information

Article

D3S: A Drone Security Scoring System

Bruno Branco [1,2], José Silvestre Silva [1,3,*] and Miguel Correia [2,4]

[1] Military Academy Research Center (CINAMIL), Portuguese Military Academy, 1169-203 Lisbon, Portugal; branco.bjc@academiamilitar.pt
[2] Instituto Superior Técnico, Universidade de Lisboa, 1049-001 Lisbon, Portugal; miguel.p.correia@tecnico.ulisboa.pt
[3] LIBPhys-UC, LA-REAL, Universidade de Coimbra, 3030-709 Coimbra, Portugal
[4] INESC-ID, Rua Alves Redol 9, 1000-029 Lisbon, Portugal
* Correspondence: jose.silva@academiamilitar.pt

Abstract: This paper explores the problem of the security of unmanned aerial vehicles (UAV) by introducing the drone security scoring system (D3S). D3S is a security assessment method that analyzes the security of a UAV model by analyzing its components. Penetration tests were carried out to support D3S and identify potential vulnerabilities in UAVs. Specific cyber-attacks, such as deauthentication, flooding, and replay, were executed in an effort to take full control of the UAVs. Eight different UAV models were assessed using D3S, revealing notable variations in performance, both in control communications and video transmission. Security scores ranging from 0.9 to 4.5 out of 5 were obtained, showing significantly divergent security levels.

Keywords: unmanned aerial vehicle; cybersecurity; cyber-attacks; drone security scoring system; vulnerability; communication; command and control

Citation: Branco, B.; Silva, J.S.; Correia, M. D3S: A Drone Security Scoring System. *Information* **2024**, *15*, 811. https://doi.org/10.3390/info15120811

Academic Editor: Katsuhide Fujita

Received: 27 October 2024
Revised: 11 December 2024
Accepted: 13 December 2024
Published: 17 December 2024

1. Introduction

Over the last two decades, UAVs have been increasingly used in warfare, providing a significant tactical advantage. In 2020, UAVs were used in the Nagorno-Karabakh war [1] and two years later in the Ukraine war [2], where small UAVs were effectively used for surveillance and guiding forces, especially when large UAVs were vulnerable in contested airspace. UAVs have drastically changed the scenario of war, with their systems being used to plan and perform military operations by collecting information and conducting missions in real time [3]. Despite their increasing significance, many UAVs possess critical security vulnerabilities, such as unencrypted communications. These flaws expose UAVs to cyber-attacks that can disrupt their operation or enable attackers to take control of the UAV [4]. Major cyberattacks targeting UAVs include jamming, hijacking, and spoofing of communication channels [5].

Commercial drones have also become increasingly sophisticated, finding applications in areas such as search and rescue missions, goods delivery, security, surveillance, real-time tracking, and wireless communication [6,7]. However, the proliferation and accessibility of UAVs have made them vulnerable to exploitation and abuse by malicious individuals [4,8]. Attacks can serve various purposes, including disconnecting the UAV from the controlling mobile device using tools like aircrack-ng [9] or overloading the UAV system, causing the user to lose control in a denial-of-service (DoS) flooding attack. Additionally, attackers may intercept communications through a man-in-the-middle (MitM) attack, capturing critical data using tools such as arpspoof and ettercap [10]. Furthermore, attackers can gain full control of the UAV by injecting packets after analyzing the communication protocol [11]. They may also exploit open ports, such as the telnet port, to access the drone system, allowing them to monitor crucial information, including flight commands, and ultimately take control [12]. The consequences of these attacks can range from complete control of the UAV by the attacker to the compromise of data integrity, including video and image [13].

This paper introduces the drone security scoring system (D3S), a method to evaluate and assign a security score to UAV models (i.e., to families of identical UAVs). This method comprises groups of metrics, each with a classification to obtain a final score for UAV security. The groups of metrics used are communication protocols for control and video transmission, software aspects, UAV characteristics, and the results of cyber-attacks. D3S is designed for multiple applications, including assessing the security of UAVs, comparing different UAVs, and supporting defensive strategies. By understanding the security level of a UAV, especially in terms of cybersecurity vulnerabilities, it becomes possible to take preventive action if the UAV is used maliciously.

D3S is inspired by two methodologies. First, the common vulnerability scoring system (CVSS) is used to assign scores to individual vulnerabilities in computing systems. These vulnerabilities can be found in different systems, including UAVs. However, unlike CVSS, D3S is not concerned with individual vulnerabilities but with the security of UAVs of a certain model. D3S assigns a score to the security of the entire drone system. Second, D3S is inspired by penetration testing methodologies such as the penetration testing execution standard [14,15]. These methodologies allow for discovering vulnerabilities in systems but do not assess the entire security of the system or assign it a score, as we aim with D3S.

The paper presents not only D3S but also its assessment of eight different commercial drones. This assessment involved systematically applying D3S, which also involved performing penetration tests on the eight UAVs. Security scores ranging from 0.9 to 4.5 out of 5 were obtained using D3S, showing significantly different security levels.

The structure of this paper is organized as follows. Section 2 provides a comprehensive literature review, highlighting previous papers on cyber-attacks targeting UAVs. Section 3 introduces the D3S method and discusses its development. Section 4 presents the experimental results obtained from the UAVs under investigation and the application of the developed system. Section 5 presents a discussion of the use of the D3S method. Lastly, Section 6 summarizes the conclusions and outlines potential future work.

2. Background and Related Work

This section outlines key theoretical concepts and reviews the relevant literature.

2.1. Unmanned Aerial Vehicles

A UAV is an automated or remotely controlled flying device equipped with communication systems, sensors, and occasionally actuators [9]. UAVs can currently be classified in several ways. One approach is based on factors such as weight, wing and rotor type, altitude and range, and their specific applications [16]. Another way of classifying UAVs is based on their command and control methods, which can be divided into the following categories [17]:

- **Remote pilot control**: All decisions for the drone are made by a human operator using a mobile device.
- **Supervised control**: The UAV operates autonomously for certain processes but allows for operator intervention if needed.
- **Autonomous control**: The drone is equipped with all the necessary components for fully autonomous operation.

A UAV is part of a larger system called an unmanned aircraft system (UAS), which includes various components like human operators, command and control, communication links, payloads, and launch/recovery elements [18].

The hardware of the system is centered on a flight controller, which acts as the central processor of the UAV. This controller interprets high-level commands transmitted via radio, with common sensors like inertial measurement units and magnetometers ensuring stability and maneuverability during flight [19]. From a software perspective, UAVs are structured into firmware (instructing the flight controller), middleware (managing communications), and operation systems (processing flight data and controlling operations) [20].

UAV communication can be divided into line-of-sight (LOS) and beyond line-of-sight (BLOS). LOS relies on direct radio waves, while BLOS uses cellular networks (2G to 5G). Protocols governing UAV communications include data packets, encryption methods, and modulation techniques like orthogonal frequency-division multiplexing (OFDM), the direct sequence spread spectrum (DSSS), and the frequency-hopping spread spectrum (FHSS) [21]. Wireless communication technologies such as that of the Institute of Electrical and Electronics Engineers (IEEE) 802.11 protocol are used in UAVs with security protocols like wired equivalent privacy (WEP), Wi-Fi protected access (WPA), WPA2, and WPA3 to protect data transmission [22]. In addition to the IEEE 802.11 protocol, several other protocols are employed in drone communications:

- **Micro Air Vehicle Link (MAVLink)**: This protocol is essential for transmitting telemetry and control data in drones. It has two versions: the first features an 8-byte header with packet loss detection, while the second includes a 14-byte header with added security mechanisms [23].
- **OcuSync**: Developed by Da Jiang Innovations (DJI), OcuSync focuses on improving the security of UAVs, incorporating features to protect against various cyber threats [24].
- **Lightbridge**: This protocol employs both FHSS and DSSS modulation. It supports multiple video and output formats, making it compatible with remote controllers and mobile devices [25].
- **Futaba Advanced Spread Spectrum Technology (FASST)**: Created by Futaba, this protocol operates in the 2.4 GHz band using FHSS and DSSS modulation. It offers various channel selection modes and supports 7, 8, or 14 channels [21].
- **Digital Signal Modulation (DSM)**: The DSM2 version operates in the 2.4 GHz band with DSSS modulation, utilizing DuaLink technology for dual-channel operation. The DSMX version employs both FHSS and DSSS modulation with a unique frequency hopping mechanism [21].
- **Advanced Communication Control Elevated Spread Spectrum (ACCESS)**: This protocol boasts 24 channels, an automatic binding mechanism, and a spectrum analyzer to monitor signal strength, noise, and surrounding frequencies. It also incorporates advanced encryption algorithms [26].
- **Automatic Frequency Hopping Digital System (AFHDS)**: The latest version, AFHDS 3, supports bidirectional data transmission, enhancing security and stability. It features automatic frequency hopping and an authentication mechanism with low power consumption components [27].

