International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/223417 Volume 10, Issue 5, September – October (2023)

SURVEY ARTICLE

A Survey on Cybersecurity in Unmanned Aerial Vehicles: Cyberattacks, Defense Techniques and Future Research Directions

Simon Niyonsaba
Mathematics and Computer Science Department, Cheikh Anta Diop University, Dakar, Senegal
simon.niyonsaba@ucad.edu.sn

Karim Konate
Mathematics and Computer Science Department, Cheikh Anta Diop University, Dakar, Senegal
karim.konate@ucad.edu.sn

Moussa Moindze Soidridine
Mathematics and Computer Science Department, Cheikh Anta Diop University, Dakar, Senegal
moussa.soidridine@ucad.edu.sn

Received: 14 June 2023 / Revised: 11 August 2023 / Accepted: 02 September 2023 / Published: 30 October 2023

Abstract – Today, Unmanned Aerial Vehicles (UAV), also known as drones, are increasingly used by organizations, businesses and governments in a variety of military and civilian applications, including reconnaissance, border surveillance, port security, transportation, public safety surveillance, agriculture, scientific research, rescue and more. However, drone cybersecurity has become a major concern due to the growing risk of cyberattacks aimed at compromising the confidentiality, integrity and availability of drone systems. These cyberattacks can have serious consequences, such as disclosure or theft of sensitive data, loss of drones, disruption of drone performance, etc. In the existing literature, little work has been devoted to the cybersecurity of UAV systems. To fill this gap, a taxonomy of cyberattacks in UAV is proposed focusing on the three main categories, namely interception attacks against confidentiality, modification or fabrication attacks against integrity and disruption attacks against data availability. Next, a survey of defense techniques that can be used to protect UAV systems is carried out. Finally, a discussion is held on technologies for improving drone cybersecurity, such as Blockchain and Machine Learning, as well as the challenges and future direction of research.

Index Terms – Cybersecurity, UAV, Taxonomy, Cyberattacks, Defense Techniques, Machine Learning, Blockchain.

1. INTRODUCTION

Unmanned Aerial Vehicles (UAV), also known as drones, have become a very popular technology with remarkable growth. They are widely used in both civilian and military applications [1]. In the civilian field, Unmanned Aerial Vehicles have a wide range of applications, including agriculture, logistics, mapping, disaster management, scientific research, forest surveillance, trade, etc. Similarly, in the military field, Unmanned Aerial Vehicles are used in a wide range of applications, such as surveillance of military zones, border surveillance, combat, electronic warfare, reconnaissance, intelligence, explosion detection, etc.

The use of Unmanned Aerial Vehicles for these various applications is an emerging research topic due to its cost and performance advantages. However, cybersecurity in UAV remains a major challenge today, as UAV are vulnerable to various forms of attack. Currently, attacks on UAV systems such as Man in The Middle attacks, Eavesdropping attacks, DDoS/DoS attacks, GPS spoofing, Viruses, etc., which can compromise data confidentiality, integrity and availability, are on the increase. These attacks can target the UAV's main components including the Unmanned Aerial Vehicle (UAV), the Ground Control Station (GCS) and the communication links [2]. An attack on UAV systems can have serious consequences, such as loss of data, disclosure of sensitive data, disruption of UAV operations, hijacking, etc. To reduce these consequences, there are several defense techniques such as the use of data encryption, authentication, intrusion detection systems (IDS), firewalls, Machine Learning, etc.

The survey on cyber security in UAVs, including cyberattacks, defense techniques and future research directions, is very important. It helps entities to protect themselves against UAV attacks and to gain a better understanding of them. In addition, it enables the design and development of the most effective defense techniques against attacks on UAV systems, as well as coping with a new attack.

In addition, it can help to clarify the situation for decision-makers in the implementation of laws and standards concerning UAV security.

However, little work has been done on the investigation of cyber security in Unmanned Aerial Vehicles, and more specifically on cyberattacks, defense techniques and future research direction. In addition, this work has its limitations (see section ...). To fill this gap, a presentation on the taxonomy of cyberattacks is made based on confidentiality, integrity and availability (CIA). This is followed by a presentation of defense techniques, UAV security enhancement technologies and future research directions.

1.1. Contribution

This article aims to provide a comprehensive survey of cybersecurity issues in UAV systems and their associated concepts. The main contributions of this article are:

- Proposal of a taxonomy of cyberattacks, through which we classify and discuss the main cyberattacks targeting UAVs, the actors of these cyberattacks and their consequences;
- Presentation of existing defense techniques for detecting and mitigating the above mentioned cyberattacks;
- Discussion of technologies that can improve the cybersecurity of UAV systems, such as Blockchain and Machine Learning;
- Discussion of challenges and future research directions.

1.2. UAV Applications

Today, UAVs have numerous applications in both the military and civilian domains [3].

- Military applications [4]: Military surveillance, Air strikes, Missile launching, Border surveillance, Military security, Combat, etc.
- Civil applications [5]: Agriculture, Mining, Disaster management, Health care, Mapping, Environmental monitoring, Geographic mapping, Infrastructure inspection, etc.

1.3. UAV Architecture

UAVs are made up of several components that enable them to receive and transmit data in real time. Typically, UAV architecture is made up of three main components: Unmanned Aerial Vehicle (UAV), Ground Control Station (GCS) and communication links [2].

