Revista de Ciencias Tecnológicas (RECIT). Universidad Autónoma de Baja California ISSN 2594-1925
Volumen 9 (2): e444. Abril-Junio, 2026. https://doi.org/10.37636/recit.v9n2e444

Review article

Wireless attacks against commercial drones: a systematic mapping study

Ataques inalámbricos contra drones comerciales: un estudio de mapeo sistemático

Brayan Pajuelo -Martin[1], William-Rogelio Marchand-Niño[2]

[1] Universidad de Buenos Aires. Viamonte 430, Ciudad Autónoma de Buenos Aires, Argentina
[2]Universidad Nacional Agraria de la Selva. Carretera Central km. 1.21; Tingo María, Huánuco, Perú

Corresponding author: William-Rogelio Marchand-Niño. Universidad Nacional Agraria de la Selva. william.marchand@unas.edu.pe. ORCID: 0000-0003-2650-4226.

Received: March 1st, 2026 **Accepted:** June 4th, 2026 **Published:** June 12, 2026

Abstract. - *This study compiles wireless cyberattacks carried out experimentally against drones. It focuses on three areas of analysis: first, the types of attacks; second, their vulnerabilities; and finally, the proposed mitigation measures. The scope is limited to studies conducted between 2020 and 2024. Following the methodology, a search query was applied to the Scopus and IEEE Xplore databases. An initial search yielded 6,860 articles, and after applying our inclusion and exclusion criteria, 28 articles were selected, which guided the entire analysis of this research. The most common attacks found were spoofing and jamming. These attacks exploit the reliance on the Global Navigation Satellite System (GNSS) and, furthermore, the lack of a robust authentication system. Among the vulnerabilities identified are the absence of an intrusion detection system (IDS) as well as weaknesses in encryption. The literature proposed mitigation measures such as the use of anti-interference techniques (DSSS and FHSS), cross-validation of signals, IDS, and strong authentication. It was concluded that strict regulatory policies are needed to improve cybersecurity in drones. These types of attacks must also be validated on high-end drones.*

Keywords: Wireless attacks; Drones; Vulnerabilities; Mitigation; Cybersecurity; Systematic mapping.

Resumen. – *El presente trabajo recopila los ciberataques inalámbricos ejecutados de forma experimental en contra de drones. Se centró en tres puntos del análisis, comenzando por los tipos de ataque, seguido de sus vulnerabilidades y finalizando con las medidas de mitigación propuestas. Delimitándose a estudios que van del 2020 al 2024. Siguiendo la metodología se aplicó la cadena de búsqueda en las bases de datos de Scopus y IEEE Xplore. En un primer barrido se obtuvieron 6,860 artículos, y después de aplicar nuestros criterios de inclusión y exclusión se seleccionaron 28 artículos, que guiaron todo el análisis de la presente investigación. Los ataques más comunes que se encontraron fueron el spoofing y jamming. Estos ataques aprovechan la dependencia de la Señal Global de Navegación por Satélite (GNSS), y además, la falta de un sistema de autenticación robusto. Dentro de las vulnerabilidades encontradas está la ausencia de un sistema de detección de intrusiones (IDS) como también debilidades en la encriptación. En la literatura se propusieron medidas de mitigación como el uso de técnicas de anti-interferencias (DSSS y FHSS), validación cruzada de señales, IDS, y contar con autenticación fuerte. Se concluyó que hace falta utilizar políticas de regulación estrictas que mejoren la ciberseguridad en drones. También se deben validar estos tipos de ataques en drones de alta gama.*

Palabras clave: Ataques inalámbricos; Drones; Vulnerabilidades; Mitigación; Ciberseguridad; Mapeo sistemático.

1. Introduction

The growing adoption of commercial drones across various industries including surveillance, transportation, aerial photography, and others has expanded the scope of risks in airspace [1, 2]. The main issue addressed in this study is the rise in wireless attacks against drones, as they have become a product relied upon by multiple industries, used for work, recreation, research, or even in warfare. Some studies have found that the specific characteristics of different models of unmanned aerial vehicles (UAVs) have introduced new threats. Among these are autonomous functionalities, which may contain vulnerabilities in communication channels. This can allow vulnerabilities to be exploited through wireless attacks such as GPS (Global Positioning System) spoofing, jamming, injection of false data, and attacks on data integrity [3].

The widespread adoption of drones across multiple sectors increases the level of risk they pose; for example, they can compromise drone operations as well as data privacy. Therefore, as their use increases, safeguards must also be strengthened to mitigate the risks associated with the adoption of UAVs [4].

One innovative aspect that cuts across all sectors is Artificial Intelligence (AI), which is emerging as a promising option for protecting UAVs. This technology focuses on the drone system and its control, as well as on managing communications and analyzing the data it contains. It is becoming a solution worth considering for protecting drones. However, its real-world application may face some limitations, as it is not yet a mature solution [5]. Furthermore, if we take it a step further and integrate the use of AI with technologies such as blockchain, which operate on the basis of decentralized architectures, this will reinforce mitigation against these types of attacks through multiple layers. However, even with all this, limitations remain, such as the management of available energy resources. These are among the main vulnerabilities in the security systems of current drones [6].

On the other hand, it is well known that we are seeing a growing trend in the use of the Internet of Things (IoT). This growth increases our cybersecurity risks. This is because, when we look at it specifically particularly when working with the Internet of Drones (IoD) we encounter a critical issue, such as communication authentication. Data privacy is a key issue when we want to ensure confidentiality; data is compromised when exposed to jamming, GPS spoofing, and data injection. Furthermore, the industry is exploring emerging technologies applied to drone cybersecurity, such as Q-learning and blockchain. These aim to provide new protection alternatives, but their implementation in a real-world environment presents various challenges [4, 7, 8].