In summary, UAV systems rely on a combination of hardware, software, and advanced communication protocols to function effectively, with significant emphasis on securing data transmission and enhancing operational control.

2.2. Cyber-Attacks on UAVs

This section summarizes different attacks reported on UAVs. According to Gran and Mickols [9], a deauthentication attack was successful when the drone was connected to a mobile phone but failed when the controller was used. Similarly, Feng and Tornert [28] found that the remote controller, which operated using the IEEE 802.11w protocol, was resistant to such attacks due to mechanisms like management frame protection. Additionally, Intwala et al. [29] demonstrated that switching frequency channels upon detecting communication disruption is another effective defense, as shown in their evaluation of repeated attacks on the DJI Tello Drone.

In the study by Rubbestad and Söderqvist [10], flooding attacks caused issues like video transmission interruption and loss of drone control. In contrast, Feng and Tornert [28] found that using the Low Orbit Ion Cannon and Netwox tools for a flooding attack on the drone's web server was ineffective, although it did disrupt video transmission. Vasconcelos et al. [30] also tested this type of attack on two drones and noted that the connection between the controllers and the drones was impacted, with one drone experiencing greater

disruption than the other. This discrepancy was attributed to the more robust processor in one of the drones.

Bertoli et al. [31] analyzed the number of packets transmitted between the drone and controller. The results show that the transmission control protocol (TCP) flood had the most significant impact, drastically reducing the number of packets received by the UAV. Despite the difference in packet numbers between the user datagram protocol (UDP) and TCP flood attacks, both were equally effective in disrupting communications.

Karmakar et al. [32] conducted a medium access control (MAC) spoofing attack utilizing Wireshark to capture the MAC address and employing the Oden tool to modify the MAC address within the firmware. This enabled control of the drone by preventing the original controller from reconnecting. Westerlund and Asif [12] used a similar topology but opted not to use the Oden tool. Instead, they created a script to replicate the drone controls based on the captured data.

Slimeni and Dalleji [33] used a software-defined radio (SDR) to develop a system capable of detecting, identifying, and jamming the communications of the Parrot AR drone. Similarly, Mekdad et al. [34] applied the same method to target the crazy real-time protocol of the Crazyflie 2.0 UAV. Saputro et al. [35] conducted a global positioning system (GPS) jamming attack on the DJI Phantom 3 drone. They used GPS-SDR-SIM software to generate a GPS signal, which was converted to an RF signal via an SDR, successfully interrupting the drone's GPS functionality. Rahman et al. [36] conducted a similar jamming attack on a DJI Phantom 4 Pro drone, focusing on determining the maximum effective range of the jamming signal.

2.3. Common Vulnerability Scoring System

The CVSS is used to score vulnerabilities based on their severity, considering exploitability, threat characteristics, and environmental factors. It provides a scale from zero to ten, where ten represents the most severe vulnerabilities [37].

This vulnerability classification model was used as the basis for developing the D3S method. Therefore, its entire construction was developed based on an in-depth analysis of the CVSS, such as the group of metrics and the score that each metric has in each group. Despite that, CVSS and D3S differ in some characteristics since CVSS evaluates vulnerabilities found in systems according to impact, risk, and severity, while D3S assesses the security of a UAV by considering its security characteristics. CVSS version 4.0 uses the following groups of metrics:

- **Base**: Describes the core characteristics of a vulnerability that remain unchanged, focusing on exploitability (e.g., attack vector, complexity) and the impact on confidentiality, integrity, and availability.
- **Threat**: Covers changing aspects of a threat over time, such as current exploit techniques and exploit code availability.
- **Environmental**: Represents the characteristics that are relevant and unique to a user's environment, such as the presence of security protocols. Also, this group has the modified base subgroup, which consists of a new analysis of the base group's metrics, taking into account the user's environment.
- **Supplementary**: This group is optional and describes the extrinsic attributes of a vulnerability in order to better understand the impact of a vulnerability in a unique environment.

3. Drone Security Scoring System

The main goal of D3S is to assess a UAV's security by providing groups of metrics. These metrics are grouped into categories like **communications**, **characteristics**, **cyberattacks**, and **software**, each with subgroups and corresponding scores, as represented in Figure 1.

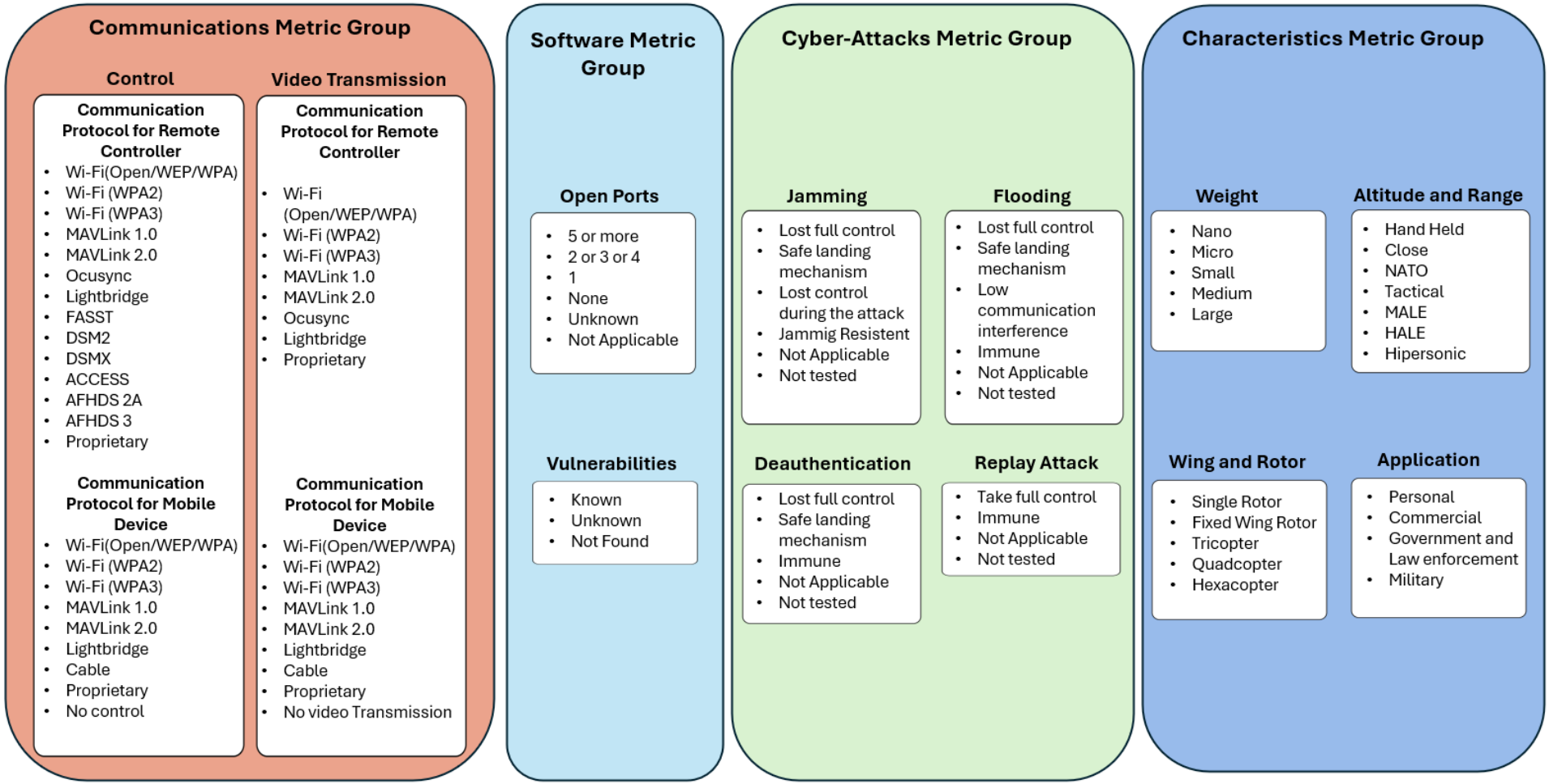

Figure 1. The D3S metric groups.