- Unmanned Aerial Vehicle (UAV): this is considered the heart of the drone's operation. The UAV is responsible for performing various functions (gathering information, sending control signals, calculating position, etc.);
- Ground control station: this consists of hardware and software enabling the human operator to communicate with and control the UAV and its payloads remotely. It should be noted that the ground control station communicates with the UAV via a command and control link over a communication link mounted from the ground to the UAV;
- Data links: these are wireless links enabling bidirectional communication and transmission of information between the ground station and the UAV. The data link uses radio frequency transmission to send and receive information (target position, remaining flight time, payload information, speed, altitude, operator position, etc.) to and from the UAV.

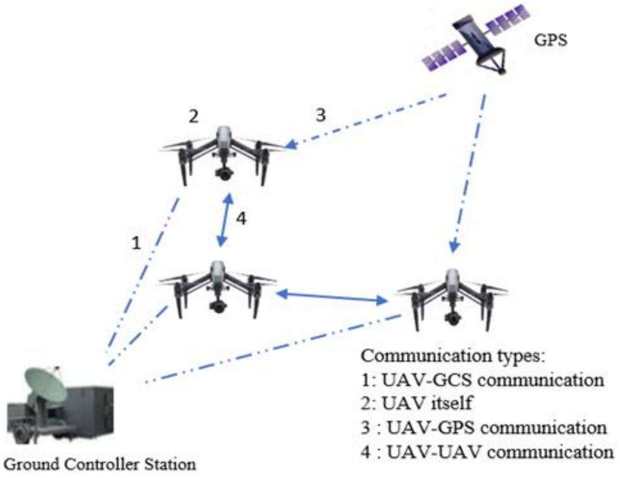
GPS
2
3
4
1
Communication types:
1: UAV-GCS communication
2: UAV itself
3 : UAV-GPS communication
4 : UAV-UAV communication
Ground Controller Station

Figure 1 UAV Architecture

Considering Figure 1, there are four types of communications such as communications between: UAV-GCS, UAV itself, UAV-GPS and UAV-UAV [6]. These types of communication are important for information exchange and for UAV control, coordination, precise navigation and cybersecurity.

1.4. UAV Classification

There are several types of UAVs/drones, which we can classify according to different parameters.

Based on their wings and rotors, UAVs/drones can be classified as follows [7]:

- Single-rotor UAVs: known as single-wing helicopters or radio-controlled helicopters. These types of UAVs have a single rotor that allows them to control their movement and stability;
- Multi-rotor UAVs : also known as rotary-wing UAVs, these are equipped with several rotors to facilitate take-off, landing and movement;

- Fixed-wing drones : is a type of drone that flies over long distances and at higher altitudes;
- Hybrid fixed-wing UAVs: are UAVs with rotating wings and fixed wings. These types of UAV combine the characteristics of both fixed-wing and rotor UAVs.

Table 1 Summary of Advantages, Disadvantages of UAV Types based on Wings and Rotors

Types of drone	Advantages	Disadvantages
Single-rotor drone [8] 	- Easy to change direction - Lower energy consumption - Good payload capacity with a single rotor	- Dangerous - High cost - Difficult to pilot - Training required
Multi-rotor drone [9] 	- Affordable cost - Easy to control and manoeuvre - Practical portability - No need for take-off or landing runways	- Energy consumption - Limited flight speed - Less wind stability -Limited flight time
Fixed-wing drone [10] 	- Good range - High-altitude flight - Ability to carry heavier loads - Higher flight speeds - Stability in windy conditions	- Costly - Requires a good knowledge of aerodynamics - Difficult to launch and land
Hybrid fixed-wing drone [10] 	- Overflight capability - Long-endurance flight - High speed - Greater payload capacity	- High cost - More training required

UAVs can be divided into several categories [11]. The summary of advantages, disadvantages of UAV types based on wings and rotors are depicted in Table 1. In Table 2, UAVs have been classified on the basis of range, climb rate, endurance and mass.

Table 2 UAV Classification According to the Unmanned Aerial Vehicle Systems Association [11]

Categories UAV	Acronym	Range (Km)	Climb rate (Km)	Endurance (hours)	Mass (kg)
Micro	M (Micro)	< 10	250	1	< 5
Mini	Mini	< 10	150-300	< 2	150
Close Range	CR	10-30	3000	2-4	150
Short Range	SR	30-70	3000	3-6	200
Medium Range	MR	70-200	5000	6-10	1250
Medium Range Endurance	MRE	>500	8000	10-18	1250
Low Altitude Deep Penetration	LADP	>250	8000	10-18	1250

Low Altitude Long Endurance	LALE	>500	3000	>24	< 30
Medium Altitude Long Endurance	MALE	>500	14000	24-48	1500

The rest of this article is structured as follows: Section 2 provides an overview of related work. Section 3 presents a taxonomy of cyberattacks in UAV. Section 4 focuses on cybersecurity solutions in UAVs including defense techniques against the cyberattacks studied. Section 5 describes technologies for improving cybersecurity in UAV systems. Section 6 discuss real cyberattacks against UAV. In section 7, challenges and future research directions are presented. Finally, Section 8 is about the conclusion.

