

Using Statistical Methods in Electrical Engineering to improve Detection Algorithms for UAVs

Taqi Mohammed Khattab Al-Rubaye
Department of Medical Laboratory Technology,
College of Medical Technologies,
The Islamic University Najaf , Iraq
kaboos287@gmail.com

To Cite this Article

Taqi Mohammed Khattab Al-Rubaye, "Using Statistical Methods in Electrical Engineering to improve Detection Algorithms for UAVs", *Journal of Science Engineering Technology and Management Science*, Vol. 03, Issue 10, October 2026, pp: 09-27, DOI: <http://doi.org/10.64771/jsetms.2026.v03.i10.pp9-27>
Submitted: 01-09-2026 Accepted: 04-10-2026 Published: 10-10-2026

Abstract

This study presents techniques for detecting drones in controlled airspace, specifically for use in an airport context. The aim of the application was to identify small drones, given the increasing popularity of these devices that have become widely available. The study statistically identified three types of attacks that can be launched by malicious actors and that could affect airport operations and aviation safety. In order to propose solutions to these needs, the best relevant technologies and electrical tools identified in the literature and also available were analyzed. The comparative analysis of detection techniques allowed for optimize solutions to be proposed aimed at preventing drone attacks. The results show that a combination of different approaches is the best response to drone attacks on airports, thus promoting safer skies. It is recommended that each solution be tailored to the specific characteristics electrical of the airport in question in order to ensure the effectiveness of the proposed solution and maintain airspace security.

Keywords: Air transport; Operational safety, Drone Detection ,Statistical Methods ,Electrical Engineering

This is an open access article under the creative commons license
<https://creativecommons.org/licenses/by-nc-nd/4.0/>



Introduction

The use of drones has become widespread in contemporary society, covering activities ranging from military applications, such as surveillance of hazardous areas and extensive airspace surveillance in surveillance systems, to the delivery of equipment and inputs in difficult-to-access areas, especially in cases of natural disasters and catastrophes (SOUZA; HENKES, 2023), to the surveillance of construction sites, aerial photography and topographic surveys (MOSLY, 2017), as well as precision agriculture in the collection of data on rural properties (JÚNIOR; NUÑEZ, 2023), among others.

With the development of these remotely piloted aircraft, there is a need to develop effective methods for the detection and surveillance of drones of various models and sizes, especially in areas with restricted use of airspace, such as areas around airports due to aircraft operations and the potential vulnerability to damage from cyber attacks caused by these flying objects.

In this study, different technologies capable of detecting different flying objects that may pose cyber threats to airport operations security are identified, solutions available in the literature and on the market are presented, and their potential uses in cases of cyber attacks on airports are analyzed.

1.1 REMOTELY PILOTED AIRCRAFT – DRONES

Unmanned aircraft are called UAVs (Unmanned Aerial Vehicles), and when they are remotely controlled they are classified as Drones. Another classification occurs when aircraft are controlled remotely by an operator, for non-recreational purposes, and are then identified as RPAs, an acronym for Remotely Piloted Aircraft System (DECEA, 2018). Drones first emerged during the Second World War, with the introduction of remotely launched bombs by the Germans. Since then, remotely controlled aircraft have been increasingly developed, approaching the most recent standards only with the work of aerospace engineer Abraham E. Karem (WHITTLE, 2013). As a result, drones are no longer used exclusively in military contexts and have become part of commercial sectors of society. The most common types of drones are: fixed-wing drones, rotary-wing drones, airships, and ornithopters (DECEA, 2023). Figure 1 illustrates a rotary-wing UAV, while Figure 2 illustrates a fixed-wing UAV.



Figure 1 - Rotary wing UAV



Figure 2 - Fixed wing UAV

The popularity of drones has increased due to their versatility, ease of operation and wide range of applications in various sectors (ZMYSIOWSKI et al., 2023). These technologies, when using sensors,

cameras and GPS, have a variety of uses such as deliveries, cartography, environmental monitoring, aerial recordings, among others.

2017, when the first remotely piloted aircraft received approval from the Ministry of Defense. After this event, they began to be used in areas such as precision agriculture, environmental monitoring, border control, and also for recreational purposes (BRUM, 2019). Drones have become increasingly accessible and complete for carrying out various activities, which has required the development of effective solutions for their identification and monitoring, especially during their flight in restricted areas, such as airports and military installations, which can present risks to air operations. The dangers related to drones were highlighted in attacks such as the one that occurred in Abu Dhabi in January 2022, when fuel trucks were attacked by drones and ended up exploding. The accident resulted in the death of 3 people (CNN, 2023). In August 2018, a serious attack on President Nicolas Maduro occurred in Caracas, Venezuela, in which drones loaded with explosives were used to trigger explosions that caused panic and injured around seven people (BBC NEWS, 2018). Also in December 2018, Gatwick Airport, the second largest in the United Kingdom, had to be shut down for 30 hours due to 129 different police reports of drone activity in the vicinity of the airport (BBC, 2019).

Another similar situation occurred in May 2019 at Frankfurt Airport in Germany, when 143 takeoffs and landings were canceled at the airport after a 1.5-meter-diameter drone was identified in the southern part of the airport area (THE LOCAL, 2019). Such risks and attacks point to the need for aerial monitoring to ensure the safety of operations and prevent possible accidents or incidents.

The increase in the use of RPAs also makes it necessary to create regulations and agencies capable of monitoring this type of technology. This situation prompted the National Civil Aviation Agency (ANAC) to make it mandatory to register drones weighing between 250 grams and 25 kilograms.

For equipment weighing more than 25 kilograms, pilots are also required to register their license, while drones weighing less than 250 grams do not have any type of restriction (ANAC, 2017), which are potentially critical elements in air traffic management.

The rise of drones has raised concerns on a global scale, with several countries simultaneously identifying their potential and the threats they pose. As a result, there has been increasing emphasis on research and development of anti-drone sensors and systems (ZMYS-IOWSKI et al., 2023). This need has intensified due to the increasing number of incidents, invasions of restricted areas and cyberattacks targeted through these devices, which demands innovation in increasingly advanced detection equipment (ZMYS-IOWSKI et al., 2023).