The construction of D3S was based on CVSS but with a different objective. CVSS aims to evaluate and characterize a software, hardware, or firmware vulnerability found in a system to observe its characteristics in terms of its impact on the target. On the other hand, D3S does not assess a vulnerability but rates the security of a UAV, where the rating indicates the possibility of vulnerabilities being found. Thus, the D3S method is not like CVSS, which is only used to assess vulnerabilities once they have been found.

Therefore, D3S is capable of being used initially, thus obtaining a security rating, which could help discover future vulnerabilities in a drone. It can also be adapted if vulnerabilities are discovered.

The scoring method for D3S is based on the CVSS approach. However, instead of expanding to ten as the CVSS method, the D3S classification only goes up to five. This classification translates into an inversion of the CVSS values, as the highest CVSS value corresponds to a vulnerability with the highest risk, the worst case. As D3S is related to security, the highest value was assigned to the UAV with the highest security. In addition, the final score is obtained from the average of all the metrics selected from the different groups. The metrics can have seven different values, from zero to five, and the - parameter. This parameter means that the metric in question was not performed and, therefore, will not be included in the average score.

3.1. D3S Development

The development of the D3S method consisted of two preliminary versions and then the final version that had already been presented. The preliminary versions are shown in Figures 2 and 3 and include separate groups and subgroups of metrics.

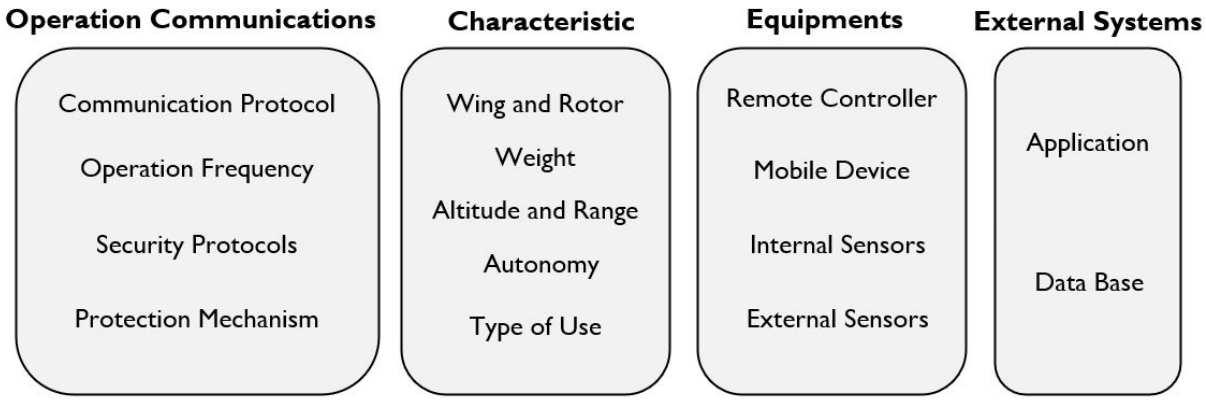

Figure 2. First preliminary version of D3S.

The first preliminary version of this method consisted of identifying the most effective way to categorize UAV components into evaluation groups, resulting in the following groups of metrics: **operation communications**, **characteristics**, **equipments**, and **external systems**. Within the operation communications group, a division of subgroups was made to obtain all the fields of communications security, which are as follows: security protocols; the drone's operating frequencies, because the more frequency bands the drone has, the more robust it is; security protocols; protection mechanisms, such as frequency or frequency band hopping. The problem with this division into these subgroups is that when evaluating communication protocols, it also evaluates protection mechanisms, which makes this evaluation redundant, and the same applies to operation frequencies. The equipment group consists of observing the functionalities of the remote controller, mobile device, and internal and external sensors. External systems to the UAV were also considered, such as the mobile application and the database, which can be internal or in an external system. As far as sensors are concerned, it is a difficult subgroup to obtain a security classification, as their purpose is not security but rather the use of the drone, and external systems do not demonstrate UAV security, which is the priority in this method.

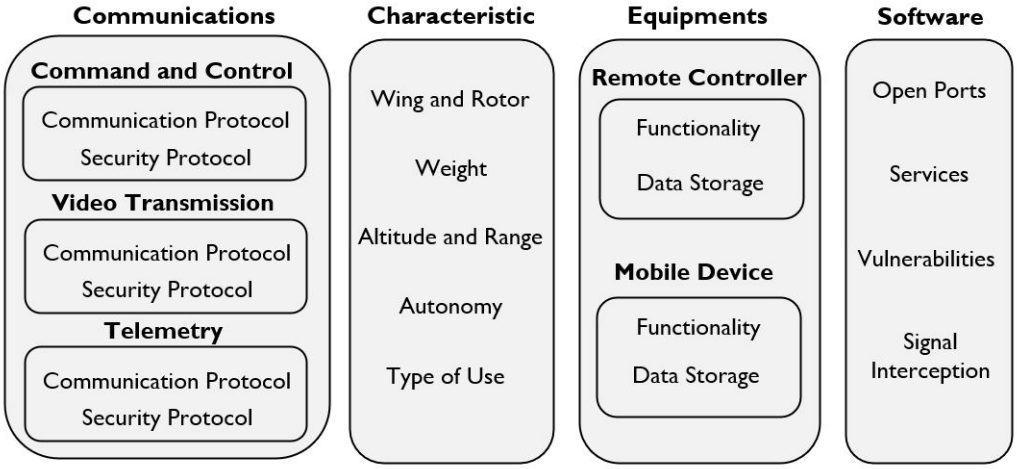

Figure 3. Second preliminary version of D3S.

Thus, a second preliminary version was generated, which resulted in the following groups: **communications**, **characteristics**, **equipments**, and **software**. The **communications** group was divided into command and control, video transmission, and telemetry data. This division of three subgroups was intended to obtain the best possible division of communication channels between the remote controller/mobile device and the drone. However, the communication protocols used for command and control and telemetry data are identical to the UAVs analyzed, so these two subgroups were merged into the control subgroup.

The **equipments** group includes the remote controller and mobile device divisions. The purpose of this group is to determine the various functionalities that a remote controller or mobile device can have. However, **equipments** group is not part of the D3S because it does not assess the security of the drone but rather the impact it may have on the UAV devices.

The **software** group was created to achieve potential vulnerabilities that a drone may have, including the following: open ports, which are directly related to the drone's security; the number of existing services, which, in turn, is related to the drone's open ports and is not in the final version of the method; vulnerabilities; signal interception, related to the jamming cyber-attack, and, for this reason, this subgroup was removed and the cyber-attacks group was created. Finally, the **characteristic** group was dimensioned into different drone classification categories. The autonomy subgroup was removed because it was a difficult parameter to compare, and the type of use was replaced by the application subgroup.

3.2. Characteristics

The **characteristics** group serves a purely documentary purpose, which means that it does not involve any classification. The subgroups are weight, wing and rotor, altitude and range, and application. The purpose of this group is to provide a set of basic classifications for a UAV within the D3S framework. This allows for an overview of the fundamental characteristics of a UAV alongside its D3S score, enabling comparisons with the D3S classifications of other UAVs.

3.3. Communications

The **communications** metrics group is divided into two parts: **control** and **video transmission**. In turn, each part has groups of metrics for the **remote controller** and **mobile device**, represented in Tables 1 and 2.

Table 1. Metrics of the control subgroup.

Communications Protocol for Remote Controller	Value	Communications Protocol for Mobile Device	Value
Wi-Fi (Open/WEP/WPA)	0	Wi-Fi (Open/WEP/WPA)	0
Wi-Fi (WPA2)	1	Wi-Fi (WPA2)	1
Wi-Fi (WPA3)	3	Wi-Fi (WPA3)	3
MAVLink 1.0	0	MAVLink 1.0	0
MAVLink 2.0	1	MAVLink 2.0	1
Ocusync	5	Lightbridge	3
Lightbridge	3	Cable	5
FASST	3	Proprietary	2
DSM2	2	No control	5
DSMX	3		
ACCESS	4		
AFHDS 2A	2		
AFHDS 3	2		
Proprietary	2		

Table 2. Metrics of the video transmission subgroup.

Communications Protocol for Remote Controller	Score	Communications Protocol for Mobile Device	Score
Wi-Fi (Open/WEP/WPA)	0	Wi-Fi (Open/WEP/WPA)	0
Wi-Fi (WPA2)	1	Wi-Fi (WPA2)	1
Wi-Fi (WPA3)	3	Wi-Fi (WPA3)	3
Ocusync	5	Lightbridge	3
Lightbridge	3	Cable	5
Proprietary	2	Proprietary	2
No video transmission	5	No video transmission	5

Communication protocols were evaluated based on their security characteristics, modulations, and overall resistance to cyber threats. Each metric contributes to a comprehensive assessment of UAV communication security.