2. RELATED WORK

Research work on UAV security has been carried out, but most of it has not been sufficiently detailed.

For example, in [12], the authors Javaid et al. analyze threats to UAV systems and propose a cybersecurity threat model. In their work, the authors present the different threats in UAV systems, such as attacks on confidentiality, attacks on integrity and attacks on availability. In addition, they present the architecture of a UAV system, identifying the data acquisition module, the navigation system, the control module, etc. In addition, the authors propose a risk assessment grid for evaluating the probability and impact of threats. Simulations are used to assess the impact of each threat on UAV systems. They also present results using FlighGear software, showing how certain threats can lead to system failures or even drone crashes. The model proposed by the authors enables users and designers to better assess and prepare for attacks on UAV systems. However, their work lacks information on defense techniques to minimize the impact of attacks. In addition, their work lacks real-world data due to UAV data confidentiality, which may limit the accuracy of real-world threat analysis in UAV systems.

In [13], author Manesh et al. highlight cyberattacks in UAS (Unmanned Aerial System). They also present defense strategies and the importance of addressing cybersecurity challenges in UAS. The authors discuss the types of cyberattacks in UAVs and their impact on security. They classify attacks into three categories such as data interception, data manipulation and DoS, and show existing defense techniques for each category, including cryptography-based approaches, machine learning and spatial processing. They also show the challenges and future directions of research, especially in UAS security. However, they focus solely on UAS security and do not discuss actual attacks on UAS systems.

The authors Benkraouda et al. [14] present cyberattacks targeting data communication from UAVs used for critical infrastructure surveillance. The authors present a taxonomy of cyberattacks based on the confidentiality, integrity and availability of data transmitted by UAVs to GCSs. They also propose solutions that can enhance security in UAV communications systems. Their article has advantages in that it deals with a topical issue concerning the cybersecurity of UAVs used for critical infrastructure surveillance. However, their article is limited to an analysis of the threats facing communications in UAVs, and solutions to prevent attacks using methods such as user authentication, algorithms, encryption to guarantee data confidentiality, the use of hashes and digital signatures, etc.

In [2], authors Hamza et al. review the literature, presenting the various UAV components, the main attacks against UAVs and defense techniques. The attacks identified are GPS spoofing, GPS jamming, De-Authentication attacks, keyloggers, DoS, viruses, Buffer Overflow, MEMS Gyroscope and Camera Spoofing. Their work tackles a topical subject concerning UAVs, threats and defense techniques such as IDS, machine learning and the use of encryption algorithms. However, it does not present actual attacks against UAVs. Furthermore, it does not provide details of security threats in UAV systems, nor does it take into account new research.

Authors Khan et al., in [15], present UAV applications, architecture, attacks against UAV systems as well as actual attacks against UAVs. According to these authors, data transmitted between UAVs and the GCS requires appropriate security mechanisms, as it is vulnerable to attacks such as Man in The Middle attacks, DoS/DDoS attacks, GPS spoofing, Eavesdropping, Identity spoofing, hijacking attack, replay attack, GCS spoofing and fabrication attacks. In their work, the authors propose the importance of developing a secure communication protocol to enhance security in UAVs. However, they do not provide detailed information on these attacks against UAVs. In addition, they do not propose defense techniques to mitigate the attacks studied, and the proposed secure communication protocol has not been developed.

In [16], author M.Cosar identifies security threats and cyberattacks on UAV systems and proposes cyber security solutions that can mitigate the risks. The author presents the different types of attack against UAVs, including hardware attack, software attack, network attack, communication attack and sensor attack. His paper offers a classification of the different types of attack in UAV systems, enabling researchers and professionals to gain a clear understanding of the threats and the security measures to counter these threats, such as the use of firewalls, data encryption, access control, intrusion detection and prevention systems (IDS/IPS) and secure communications protocols. However, it does not take into account recent research on cyber security in UAVs. What's more, his work requires further research, as it fails to provide details of the threats and proposed measures.

In [17], author P. Kong classifies attacks according to their points of entry (radio channels, messages, embedded systems) and examines existing countermeasures, classifying them into three categories: preventive, detection and mitigation countermeasures. However, some of the proposed countermeasures have limitations linked to the complexity of their implementation, and are resource-intensive in terms of reliable communication capacity and on-board computing power. The summary is shown in Table 3.

Table 3 Comparison of the Current Survey and Existing Review Papers

Categories discussed	[12]	[13]	[14]	[2]	[15]	[16]	[17]	This paper
Application domains					✓			✓
Architecture	✓	✓	✓	✓	✓	✓	✓	✓
Classification							✓	✓
Taxonomy/ classification of cyberattacks	✓	✓	✓	✓	✓	✓	✓	✓
Defense techniques		✓	✓	✓		✓	✓	✓
Real cyberattacks	✓				✓			✓
Challenges and future direction		✓		✓			✓	✓

3. TAXONOMY OF CYBERATTACKS IN UAVs

The taxonomy of cyberattacks in UAVs is important because it provides a classification of the types of attacks that can compromise the security of UAV systems. The proposed taxonomy of cyberattacks can help UAV users, professionals, and cybersecurity researchers understand cyberattacks and implement defense strategies tailored to each type of attack.