This research is based on a systematic review, limited in scope to common attacks, their vulnerabilities, and the mitigation strategies proposed in the literature. The objective is to provide an overview of the current state of drone security and to offer readers guidance for future research. Moving on to the structure of the study. Section 2 describes our methodology, focusing on a systematic mapping that includes the application of search strategies and selection criteria. Section 3 presents our synthesis of the findings. These detail the results and answers to the research questions. Among these are the types of attacks identified, the vulnerabilities exploited, and the mitigation measures proposed in the literature. Section 4 analyzes the results to identify key findings. Finally, Section 5 presents the conclusions and suggests topics for future research.

ISSN: 2594-1925

2. Methodology

This research follows the methodological guidelines for systematic mapping and focuses on the field of computer science [9]. The research follows a structured process consisting of four stages: protocol development, technical implementation, systematic analysis, and formulation of answers to the research questions. In the first phase, which guides the entire study, the research questions were determined, aiming to identify the most common types of wireless attacks, the vulnerabilities they exploit, and the mitigation strategies proposed in the literature. Also in this phase, the search strategy was defined, including the selection of databases to consult, the keywords in the search string, the time frame, and the consolidation of inclusion and exclusion criteria, which will be filtered step by step.

The next phase, implementation, began with the extraction of primary research studies using the search string defined in the previous phase. A study screening process was conducted using progressive filtering. First, titles and abstracts were reviewed. Subsequently, the full texts were analyzed, applying the inclusion and exclusion criteria, to identify primary research containing information relevant to addressing the research questions posed. Finally, in the final phase, the collected information was organized under a specific classification scheme (types of attacks, vulnerabilities, and mitigation measures), thereby enabling us to answer the research questions that guided this study:

- RQ1: What are the most common types of attacks against drones?
- RQ2: What vulnerabilities are exploited in these attacks?
- RQ3: What mitigation measures have been proposed in the literature?

The search string established is as follows:
("wireless attacks" OR "wireless intrusion" OR "wireless cyber attack " OR "wireless threat" OR "wireless vulnerability" OR "wireless security" OR "wireless hacking" OR "wireless interception" OR "radio frequency attacks" OR "rf attack" OR jamming OR spoofing OR " gps spoofing" OR "data injection" OR deauthentication) AND (drones OR "unmanned aerial vehicles" OR uav OR "autonomous vehicles" OR "unmanned aerial systems" OR uas OR "unmanned aircraft")

To ensure the quality of the selected studies, the search was conducted in the Scopus and IEEE Xplore databases. These databases were chosen due to their leading position in technologies such as UAVs, wireless communications, and cybersecurity. Both Scopus and IEEE Xplore are top-tier sources for indexing peer-reviewed research. This choice guarantees that the studies selected through the inclusion and exclusion criteria are of the highest quality for this type of research.

The study period for published research is limited to 2020–2024. This five-year period reflects the growth in the use of drones for civilian applications during that time. This growth has led to an increase in attack vectors and vulnerabilities in recent years. We believe that mitigation strategies documented before this period may lack the necessary effectiveness to neutralize current emerging threats. Finally, it is worth noting that the data collection and literature review phase was carried out in January 2025.
The inclusion and exclusion criteria are detailed in Table 1.

ISSN: 2594-1925

Table 1. Inclusion and exclusion criteria.

ID	Type	Description
CI1	Language	Study published in English.
CI2	Temporality	The document was published between 2020 and 2024 to ensure that information on wireless attacks on commercial drones is relevant and up to date, as new vulnerabilities and attack methods have emerged during this period.
CI3	Type of study	Primary research published in academic journals or conference proceedings related to cybersecurity, drone vulnerabilities, and wireless attacks.
CI4	Relevance	Document on wireless attacks on commercial drones or security vulnerabilities in drone systems. This includes attacks such as jamming, spoofing, data injection, radio frequency (RF) attacks, among others.
CE1	Language	Document that is not written in English
CE2	Temporality	Document outside the selected year range (2020–2024)
CE3	Duplicity	Duplicate documents
CE4	Type of study	Document that is not primary or published in journals or conferences (reviews, books, book chapters, and letters to the editor)
CE5	Relevance	Document that does not cover at least one of the research questions.

A total of 6,860 articles were retrieved during the search. After applying the inclusion and exclusion criteria, 28 articles were selected for analysis and responses to the research questions. The details of this process are summarized in Figure 1.