Wi-Fi protocols received varying scores based on their security features. Wi-Fi (Open) received a score of zero due to the absence of security, while Wi-Fi (WEP) and Wi-Fi (WPA) also scored zero because of their vulnerabilities, particularly in terms of cyber-attacks. Wi-Fi (WPA2) received a score of one, while WPA3 was rated three for improved security features, such as a better encryption mechanism and protection against several attacks.

Evaluation of MAVLink protocols revealed that MAVLink 1.0 lacked any security features, resulting in a zero score. In contrast, MAVLink 2.0 incorporated basic security measures, including encryption and authentication, achieving a score of one. OcuSync stands out with a score of five, providing robust protection against various cyber threats, while ACCESS scored four to ensure secure communication with advanced encryption. The remaining protocols were classified by their modulation, mainly because it was one of the few security characteristics found in them. Protocols using a combination of FHSS and DSSS modulation were given a score of three because of their stronger protection against interference attacks. This score was applied to the Lightbridge, FASST, and DSM X protocols. In contrast, the protocols DSM 2 and AFHDS 2A, which use only one modulation, received a score of two. However, the AFHDS 3A protocol, although it has only one modulation, was rated three because it includes a unique frequency-hopping algorithm and an authentication mechanism.

In addition to the protocol metrics, others have been added to provide all possible cases. A metric used in all subgroups is designated as proprietary, with a value of two. This metric is applicable when the protocol used in UAV communications is unknown. A rating of two was deemed the most appropriate on the scale used, as an unknown protocol is more likely to lack robust security features, warranting a low intermediate value. This choice was also influenced by the classifications of all other communication protocol metrics.

Another metric is the cable, which corresponds when the mobile device's communication is not directly to the UAV but to the remote controller via a cable. This gives the UAV one less communication channel, which in turn is attributed to a score of five. From the same perspective and using the same scoring value, UAVs with fewer communication channels were evaluated using the metrics no video transmission and no control.

3.4. Software

The **software** metrics group is divided into two subgroups: **open ports** and **vulnerabilities**, as detailed in Table 3.

Table 3. Metrics of the open ports and vulnerabilities subgroup.

Open Ports	Score	Vulnerabilities	Score
5 or more	0	Known	CVE score
2 or 3 or 4	1	Unknown	2
1	3	Not Found	4
None	5		
Unknown	2		
Not Applicable	-		

The **open ports** subgroup evaluates the number of open ports in a UAV. Additionally, there is an unknown metric, which indicates that the number of open ports is unknown because no tests have been performed. Finally, the not applicable metric is not assigned a score because it represents when the UAV does not use network ports, as certain communication protocols are not IP-based.

The **vulnerabilities** subgroup corresponds to the classification of vulnerabilities according to the common vulnerabilities and exposures (CVE) system, ensuring D3S interoperability. In the known metric, the CVE value is used with a scaled reduction by half and an inverted transformation of the score since a higher score in D3S indicates a greater degree of security. Other metrics in this subgroup include unknown (no vulnerability search performed) and not found (no vulnerabilities detected).

3.5. Cyber-Attacks

The **cyber-attacks** group reflects the several attacks performed on a UAV and the outcomes that determine its security level in the targeted component. All subgroups in this category include two unclassified metrics: Not Applicable, which indicates that the attack could not be executed, and Not Tested, meaning the attack was not attempted.

The **jamming** and **flooding** subgroups (Table 4) share almost the same metrics. These begin with the worst-case scenario, in which the operator loses complete control of the UAV. The next possible outcome is when the UAV has a security mechanism that either initiates a safe landing or stabilizes the UAV in the air. These two outcomes receive the same classification since both provide an intermediate level of security. The highest score is assigned when the UAV is immune or resistant to the attack.

Table 4. Metrics of the jamming and flooding subgroups.

Jamming	Score	Flooding	Score
Lost full control	0	Lost full control	0
Safe landing mechanism	3	Safe landing mechanism	3
Lost control during the attack	3	Communication interference	3
Jamming Resistant	5	Immune	5
Not Applicable	-	Not Applicable	-
Not Tested	-	Not Tested	-

The **deauthentication** and **replay attack** subgroups are represented in Table 5. In the **deauthentication** subgroup, the metrics are similar to those of the previous subgroups, with the exception of low communication interference and lost control during the attack. The **replay attack** subgroup includes two metrics to assess whether the attack was successful or not, with no intermediate outcomes.

Table 5. Metrics of the deauthentication and replay attack subgroup.

Deauthentication	Score	Replay Attack	Score
Lost connection	0	Take full control	0
Safe landing mechanism	3	Immune	5
Immune	5	Not Applicable	-
Not Applicable	-	Not Tested	-
Not Tested	-		

4. Experimental Evaluation

This section presents the data and experimental tests conducted to evaluate the D3S method with a selection of UAVs.

The choice of materials was critical for ensuring accurate data and valid results. This selection covered the operating system, penetration testing tools, antennas, and, most importantly, UAVs. Price was used as a metric to enable the selection of UAVs with possibly different levels of sophistication. The UAVs used are the following: E88 (Figure 4a), JJR/C Elfie+ (Figure 4b), S2S (Figure 4c), ZLL SG108 (Figure 4d), Hubson Zino Mini Pro (Figure 4e), Autel Evo Nano+ (Figure 4f), DJI Mini 3 (Figure 4g), and DJI Mini 3 Pro (Figure 4h).

The specific names of the UAVs and prices are omitted to prevent attributing vulnerabilities to particular brands, which is not the goal of the study. The price is represented on a scale using the euro symbol (€); the more symbols a drone has, the more expensive it is. Also, the UAVs are labeled as UAV A, UAV B, and so on through UAV H, as represented in Table 6.

Kali Linux was chosen as the operating system for conducting penetration testing. The ALFA AC1900 Long Range USB Wireless Adapter was selected for its high-performance capabilities in long-range Wi-Fi connections. It supports dual-band (2.4 GHz/5 GHz), can monitor and inject packets, and is compatible with WEP, WPA, WPA2, and WPA3 security protocols. This adapter works on Windows, macOS, and Linux and provides the necessary range for testing UAVs in flight.

Table 6. Characteristics of the UAVs under study.

UAV	Price	Year of Purchase	Remote Controller Protocol	Mobile Device Protocol	GNSS
A	€	2023	Unknown/Proprietary	Wi-Fi	No
B	€€	2023	Unknown/Proprietary	Wi-Fi	No
C	€€	2024	Unknown/Proprietary	Wi-Fi	Yes
D	€	2016	Unknown/Proprietary	Wi-Fi	No
E	€€€	2024	OcuSync	Do not use	Yes
F	€€€	2024	Unknown/Proprietary	Do not use	Yes
G	€€€	2024	Unknown/Proprietary	Do not use	Yes
H	€€€	2024	OcuSync	Do not use	Yes

(**a**) E88 UAV.

(**b**) JJR/C Elfie+ UAV.

(**c**) S2S UAV.

(**d**) E88 UAV.

(**e**) JJR/C Elfie+ UAV.

(**f**) Autel Evo Nano+ UAV.

(**g**) DJI Mini 3 UAV.

(**h**) DJI Mini 3 Pro UAV.

Figure 4. Photos of the UAVs used.

4.1. Information Gathering

To perform any cyber-attacks on a UAV, it is crucial to understand its system and gather as much information as possible. Several information-gathering tests were performed, including network traffic monitoring and port scanning.

4.1.1. Network Traffic Analysis

To capture packets sent and received by the UAV, the antenna was placed in monitor mode using several commands and tools.

- `iwconfig`: Used to identify which interface the antenna was connected to.
- `sudo iwlist <interface> scan`: Consists of scanning available Wi-Fi networks and revealing details like MAC address, channel, and frequency.

- `sudo airmon-ng check kill`: Executed to stop any processes that might interfere with aircrack-ng tools.
- `sudo airmon-ng start <interface>`: Used to put the antenna into monitor mode.
- `sudo airodump-ng -bssid <bssid> -write <file> <interface>`: Used to capture and monitor packets on the specified network with filters for the channel, MAC address, and file name for saving packets.