Figure 2 shows the most common cyberattacks against confidentiality, integrity and availability. These cyberattacks are grouped into three categories: data interception, data fabrication/modification and data interruption. In Figure 2, cyberattacks are grouped into three categories: data interception, data fabrication/modification and data interruption.

3.1. Actors of Cyberattacks in UAV

Actors of cyberattacks in UAVs systems can be:

- Nation-states: state-sponsored actors who use hacking techniques to gather intelligence or conduct attacks;
- Cybercriminals: individuals or groups who engage in criminal activities such as data theft, selling confidential information, or disrupting services;

- Cyberterrorists: actors in cyberattacks that can cause nationwide damage, conduct sabotage with far-reaching effects;
- Hacktivists: hacktivists use their technical skills to defend political or social causes. They can carry out protest actions or information gathering.

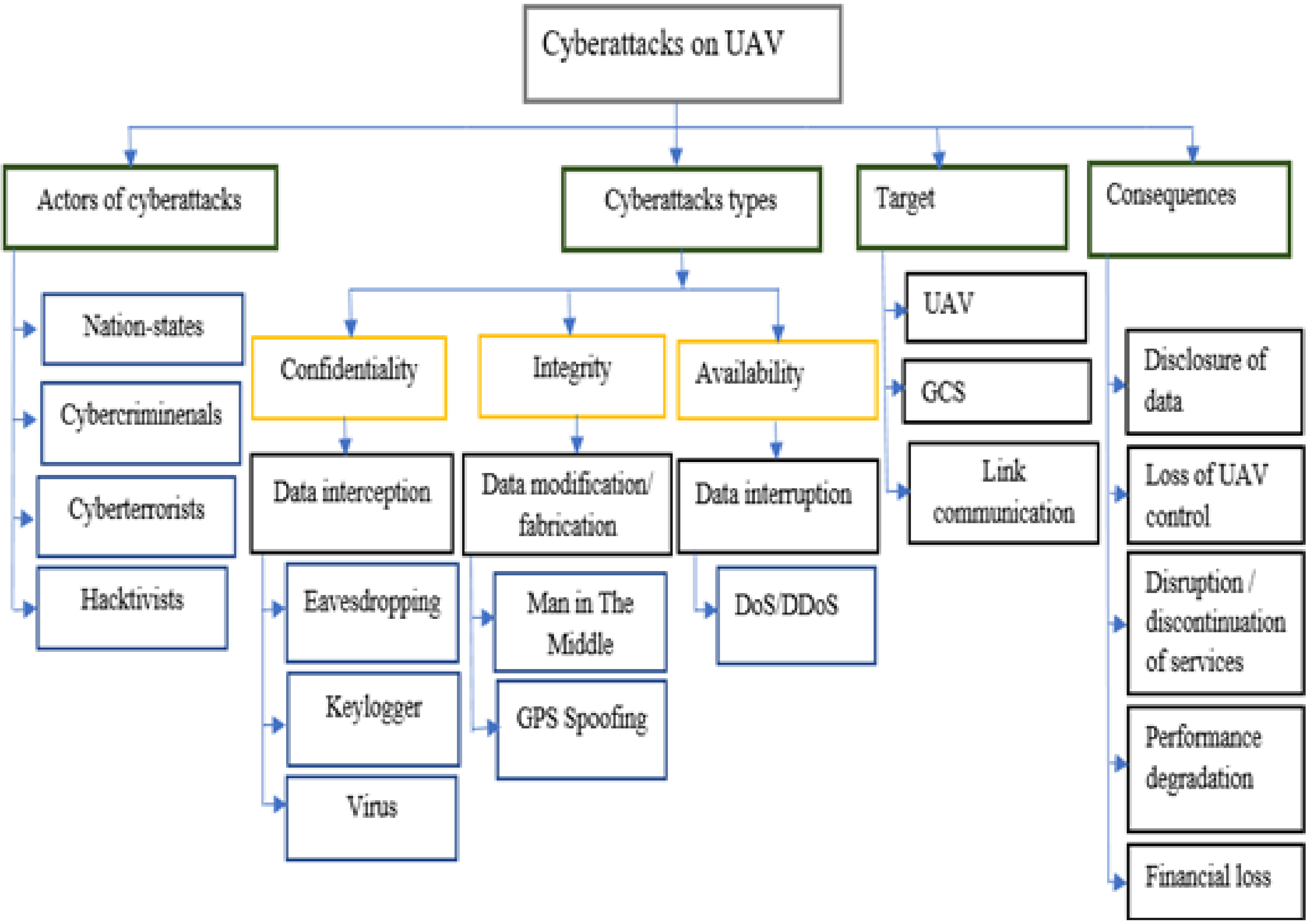

Figure 2 Taxonomy of Cyberattacks in UAVs

3.2. Types of Cyberattacks in UAVs

3.2.1. Attacks Against Confidentiality

Attacks on confidentiality are carried out by intercepting data in drone systems. The main attacks to be discussed that can affect confidentiality are: eavesdropping, keyloggers and viruses.

3.2.1.1. Eavesdropping Attack

Eavesdropping represents the most important attack in UAV networks, as it enables an attacker to eavesdrop on sensitive communications between UAVs and other devices available in the network. Figure 3 shows an example of an eavesdropping attack in which the attacker eavesdrops on communications between UAVs and between the GCS and the UAV. The attacker may have confidential information such as location data, flight plan, sensor data, etc.