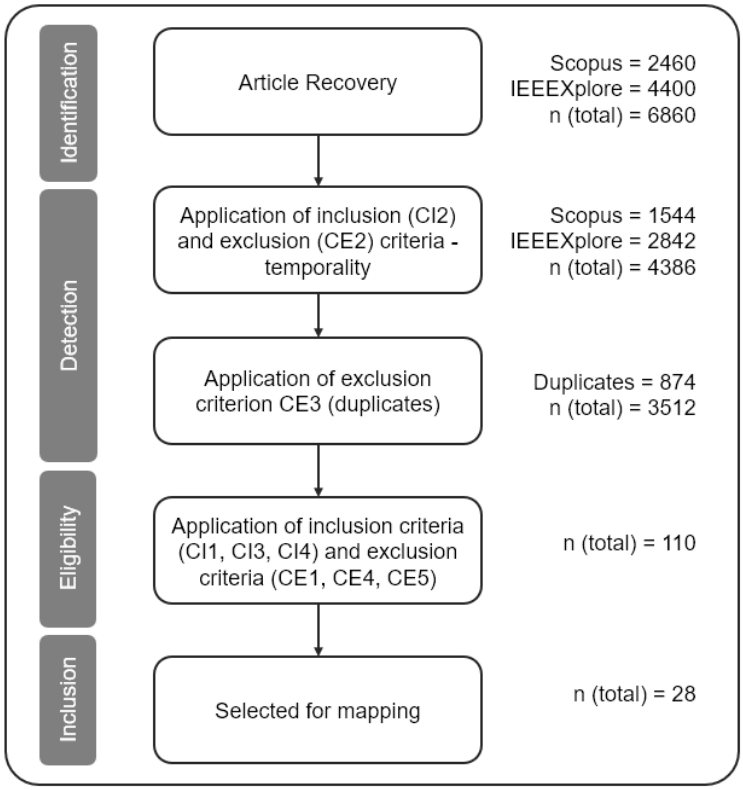

Figure 1. Diagram of the document selection process.

ISSN: 2594-1925

3. Results

3.1 Answering research questions

3.1.1 RQ1: What are the most common types of attacks against drones?

The nine wireless attacks found in the primary research literature were categorized. These attacks focused on commercial drones. The most frequently identified attack types in the literature were spoofing and jamming. However, in addition to identifying the frequency of each attack type, it is relevant to analyze the conditions necessary for a wireless cyberattack to be successful. Another key point is the sophistication that cyber attackers develop to achieve their objective, as this allows us to understand the problem and, in turn, provide mitigation solutions.

Table 2 summarizes the types of wireless attacks and their frequency.

Table 2. Frequency of wireless attack types identified in the selected studies.

Attack Type	Number of Studies	Percentage (%)
Spoofing	15	53.57%
Jamming	12	42.86%
Deauthentication	4	14.29%
Hijacking	3	10.71%
False Data Injection	1	3.57%
Man-in-the-Middle	1	3.57%
Replay Attacks	1	3.57%
IMU Spoofing	1	3.57%

The study identified a frequency of 16 investigations of the spoofing attack type. This is due to our reliance on GNSS signals without any validation to ensure the authenticity of the received data [10–24]. One of the inclusion criteria was that the studies had to be primary and that the demonstrated attacks had to have been carried out in simulated environments and field tests. The analyzed studies used software-defined radios (SDRs), such as the HackRF-One or the BladeRF X40. The results showed that drones can be diverted to unauthorized areas, such as airports [20], or even crashed due to altitude manipulation [12]. Although some high-end models, such as the DJI Mavic 2 Pro, have demonstrated resistance to asynchronous spoofing, most lack effective defenses.

Jamming attacks, which were mentioned in 12 studies, directly affect the control, navigation (GPS), video, and telemetry channels [17, 25–31]. The use of jamming has been particularly problematic in scenarios such as the protection of critical infrastructure. It has been shown that drones can be completely disabled by frequency sweeps (sweep jamming) or high-power microwave pulses (EMP) [10]. Effective attacks were also reported at distances of up to 150 m and heights of 350 m [29].

Wi-Fi deauthentication attacks have been particularly effective against low-end commercial drones using insecure IEEE 802.11 networks [32–35]. These attacks allow a drone to be disconnected from its legitimate controller, thereby facilitating hijacking attacks or access to private data [34]. They have been

ISSN: 2594-1925

successfully executed with available tools such as aircrack-ng, ESP8266 (NodeMCU), Raspberry Pi, and Wi-Fi Pineapple, enabling them to make accessible threats even for non-specialized attackers [33]. However, these attacks may not be effective for sophisticated or updated drones.

Command hijacking relies on exploiting unauthenticated control protocols [24, 25, 32]. For example, it has been demonstrated that command injections can take control of the Crazyflie drone, even causing it to crash in standalone mode [25].

In emerging but infrequent categories, sophisticated attacks were identified. These include false data injection (FDI), which involves the stealthy manipulation of feedback/control channels in DJI Tello drones through state estimation using Kalman filters [36]. Other attacks include man-in-the-middle (MitM), which enables access to Wi-Fi packets using tools such as Wireshark and command replay [18]. In addition, it was found that IMU (Inertial Measurement Unit) spoofing uses neural networks to generate fake inertial data, allowing these types of attacks to be carried out without triggering alarms [22]. Replay attacks were also identified; this type of attack allows RF signals to be reused in order to perform unauthorized actions on the drone [37].

All of this creates a need to develop robust security measures, authentication standards, and encryption protocols for UAVs. Approximately 89.3% of the analyzed studies were conducted in real-world environments. The remaining 10.7% combined simulation environments with field testing. The tools used in these scenarios were Gazebo or PX4 SITL.

3.1.2 RQ2: What vulnerabilities are exploited in these attacks?

Eight vulnerabilities in commercial drones were identified. These vulnerabilities have been exploited in real-world experimental environments, controlled laboratories, and hybrid scenarios, impacting sectors such as critical infrastructure, urban surveillance, education, and entertainment. A key point is that all reviewed studies included experimental validation, ensuring high-quality research. The documented attacks were carried out using real hardware from brands such as DJI, Tello, Holy Stone, SkyViper, and Crazyflie.

Table 3 summarizes the identified vulnerabilities along with their frequency.

