AGL	Above ground level
API	Application programming interface
JSON	JavaScript object notation
MMI	Man-machine interface
ANRT	Association Nationale de la Recherche et de la Technologie
RCS	Radar cross-section
IR	Infrared
EO	Electro-optical
VSWR	Voltage standing wave ratio

References

1. Dilshad, N.; Hwang, J.; Song, J.; Sung, N. Applications and challenges in video surveillance via drone: A brief survey. In Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 21–23 October 2020; pp. 728–732.
2. Fine, J.D.; Litsey, E.M. Drone Laying Honey Bee Workers in Queen Monitoring Cages. *J. Insect Sci.* **2022**, *22*, 13. [[CrossRef](#)] [[PubMed](#)]
3. Meng, S.; Guo, X.; Li, D.; Liu, G. The multi-visit drone routing problem for pickup and delivery services. *Transp. Res. Part E Logist. Transp. Rev.* **2023**, *169*, 102990. [[CrossRef](#)]
4. Mora, P.; Araujo, C.A.S. Delivering blood components through drones: A lean approach to the blood supply chain. *Supply Chain. Forum Int. J.* **2022**, *23*, 113–123.
5. Hiebert, B.; Nouvet, E.; Jeyabalan, V.; Donelle, L. The application of drones in healthcare and health-related services in north america: A scoping review. *Drones* **2020**, *4*, 30. [[CrossRef](#)]
6. Hanover, D.; Loquercio, A.; Bauersfeld, L.; Romero, A.; Penicka, R.; Song, Y.; Cioffi, G.; Kaufmann, E.; Scaramuzza, D. Past, Present, and Future of Autonomous Drone Racing: A Survey. *arXiv* **2023**, arXiv:2301.01755.
7. Tang, J.; Chen, X.; Zhu, X.; Zhu, F. Dynamic reallocation model of multiple unmanned aerial vehicle tasks in emergent adjustment scenarios. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *59*, 1139–1155. [[CrossRef](#)]
8. Tang, J.; Liu, G.; Pan, Q. A review on representative swarm intelligence algorithms for solving optimization problems: Applications and trends. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 1627–1643. [[CrossRef](#)]
9. Lykou, G.; Moustakas, D.; Gritzalis, D. Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. *Sensors* **2020**, *20*, 3537. [[CrossRef](#)] [[PubMed](#)]
10. Tataru, B.A. The Role of Law in Facing Asymmetric Warfare Through Illicit Drug Trafficking in Indonesia. *J. Law Sci.* **2023**, *5*, 1–9. [[CrossRef](#)]
11. Evangelista, M.; Shue, H. *The American Way of Bombing: Changing Ethical and Legal Norms, from Flying Fortresses to Drones*; Cornell University Press: Ithaca, NY, USA, 2014.
12. Michel, A.H. *Counter-Drone Systems*, 2nd ed.; Center for the Study of the Drone at Bard College: Annandale-On-Hudson, NY, USA, 2019.
13. Congressional Research Service (CRS). Department of Defense Counter-Unmanned Aircraft Systems. Available online: <https://sgp.fas.org/crs/weapons/IF11426.pdf> (accessed on 31 August 2023).
14. 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](#)]
15. Castrillo, V.U.; Manco, A.; Pascarella, D.; Gigante, G. A review of counter-UAS technologies for cooperative defensive teams of drones. *Drones* **2022**, *6*, 65. [[CrossRef](#)]
16. Park, S.; Kim, H.T.; Lee, S.; Joo, H.; Kim, H. Survey on anti-drone systems: Components, designs, and challenges. *IEEE Access* **2021**, *9*, 42635–42659. [[CrossRef](#)]
17. 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. [[CrossRef](#)] [[PubMed](#)]
18. Coluccia, A.; Parisi, G.; Fascista, A. Detection and classification of multirotor drones in radar sensor networks: A review. *Sensors* **2020**, *20*, 4172. [[CrossRef](#)]
19. Guvenc, I.; Koohifar, F.; Singh, S.; Sichertiu, M.L.; Matolak, D. Detection, tracking, and interdiction for amateur drones. *IEEE Commun. Mag.* **2018**, *56*, 75–81. [[CrossRef](#)]
20. Zitar, R.A.; Mohsen, A.; Seghrouchni, A.E.; Barbaresco, F.; Al-Dmour, N.A. Intensive Review of Drones Detection and Tracking: Linear Kalman Filter Versus Nonlinear Regression, an Analysis Case. *Arch. Comput. Methods Eng.* **2023**, *30*, 2811–2830. [[CrossRef](#)]
21. Kamanli, A.F. Real Time Uav (Unmanned Vehicle) Tracking with Object Detection in the Air: From Simulation to Real Life Application. Available at SSRN 4329687. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4329687 (accessed on 31 August 2023).