The authors of [18], show that UAV communications are extremely vulnerable to various attacks including active full-duplex eavesdropping and jamming. Their approach is based on game theory to model the interactions between the legitimate user and the active eavesdropper in full-duplex mode. The authors launched the jamming attack to improve eavesdropping, which is highly relevant to security. They also considered the self-interference resulting from jamming attacks to better assess the impact of the actions performed by the eavesdropper. However, the proposed approach is complex when it comes to determining optimal strategies.

What's more, some of their assumptions may not fully reflect a real-life situation.

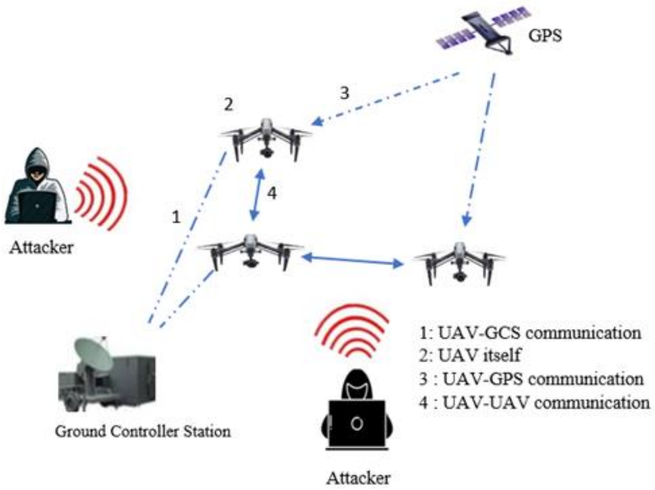
GPS
1
2
3
4
Attacker
Ground Controller Station
Attacker
1: UAV-GCS communication
2: UAV itself
3 : UAV-GPS communication
4 : UAV-UAV communication

Figure 3 Example of Eavesdropping Attack

A new active eavesdropping technique has been proposed by [19] and in this type of attack, the attacker acts as a spoofing relay, which could cause security risks including the high rate of information leakage from the source. In their work, the authors present mathematical analyses to determine the best strategies for eavesdropping depending on channel conditions. To validate the results and show the effectiveness of the attack compared with the passive eavesdropping attack, the authors carried out simulations. This article has several advantages. For example, the active eavesdropping technique, using the spoofing relay attack, allows the attacker to increase the information rate compared with the classic passive eavesdropping attack, enabling access to confidential information. In addition, the spoofing relay attack can be applied in several scenarios, making it potentially more damaging. However, their work has disadvantages in that detection of the attack is not easy, since changes in the communication channel can be attributed to environmental variations rather than to an intentional attack. In addition, this work can be used by ill-intentioned individuals wishing to exploit vulnerabilities in wireless communication systems such as UAV.

In [20], the authors Wu et al. analyze a beamforming design problem for proactive eavesdropping via jamming in a cognitive radio communication network aboard a UAV. Jamming signals were developed to disrupt both the main receiver and suspect receivers at the same time, while maintaining a good compromise between these two effects. The advantage of the proposed method is to optimize jamming while maximizing the achievable listening rate in UAVs. However, it does not provide enough information on the limitations and specific conditions with regard to the proposed approach.

Using the BCD (Block Coordinate Descent) and SCA (Successive Convex Approximation) models, authors Shen et al. [21] proposed a secure UAV communication system to reduce active clandestine attacks. They used a method to optimize the communication connection, 3D trajectory and transmit power to increase the average secrecy rate. However, applying the proposed SCA-based iterative algorithm is not only computationally intensive, but also resource-intensive.

3.2.1.2. Keylogger

Keyloggers are defined in [22] as rootkit malware or spyware that captures keystroke events and records them in a log file. During software development, keyloggers can be hidden in the program by malicious persons or can be injected by them after delivery. Keyloggers can be used to compromise confidentiality in UAV [23]. If an attacker managed to install a keylogger on a user's computer or mobile device to monitor and analyze the activities performed by the UAVs, it could retrieve sensitive information as it will be transmitted to the attacker without the knowledge of the legitimate user. The attacker can obtain login information for the wireless networks that the UAVs are connected to.

3.2.1.3. Virus

The virus is one of the main types of malicious programs [24] considered as small computer programs that attach themselves to others and are usually executed before the host programs [25]. Viruses are designed to propagate through electronic systems and perform the required tasks specified in the code. Malicious people can create viruses with the aim of stealing data, disrupting UAV missions, causing damage, controlling UAVs, etc. The Viruses can be introduced into electronic systems and used to control them. They can be introduced into UAV systems, for example, on a computer used by an operator through malware downloads and infected files or other attack vectors.

3.2.2. Attacks on Integrity

Integrity attacks can be either modification attacks or fabrication attacks. These types of attacks can modify the original data or fabricate the new data without authorization. In this article, the man-in-the-middle attack and the GPS spoofing attack are analyzed.