The development of security systems for drone detection has led to the adoption of hybrid systems, based on the fusion of sensor and hardware control technologies, which are prevalent in airport facilities, prisons, and large events (PARK et al., 2021). However, despite advances in detection systems, many of these mechanisms still lack full integration with threat identification and neutralization steps. Zmyslowski et al., (2023) determine that to analyze the efficiency of an anti-drone system, the fundamental criterion lies in the protection capacity it provides to a specific facility. This efficiency must be measured considering the unique characteristics of the facility, such as location, size, technological processes in use, functions performed, and other activities. Furthermore, Gopal (2020) understands that an effective system must have a detection range of at least three kilometers. The system must detect and also be able to track a drone at a distance of at least one kilometer, especially when there are signs that the device may be carrying a potentially destructive payload.

Drones typically emit heat, sound and radio frequency (RF) signals to communicate with their controllers. There are systems that use these signals to identify if there are drones nearby and their locations. Radars

must be combined with other technologies, such as cameras and radio frequency scanners, to obtain an effective detection overview (PARK et al., 2021). However, radar systems emit powerful RF signals, requiring national permissions to use certain frequencies and installation locations. In high-security areas, the use of varied detection methods is essential, especially to identify drones that do not emit RF signals, such as those used in terrorist acts, which may use specific cloaking technologies.

2-DRONE IDENTIFICATION IN FLIGHT

The increase in popularity and technology of drones has brought several benefits to commercial, military, and even search and surveillance missions. However, the proliferation of these devices has ended up raising security-related issues and potential risks to air traffic operations. Given this scenario, it has become necessary to identify and track drones in flight to ensure air safety and neutralize potential threats. To address these issues, different methods of identification and tracking in flight have been developed by the academic community. Among them, the most prominent are ADS-B technology, pulse-chirp, the use of deep learning with cameras, Micro-Doppler signature with FSR, the use of RF scanners, and the use of infrared cameras.

a. ADS-B

ADS-B (Automatic Dependent Surveillance-Broadcast) is a technology used primarily for tracking and monitoring aircraft in controlled airspace. This technology facilitates the exchange of accurate information between aircraft, using reliable information mainly from the Global Positioning System (GPS) and makes use of radio frequency communication. The exchange of information about the updated positions and speeds of aircraft occurs using transponders installed on them (RODRIGUES, 2010).

Drone tracking can benefit from this method, which is widely used with aircraft, in which it is possible to obtain real-time information about their location and speed. Monitoring this type of aerial activity makes it possible to avoid collisions between drones and aircraft. Aircraft equipped with ADS-B sensors use receivers to send their positions and combine data such as their headings, speeds and altitudes. According to Rodrigues (2010), the information is transmitted to other aircraft that have the system equipped (ADS-B IN) and to stations with receiving antennas on the ground or at sea (ADS-B OUT). The stations forward the information in real time to the air traffic control centers.

In the study carried out by Giladi (2020), the speed frequency used for the transmission of ADS-B messages is 1090 MHz, a frequency designated for surveillance communications in several countries (ICAO, 2012). Through this frequency, aircraft emit signals containing crucial information for monitoring air traffic and for mutual awareness between aircraft in shared airspace. These messages are transmitted at intervals of approximately 0.5 seconds, providing frequent updates of the information.

In this study, any aircraft flying above the area of interest and below 1.2 km above ground level (AGL) can be detected by the measurement system. When an ADS-B message is received from an aircraft flying within the defined intensive monitoring area, the measurement system performs the final steps, simultaneously receiving, recording and analyzing the aircraft data and the measured noise. In this way, all ADS-B messages from the specific aircraft that activated the recording are recorded, along with the measured noise level, starting from a noise level above a pre-defined threshold. The geometric representation of the situation can be explained in Figure 3.

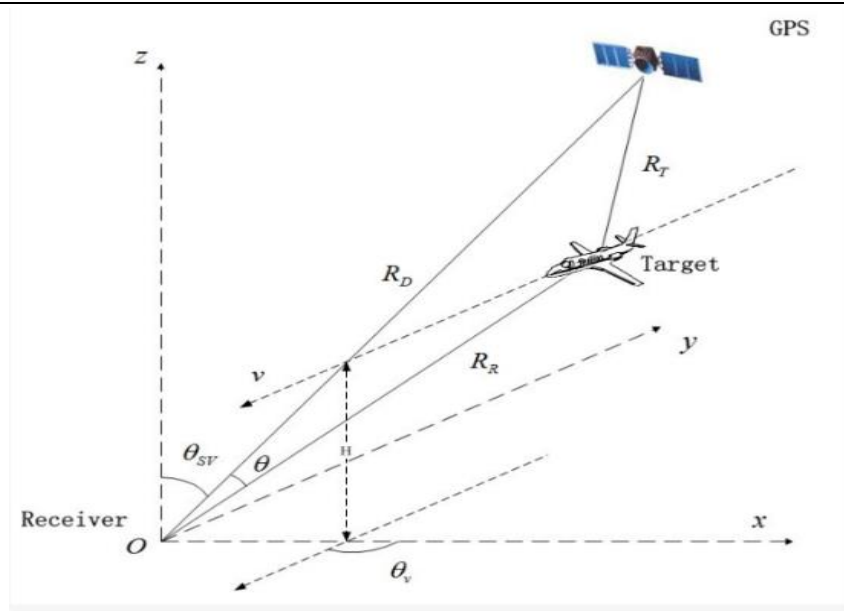


Figure 3 - Distances for noise monitoring

ADS-B is quite effective in identifying sound events and other aircraft information through the use of this technology, even when the environments have several obstacles and background noise. It was found that because the use of this technology depends on reliable GPS satellites, this method stands out compared to the use of other traditional radars that depend on other external sources. Despite this, the method proposed by Giladi (2020) may present noise detection failures during propagation, due to the dissipation of sound from aircraft that are far from the installed microphones or due to interference from other noises during propagation. The ADS-B transponders usually used are excessively large for the drone model covered by this study, being more suitable for larger drones. One possibility for small drones would be the ADS-B technology belonging to the Ping2020 family from UAV ionic (2023), a ready-to-use drone-level ADS-B product that can be connected to the drone's flight controller and transmit flight information through the RF channel (frequency band within the radio frequency spectrum used for signal transmission) (PARK et al., 2021). The aforementioned transponder has a high acquisition cost, and it was previously necessary for there to be low-cost production options throughout the country for the identification method to be economically viable.

b. Pulse-chirp radar

Pulse radar can be used to identify and locate drones in airspace, as the radar emits a short, high-intensity pulse of electromagnetic energy that undergoes alliteration when the pulse is reflected by the drone. The pulses are emitted at standard intervals, and the intervals between the moments of emission and the moments in which the echoes reflected by the object are detected are recorded (CURRIE, 2005).