22. Zheleva, M.; Anderson, C.R.; Aksoy, M.; Johnson, J.T.; Affinnih, H.; DePree, C.G. Radio Dynamic Zones: Motivations, Challenges, and Opportunities to Catalyze Spectrum Coexistence. *IEEE Commun. Mag.* **2023**, *61*, 156–162. [[CrossRef](#)]
23. He, Z.; Tan, T. Survey on Worldwide Implementation of Remote Identification and Discussion on Drone Identification in China. In Proceedings of the 2021 IEEE 3rd International Conference on Civil Aviation Safety and Information Technology (ICCSIT), Changsha, China, 20–22 October 2021; pp. 252–258. [[CrossRef](#)]
24. Zitar, R.A.; Al-Betar, M.; Ryalat, M.; Kassaymehd, S. A review of UAV Visual Detection and Tracking Methods. *arXiv* **2023**, arXiv:2306.05089
25. Aydin, B.; Singha, S. Drone Detection Using YOLOv5. *Eng* **2023**, *4*, 416–433. [[CrossRef](#)]
26. Svanström, F.; Alonso-Fernandez, F.; Englund, C. Drone Detection and Tracking in Real-Time by Fusion of Different Sensing Modalities. *Drones* **2022**, *6*, 317. [[CrossRef](#)]
27. Go, Y.J.; Choi, J.S. An Acoustic Source Localization Method Using a Drone-Mounted Phased Microphone Array. *Drones* **2021**, *5*, 75. [[CrossRef](#)]
28. Salvati, D.; Drioli, C.; Ferrin, G.; Foresti, G.L. Acoustic source localization from multirotor UAVs. *IEEE Trans. Ind. Electron.* **2019**, *67*, 8618–8628. [[CrossRef](#)]

29. Gong, J.; Yan, J.; Li, D.; Kong, D.; Hu, H. Interference of radar detection of drones by birds. *Prog. Electromagn. Res. M* **2019**, *81*, 1–11. [[CrossRef](#)]
30. Ezuma, M.; Anjinappa, C.K.; Funderburk, M.; Guvenc, I. Radar cross section based statistical recognition of UAVs at microwave frequencies. *IEEE Trans. Aerosp. Electron. Syst.* **2021**, *58*, 27–46. [[CrossRef](#)]
31. Basak, S.; Rajendran, S.; Pollin, S.; Scheers, B. Combined RF-based drone detection and classification. *IEEE Trans. Cogn. Commun. Netw.* **2021**, *8*, 111–120. [[CrossRef](#)]
32. Allahham, M.S.; Al-Sa'd, M.F.; Al-Ali, A.; Mohamed, A.; Khattab, T.; Erbad, A. DroneRF dataset: A dataset of drones for RF-based detection, classification and identification. *Data Brief* **2019**, *26*, 104313. [[CrossRef](#)]
33. Alam, S.S.; Chakma, A.; Rahman, M.H.; Bin Mofidul, R.; Alam, M.M.; Utama, I.B.K.Y.; Jang, Y.M. RF-Enabled Deep-Learning-Assisted Drone Detection and Identification: An End-to-End Approach. *Sensors* **2023**, *23*, 4202. [[CrossRef](#)]
34. Al-Sa'd, M.F.; Al-Ali, A.; Mohamed, A.; Khattab, T.; Erbad, A. RF-based drone detection and identification using deep learning approaches: An initiative towards a large open source drone database. *Future Gener. Comput. Syst.* **2019**, *100*, 86–97. [[CrossRef](#)]
35. Feng, Z.; Guan, N.; Lv, M.; Liu, W.; Deng, Q.; Liu, X.; Yi, W. Efficient drone hijacking detection using two-step GA-XGBoost. *J. Syst. Archit.* **2020**, *103*, 101694. [[CrossRef](#)]
36. Medaiyese, O.O.; Ezuma, M.; Lauf, A.P.; Guvenc, I. Wavelet transform analytics for RF-based UAV detection and identification system using machine learning. *Pervasive Mob. Comput.* **2022**, *82*, 101569. [[CrossRef](#)]
37. Kılıç, R.; Kumbasar, N.; Oral, E.A.; Ozbek, I.Y. Drone classification using RF signal based spectral features. *Eng. Sci. Technol. Int. J.* **2022**, *28*, 101028. [[CrossRef](#)]
38. 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](#)]
39. Zhang, H.; Li, T.; Li, Y.; Li, J.; Dobre, O.A.; Wen, Z. RF-based drone classification under complex electromagnetic environments using deep learning. *IEEE Sens. J.* **2023**, *23*, 6099–6108. [[CrossRef](#)]
40. Christof, T. DJI Wi-Fi Protocol Reverse Engineering. Bachelor's Thesis, Institute of Networks and Security, Johannes Kepler Universität Linz, Linz, Austria, November 2021.
41. Bender, C. DJI drone IDs are not encrypted. *arXiv* **2022**, arXiv:2207.10795
42. Department 13, Anatomy of DJI's Drone Identification Implementation, White Paper, Canberra, Australia, 2017. Available online: <https://petapixel.com/assets/uploads/2022/08/Anatomy-of-DJI-Drone-ID-Implementation1.pdf> (accessed on 31 August 2023).