3.2.2.1. Man in the Middle Attack

This type of attack consists of an attacker placing himself between the UAV and the user of the remote control (RC) device to usurp and take control of the communication between these two entities [26]. Using the collected information, it is possible for the attacker to send authentication commands to the UAV as if it were a legitimate original user. In the UAV, an attacker can intercept and then modify communications to take control of the device remotely. The attacker can also target the GCS that is used to pilot and control the UAV. By impersonating the GCS, the attacker can intercept data and commands from the operator and modify them to take control of the UAV or manipulate the displayed data to mislead the operator. In Figure 4, the attack is performed by interrupting the communications between the UAVs and between the GCS and the UAV, this means that the attacker could listen to all communications. The attacker can also modify or even send false messages to the recipient.

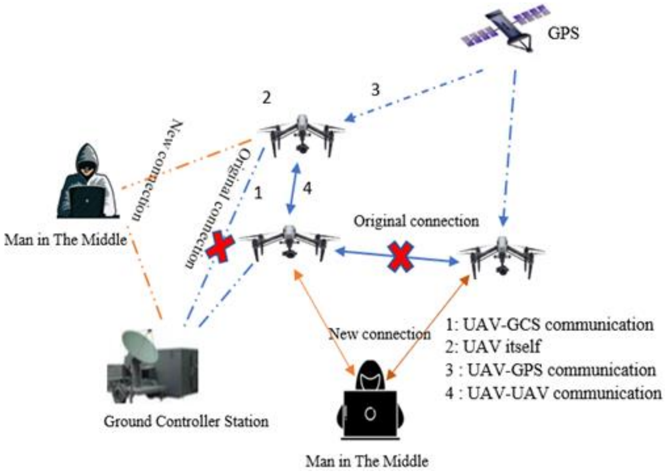

Figure 4 Example of Man in the Middle Attack in UAV

This may allow the attacker to take control of the UAV or stop its operation, which could cause adverse consequences to devices or even humans. In addition, the attacker can intercept and modify the data transmitted between the devices or even inject false signals.

In [27], the man in the middle attack is considered a destructive attack because the intruder can access sensitive data such as data packets, modify the information or simply replay the captured data packets to ruin the UAV mission or even cause physical damage.

A practical case on the man-in-the-middle attack was carried out in [28] where authors O.Westerlund and R. Asif showed that it is possible for an adversary to hack drones using Raspberry-Pi3 and Wi-Fi Pineapple, which lures drones and users into believing that it is a real, legitimate network. In this work, the authors carried out this attack to demonstrate the security vulnerabilities of drones in the IoT context. However, the methodology relies on experimentation carried out in a laboratory without taking into account real field conditions. In addition, the authors focus only on specific drones and do not address all available drone variations.

In [29], authors Rodday et al. show how to perform a Man in The Middle by modifying and injecting false information into the UAV system. They demonstrated security vulnerabilities in UAVs, raising awareness among users and manufacturers of the importance of strengthening security in UAV systems. The vulnerabilities were identified in the telemetry link, focusing on WiFi8022.11 and XBee868LP chips. However, for confidential reasons, the authors do not provide much information on the methodology used to identify these vulnerabilities.

3.2.2.2. GPS Spoofing

GPS Spoofing involves sending deceptive signals to disrupt GPS receivers and distort their positioning and time stamps without altering the received ephemeris data [30].

The GPS system plays an important role in UAVs because it provides useful information to UAVs such as timing, speed and position. This information is essential for an attacker because he can use it to hack the UAVs. In [31], the GPS system is vulnerable on three fronts: unintentional interference, intentional interference and human factors. A proposed approach models a drone hijacking attack using electronic warfare attacks. Vulnerabilities related to and threats to the use of drones and GPS systems have been identified, which is useful for the attacker as he can access personal information, manipulate or modify GPS position and divert the drone to the adversary's areas. However, the article does not go into detail about the methods used to hijack drones. The example of GPS spoofing attack is shown in Figure 5.

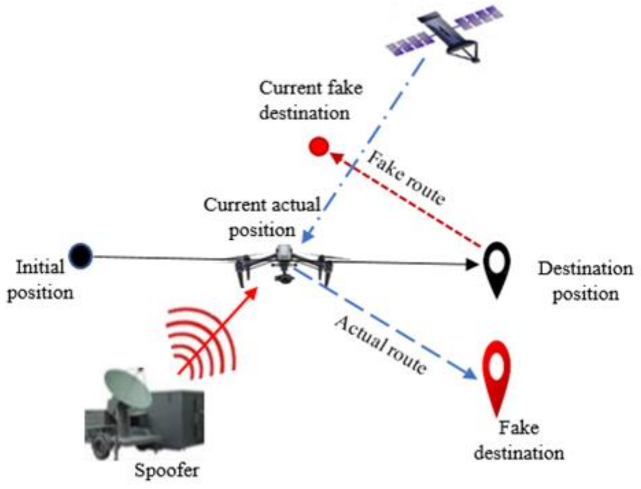

Figure 5 Example of GPS Spoofing Attack

The authors, E. Basan et al [32], conducted a study on GPS spoofing attack against a UAV. To perform this attack, they used a Pixhawh4 flight controller [33] and a device called HackRF that allows an attacker to create fake signals and satellites using high power that can be picked up by a drone. According to the results, it is possible to move the UAV to a location desired by an attacker because he will have changed the initial coordinates of the UAV by transmitting its false coordinates. Another work was conducted in [34] on the GPS spoofing attack and this time, the authors Demir et al. performed an analysis on the impact of modifying or falsifying the GPS timestamp. Their results show that they are more effective than attacks based on the signal travel time when the GPS signal is not encrypted.