Wireshark was employed to analyze these packets in detail, focusing on identifying the ports used by the UAV, the number of bytes in the payloads, and any recurring patterns. Several diagrams were created to visually represent this analysis, with key elements such as payload size, constant values in the payloads, and significant interactions between the UAV and the mobile device.

- **UAV A (Figure 5)**: Port 52612 is likely used for video transmission, as the payload varies between a small number of bytes and 1420 bytes. Port 8800 consistently sends the same payload from another Internet protocol (IP) address on the UAV, possibly to confirm data reception. Port 7099 appears to be related to control commands, with 9-byte commands being sent and confirmed with a specific payload response. Additionally, a periodic "0101" payload seems to keep the communication channel active. However, the purpose of port 7070 could not be determined.

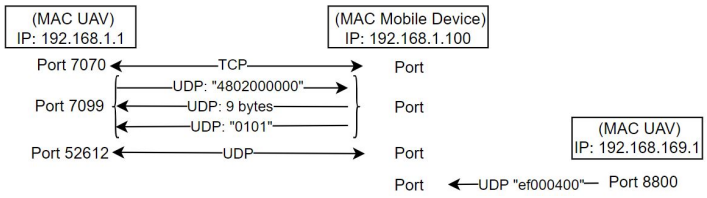

Figure 5. UAV A communication diagram.

- **UAV B (Figure 6)**: Port 1234 likely handles video transmission, with payloads ranging from a few bytes to 1420 bytes sent to the mobile device. Port 8080 receives packets in varying sizes, which could be commands or related to other UAV functions. Meanwhile, port 18881 handles TCP packets associated with a three-way handshake.

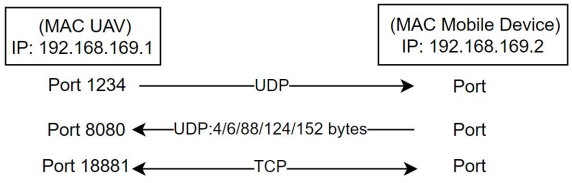

Figure 6. UAV B communication diagram.

- **UAV C (Figure 7)**: Port 19798 exchanges packets between the UAV and mobile device, with consistent 17-18 byte packets sent to the mobile device and 16–21 byte packets returned. A periodic 255-byte packet is sent to the mobile device, although its purpose remains unclear. Video transmission likely occurs over port 554, which in initial packets displays a link to a webpage, possibly used for video streaming.

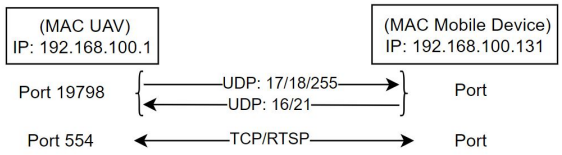

Figure 7. UAV C communication diagram.

- **UAV D (Figure 8)**: Port 8888 appears to be used for video transmission, with packets ranging from small sizes to 1460 bytes being sent to the mobile device, accompa-

nied by acknowledgment packets. Port 8080 sends smaller packets, starting with 1–29 byte payloads, later becoming consistent 11-byte packets, which may be related to flight commands.

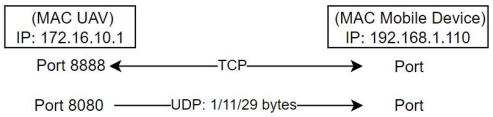

Figure 8. UAV D communication diagram.

Although the ways in which commands are sent and received vary significantly between different UAVs, there are some uncertainties regarding the function of certain ports. Therefore, port scanning was conducted to discover the services running on these ports and investigate others that were not captured.

4.1.2. Port Scanning

Several port scanning tests were conducted using Nmap to gather additional information about the UAVs under study. UAV A had the highest number of open ports, including ports 5007 and 5555, which were not detected during the earlier network traffic analysis. Port 7070, which was initially unclear, was later identified as running the real-time streaming protocol (RTSP) service, which is responsible for controlling video transmission. Most of the identified services did not provide useful information for further attacks, except for UAV D, which had an open telnet service corresponding to the vulnerability CVE-2024-6422.

4.2. Exploitation

This section details the cyber-attacks performed on UAVs, focusing on two types of DoS attacks: deauthentication and flooding, along with a replay attack aimed at gaining control of the UAV. Additionally, a telnet vulnerability was exploited on UAV D, allowing access to its system, which appeared to be based on Linux but had some modified commands. Further exploration could reveal more about its internal workings.

4.2.1. Deauthentication Attack

A deauthentication attack involves sending packets to break the connection between connected devices, such as the connection between the UAV and the controller or a mobile device [12]. The aireplay-ng tool from the aircrack-ng suite was used, and the results can be observed in Table 7.

Table 7. Results of the DoS deauthentication attack on the UAVs under study.

UAV	Result	Observation
A	Successful (lack of authentication)	User lost connection with UAV immediately
B	Successful (lack of authentication)	User lost connection with UAV immediately
C	Successful (lack of authentication)	User lost connection with UAV immediately but made a safe landing
D	Successful (lack of authentication)	User lost connection with UAV immediately

This attack successfully disrupted the connection on all tested UAVs but resulted in different behaviors. UAVs A, B, and D lost video transmission and control, eventually crashing, and only reconnected after the Wi-Fi networks reappeared.

In contrast, UAV C remained stable in the air after losing connection and executed an emergency landing, stopping its propellers and waiting for reconnection, offering better safety for people and surroundings. All UAVs were found to lack proper authentication mechanisms, as the monitored packets revealed an open system for re-establishing connections. The effectiveness of the deauthentication attack was not influenced by the number of packets sent, as even one packet was enough to succeed in each case.

4.2.2. Flooding Attack

A flooding attack overloads a device or communication channel with packets. To assess the robustness of various UAV systems, a DoS flooding attack was conducted using the command `hping3 −V <options> <mode> −p <port> <IP address> -I <interface>`. The −V option enabled verbose mode, providing detailed information on the number of packets sent and received by the target system. The primary attack mode used was `-flood`, which sends the maximum number of packets per second, though other modes with different packet rates were also tested for comparison. The mode option defined the packet protocol, with the default mode for TCP packets and −2 for UDP packets. Additional parameters specified the target port (−p), the UAV's IP address, and the network interface (−I).

The effectiveness of the attack was evaluated on the basis of its impact on the UAV control and communication systems. The results can be observed in Table 8, where a successful attack was marked with a check symbol (✓), while partial successes were observed that caused communication delays and unsuccessful attacks (✗).

Table 8. Results of the DoS flooding attack on the UAVs under study.

UAV		Number of Packets Sent in the DoS Attack			
		–Fast (10 Packets/s)	**75 Packets/s**	**–Faster (100 Packets/s)**	**–Flood**
A	Control	✗	✗	✗	✓
	Video	✗	✗	✗	delay
B	Control	✗	✗	✗	delay
	Video	✗	✗	✗	delay
C	Control	✗	✗	✗	✗
	Video	✗	✗	✗	✗
D	Control	✗	delay	✓	✓
	Video	✗	delay	delay	✓

The attack results showed different levels of impact on different UAVs. UAV C proved to be immune to all forms of DoS flooding attacks. UAV A experienced minor interference in video transmission, but complete control was lost shortly after the attack began. UAV B showed a delay in processing control packets and video transmission, although control of the UAV was not fully compromised. UAV D was the most vulnerable, losing complete control even at lower packet rates.

In conclusion, UAV D exhibited the weakest system in response to overload attacks, while UAVs A and B encountered moderate delays without completely losing control. UAV C remained unaffected by the DoS attacks, demonstrating immunity. The results were consistent across different ports; therefore, detailed outcomes per port are not included. This analysis highlights the varying degrees of vulnerability among different UAVs, with UAV D being the most susceptible and UAV C the most resilient against DoS flooding attacks.

4.2.3. Replay Attack

To gain control of a UAV, captured flight commands from the information gathering phase, which include the payload of the analyzed packets, were used. This makes a thorough communication analysis and port scanning critical to identify the control port. A Python script was used to send packets with specific payloads, enabling a replay attack. The code is divided into three main parts: variable declaration, packet construction, and packet transmission. The variables include the IP and MAC addresses of both the mobile device and the UAV, as well as the port, protocol, interface, and command list. The function builds packets using these variables, and another version of the function excludes MAC addresses to test if the UAV verifies MAC or only IP addresses. The commands used were captured after a deauthentication attack, reflecting critical control phases like takeoff. Each UAV (A, B, C, and D) required a different number of commands, depending on their operational procedures. Some UAVs used a single command for takeoff, while others used a series of commands.