Table 3. Frequency of vulnerabilities exploited in wireless attacks against drones

Vulnerability	Number of Studies	Percentage (%)
Lack of intrusion detection (IDS)	28	**100.00%**
Weak authentication mechanisms	22	**78.57%**
Lack of strong encryption	20	**71.43%**
Overreliance on external data	19	**67.86%**
Vulnerable Wi-Fi protocols	16	**57.14%**
Reliance on insecure GNSS signals	14	**50.00%**
Electromagnetic interference exposure	12	**42.86%**
MAC address exposure	5	**17.86%**

ISSN: 2594-1925

- *Reliance on unreliable GPS/GNSS signals.* Many drones rely solely on open GNSS signals, which are not authenticated. This vulnerability makes them susceptible to spoofing and jamming, which can alter their flight path or even force them to land. For example, the DJI Phantom 4 model has been compromised, despite being one of the most widely sold models [10, 20].

- *Excessive reliance on external data.* This is another vulnerability identified in the studies reviewed, stemming from the acceptance of data from GNSS sensors, IMUs, or Wi-Fi links without cross-validation. This allows tampered data to influence drone control. This vulnerability is exploited in spoofing and command injection attacks; for example, the drone compromised in this type of attack was the DJI Tello EDU model [36].

- *Lack of intrusion detection.* For this vulnerability, the drones lacked a monitoring system. Since constant monitoring enables the detection of malicious activities, this allows replay attacks or hijackings to be carried out undetected [22, 37]. This vulnerability was identified in all the studies reviewed and is considered a critical risk factor.

- *Weak authentication mechanisms.* This vulnerability stems from the lack of strong authentication in the control and navigation channel. Without a robust authentication system, the system is susceptible to deauthentication or hijacking attacks on drones. An attacker with basic knowledge of aircrack-ng can compromise the communication between the drone and its remote control. Studies highlight the need to implement identity checks or bidirectional authentication [18, 32].

- *Wi-Fi Protocols.* The vulnerability arises because the Wi-Fi protocol, specifically 802.11b/g/n, is still used for communication between the drone and its remote control. Since the drone relies on Wi-Fi, cyber attackers can execute attacks using common wireless cards without needing specialized hardware. This vulnerability results in a disconnection, which is critical for UAVs. Several studies have shown that drones such as the DJI Mavic Air and DJI Tello are vulnerable to these attacks. However, other models, such as the Yuneec H520E, have also been shown to be resistant to these types of attacks, as they incorporate MAC address hiding and frequency hopping [32, 34, 35].

- *Insufficient or absent encryption protocols.* This vulnerability was identified in the communication channel between the drone and its remote control. Since many drones transmit their data using outdated algorithms or even in plain text, this poses a critical threat to data confidentiality, allowing an attacker to intercept and modify information. That is why the lack of robust protocols such as TLS or WPA3 compromises drone security. For example, the use of Wireshark has made it possible to intercept commands or multimedia files [34].

- *Exposure of the MAC address.* Exposing the MAC address allows an attacker to carry out a targeted attack, since there are multiple devices on a wireless network. This is why, in the initial phase of an attack, the attacker seeks to identify the MAC address of the target they wish to attack, in order to subsequently carry out attacks such as deauthentication or control hijacking. This is in contrast to using proprietary links such as OcuSync or Lightbridge, which are more difficult to detect [32, 35].

ISSN: 2594-1925

- *Intense electromagnetic interference.* This vulnerability stems from a lack of protection against high-energy disturbances. This type of attack can result in a complete loss of control, navigation failure, or structural damage to the drone. The studies analyzed have documented that spectral noise and electromagnetic pulses (EMP) affect devices such as the DJI Phantom 4 Pro and the Mavic Air, due to their high power and electromagnetic intensity [26, 29].

3.1.3 RQ3: What mitigation measures have been proposed in the literature?

It was noted that not all of the studies analyzed proposed mitigation measures for the attacks. However, some studies not only demonstrated how the attacks were carried out but also proposed defensive strategies to strengthen drone security against threats such as jamming, spoofing, hijacking, and deauthentication.

Table 4 summarizes the identified mitigation measures, along with their frequency of occurrence.

Table 4. Mitigation measures against wireless attacks on drones.

Mitigation Measure	Number of Studies	Percentage (%)
Anti-jamming techniques	3	10.71%
Strong authentication mechanisms	6	21.43%
Data encryption (communication/storage)	5	17.86%
Safe mode activation	1	3.57%
Anti-replay mechanisms	1	3.57%
IDS / Firewall systems	3	10.71%
Robust communication protocols	4	14.29%
GNSS cross-validation	2	7.14%
Regulatory policies	1	3.57%
Anomaly detection (AI/Kalman)	3	10.71%

- *Anti-jamming techniques.* This mitigation measure was proposed in three studies, which include the use of techniques such as FHSS, DSSS, and MIMO (Multiple-Input Multiple-Output) as defenses against electromagnetic interference [25, 29, 30].

These techniques aim to prevent communication from being interrupted. This is because they allow for automatic channel hopping when a channel is compromised. Alternatively, the electromagnetic spectrum can be diversified. The Crazyflie 2.1 drone was used as an example, and it was observed that Gaussian noise interference attacks [25] cause the drone to crash. This is because this model does not include a return-to-home function when exposed to these types of attacks that cut off communication.