The use of this method consists of directing the pulse in a given direction and analyzing the change in frequency that occurs after the reflection phenomenon. This analysis is capable of providing information about the object with which the collision occurs. For Misreads et al. (2000), the advantages of using pulse-chirp radar compared to conventional radars are related to greater resolution capacity at a distance, better discrimination of targets in environments with many reflective objects, and better analysis speed. The radar in question is capable of emitting pulses with variable frequencies and can also provide analysis of the reflected signals, identifying whether or not there are drones present in the monitored space. The reflected signals are analyzed for amplitude and phase fluctuations that occur in this reflection

phenomenon. The fluctuations are considered to be distinctive characteristics of drones compared to other objects, so that data from these variations are used to build target fluctuation models. These models represent the specific characteristics of the fluctuations that are expected when a drone is present.

In order to identify drones by the target's drift model, Kim et al. (2018) propose an algorithm capable of recognizing characteristics of radar signals and making comparisons with drift models that already make up their database. Signal processing and statistical analysis techniques are used during the comparisons, so after checking the similarity of the observed signals and the target's drift models, it can be said whether the target is a drone or not. In this method, the radar equation is used to determine the maximum detectable RCS (Radar Cross Section). RCS is a measure of the amount of energy reflected by an object when illuminated by a radar. From the basic radar equation, it is possible to relate the power of the signal received by the radar with the power of the transmitted signal and the RCS of the object. Equation 1 shows how the maximum detectable RCS of drones can be obtained.

$$P_r = \frac{P_t \cdot G_r \cdot G_t \cdot \lambda^2 \cdot RCS \cdot A}{4\pi \cdot R^4} \quad (1)$$

where P_r is the power of the signal received by the radar, P_t is the power of the signal transmitted by the radar, G_t is the gain of the transmitting antenna, G_r is the gain of the receiving antenna, λ is the wavelength of the transmitted signal, RCS is the radar cross section of the object, A is the effective area of the target, and R is the distance between the radar and the object.

In the context of the study proposed by Kim et al. (2018), Equation 1 is used to determine the maximum detectable RCS of different drones using a pulse-chirp radar. The maximum detectable RCS is a necessary parameter to define the radar's ability to detect and track drones efficiently. The results obtained prove the quality of the method in successfully identifying drones, distinguishing them from other objects such as birds or aircraft. However, the use of pulse-chirp radar has limitations regarding the existence of external interference that affects the radar, and may fail if there are signals from other electronic devices and there are physical obstacles that alter the properties of the signal.

The effectiveness of identification may be compromised depending on the location of the protected area. Drones have the ability to fly at extremely low altitudes and this ability to fly over uneven terrain is one of the factors that can make their detection by radar more complex (LUKASIEWICZ; TWARDOWSKA, 2022). Another limitation of the method is the dependence on specific characteristics of drones, so that it does not recognize drones with atypical fluctuation characteristics. A different approach to drone monitoring consists of the approach that involves obtaining images and computational strategies, presented below.

c. Deep learning in drone detection and tracking through images

Drone detection and tracking can be performed using deep learning technology in conjunction with several coordinated cameras. Deep learning technology is used to allow the system to learn and adapt based on the available data, making the results obtained increasingly accurate.

One way to enhance the results obtained is to use deep learning and integrate convolutional neural networks to extract important features from the images obtained from the footage (CUNHA, 2020). The difference with convolutional networks lies in the quality with which they extract features within the network itself, enabling them to obtain information about the shapes, sizes, colors, and movements of the drone to identify its positions and trajectories. The most relevant algorithms used are YOLO (You Only Look Once) classifiers that divide images into regular grids of cells capable of identifying the boundaries of objects using bounding boxes and predicting the classes of objects contained within them through

probabilities. Figure 4 illustrates the comparison of detections produced by different algorithm architectures.

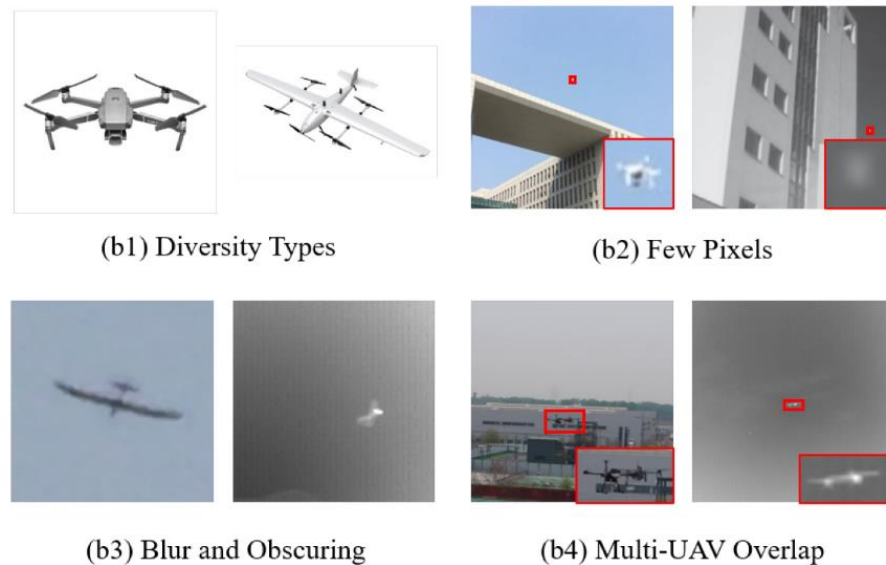


Figure 4 - detections produced by different architectures

Detections by the YOLO architecture are represented by green colors and the others by blue and red colors. The YOLO architecture is the one that best identified the presence of 2 birds and 1 drone approaching in flight in the image. Training this algorithm architecture with large data sets that contain examples of different drones is effective to ensure that the method identifies possible threats and contributes to the creation of a reliable monitoring system. Unlu et al. (2019) propose a system that employs a wide-angle static camera and a lower camera mounted on a rotating tower for drone detection and tracking in order to optimize memory usage and processing time. This study suggests a deep learning approach that combines multiple frames. The frame captured by the zoomed camera on the tower is superimposed on the wide-angle frame of the static camera, resulting in an efficient processing flow. Thus, the initial detection of small aerial incursions is performed simultaneously in both the main image plane and the zoomed image plane. The developed method is capable of providing panoramic and three-dimensional views while monitoring the desired environments, which ends up allowing the detection and tracking of drones to be carried out more precisely.