Table 9 outlines the results of these attacks in different scenarios. The first scenario involved connecting the attacker's personal computer (PC) directly to the UAV. This was successful for all UAVs without needing the MAC addresses of the mobile device. The second scenario tested whether the PC could send commands when the UAV was already connected to a mobile device. This was impossible for UAV A, as it allowed only one device to connect at a time. However, UAVs B, C, and D accepted overlapping commands from the PC. For UAVs C and D, the PC had to use the correct MAC address for commands to be accepted. If the MAC address was different from the mobile device's, only the first command was executed before the remaining commands were rejected, indicating a partial MAC address verification.

Table 9. Replay attack results with the different options used.

UAV	Replay Attack Testing Options		
	Only the PC Connected	**PC and Mobile Device Connected**	**Connected PC and a Deauthentication Attack**
A	✓	Impossible (Only One Device)	✓(First the Attack)
B	✓	✓	✓(Continuous attack)
C	✓	✓ (Only with MAC address)	✓(Continuous attack)
D	✓	✓ (Only with MAC address)	✓(Continuous attack)

The third scenario involved a deauthentication attack. For UAV A, the attack forced the mobile device to disconnect, allowing the PC to take over. For UAVs B, C, and D, continuous deauthentication attacks were necessary to maintain control, as these UAVs allowed multiple device connections. The attack disrupted the connection between the UAV and the mobile device, allowing the PC to send commands without interference.

In conclusion, the replay attack demonstrated that it is possible to send commands and control a UAV.

4.3. Experimental D3S Results

After completing the information gathering and exploitation phases, the results from each UAV were analyzed using the D3S method. Table 10 presents the theoretical and experimental scores. The theoretical scores were based on information gathered from the Internet and through regular use of UAVs without performing any cyber-attacks. In contrast, the experimental scores were derived from the information-gathering and

exploitation phases, where actual cyber-attacks were conducted. It is important to note that the **jamming** attack was performed superficially in collaboration with a working group, unlike other attacks.

Table 10. UAV D3S theoretical and experimental scores.

UAV	Theoretical Scores	Experimental Scores
A	1.8	1.3
B	1.8	1.9
C	1.8	2.4
D	1.8	0.9
E	4.4	4.5
F	3.8	4.3
G	3.8	4.0
H	4.4	4.5

Regarding open ports, UAV D had a notable vulnerability: an open port running a Telnet service, which allowed unauthorized access to the UAV's system. The DoS deauthentication attack was successfully executed on all UAVs, with UAV C responding by initiating an emergency landing when it lost connection. This attack was possible due to the use of an open system without any pairing mechanisms for secure communication. The DoS flooding attack was only unsuccessful for UAV C, demonstrating its system's ability to handle and reject large volumes of packets without overloading them. The replay attack allowed the attacker to gain control of the four UAVs on which the attack was performed (UAVs A, B, C, and D). To maintain control and prevent interference from the original user, a deauthentication attack was conducted alongside the replay attack. For UAV A, only a single deauthentication was required since it allowed only one connection at a time. For the other UAVs, continuous deauthentication attacks were necessary to prevent the mobile device from reconnecting and interfering with the attack.

The metrics chosen to evaluate the experimental scores are detailed extensively in Tables 11 and 12. The D3S scores reflect the overall security performance of the UAVs. As the classification increases, the UAVs exhibit stronger security mechanisms, making them progressively less vulnerable to cyber-attacks. This demonstrates the effectiveness of secure communication protocols.

One noteworthy factor is the price of the UAVs, which may be related to their security levels. A comparison of the D3S scores with UAV prices is in Figure 9. It shows that as the price increases, the D3S value also tends to rise. However, it is important to highlight that some UAVs were not subjected to all the cyber-attacks, resulting in unscored metrics. This means that some scores were based on incomplete data, limiting a direct comparison. Despite this, it is possible to observe that the communication protocol values of drones with a higher number of unscored metrics have higher scores, explaining why some cyber-attacks were not performed. Thus, within the UAV groups under study, it is evident that higher prices generally correlate with better security features in drones.

To further analyze the unscored metrics, Figure 10 was created. This chart helped visualize the number of metrics that were not assigned in the D3S classification, particularly for UAVs in the higher D3S group. These UAVs had more unscored metrics because only jamming attacks were performed, whereas other cyber-attacks (e.g., Wi-Fi-based) could not be executed due to their secure communication protocols.

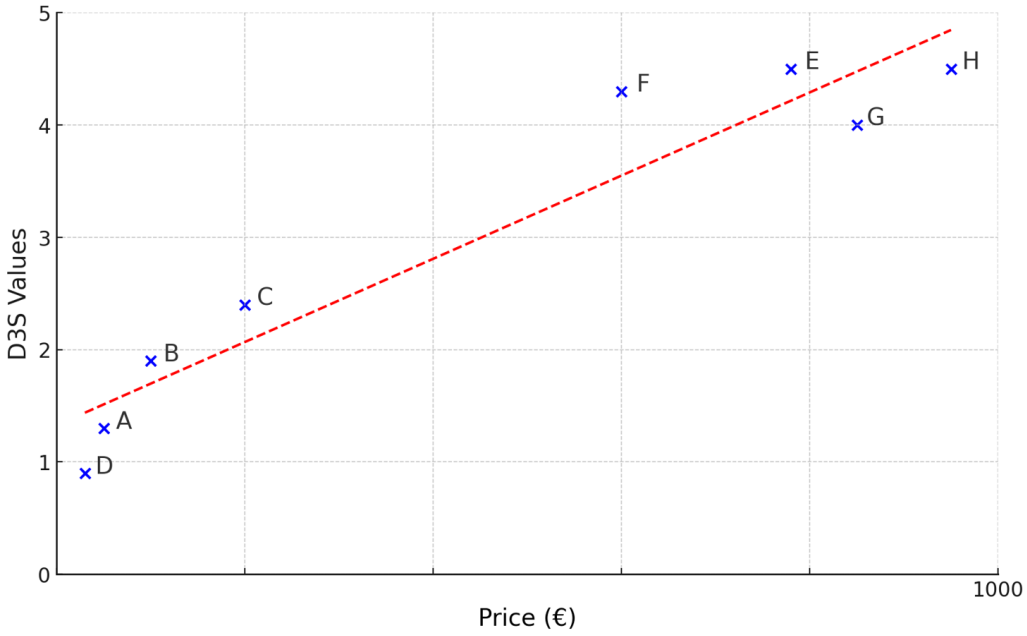

Figure 9. Graph of the price versus experimental D3S scores.

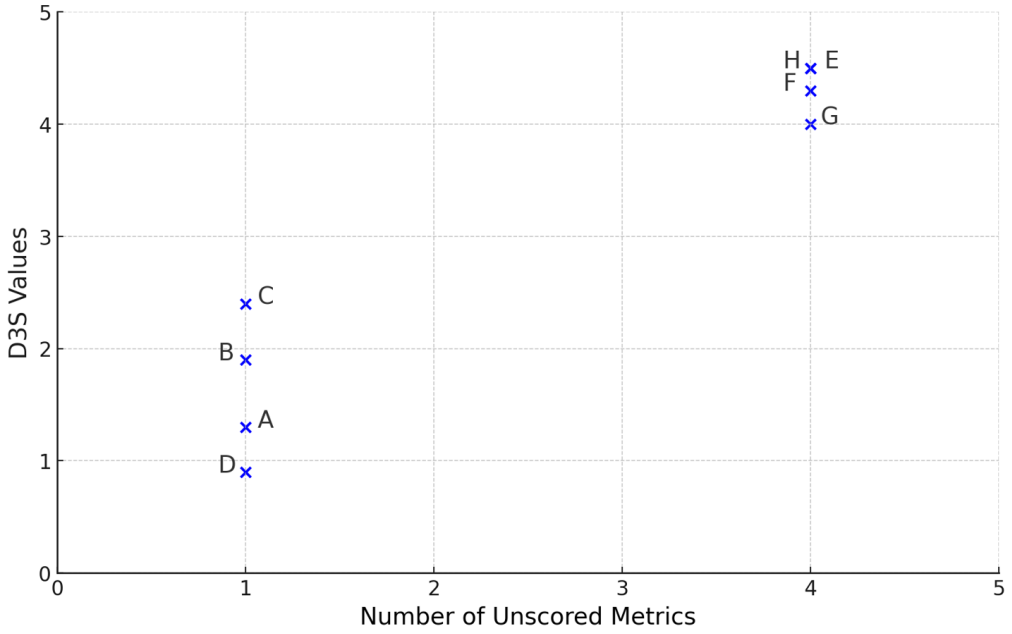

Figure 10. Graph of the number of unscored metrics and the experimental D3S scores.