3.2.3. Attacks on Availability

Availability ensures that the services provided by the UAVs are accessible even in the event of a cyberattack. Attacks against availability aim to compromise availability by, for example, disrupting or blocking access to the UAV control system or data. DoS/DDoS attacks are the most common attacks against UAV system availability.

3.2.3.1. DoS / DDoS Attacks

Denial of Service (DoS) attack is a type of cyberattack performed by a source host with the aim of making services inaccessible or preventing legitimate users from using the services. This type of attack can overload a target's resources with an excessive amount of data causing it to malfunction or shut down. Unlike DoS attacks that come from a single source, Distributed Denial of Service (DDoS) attacks come from multiple sources. To perform DDoS attacks, the attacker usually uses botnets [35]. DoS/DDoS attacks can make a service unavailable by saturating its processing or storage capacity. In the case of UAVs, this can result in an interruption of communication between the UAVs and between the UAV and GCS, which can lead to the loss of control of the UAV or the loss of sensitive data. Example of DoS attack is shown in Figure 6.

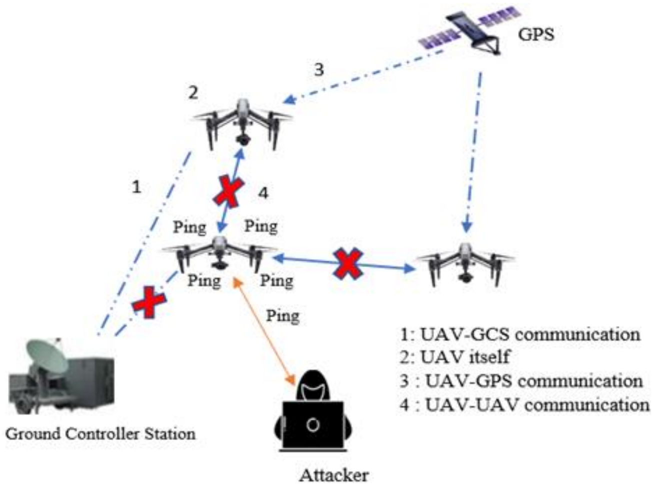
GPS
3
2
1
4
Ping
Ping
Ping
Ping
Ping
1: UAV-GCS communication
2: UAV itself
3 : UAV-GPS communication
4 : UAV-UAV communication
Ground Controller Station
Attacker

Figure 6 Example of DoS Attack

The authors Vasconcelos et al [36] carried out DoS attacks on the AR drone 2.0 and were able to assess its impact on the AR drone 2.0's behavior. After performing reconnaissance attacks using Nmap, the attacker launched DoS attacks using DoS attack tools such as LOIC (Low Orbit Ion Cannon), Netwox and Hping 3, and Hping3 was the best with the highest latency value. In this attack, the authors concluded that DoS attacks can compromise the video streaming application. Given that the experiments were carried out in a specific environment, this may be a limitation in terms of generalizing the results to other situations. Vasconcelos et al., in [37], show that the DoS attacks were performed on the Parrot ANAFI drone, a type of quadricopter drone that uses Wi-Fi for communication. Among ten tests performed, seven of them caused the DoS attacks.

3.3. Target of Cyberattacks

Targets of cyberattacks in UAV can be the UAV itself, the ground control system (GCS), and the communications links that connect these two systems.

3.4. Consequences of Cyberattacks

Cyberattacks on UAV can have serious consequences. For example, attackers can disclose or steal sensitive data (images, video, location information), cause the drone to be lost and take control of it and use it for malicious purposes. The attack can also disrupt or interrupt the services provided by the drone such as mapping, surveillance, etc. Another consequence is that it can disrupt the drone's performance by altering its sensors for example. In addition, the consequences can be financial related to material damage, service restoration costs, data loss, etc.

4. CYBERSECURITY SOLUTIONS FOR UAVs

Today, cybersecurity has become a major concern due to the exponential increase in cyberattacks. It is the ability of an information system to withstand events that could compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and the related services that this system offers or makes accessible [39]. This section discusses the various defense techniques used to detect and mitigate the cyberattacks analyzed in Section 3.

4.1. Eavesdropping Defense Techniques

In [13], the authors propose two solutions to mitigate the eavesdropping attack: cryptography and spread spectrum. Cryptographic techniques include symmetric encryption and asymmetric encryption [38]. Unlike symmetric encryption, which uses the same key for encryption and decryption, asymmetric cryptography uses a public key known to everyone and a private key known only to the recipient. Even though these cryptographic techniques are used, the radio frequencies used in civilian communications are not encrypted. Spread spectrum methods such as direct sequence spread spectrum (DSSS) [39] and frequency hopping spread spectrum (FHSS) make transmission signals more resistant and robust to interference and jamming, making them difficult for third parties to intercept and decode. Q.Wang, in [40], presents artificial interference as another method that can mitigate eavesdrop attacks because it makes legitimate communication signals more complex by disrupting vegetable communication signals. However, artificial interference can cause quality of service problems. Methods of mitigating eavesdropping attacks are listed in table 4.