By obtaining and combining images from different cameras in real time, monitoring allows for rapid responses in the event of identifying drones or other aerial threats. However, the method needs to be adapted to overcome limitations such as variations in ambient brightness and visual noise that interfere with the results obtained.

Drone detection equipment that uses optical cameras is more affordable and has fewer regulatory restrictions compared to the other techniques presented (PARK et al., 2021). This allows the application of dense camera systems that complement each other in monitoring. Despite this, they have limitations such as limited range. These limitations highlight the need to integrate them with other detection systems. Military electro-optical and infrared (EO/IR) systems are usually used on a large scale and use optical cameras with infrared sensors to identify drones (PARK; AHN; BAEK, 2012).

d-Micro-Doppler signature for drone detection using FSR

The Micro-Doppler signature is a technique used to detect and classify moving objects, such as drones, based on the Doppler phenomenon (MUSA et al., 2019). It consists of analyzing the modulation patterns

of the Micro-Doppler signals reflected by the interaction between the drone's propellers and the environment around it. An additional frequency modulation format also occurs due to specific parts of the drone's body that are in micro movement. These movements, as analyzed by Chen (2011), can be caused by vibrations or small regions of the object that reflect the signals and cause variations in the frequencies of the reflected signals (CAMMENG et al., 2014). The use of the signature allows the identification of distinct characteristics and patterns in the signal reflected by the drone, enabling the detection and accurate classification of the moving object.

In the process of receiving the waves generated by these described movements, the Forward Scatter Radar (FSR) geometry is chosen to receive the reflected signals and the radar antennas are arranged in a straight line or in a two-dimensional array (MUSA et al., 2019). This linear or planar arrangement allows the radar to acquire multiple samples of the signal reflected by the target from different positions. This is due to its advantage for highly accurate range detection based on the phase difference between the transmission and reception signals obtained separately at more than two operating frequencies (PARK et al., 2019)

The FSR configuration is capable of measuring the frequency variation of the signal reflected by the drone, allowing the analysis of the micro-Doppler signature, which contains information about the drone's movement patterns. In addition, this radar has high sensitivity and resolution, which allows the detection of small moving objects, such as drones, in different environmental conditions.

Musa et al., (2019) propose the use of FSR from a parabolic dish antenna as a receiver. The objective is to perform the detection and analysis of drones through the analysis of the scattered signal. To this end, the signal received by the radar is combined with a reference signal, which plays a crucial role in the formation of the scattered signal. The reference signal acts as a comparative reference for the echoed signal, allowing the identification of differences between them (MALANOWSKI, 2011).

These differences contain relevant information about the presence and characteristics of the drone under analysis. The combination of the reference signal with the echoed signal enables the separation and extraction of specific components of the scattered signal, facilitating the detection and accurate analysis of the drone (MALANOWSKI, 2011). The proposed model using an antenna is shown in Figure 5.

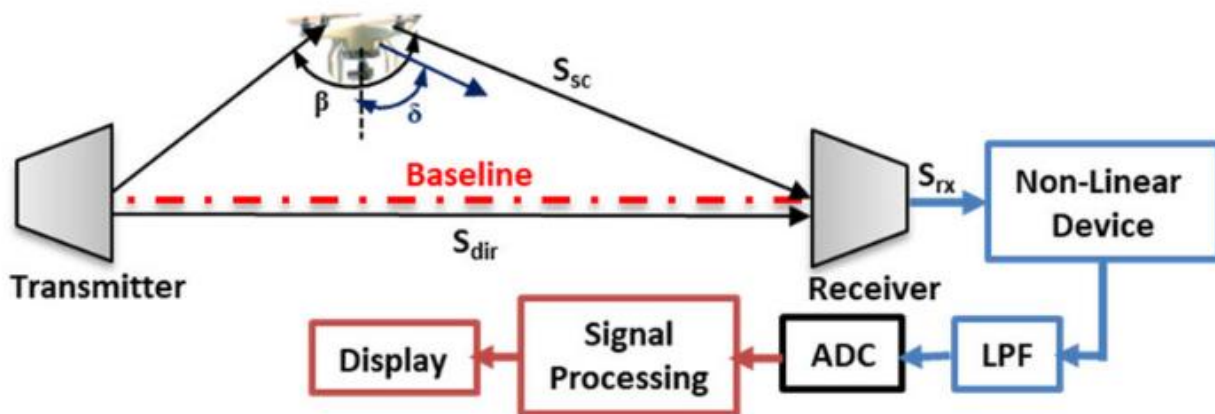


Figure 5 - Forward scatter radar geometry

In the proposed drone detection system, the parabolic antenna is used to direct and concentrate the signal reflected by the drone. The received signal is amplified by the low-noise amplifier (LNA) before being processed and a non-linear device performs a power operation on the signal. This operation is described mathematically by an Equation that establishes the non-linear relationship between the input and output signal. The output of this non-linear device contains relevant information about the Micro-Doppler

signature generated by the rotation of the drone blades. After passing through the non-linear device, the signal has its frequency range limited in a low-pass filter (LPF), then undergoes conversion into digital form by the analog-to-digital converter (ADC) and has the information that characterizes its Micro-Doppler signature identified with signal processing using algorithms. The results obtained in the process are provided on a Display that represents the output device, such as a computer or monitor. Equation 2 represents the phase modulation generated as a result of a circumferential micro-movement of each blade.

$$\phi_{md}(t) = -\frac{2\pi Lb}{\lambda} \cos\left(\frac{\beta}{2}\right) \cos(\delta) \cos(\Omega t + \theta) \quad (2)$$

where λ is the wavelength, Lb is the blade length, β is the bistaic angle, δ is the incidence angle, Ω is the angular velocity of the blades, t is the time instant, and θ is the initial angle. The bistaic angle β is a parameter that describes the geometry of a radar system, specifically the angular configuration between the transmitter, the target and the receiver. For a rotor with N blades, there will be N rotating scatterers with different initial angles, which are given by Equation 3 (MARTIN; MULGREW, 1990).

$$\theta_n = \theta_0 + \frac{2\pi n}{N} \quad (3)$$

where n ranges from 0 to $N-1$. The total signal received for N blades is given by Equation 4.

$$S_{rx}(tot) = \sum_{k=0}^{N-1} A_{rx}(n) \sin(2\pi f dt + \phi_{md}n(t)) \quad (4)$$

where f is the frequency of the wave generated by the interaction between the drone's propellers and the surrounding environment, dt is the time differential, $A_{rx}(n)$ is the amplitude of the signal received for each blade, and ϕ_{md} is a numerical value representing the phase modulation.