Despite these unscored metrics, D3S scores still accurately reflect the security of these UAVs, including the use of more secure communication protocols combined with the inability to perform certain cyber-attacks. Although the UAVs with the highest D3S score were less vulnerable to attacks, this does not undermine the accuracy of their scores but rather underscores the effectiveness of their security protocols.

Table 11. First part of the metrics used to calculate the UAV security scores with D3S.

Drone Security Scoring System			UAV A	UAV B	UAV C	UAV D
Characteristics		**Weight**	Nano	Nano	Nano	Nano
		Wing and Rotor	Quadcopter	Quadcopter	Quadcopter	Quadcopter
		Altitude and Range	Hand Held	Hand Held	Hand Held	Hand Held
		Application	Personal	Personal	Personal	Personal
Communications	**Control**	**Communication Protocol for Remote Controller**	Proprietary	Proprietary	Proprietary	Proprietary
		Communication Protocol for Mobile Device	Wi-Fi (Open/WEP/WPA)	Wi-Fi (Open/WEP/WPA)	Wi-Fi (Open/WEP/WPA)	Wi-Fi (Open/WEP/WPA)
	Video Transmission	**Communication Protocol for Remote Controller**	No Video Transmission	No Video Transmission	No Video Transmission	No Video Transmission
		Communication Protocol for Mobile Device	Wi-Fi (Open/WEP/WPA)	Wi-Fi (Open/WEP/WPA)	Wi-Fi (Open/WEP/WPA)	Wi-Fi (Open/WEP/WPA)
Software		**Open Ports**	4 Open Ports	1 Open Port	1 Open Port	2 Open Ports
		Vulnerabilities (CVE)	Not found	Not found	Not found	Know
cyber-attacks		**Jamming**	Not tested	Not tested	Not tested	Not tested
		Flooding	Lost full control	Communication interference	Immune	Lost full control
		Deauthentication	Lost connection	Lost connection	Safe landing mechanism	Lost connection
		Replay Attack	Take full control	Take full control	Take full control	Take full control
Final Score			1.3	1.9	2.4	0.9

Table 12. Second part of the metrics used to calculate the UAV security scores with D3S.

Drone Security Scoring System			UAV E	UAV F	UAV G	UAV H
Characteristics		**Weight**	Nano	Nano	Nano	Nano
		Wing and Rotor	Quadcopter	Quadcopter	Quadcopter	Quadcopter
		Altitude and Range	Hand Held	Hand Held	Hand Held	Hand Held
		Application	Personal	Personal	Personal	Personal
Communications	**Control**	**Communication Protocol for Remote Controller**	Ocusync	Proprietary	Proprietary	Ocusync
		Communication Protocol for Mobile Device	No control	Cable	Cable	No control
	Video Transmission	**Communication Protocol for Remote Controller**	Ocusync	No Video Transmission	No Video Transmission	Ocusync
		Communication Protocol for Mobile Device	No Video Transmission	Cable	Cable	No Video Transmission
Software		**Open Ports**	Not Applicable	Not Applicable	Not Applicable	Not Applicable
		Vulnerabilities (CVE)	Not found	Not found	Not found	Not found
Cyber-attacks		**Jamming**	Lost control during the attack	Jamming Resistant	Lost control during the attack	Lost control during the attack
		Flooding (DoS)	Not Applicable	Not Applicable	Not Applicable	Not Applicable
		Deauthentication (DoS)	Not Applicable	Not Applicable	Not Applicable	Not Applicable
		Replay Attack	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Final Score			4.5	4.3	4.0	4.5

5. Discussion

The choice and determination to develop the D3S method was based on the danger that UAVs can pose if used incorrectly. An increasing number of UAVs are being used as a tool for many of society's tasks, which makes it essential to establish their security, as well as for the operator and the environment. Therefore, it is essential to create methods and mechanisms to assess UAV security.

The D3S method was developed to address the reasons outlined above and can be applied in a wide range of scenarios. It can be used as a process to obtain a higher security UAV that is better protected against possible attacks, depending on the score obtained. However, it can also be used to determine how to act against a UAV that is being used maliciously.

Additionally, one of the objectives of the D3S method is to ensure accessibility for anyone, although it was designed primarily for technicians who specialize in the field. For instance, performing cyberattacks is not mandatory when using D3S, as there are metrics available even in their absence, making it flexible in this regard. This adaptability was one of the key criteria we aimed for, ensuring that it is not a classification method exclusively for drone professionals.

6. Conclusions

Malicious use of UAVs poses significant security risks, making it vital to establish mechanisms that protect UAVs from attacks and protect against their improper use. The D3S method was created to provide security scores for UAVs, which helps defense strategies. This paper highlights the complexity of UAVs and the need for in-depth security analysis of their components. The D3S method was developed through a continuous study, with a focus on interoperability with CVE and the selection of comprehensive metrics. The system evaluates software, communication protocols, and defense against cyber-attacks based on a structured process, including information gathering and exploitation phases. From the research, significant security differences were identified between UAVs, particularly in their responses to DoS flooding, deauthentication, and replay attacks. Two distinct groups emerged: those using Wi-Fi communication and those relying solely on remote controllers. The D3S ratings reflected these differences, and a clear correlation was observed between the price of the UAV and the security level. The work successfully implemented a UAV security classification method, evaluating protocols, software, and cyber-attacks. It also demonstrated strong performance in the information-gathering and exploitation phases, achieving key objectives such as interfering with UAV communications and gaining full control of the UAV.

In the course of developing the D3S method and using it, several limitations were encountered. Among these was the establishment of scores between the different communication protocols since a lot of their information is not published to the public, making it difficult to classify them. Another limitation is that almost all the cyber-attacks performed in this paper are for Wi-Fi communications, which are inefficient if the user employs a remote controller, as the majority do not rely on this type of communication.

The D3S method was built to be applied to UAVs but can be adapted to other systems, such as unmanned land and sea vehicles. This involves changing the communication protocols, as well as creating new groups of metrics on security equipment that are unique to each system. It is also necessary to change the metrics of the characteristics group in order to obtain a single document classification for each system. Most of the D3S metric groups can be deployed as the basis for unmanned marine and land vehicles.

On the other hand, the D3S method can also be applied to existing UAV manufacturing or regulatory frameworks. In other words, the D3S method can be implemented during the construction process of a UAV and thus be a security certification method. The D3S value of a drone can serve as a benchmark in the manufacturing and sale of UAVs for various purposes, such as conveying the drone's security level, which directly impacts the user. The use of this method can lead to public disclosure of UAV vulnerabilities, which can be a

problem if used incorrectly. It is, therefore, necessary to use this method ethically, following the best vulnerability disclosure practices.

For future work, D3S can be improved in several aspects to create a more complex and extensive method. An improvement that could be made is to increase the number of metrics in the communications and software groups to achieve a more complete method. In addition, more cyber-attacks could be executed to gather more metrics for security analysis and the automated execution of cyber-attacks, as time is a critical factor in this context. The penetration testing process is time-consuming, as it requires writing many commands and analysing several results to obtain multiple information fields, such as IP and MAC addresses, as well as control and video transmission ports. To achieve a more reliable security classification system, it is important to validate it with a larger number of UAVs covering a wide range of characteristics, prices, and components.

Author Contributions: Conceptualization, J.S.S. and M.C.; methodology and software, B.B.; validation and formal analysis, J.S.S. and M.C.; resources, J.S.S.; writing—original draft preparation, B.B.; writing—review and editing, all authors; supervision, J.S.S. and B.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors acknowledge FCT-Fundação para a Ciência e Tecnologia for the Research Unit INESC-ID under project UIDB/50021/2020, and the Research Unit LIBPhyis-UC, LA-REAL under the project UIDB/FIS/04559/2020 (DOI: 10.54499/UIDB/04559/2020).