This led to the proposal of DSSS and FHSS, particularly for these drone models. However, for low-cost drones, this leads to limitations due to their inexpensive hardware architecture. Another significant limitation is ensuring stable power consumption when attempting to implement these defenses in a real-

ISSN: 2594-1925

world environment. For example, a study on the DJI Mavic Air demonstrated that Wi-Fi-only communications are vulnerable. Meanwhile, drones using FHSS or encrypted links exhibit greater resilience [29].

- *Strong authentication in communication and sensors.* A lack of authentication has been identified as the leading cause of successful attacks. The Crazyflie CRTP protocol allows unverified command injections. The incorporation of cryptographic authentication along with safe modes against loss of control has been proposed [25]. Drones, such as the DJI Tello EDU and Mavic Air, which operate over Wi–Fi without authentication, are vulnerable to deauthentication and takeovers. The implementation of WPA2-Enterprise, IEEE 802.11w, 802.1X, and management-frame protection (MFP) has been recommended. It has been suggested that GPS signals be validated during navigation through cross-authentication or session tokens to avoid spoofing [18, 20, 25, 32, 34, 37].

- *Strong encryption of data in transit and storage.* Five studies have shown that many drones transmit commands and data in plain text, allowing for spoofing and replay attacks. For example, DJI Tello EDU accepts critical commands without validation. End-to-end encryption was proposed for commands and telemetry. In addition, storage flaws have been detected, such as in Mavic Air, which allows access to photos and videos without credentials following a deauthentication attack. Mobile traffic redirection using fake stations has also been reported. Standards such as AES, TLS, and WPA3 are recommended to protect both communication and persistent data [18, 20, 32, 34, 37].

- *Activation of safe modes in case of communication loss.* The Crazyflie 2.1 drone can experience this type of failure when in autonomous deployment mode. A "safe mode" is proposed that includes various safety features such as emergency landing, return to home (RTH), and transmission of GPS coordinates. Safe mode is a mitigation measure because it does not require complex mechanisms. This mode is important for drone safety, since a loss of communication in UAVs can cause the drone to free fall [25].

- *Anti-replay mechanisms.* This type of attack, found in the literature, is simply based on capturing and then illegitimately retransmitting signals. For an attacker to set up the attack scenario, they need a System-on-a-Drone (SDR). One of the most widely used SDRs is HackRF One. This tool records the communication flow from a remote control to a drone, allowing the execution of commands such as takeoff and shutdown without breaking the communication encryption. The attack relies on storing instructions for later replication. For example, the 4DRC-4DV2 drone lacked a session validation mechanism. As a mechanism to counter replay attacks, the literature proposed the development of dynamic timestamps, unique nonces per session, and context validation to validate the authenticity of messages. This mitigation measure could block replay attacks without robust encryption, thus promoting cybersecurity in low-cost UAVs. [37].

- *Intrusion detection systems or firewalls*. Three studies proposed the development of IDSs to detect attacks, such as jamming, spoofing, or hijacking. Although complete systems have not yet been implemented, their importance has been recognized. IDSs are suggested for drones or control stations to identify malicious traffic, although warnings are provided regarding the power

ISSN: 2594-1925

consumption and delays that an IDS can introduce [25]. Defending against deauthentication attacks [32] and monitoring of deficiencies that enable the execution of malicious commands [18] have been emphasized.

- *More Robust Communication Protocols.* Several studies recommend adopting modern protocols, such as Wi-Fi 802.11 ac/ax, encrypted FHSS, and IEEE 802.11w, to mitigate wireless attacks. Drones using standard Wi-Fi (802.11b/g/n) are vulnerable to deauthentication, spoofing, and interference. The Yuneec H520E exhibited greater resilience owing to MAC hiding and dual-frequency operations. They proposed migrating to more secure protocols and proprietary links using better encryption algorithms. The use of FHSS and dynamic MAC hiding significantly reduced the attack surface[29, 30, 32, 34].

- *Cross-validation of GNSS signals.* The exclusive reliance on open GNSS signals, such as GPS L1, represents a critical vulnerability to spoofing. In light of these vulnerabilities, a proposed mitigation measure involves validating GPS coordinates by cross-referencing them with the location of the mobile base station connected via SIM. This cross-validation serves as a double-check, as it detects inconsistencies in the received data. For example, when an attacker sends signals with false GPS coordinates in an attempt to trick the drone into moving to a false location. However, performing the second validation using cellular geolocation detects the attempted GPS spoofing attack. Additionally, among the mitigation measures proposed by these studies is combining GNSS with auxiliary sources such as IMUs, altimeters, and geofences. This combined architecture would improve security without requiring complex hardware [14, 24].

- *Stricter regulatory policies.* In addition to the hardware and software solutions proposed by the studies, cybersecurity regulations or standards for UAVs are also necessary. In this regard, some laws have already increased oversight and proposed penalties for negligence. This is because the use of unencrypted navigation systems, weak protocols, and the lack of regulations in each country constitute a structural vulnerability. Even with the best technology to provide UVA protection, if rules aren't defined from the outset as a regulatory framework for drone construction, the drone industry, in order to maximize sales, may relegate safety to a secondary or even ignored priority [24].

- *Anomaly validators.* For this mitigation measure, we are focusing on the sensors on the drones. An anomaly validation system will detect inconsistencies in the data collected from the sensors. In some cases, AI navigation, Kalman filters, or even cross-validation of information between IMU and GPS data could also be applied. Among the studies analyzed, the use of the IMU to capture the drone's actual state when anomalous conditions arise has been proposed [25].