Equation 5 quantifies the amplitude of the composition between the reflected and reference signals.

$$A_{rx}(n) = A_{ref} A_{surv}(n) \quad (5)$$

e- identification using radio frequency scanners

Drones operated by controllers tend to exchange specific messages using radio frequency (RF) signals, containing information such as flight commands and sensor readings (PARK et al., 2021). In this regard, Al-Sa'd et al., (2019) developed a system that uses deep neural networks with several hidden layers to analyze and categorize RF signals. This system is capable of identifying different types of drones and their respective flight modes. RF scanners capture the electromagnetic signals emitted by drones, while direction finders indicate where the drone is transmitting from (ZMYS-IOWSKI et al., 2023). Thus, this system together enables the identification and location of drones so that airport operators can act quickly and contain potential risks. RF-based detection is limited by its inability to identify drones that do not constantly emit RF signals, such as those operating with autonomous navigation. There is also a limitation because RF scanners identify drones by analyzing their signals, which can be challenging when drones use unknown control protocols (PARK et al., 2021). RF scanners are quite efficient in detecting the presence of a drone and identifying its category by comparing them with known bands. Despite this, these scanners face limitations in accurately locating a drone in space, unless they are used in a triangulation configuration that is defined by the use of multiple receivers to determine the exact location of drones (MOTOTOLEA; STOLK, 2018).

f. Identification using infrared cameras

Detecting drones in flight can be very difficult at night or in urban environments. An alternative for this scenario is the use of infrared thermal cameras that are capable of detecting small variations in heat at a level of tens of mK (ANDRAS'I et al., 2017). These cameras have the ability to identify objects that emit

heat, which allows them to operate efficiently at night. This is because they are capable of capturing thermal emissions in the infrared range resulting from the generation of heat by the electronic components of drones. Thus, the thermal signatures of these devices can be easily recognized (STURDIVANT; CHONG, 2017).

The study by Andrasi et al. (2017) with drones highlighted that contrary to expectations, the engines are not the main sources of heat detectable in the thermal spectrum, due to efficient cooling by air circulation. The batteries, contained in the main body of the drone and which end up receiving limited air circulation, are easily visible in thermal images, especially in drones with a fully enclosed body where the temperature remains higher. The quality of the method can also be observed in identifying even small drones that would go unnoticed by other types of radars. Table 1 presents a summary of the main characteristics of the presented methods identified in the literature. It should be noted from the study by Gopal (2020) that the amount of heat produced by the drone varies according to the type of propulsion used, being more difficult to detect drones with electric propulsion, which is more discreet compared to the method. For civilian drones, the range of this detection method is currently only about 100 m.

g. Detection solutions available on the market

The need to monitor and control drone traffic in airspace has become an opportunity for innovation in this market. Different solutions are identified for different scenarios and needs, and can act in reactive or preventive ways, seeking the optimized integration of available detection technologies.

i. Dedrone

The company Dedrone has innovated in the DedroneTactical line of anti-drone defense with its autonomous C2 (control and coordination of operations) platform guided by AI. Going beyond simple sensor correlation, the platform integrates advanced algorithms and machine learning techniques, such as behavior model filters and neural networks, processing more than 18 million AI-based images (DEDRONE, 2023). Its data processing capacity seeks to eliminate false positives, providing drone detection with high precision and reliability.

The company offers the CsUAS Agile Response Kit that provides modular flexibility in sensor fusion and field mitigation, covering RF detection and making use of cameras (DEDRONE, 2023). The system is equipped with a rugged laptop, rugged RF sensors, and related accessories. The model can also be expanded to integrate remote points and other tactical sensors via a mesh network, a network in which devices or nodes are directly connected, dynamically and non-hierarchically. The system offered by Dedrone integrates with several other security systems and can be considered a complete airspace security solution (ZMYS-IOWSKI et al., 2023). Figure 6 shows the CsUAS Agile Response Base Kit provided by Dedrone.

v. Geofencing

Geofencing is a technological resource that establishes virtual boundaries to prevent drones from entering prohibited airspace, such as airports, making it essential for airspace security (STEVENS; ATKINS, 2018). There are geofencing systems adapted to small drones and also models of modern autopilot systems that already incorporate virtual barriers as a containment measure in highly sensitive regions (HAYHURST et al., 2015). When integrated into a drone's software, geofencing proves to be a highly effective security barrier, especially when drones have GPS or GNSS systems, preventing them from entering unauthorized areas (AISC, 2015).

Drone manufacturers frequently update geofencing systems to make changes to restricted zones, including new areas or temporary alterations. Some manufacturers have developed three-dimensional geofences around airports, increasing safety on aircraft approach and departure routes and minimizing the

risk of dangerous interference during takeoffs and landings (DJI, 2019). Despite these precautionary measures, it should be noted that geofences can fail, especially if drone operators disable the geofences' capabilities.

3 METHOD

This study identifies and compares different technologies capable of detecting drones in controlled airspace, especially near sensitive areas of airports. The study objects were defined as technologies for detecting small drones (payload less than 250g), and their potential implications in cyberattack scenarios at airports.

a. Reference drone

The DJI mini 2 drone was used as the object of analysis, since it is immensely popular due to the combination of a modern design with attractive prices and the trust associated with the DJI brand, a global leader in the drone sector, with approximately 70% of this market (INSIDER, 2020). The model in question has the highest number of registrations with ANAC (2022), corresponding to 9.43% of registrations and, in addition, stands out as the drone predominantly sold in Brazil in 2023. The relevance of this drone is enhanced by its portability and ease of use, making it suitable for applications in different contexts. Figure 10 shows the chosen drone model.



Figure 6 - DJI Mini 2 drone model

The main specifications of the reference drone are:

Takeoff weight: 242g;

Dimensions: Folded (without propellers): 138×81×58 mm (L×W×H), Unfolded (without propellers): 159×203×56 mm (L×W×H), Unfolded (with propellers): 245×289×56 mm (L×W×H);

Maximum horizontal speed: 16m/s; Maximum flight time: 31 minutes; Maximum flight distance: 16 km;

Global Navigation Satellite System: GPS + GLONASS + Galileo; 360° rotation; ➤

It has 4 motors; With Wi-Fi connection; Automatic return function.