43. DJI Aeroscope. Available online: <https://www.dji.com/fr/aeroscope> (accessed on 19 July 2023).
44. Swinney, C.J.; Woods, J.C. Low-Cost Raspberry-Pi-Based UAS Detection and Classification System Using Machine Learning. *Aerospace* **2022**, *9*, 738. [[CrossRef](#)]
45. heliguy™ Blog. DJI Transmission Systems: Wi-Fi, OcuSync, Lightbridge. Published Online on 1 March 2022. Available online: <https://www.heliguy.com/blogs/posts/dji-transmission-systems-wi-fi-ocusync-lightbridge> (accessed on 31 August 2023).
46. Flynt, J. The DJI Transmission Systems OcuSync 2 vs. Lightbridge 2. Published on 25 September 2020. Available online: <https://3dinsider.com/ocusync-2-vs-lightbridge-2/> (accessed on 31 August 2023).
47. Travel, E.W. What Is DJI Ocusync And How Does It Work? Expert World Travel, 4 February 2017. Available online: <https://store.dji.bg/en/blog/what-is-dji-ocusync-and-how-does-it-work#:~:text=Ocusync%20can%20transmit%20video%20at,much%20data%20at%20longer%20distances> (accessed on 7 April 2023).
48. TheDronestop. DJI Ocusync (What Is It, Why It's so Important, Updates of Ocusync). Published on 1 January 2023. Available online: <https://thedronestop.com/dji-ocusync-everything-you-need-to-know/> (accessed on 7 April 2023).
49. Belwafi, K.; Alkadi, R.; Alameri, S.A.; Hamadi, H.A.; Shoufan, A. Unmanned Aerial Vehicles' Remote Identification: A Tutorial and Survey. *IEEE Access* **2022**, *10*, 87577–87601. [[CrossRef](#)]
50. Tedeschi, P.; Al Nuaimi, F.A.; Awad, A.I.; Natalizio, E. Privacy-Aware Remote Identification for Unmanned Aerial Vehicles: Current Solutions, Potential Threats, and Future Directions. *IEEE Trans. Ind. Inform.* **2023**. [[CrossRef](#)]
51. Friis, S. Open Drone ID Online GitHub Repository Version 2.0 Published on 6 April 2022. Available online: <https://github.com/opedroneid/opedroneid-core-c> (accessed on 31 August 2023).
52. Intel Corporation. Intel Wireless AC 8265 Dual Band. Product Datasheet. Available online: <https://www.intel.fr/content/www/fr/fr/products/sku/94150/intel-dual-band-wirelessac-8265/specifications.html> (accessed on 31 August 2023).
53. Panda Wireless. Panda Wireless PAU06 300Mbps, Centos, Kali Linux and Raspbian. Available online: <https://www.amazon.fr/Panda-Wireless-PAU06-Adaptateur-Raspbian/dp/B00JDVRCI0> (accessed on 31 August 2023).
54. Allan, A. List of MAC Addresses with Vendors Identities. Online GitHub Repository, Created on 2 February 2017. Available online: <https://gist.github.com/aallan/b4bb86db86079509e6159810ae9bd3e4> (accessed on 31 August 2023).
55. Wikipédia. Adresse MAC. Last Modification on 19 July 2023. Available online: [https://fr.wikipedia.org/wiki/Adresse_MAC#:~:text=Une%20adresse%20MAC%20\(de%20Elle%20est%20unique%20au%20monde](https://fr.wikipedia.org/wiki/Adresse_MAC#:~:text=Une%20adresse%20MAC%20(de%20Elle%20est%20unique%20au%20monde). (accessed on 31 August 2023).
56. Secrétariat Général de la Défense et de la Sécurité Nationale. OUI: 6A:5C:35, 2019. Available online: <https://maclookup.app/macaddress/6A5C35> (accessed on 31 August 2023).
57. Kershaw, M. Drone ID. Online GitHub Repository. Available online: https://github.com/kismetwireless/kismet/blob/master/kaitai_definitions_disabled/dot11_ie_221_dji_droneid.kys (accessed on 31 August 2023).
58. Kershaw, M.; Dragorn. Online Resource: kismet_rest Documentation. Available online: https://kismet-rest.readthedocs.io/_/downloads/en/latest/pdf/ (accessed on 31 August 2023).

59. Andreou, A.; Mavromoustakis, C.X.; Batalla, J.M.; Markakis, E.K.; Mastorakis, G.; Mumtaz, S. UAV Trajectory Optimisation in Smart Cities using Modified A* Algorithm Combined with Haversine and Vincenty Formulas. *IEEE Trans. Veh. Technol.* **2023**, *72*, 9757–9769. [[CrossRef](#)]
60. Matic, V.; Kosjer, V.; Lebl, A.; Pavić, B.; Radivojević, J. Methods for Drone Detection and Jamming. In Proceedings of the 10th International Conference on Information Society and Technology (ICIST), Kopaonik, Serbia, 8–11 March 2020; pp. 16–21.
61. Abunada, A.H.; Osman, A.Y.; Khandakar, A.; Chowdhury, M.E.H.; Khattab, T.; Touati, F. Design and implementation of a RF based anti-drone system. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020; pp. 35–42.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.