Among these proposed mitigation measures is the use of neural networks to provide automatic alerts [16]. Furthermore, sensor fusion and extended Kalman filters (EKF) limit attackers' ability to predict behavior, improving spoofing detection without requiring excessive device resources [19].

ISSN: 2594-1925

4. Discussion

In the previous results phase, it was determined that spoofing and jamming are the most common documented wireless attacks. These types of attacks are consistent with the findings of Sarıkaya [3] and Mahalle [8], who, during their research, identified them as potential threats to drone security. The spoofing attack, found in 15 studies that demonstrate its execution, highlights a latent vulnerability. This vulnerability involves attacking a communication channel, specifically the navigation channel, which relies on unauthenticated GNSS signals. An attacker can exploit this vulnerability to manipulate drone instructions.

Jamming, mentioned in 12 of the selected documents, disrupts key communications such as control and navigation by jamming critical frequencies. Although techniques such as FHSS and DSSS provide defense, their application in low-cost drones suffers from technical and economic barriers that require further research to provide viable solutions.

Attacks such as deauthentication of Wi-Fi and hijacking reveal vulnerabilities in standard protocols (IEEE 802.11b/g/n), particularly in low-cost drones. The use of tools such as aircrack-ng and NodeMCU enables their execution, thereby requiring regulations and standards to mitigate these risks.

However, this study identified common vulnerabilities in commercial drones, confirming the persistence of these deficiencies over time, as reported in similar studies. However, it is also evident that few studies have yet explored alternative solutions such as signal cross-validation.

It is noteworthy that some additional vulnerabilities were identified, such as the exposure of MAC addresses in basic and educational models and high susceptibility to electromagnetic interference, which particularly affects low-end drones. Other elements identified in this systematic mapping study are the use of machine and deep learning techniques for attacks, detections, and replay attacks, which should be considered for experimental research to provide effective solutions.

5. Conclusions

The predominant attack types identified were spoofing and jamming, mainly because of the widespread reliance on unauthenticated GNSS signals and the technical ease of executing interference on essential communication channels using accessible platforms, such as SDRs. Other attacks, such as deauthentication and Wi-Fi hijacking, were highly effective against commercial drones using IEEE 802.11 protocols. This demonstrates that low-cost models require much more robust wireless configurations.

Critical vulnerabilities have been identified with increasing frequency, such as the widespread absence of IDS, as well as poor implementation of authentication and encryption. Furthermore, studies have identified a tendency to blindly trust data received via GPS signals. This vulnerability allows cyber attackers to exploit various attacks, disrupting the proper functioning of UAVs.

Regarding mitigation measures proposed in the literature, some studies have addressed strategies to counter the growing threat of attacks, aiming to create a system resilient to constant attacks. These include anti-interference techniques that create protective barriers, such as FHSS, DSSS and MIMO, which

ISSN: 2594-1925

minimize the impact of wireless attacks. The objective of these mitigation measures is to protect communications between the remote controller and the drone. As with other technologies, authentication and encryption play a crucial role in securing a system. Other important considerations include incorporating anti-replay systems, using autonomous systems with their own security layer, and employing timestamps and nonces. Another key point is the adoption of modern protocols for deployment across communication channels. Furthermore, incorporating diverse information sources when receiving instructions is essential; for example, relying not only on a navigation source but also implementing GNSS cross-validation.

No system is completely secure, but the goal is to mitigate any existing risks. Beyond the technical aspects, we must also consider the regulatory environment. Cybersecurity regulations for drones must have at least minimum permissible requirements to help strengthen security from the outset. By combining all aspects that contribute to improved security, such as integrating legislation with the latest technological trends in drone cybersecurity, we can build a safe drone industry for society.

The databases used for this study were Scopus and IEEE Xplore, accessed between 2020 and 2024. Due to this limitation of scope, other databases were excluded. Furthermore, the inclusion criterion for this research focused solely on primary studies with experimental validation. The research employs a systematic mapping methodology; experimental validation was not performed, but rather the analysis focused on existing research and, in particular, the mitigation measures proposed in the literature to help researchers and manufacturers improve UAV safety.

The main contribution of this study is to understand the current state of attacks, vulnerabilities, and proposed mitigation measures against commercial drones. It provides an up-to-date overview by highlighting existing vulnerabilities and outlining emerging trends. The aim is to offer a framework for researchers, manufacturers, and all those working with drones. Future research can begin by applying experimental studies using the attacks described in this study, moving from theory to a real-world environment with practical tests of wireless attacks against some high-end drone models. Finally, it is essential to integrate tools such as AI and implement multi-layered cybersecurity to ensure that UAVs are resilient to zero-day wireless threats.

6. Acknowledgment

The authors would like to thank the Postgraduate Program of the School of Business and Public Administration – Economics of the University of Buenos Aires for partial funding of the specialization project in computer security.

7. Authorship acknowledgment

Brayan Pajuelo-Martin. Conceptualization, methodology, research, formal analysis, writing – revision and editing. *William-Rogelio Marchand-Niño*. Methodology, validation, writing – original draft, writing – revision and editing, supervision.