It is worth noting that due to its weight of less than 250 g, the DJI Mini 2 complies with the flight regulations established for most countries and is recognized as an example of success in the miniaturization and efficiency of drones, as it has specifications and features comparable to larger and more expensive models. With a sales price of around \$3,000, it includes a high-resolution camera and has a differentiated flight time for this cost range.

Another point to be noted is the operability of the model, since it has intuitive systems and assisted flight modes that are useful for a wide range of applications. It is worth noting that the drone studied is a quadcopter because it has 4 rotating wings.

Efficient drone detection is an issue of increasing relevance and still has several limitations that are explored in this study. The need to identify the presence of drones is verified, especially when they may pose threats to security, privacy or the integrity of restricted airspace. By defining the strengths and weaknesses of different detection methods, such as active radars, RF scanners, visual systems and sensors, the study contributes to a detailed understanding of how each technology responds to challenges such as variable lighting, noise interference

Method	Benefits	Limitations
Radar	Long detections; tracks different types of drones; distinguishes drones from birds; independent of climatic conditions.	Range depends on RCS; high acquisition and operating costs; requires license to broadcast.
Scanner RF	High detection accuracy; Does not identify drones with autonomous navigation; passive detection, without need for license; minor cost in relation to radars.	cannot identify multiple drones simultaneously.
Visual	Identifies drones without emitting RF signals; records occurrences for investigation.	Limited range; depends on lighting conditions.
infrared.	Efficient cameras in night environments; Highly accurate	Difficult to from differentiate drones small birds; not effective over long distances.

Table 2 - Comparison between drone detection technologies

The classification of detection methods varies according to environmental and functional factors, and their functionalities in relation to such aspects must be taken into account to understand the effectiveness of each technology in different operational conditions. Radar methods, RF scanners, visual cameras (VIS) and infrared cameras (IR) are compared in terms of performance regarding the ability to operate in adverse weather conditions.

In addition, technical aspects, such as identification and multiple detection capabilities, are also analyzed. Other crucial factors include the cost of the system, detection effectiveness and accuracy in locating drones. This classification allows users and developers of airport security systems to choose the most appropriate technology to integrate into their detection solutions. Table 3 presents a summary of the main parameters associated with such technologies.

Factor	VIS	GO	Radar	Scanners RF
Cost	\$	\$\$	\$\$\$	\$\$
Birds	✓		✓	✓
Weather Conditions Adverse		✓	✓	✓
Controller location				✓
Multiple Drone Detection	✓	✓	✓	
Drone Identification	✓	limited		✓
Noise		✓	✓	✓
Long Range Detection		limited	✓	✓
Light	✓	✓	✓	✓
Darkness		✓	✓	✓

Table 3 - Different parameters associated with technologies

a.Possible drone attacks on airports

In this study, three scenarios of possible small drone attacks on airports were identified, with the main threat being indirect and support systems, as well as possible direct collisions with aircraft. The attacks identified represent emerging and often underestimated threats. The analysis of these scenarios can be used to anticipate and prepare effective responses against these new forms of threats.

i Attack on air traffic management systems

The use of ADS-B transponders to transmit information between aircraft and ground surveillance stations can be exploited both by malicious drone operators, who aim to obtain information through espionage, and by users who intend to launch direct attacks against the airport system. According to Manesh and Kabouch (2017), the ADS-B communication system has already demonstrated security flaws, many related to the lack of encryption used in the method. Given this weakness, much information can be obtained or even tampered with with the intention of causing direct attacks on the system.

The attack could occur with an attacker positioned near the airport with a software-defined radio using an ADS-B transmitter/receiver system capable of collecting data from aircraft in transit.

By obtaining information about the spatial coordinates and identification of aircraft, he could launch drones into the airspace equipped with ADS-B transponders and capable of falsifying their identities with the data previously obtained. These drones could be used to emit adulterated ADS-B signals that imitate those of commercial aircraft and could cause chaos in the airport's surveillance system. In the worst case scenario, the drone controller would use the aircraft information to create collision risks by launching drones against the most likely trajectories of aircraft in more complex situations such as takeoffs and landings.

ii Attack on remote systems supporting air traffic management

Drones could be used to obtain information about the aeronautical telecommunications systems used by the airport, identifying vulnerabilities to be exploited in future attacks.

Using the FPV (First Person View) channel, the operator can control the drone and obtain information from a distance. Drones equipped with cameras are capable of capturing data and images in real time, which can help identify airport security breaches. In addition, drones with radio transceivers can intercept radio transmissions or cause interference (LYKOU et al., 2019). They also have the potential to attack critical infrastructure with explosive charges, as has already occurred at airports in Saudi Arabia (NEWS ANI, 2019).

Communication, surveillance and navigation systems are vital to the operation of airports and are often located in remote locations, far from central airport structures. These systems, which include aeronautical telecommunications, navigation aids and surveillance radars, are responsible for guiding, locating and directing aircraft, maintaining the safe and efficient flow of air traffic. (ICAO, 2020).

This drone attack can have two objectives: first, to collect confidential data from transmissions from remote airport facilities that contribute to air traffic management and second, to disrupt the functionality of these systems by interfering with the telecommunications signals emitted from these remote infrastructures to the control tower or physically damaging navigation and surveillance support equipment, such as radars and power stations. These systems may be vulnerable to aerial attacks because they are generally located far from the airport center. An attack of this kind can result in adverse impacts on air traffic, flight delays or cancellations. Figure 11 illustrates the interception of RF signals emitted by remote air traffic management support systems.



Figure 7 - Drone intercepting and interfering with data transmission to the airport

Another form of attack would be directed at the wireless networks and IT infrastructure of an airport. Signals sent through the air can be picked up by receivers tuned to the correct frequency. According to Lupu (2009) and Wilkinson (2014), the transmitted data can be obtained by drones equipped with wireless antennas with embedded software.

According to Guri et al. (2017), drones are also capable of intercepting and collecting information from computers that remain isolated from any other network, and Nassi et al. (2019) demonstrate that they can capture conversations remotely using spying devices. Drones equipped with signal capture technology can exploit internal airport communications, infiltrating wireless networks to intercept and capture data from network users. One of the techniques used in this attack involves the use of RFID (Radio-Frequency Identification) tags, which are small devices that store information and can be tracked via radio waves. Drones with RFID readers can detect information contained in the tags, and can obtain information even from hundreds of meters away (KLEINER et al., 2006). An undercover agent could take advantage of access to the building's roof or nearby facilities and infrastructure without being noticed by security controls. The infiltrator would be able to distribute RFID tags to mark locations such as wireless routers, airport server rooms, and security camera networks. The drone could navigate with its GPS navigation system turned off, preventing it from being easily identified, and follow the route identified by the RFID tags distributed to guide its attack.