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

Abbreviations

The following abbreviations are used in this manuscript:

ACCESS	Advanced Communication Control Elevated Spread Spectrum
AFHDS	Automatic Frequency Hopping Digital System
BLOS	Beyond Line-of-Sight
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DJI	Da Jiang Innovations
DoS	Denial-of-Service
DSM	Digital Signal Modulation
DSSS	Direct Sequence Spread Spectrum
D3S	Drone Security Scoring System
GPS	Global Positioning System
FHSS	Frequency-Hopping Spread Spectrum
FASST	Futaba Advanced Spread Spectrum Technology
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LOS	Line-of-Sight
MitM	Man-in-the-Middle
MAC	Medium Access Contro
MAVLink	Micro Air Vehicle Link
OFDM	Orthogonal Frequency-Division Multiplexing
PC	Personal Computer
RTSP	Real-Time Streaming Protocol
SDR	Software Defined Radio
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UAV	Unmanned Aerial Vehicle
UAS	Unmanned Aircraft System

WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

References

1. Hecht, E. Drones in the Nagorno-Karabakh War: Analyzing the Data. *Mil. Strategy Mag.* **2022**, *7*, 31–37.
2. Kunertova, D. The war in Ukraine shows the game-changing effect of drones depends on the game. *Bull. At. Sci.* **2023**, *79*, 95–102. [CrossRef]
3. Criollo, L.; Mena-Arciniega, C.; Xing, S. Classification, military applications, and opportunities of unmanned aerial vehicles. *Aviation* **2024**, *28*, 115–127. [CrossRef]
4. Yaacoub, J.P.; Noura, H.; Salman, O.; Chehab, A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet Things* **2020**, *11*, 39. [CrossRef] [PubMed]
5. Sharma, A. An analytical view on Unmanned Aircraft Systems. *Comput. Telecommun. Eng.* **2024**, *2*, 2620. [CrossRef]
6. Abro, G.; Zulkifli, S.; Masood, R.; Asirvadam, S.; Laouti, A. Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats. *Drones* **2022**, *6*, 284 . [CrossRef]
7. AL-Dosari, K.; Hunaiti, Z.; Balachandran, W. Systematic Review on Civilian Drones in Safety and Security Applications. *Drones* **2023**, *7*, 210 . [CrossRef]
8. Modebadze, V. The Importance of Drones in Modern Warfare and Armed Conflicts. *Kutbilim Sos. Bilim. Sanat Derg.* **2021**, *1*, 89–98.
9. Höglund Gran, T.; Mickols, E. Hacking a Commercial Drone. Master's Thesis, Stockholm University, Stockholm, Sweden , 2020.
10. Rubbestad, G.; Söderqvist, W. Hacking a Wi-Fi Based Drone. Master's Thesis, Stockholm University, Stockholm, Sweden, 2021.
11. Kwon, Y.M.; Yu, J.; Cho, B.M.; Eun, Y.; Park, K.J. Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles. *IEEE Access* **2018**, *6*, 43203–43212. [CrossRef]
12. Westerlund, O.; Asif, R. Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things. In Proceedings of the 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS), Muscat, Oman, 5–7 February 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–10.
13. Dahlman, E.; Lagrelius, K. A Game of Drones: Cyber Security in UAVs. Master's Thesis, Stockholm University, Stockholm, Sweden, 2019.
14. Fatima, A.; Khan, T.A.; Abdellatif, T.M.; Zulfiqar, S.; Asif, M.; Safi, W.; Al Hamadi, H.; Al-Kassem, A.H. Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat. In Proceedings of the 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 7–8 March 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–8.
15. Parveen, M.; Shaik, M.A. Review on Penetration Testing Techniques in Cyber security. In Proceedings of the 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 23–25 August 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1265–1270.
16. Chamola, V.; Kotesh, P.; Agarwal, A.; Gupta, N.; Guizani, M. A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques. *Hoc Netw.* **2021**, *111*, 102324. [CrossRef] [PubMed]
17. Krichen, M.; Adoni, W.Y.H.; Mihoub, A.; Alzahrani, M.Y.; Nahhal, T. Security Challenges for Drone Communications: Possible Threats, Attacks and Countermeasures. In Proceedings of the 2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 9–11 May 2022 ; pp. 184–189.
18. Barnhart, R.K.; Marshall, D.M.; Shappee, E. *Introduction to Unmanned Aircraft Systems*; CRC Press: Boca Raton, FL, USA, 2021.
19. Stewart, M.P.; Martin, S.T. Unmanned Aerial Vehicles: Fundamentals, Components, Mechanics, and Regulations. In *Unmanned Aerial Vehicles*; Barrera, N., Ed.; Nova Science Publishers, Inc.: New York, NY, USA, 2021.
20. Ebeid, E.; Skriver, M.; Jin, J. A Survey on Open-Source Flight Control Platforms of Unmanned Aerial Vehicle. In Proceedings of the 2017 Euromicro Conference on Digital System Design (DSD), Vienna, Austria, 30 August–1 September 2017 ; pp. 396–402.
21. Simon, O.; Gotthans, T. A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception. *Electronics* **2022**, *11*, 3025 . [CrossRef]
22. Halbouni, A.; Ong, L.Y.; Leow, M.C. Wireless Security Protocols WPA3: A Systematic Literature Review. *IEEE Access* **2023**, *11*, 112438–112450. [CrossRef]
23. MAVLink. MAVLink Developer Guide. Technical Report, MAVLink. 2024. Available online: https://mavlink.io/en/ (accessed on 10 September 2024).
24. DJI. Drone Security White Paper, Version 3.0. Technical Report, DJI. 2024. Available online: https://www.dji.com/pt/trust-center/resource/white-paper (accessed on 10 September 2024).
25. Da-Jiang Innovations. DJI Lightbridge Release Notes. 2014. Available online: https://www.dji.com/pt/dji-lightbridge (accessed on 10 September 2024).
26. FrSky. Advanced Communication Control Elevated Spread Spectrum. 2024. Available online: https://www.frsky-rc.com/ (accessed on 10 September 2024).
27. Flysky. Third Gen Automatic Frequency Hopping Digital System. 2024. Available online: https://www.flysky-cn.com/ (accessed on 10 September 2024).
28. Feng, J.; Tornert, J. Denial-of-Service Attacks Against the Parrot ANAFI Drone. Master's Thesis, Stockholm University, Stockholm, Sweden, 2021.

29. Intwala, K.; Jatav, S.; Kolhe, K. System to capture WiFi based Drones using IoT. In Proceedings of the 2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA), Pune, India, 26–27 August 2022; IEEE: Piscataway, NJ, USA, 2022, pp. 1–6.
30. Vasconcelos, G.; Miani, R.S.; Guizilini, V.C.; Souza, J.R. Evaluation of dos attacks on commercial wi-fi-based UAVs. *Int. J. Commun. Netw. Inf. Secur.* **2019**, *11*, 212–223. [CrossRef]
31. de Carvalho Bertoli, G.; Pereira, L.A.; Saotome, O. Classification of denial of service attacks on Wi-Fi-based unmanned aerial vehicle. In Proceedings of the 2021 10th Latin-American Symposium on Dependable Computing (LADC), Florianopolis, Brazil, 22–26 November 2021; IEEE: Piscataway, NJ, USA, 2021, pp. 1–6.
32. Karmakar, G.; Petty, M.; Ahmed, H.; Das, R.; Kamruzzaman, J. Security of Internet of Things Devices: Ethical Hacking a Drone and its Mitigation Strategies. In Proceedings of the 2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 18–20 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–5.
33. Slimeni, F.; Delleji, T.; Chtourou, Z. RF-Based Mini-Drone Detection, Identification & Jamming in No Fly Zones Using Software Defined Radio. In Proceedings of the International Conference on Computational Collective Intelligence (ICCCI), Hammamet, Tunisia, 28–30 September 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 791–798.
34. Mekdad, Y.; Acar, A.; Aris, A.; Fergougui, A.E.; Conti, M.; Lazzeretti, R.; Uluagac, S. Exploring Jamming and Hijacking Attacks for Micro Aerial Drones. *arXiv* **2024**, arXiv:2403.03858. Available online: http://arxiv.org/abs/2403.03858 (accessed on 20 September 2024).
35. Saputro, J.A.; Hartadi, E.E.; Syahral, M. Implementation of GPS attacks on DJI phantom 3 standard drone as a security vulnerability test. In Proceedings of the 2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE), Yogyakarta, Indonesia, 13–14 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 95–100.
36. Rahman, A.D.B.A.; Ghani, K.A.; Khamis, N.H.H. Unmanned aerial vehicle (UAV) GPS jamming test by using Software Defined Radio (SDR) platform. In Proceedings of the Journal of Physics: Conference Series, Kuala Lumpur, Malaysia, 30 September 2020; IOP Publishing, Bristol, UK, 2021.
37. Forum of Incident Response and Security Teams (FIRST). *CVSS v4.0 Specification*; Forum of Incident Response and Security Teams (FIRST): Cary, North Carolina, 2023.