ISSN: 2594-1925

References

[1] Zapata-Madrigal, G.D. y García Sierra, R., CyberDrone: una plataforma de ciberseguridad para detección de ataques a drones. Ingeniería y Desarrollo, 39 (1), pp. 44-65, 2021. https://doi.org/10.14482/inde.39.1.621.389

[2] Sabuwala, N.A. and Daruwala, R.D., Drones: Architecture, Vulnerabilities, Attacks and Countermeasures. Proceedings of International Conference on Intelligent Vision and Computing (ICIVC 2022), Cham, Springer Nature Switzerland, 2023, pp. 220-232. https://doi.org/10.1007/978-3-031-31164-2_18

[3] Sarıkaya, B.S. and Bahtiyar, Ş., A survey on security of UAV and deep reinforcement learning. Ad Hoc Networks, 164, p. 103642, 2024. https://doi.org/10.1016/j.adhoc.2024.103642

[4] Warkhade, P., Vetal, V., Urmude, A., and Patankar, N.S., A Comprehensive Survey of Security in Industrial Internet of Drones. 2024 MIT Art, Design and Technology School of Computing International Conference (MITADTSoCiCon), 2024. pp. 1-6. http://doi.org/10.1109/MITADTSoCiCon60330.2024.10575658

[5] Tlili, F., Ayed, S., and Chaari Fourati, L., Advancing UAV security with artificial intelligence: A comprehensive survey of techniques and future directions. Internet of Things, 27, p. 101281, 2024. http://doi.org/10.1016/j.iot.2024.101281

[6] Khan, R., Mehmood, A., Maple, C., Curran, K., and Song, H.H., Performance Analysis of Blockchain-Enabled Security and Privacy Algorithms in Connected and Autonomous Vehicles: A Comprehensive Review. IEEE Transactions on Intelligent Transportation Systems, 25 (6), pp. 4773-4784, 2024. http://doi.org/10.1109/TITS.2023.3341358

[7] Madhuvanthi, T. and Revathi, A., A survey on UAV network for secure communication and attack detection: A focus on q-learning, blockchain, IRS, and mmWave technologies. KSII Transactions on Internet and Information Systems, 18 (3), pp. 779-800, 2024. http://doi.org/10.3837/tiis.2024.03.014

[8] Mahalle, A., Khandelwal, S., Dhore, A., Barbudhe, V., and Waghmare, V., Cyber attacks on UAV networks: A comprehensive survey. Review of Computer Engineering Research, 11 (1), pp. 45-57, 2024. http://doi.org/10.18488/76.v11i1.3636

[9] Genero Bocco, M., Piattini Velthuis, M.G., Cruz-Lemus, J.A. y Díaz García, Ó., Métodos de investigación en informática [online], 1st ed., Puertollano (Ciudad Real), España, Grupo Alarcos, 2023. Available at: https://www.amazon.com/-/es/M%C3%89TODOS-INVESTIGACI%C3%93N-EN-INFORM%C3%81TICA-Spanish/dp/B0BXNBJJB6

[10] Zidane, Y., Silva, J.S., and Tavares, G., Jamming and Spoofing Techniques for Drone Neutralization: An Experimental Study. Drones, 8 (12), 2024. http://doi.org/10.3390/drones8120743

ISSN: 2594-1925

[11] Ding, J., Tang, C., Zhang, L., Yue, Z., Liu, Y., and Dan, Z., UAV Communication and Navigation Signals Jamming Methods. IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), 2024. pp. 1-6. http://doi.org/10.1109/ICSPCC62635.2024.10770465

[12] Norhashim, N., Kamal, N.L.M., Sahwee, Z., Shah, S.A., Sathyamoorthy, D., and Alfian, N.A., Effect of Global Navigation Satellite Signal (GNSS) Spoofing on Unmanned Aerial Vehicles (UAVs) via Field Measurement. IEEE 16th Malaysia International Conference on Communication (MICC), 2023. pp. 41-45. http://doi.org/10.1109/MICC59384.2023.10419775

[13] Vaddhiparthy, S.S.S., Sreya, G., Turlapati, P.R., Gangadharan, D., and Kandath, H., A Comprehensive Evaluation on the Impact of Various Spoofing Scenarios on GPS Sensors in a Low-Cost UAV. IEEE 19th International Conference on Automation Science and Engineering (CASE), 2023. pp. 1-6. http://doi.org/10.1109/CASE56687.2023.10260534

[14] Kumar, M.S., Kasbekar, G.S., and Maity, A., Identification of GPS Spoofing as a Drone Cyber-vulnerability and Evaluation of Efficacy of Asynchronous GPS Spoofing. IFAC-PapersOnLine, 55 (22), pp. 394-399, 2022. http://doi.org/10.1016/j.ifacol.2023.03.066

[15] Ferreira, R., Gaspar, J., Sebastião, P., and Souto, N., A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities. Sensors, 22 (4), 2022. http://doi.org/10.3390/s22041487

[16] Basan, E., Makarevich, O., Lapina, M., and Mecella, M., Analysis of the Impact of a GPS Spoofing Attack on a UAV. CEUR Workshop Proceedings, 3094, 2022. pp. 6-16. https://ceur-ws.org/Vol-3094/invited_paper.pdf

[17] Saputro, J.A., Hartadi, E.E., and Syahral, M., Implementation of GPS Attacks on DJI Phantom 3 Standard Drone as a Security Vulnerability Test. 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE), 2020. pp. 95-100. http://doi.org/10.1109/ICITAMEE50454.2020.9398386

[18] Colter, J. et al., Testing the Resiliency of Consumer Off-the-Shelf Drones to a Variety of Cyberattack Methods. IEEE/AIAA 41st Digital Avionics Systems Conference (DASC), 2022. pp. 1-5. http://doi.org/10.1109/DASC55683.2022.9925879