This attack could compromise the airport system, with service interruptions and possible data leaks from operations carried out. Confidential information about airports and their users is at risk of being accessed by malicious individuals. The airport may have to interrupt operations for security reasons and bear the financial losses generated in such a situation.

b. Proposed solutions for the defined attacks

Airports are characterized by different sizes, traffic flow, architecture, number of runways, among others. These structures must arrange their sensors and defense mechanisms in a unique way to achieve the greatest security for their employees and customers, as well as for the efficiency of the operations carried out. The threats generated by small drones can be minimized with integrated detection processes that guarantee protection against attacks directed at air traffic management systems, attacks on remote systems that support air traffic management, and attacks on airport communication and information systems.

Although geofencing is a valuable tool in protecting against unauthorized drones, its effectiveness can be complemented by other detection and interdiction methods. In this context, specific measures are suggested to increase airport security against malicious drone operations.

i Solutions for attacks on air traffic management systems.

The integration of drones into airspace poses challenges to airport security due to the vulnerability of the ADS-B system, used for communication between aircraft and ground stations. As indicated by Manesh and Kabouch (2017), the lack of adequate encryption in ADS-B allows attackers, with appropriate equipment, to capture aircraft data and launch drones emitting falsified signals, disrupting airport monitoring and increasing the risk of collisions during takeoffs and landings.

Solutions such as Dedrone's Base Kit can be used as a response to the proposed attack, being placed in high areas such as control towers. The solution offers broad coverage of the airspace and allows effective detection of suspicious ADS-B transmissions. This is due to the capacity of its processing system to analyze communication data. XPeller can be used in conjunction with other drones due to its versatility, making it ideal for installation in peripheral areas of the airport, where its RF detectors and acoustic sensors work together to identify and track malicious drone operators, ensuring the protection of the airport perimeter.

XPeller can identify malicious drones and use its directional radio frequency jammers to neutralize them before they approach sensitive areas. This technology can also be used to identify a malicious agent still in the vicinity of an airport, which is essential for combating this type of extremely lethal attack that requires little response time from the detection system. In addition, Dedrone's solution, upon detecting potentially dangerous signals, is quickly able to trigger an alert protocol, informing the control tower and ensuring an immediate response. This technology differentiates between legitimate and tampered signals, minimizing undue interruptions to airport operations.

It is believed that, for this type of situation, radars would be the primary option for detecting drones (differentiating them from birds). They would be located around the airport perimeter to maximize airspace coverage. The use of RF scanners would add value by passively detecting RF signals, without compromising the operation's signals. Because they are less expensive than radars, they would be used as an additional layer of security positioned near takeoff and landing runways to identify attempts to interfere with ADS-B signals. Visual cameras and infrared cameras could be used to complement identification and differentiate targets with unknown protocols.

ii Solutions for attacks on remote air traffic management support systems

Malicious agents can exploit flaws and collect confidential information using small drones using the FPV channel. This attack can expose security flaws and even lead to direct damage to remote critical infrastructure. The airport's communication, surveillance and navigation systems may be threatened and suffer fatal damage.

In this attack pattern, the defense should initially be structured with the implementation of wide-coverage radars or RF detectors to identify targets at long distances. The use of sensors such as electro-optical cameras or infrared cameras should also be integrated to increase the ability to distinguish drones as they approach and make it possible to identify their possible payloads. These defense mechanisms can be strategically positioned in critical areas, such as near remote systems, in the control tower or at high points in the airport structure. The integration of these systems with the airport operations center is sufficient for a rapid response to this type of attack.

III Solutions for attacks on airport communication and information systems

Airport infrastructures need to be agile in tracking drones, especially when they move slowly or remain stationary over critical areas. Complementing RF scanners with electro-optical or infrared cameras allows the detection system to monitor unauthorized flights and also collect additional information about possible cargo transported by the drone.

The strategy for positioning these sensors requires careful distribution around the airport perimeter, prioritizing areas of public access and being based on risk assessments carried out by experts. However, the mission of identifying and neutralizing the drone operator stands out, rather than focusing exclusively on the aerial device itself.

Security teams must be properly trained in the use of portable RF scanners and proactively intervene against suspicious activities. The technology developed by Dedrone proved to be suitable for the proposed scenario, by offering an integrated approach to the nodes in a dynamic way, where radar systems and electro-optical sensors communicate to ensure that critical points in the airport communication system are not attacked. Dedrone's advanced software also enables the strategic distribution and monitoring of sensors around the airport perimeter, optimizing coverage of high-risk and public access areas.

Conclusion

This study discussed the adoption of methods and technologies for detecting drones in controlled airspace, specifically focusing on the detection of small drones approaching airports. The study addressed the classifications of unmanned aircraft and the phenomenon of drone popularization. It was noted that the regulation and supervision of these devices are still in a state of development, mainly due to the risks of using them for criminal purposes.

Although there are several technological solutions for detecting drones, there is still a concern about the lack of international standards and manuals that guide the integration, design and application of these systems in airports and critical infrastructures. Therefore, the risks of interference in communications that may be caused by the radars and sensors used must be assessed, which may affect other legitimate forms of communication.

Interference in signals emitted by approach radars and radio communications is a critical example that can cause catastrophic damage. It is essential that airport operators respect legal limits when deploying anti-drone systems and that all risks are mapped and assessed. Actions must be guided by reliable data obtained from the systems chosen for this aerial protection, and it is essential to develop contingency plans that define clear security measures.

The use of drones can attract agents with malicious intent, since there are relatively affordable drone models that provide means of carrying out attacks with low risk to the user. Critical airport infrastructures need to be protected against these aerial attacks through effective threat assessment and resistance actions. Although airport environments are complicated, with a variety of sizes and characteristics, they have similar security requirements to protect their facilities and detect and identify drones being misused. Using extensive literature research on drone detection technologies, three categories of attack scenarios in airport facilities were developed and one or more protection plans were proposed for each case.