[19] Jung, J.H., Hong, M.Y., Choi, H., and Yoon, J.W., An Analysis of GPS Spoofing Attack and Efficient Approach to Spoofing Detection in PX4. IEEE Access, 12, pp. 46668-46677, 2024. http://doi.org/10.1109/ACCESS.2024.3382543

[20] Margana, B.S., Achanta, D.S., Songala, K.K., and Ammana, S.R., A Simple SDR-based Method to Spoof Low-End GPS-aided Drones for Securing Locations. IEEE International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON), 2021. pp. 32-36. http://doi.org/10.1109/RAAICON54709.2021.9929965

ISSN: 2594-1925

[21] Chen, W., Dong, Y., and Duan, Z., Accurately Redirecting a Malicious Drone. IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), 2022. pp. 827-834. http://doi.org/10.1109/CCNC49033.2022.9700664

[22] Kim, K.H., et al., Insights on Using Deep Learning to Spoof Inertial Measurement Units for Stealthy Attacks on UAVs. IEEE Military Communications Conference (MILCOM), 2022. pp. 1065-1069. http://doi.org/10.1109/MILCOM55135.2022.10017482

[23] Lu, W., Chen, L.W., Xiao, Q.C., and Zhu, C., Software radio-based drone eviction. International Symposium on Computer Technology and Information Science (ISCTIS), 2021. pp. 356-359. http://doi.org/10.1109/ISCTIS51085.2021.00079

[24] Meng, X.-T. and Yu, L.-L., Security Testing of Unmanned Flight System. 7th International Conference on Dependable Systems and Their Applications (DSA), 2020. pp. 468-471. http://doi.org/10.1109/DSA51864.2020.00079

[25] Mekdad, Y., et al., Exploring Jamming and Hijacking Attacks for Micro Aerial Drones. IEEE International Conference on Communications (ICC), 2024. pp. 1939-1944. http://doi.org/10.1109/ICC51166.2024.10623000

[26] Song, R., Zheng, J., Zhang, M., Chen, X., Ma, C., and U, Y.L., Communication Jamming of High-Power Microwave Pulse to UAV. 24th International Vacuum Electronics Conference (IVEC), 2023. pp. 1-2. http://doi.org/10.1109/IVEC56627.2023.10157206

[27] Šimon, O., Götthans, T. and Popela, M., Commercial UAV Jamming Possibilities. 32nd International Conference Radioelektronika (RADIOELEKTRONIKA), 2022. pp. 1-6. http://doi.org/10.1109/RADIOELEKTRONIKA54537.2022.9764904

[28] Caforio, G., Scazzoli, D., Reggiani, L., Magarini, M., Moullec, Y.L., and Alam, M.M., A Configurable Radio Jamming Prototype for Physical Layer Attacks Against Malicious Unmanned Aerial Vehicles. 17th Biennial Baltic Electronics Conference (BEC), 2020. pp. 1-6. http://doi.org/10.1109/BEC49624.2020.9277253

[29] Valderrama, S.L.R. and Aracena, N.A.M.M., Advancements in signal interference systems for targeted disruption of Unmanned Aerial Systems: An integrated approach using SDR and Custom RF Circuitry. IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), 2023. pp. 1-6. http://doi.org/10.1109/CHILECON60335.2023.10418703

[30] Yang, Y., Li, K., Li, J., Zhu, H., Zhang, Y., and Huang, K., Low-Cost, High-Power Jamming Transmitter Based on Magnetron. IEEE Transactions on Electron Devices, 67 (7), pp. 2912-2918, 2020. http://doi.org/10.1109/TED.2020.2992980

ISSN: 2594-1925

[31] Sokolov, V., Skladannyi, P., and Platonenko, A., Video Channel Suppression Method of Unmanned Aerial Vehicles. IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO), 2022. pp. 473-477. http://doi.org/10.1109/ELNANO54667.2022.9927105

[32] Krasnyánszki, B., Brassai, S.T. and Németh, A., UAV weaknesses against deauthentication-based hijacking attacks. IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics (SAMI), 2024. pp. 493-498. http://doi.org/10.1109/SAMI60510.2024.10432859

[33] Kadripathi, K., Ragav, L.Y., Shubha, K., and Chowdary, P.H., De-Authentication Attacks on Rogue UAVs. 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020. pp. 1178-1182. http://doi.org/10.1109/ICISS49785.2020.9316032

[34] Gabrielsson, J., Bugeja, J., and Vogel, B., Hacking a Commercial Drone with Open-Source Software: Exploring Data Privacy Violations. 10th Mediterranean Conference on Embedded Computing (MECO), 2021. pp. 1-5. http://doi.org/10.1109/MECO52532.2021.9460295

[35] Intwala, K., Jatav, S., and Kolhe, K., System to capture WiFi-based Drones using IoT. 6th International Conference on Computing, Communication, Control and Automation (ICCUBEA), 2022. pp. 1-6. http://doi.org/10.1109/ICCUBEA54992.2022.10011038

[36] Mughal, U.A., Ismail, M., and Rizvi, S.A.A., Stealthy False Data Injection Attack on Unmanned Aerial Vehicles with Partial Knowledge. IEEE Conference on Communications and Network Security (CNS), 2023. pp. 1-9. http://doi.org/10.1109/CNS59707.2023.10289001

[37] Omar, T., Duran, T., Al-Tarazi, M., and Ketseoglou, T., SDR-Based Replay Attack for Drone Intervention. Wireless Telecommunications Symposium (WTS), 2024. pp. 1-5. http://doi.org/10.1109/WTS60164.2024.10536682

ISSN: 2594-1925