Three scenarios of small drone attacks stand out for their potential damage: the compromise of air traffic management systems through the exploitation of flaws in the ADS-B system encryption, attacks on remote auxiliary systems that can affect the efficiency of airspace management, and attacks against critical communication and information infrastructures, which can trigger security breaches and data theft. The detection methods adopted included the integration of radars and sensors, as this combination is considered in the literature as the most effective way to cover various types of threats and attack configurations. To ensure complete primary surveillance at airports, the use of several radars with different detection ranges is suggested. It is also recommended that visual detection sensors (electro-optical and infrared cameras) and RF scanners be combined to identify drones and their payloads.

Detecting drones at airports to prevent unwanted activity is a broad and profound dilemma. While there are a variety of technological solutions available, airport operators must remain within the law when deploying disruptive technologies and the risks to the community must be fully assessed and understood. Critically, airports must develop contingency action plans detailing appropriate responses that occur before, during and after any drone incident. Additionally, the anti-drone systems industry still lacks unified standards, resulting in a wide variation in the effectiveness and reliability of available systems.

Reference

1. 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.*, Elsevier Science Publishers B. V., v. 100, p. 86–97, 2019.

2. ANAC. Brazilian Special Civil Aviation Regulation (RBAC-E) 94: General requirements for unmanned aircraft for civil use. Brasília, 2017. ANAC. Drones. 2022. Available at: <<https://www.anac.gov.br/aceso-a-informacao/dados-abertos/areas-de-atuacao/aeronaves/drones-cadastrados/painel-de-drones-cadastrados>>. Accessed on: May 23, 2023.
3. ANDRAS[~]I, P.; RADIS[~]IC[~], T.; MUS[~]TRA, M.; IVOS[~]EVIC[~], J. Night-time detection of UAVs using thermal infrared camera. *Transportation Research Procedia*, v. 28, p. 183–190, 2017.
4. BBC. Gatwick Airport Drone Attack: Police Have No Lines Inquiry. 2019. Available at: <<https://www.bbc.com/news/uk-england-sussex-49846450>>. Accessed on: September 27, 2023.
5. BBC NEWS. Venezuela President Maduro survives ‘drone assassination attempt’. 2018. Available at: <<https://www.bbc.com/news/world-latin-america-45073385>>. Accessed on: October 12, 2023.
6. BIRCH, G. C.; GRIFFIN, J. C.; ERDMAN, M. K. UAS Detection, Classification, and Neutralization: Market Survey 2015. Albuquerque, New Mexico and Livermore, California, 2015.
7. BRUM, C. B. D. Use of drones in civil and criminal proceedings in Brazil: Considerations from the perspective of fundamental rights. *DRONES AND SCIENCE*, p. 28, 2019.
8. CAMMENGA, Z. A.; BAKER, C. J.; SMITH, G. E.; EWING, R. Micro-doppler target scattering. In: 2014 IEEE Radar Conference. Cincinnati, Ohio: IEEE, 2014.
9. CHEN, V. The Micro-Doppler Effect in Radar. 3rd ed. London, England: Artech House Radar Library, 2011.
10. CUNHA, L. C. D. Convolutional neural networks and image segmentation: a literature review. 2020. Course Conclusion Work (Specialization) - School of Mines, Federal University of Ouro Preto, Ouro Preto.
11. CURRIE, G. Introduction to radar systems. *IEEE Aerospace and Electronic Systems Magazine*, v. 20, n. 1, p. 3–36, 2005.
12. DECEA. AIC No. 24, June 11, 2018. Remotely piloted aircraft for exclusive use in operations by Public Security, Civil Defense and Federal Revenue Inspection agencies. Rio de Janeiro: DECEA, 2018.
13. DECEA. ICA No. 100-40, June 6, 2023. Remotely piloted aircraft system and access to Brazilian airspace. 2023.
14. DEDRONE. Dedrone Tactical. 2023. Available at: <<https://www.dedrone.com/solutions/dedrone-tactical>>. Accessed on: October 22, 2023.
15. DJI. DJI Enhances Geofencing Technology to Protect Airports. 2019. Available at: <<https://www.dji.com/ae/newsroom/news/dji-improves-geofencing-to-enhance-protection-of-european-airports-and-facilities>>. Accessed on: November 3, 2023.
16. HAYHURST, K.J.; MADDALON, J.M.; NEOGI, N. A.; VERSTYNEN, H. A. Case Study for Assured Containment. *Proceedings of the International Conference on Unmanned Aircraft Systems (ICUAS)*. 2015.
17. Kim, B.; PARK, J.; PARK, S.-J.; KIM, T.-W.; JUNG, D.-H.; KIM, D.-H.; Kim, T.; PARK, S.-O. Drone detection with chirp-pulse radar based on target fluctuation models. *ETRI Journal*, vol. 40, no. 2, 2018.

18. KLEINER, A.; PREDIGER, J.; NEBEL, B. Rfid technology-based exploration and slam for search and rescue. In: 2006 IEEE/RSJ International Conference on Intelligent Robots and Systems. Beijing, China: IEEE, 2006. LUPU, T. Main types of attacks in wireless sensor networks. Recent Advances in Computer Engineering, Vasile Parvan 2, 300223, Timisoara, ROMANIA, n. 9, 2009.
19. LYKOU, G.; ANAGNOSTOPOULOU, A.; GRITZALIS, D. Smart airport cybersecurity: Threat mitigation and cyber resilience controls. Sensors, vol. 19, no. 1, p. 19, 2019. ISSN 1424-8220.
20. MALANOWSKI, M. Signal Processing for Passive Bistatic Radar. 3rd ed. London, England: Artech House Radar Library, 2011.
21. MANESH, M. R.; KABOUCH, N. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system. International Journal of Critical Infrastructure Protection, vol. 19, p. 16–31, 2017.
22. MARTIN, J. L.; MULGREW, B. Analysis of the theoretical radar return signal form aircraft propeller blades. IEEE International Conference on Radar, p. 569–572, 1990.
23. MISARIDIS, T. X.; GAMMELMARK, K. L.; JØRGENSEN, C. H.; LINDBERG, N.; THOMSEN, A. H.; PEDERSEN, M. H.; JENSEN, J. A. Potential of coded excitation in medical ultrasound imaging. Ultrasonics, vol. 38, no. 1, p. 183–189, 2000.
24. MOSLY, I. Applications and issues of unmanned aerial systems in the construction industry. International Journal of Construction Engineering and Management, p. 235–239, Jun 2017.