Table 4 Methods of Mitigating Eavesdropping Attacks

Mitigation methods	Advantages	Limitations
Cryptography [41]	- Data confidentiality - Data integrity guaranteed by means of hash codes - Data authenticity	- Lack of signal encryption for civil communications - Electromagnetic interference for the quality of the communication signal
Spread spectrum [13]	- Resistance to interfaces Difficult to intercept transmitted data	- Need for more bandwidth - Complexity of implementation - Dependence on the environment
Artificial interference [40]	-Dissimilation of communications using noise Easy to implement - Flexible	- Impact on the quality of service of communications when bandwidth is reduced - Sometimes there is interference with other systems

The authors Hoang et al , in their paper [42], used unsupervised learning methods for the detection of Eavesdropping attacks. Eavesdropping attacks are detected from models built using One-Class Support Vector Machines (OC-SVM) and K-means clustering. The data set used to train the models was generated from wireless signals. The results were obtained from simulations, and K-means clustering can be more effective in cases where the attacker uses high power during transmission. However, model performance depends on the quality of the data used for training and the parameters chosen.

Other solutions to prevent eavesdropping require a multi-layered approach that includes measures such as secure communication protocols, antivirus software, firewall, VPN, physical limitations and user awareness.

4.2. Defense Techniques Against Keylogger

The authors S. Sreenivas and R. Anitha [43] proposed an anomaly-based method for detecting Traffic Analysis Keylogger Detection (TAKD). Their approach is to show traffic patterns that could be generated by keyloggers and identify suspicious data. Nowadays, keyloggers can sometimes escape detection by antivirus and anti-adware software. However, there are other measures to protect against keyloggers such as: firewalls, use of on-screen keyboards, security patch updates, use of licensed software as well as virtual keyboards [44]. The use of two-factor authentication [45] is also an effective way. Keyloggers cannot intercept verification codes generated from a source external to the user's keyboard.

4.3. Defense Techniques Against Viruses

Firewall, cryptography and access control are proposed in [46] as solutions for defense against malware in general and viruses .systems against viruses. In [47], virus detection technology is generally divided into two categories namely: static detection and dynamic detection. Static virus detection analyzes the code of a file to detect virus signatures. On the other hand, dynamic virus detection consists of running files in the virtual environment to observe their behavior and detect malicious activity. The different methods of virus detection can be: signature based detection, heuristic based detection, behavior based virus detection and emulation based [48] [49]. Virus detection methods are shown in Figure 7.

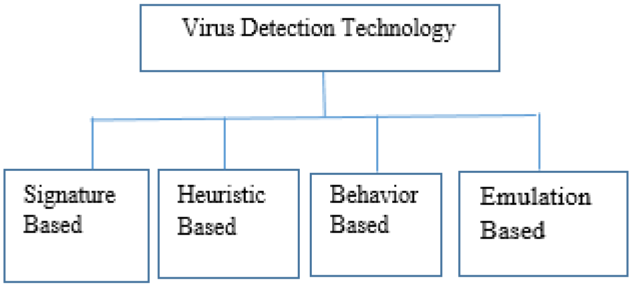

Figure 7 Virus Detection Methods

- Signature based virus detection: Compares a known virus signature to a file or email attachment to identify whether it is infected or not;
- Heuristic based virus detection: A method of virus detection that relies on analysis of program behavior or characteristics to identify unknown malware or variants of known viruses;
- Behavior based virus detection: This type of method involves monitoring the execution of files and programs to detect malicious activity;

- Emulation based virus detection: is a malware detection method that consists of mimicking the execution of a file in a virtual environment to determine if it has malicious intent. Using this emulation-based technique, the antivirus monitors the behavior of the suspicious file during its execution each time and records all its actions in an isolated and controlled environment called a sandbox.

The comparison of virus detection methods are listed in table 5.

Table 5 Comparison of Virus Detection Methods

Virus detection methods	Advantages	Limitations
Behavior based detection [49]	-Ability to detect unknown and recent viruses; -Faster than signature-based detection -Ability to block malicious actions of the virus	-Possibility of slowing down system performance because it monitors file activity -Viruses using sophisticated techniques can bypass this type of detection by simulating legitimate behavior or masking their actions -Ineffective for viruses that do not have immediate malicious actions
Signature based detection [49]	-Effective in detecting known viruses for which it has a corresponding signature -Fast and accurate recognition -Low computer resource requirements -Low error rate	-New viruses not yet identified may go unnoticed -Need for regular updates -Possibility of confusing legitimate files as infected due to signature matching -Polymorphic viruses that change their code cannot be detected
Heuristic based detection [50]	-Ability to detect new viruses -Ability to detect polymorphic viruses by analyzing their behavior -Protection against unknown threats -Lower false positive rate	-High resource consumption -Difficult to identify more sophisticated threats -Need to be updated although its programs require less frequent updates than signature-based ones -Dependence on the quality of the algorithms
Emulation based detection [51]	-Malware execution in an isolated and controlled environment -Real-time analysis of malware behavior	-Costly in terms of computer resources -Possibility of being bypassed by very sophisticated viruses -Need to be updated

There are other techniques for virus detection. For example, in [52], the authors proposed a virus detection model based on Artificial Intelligence and it is more effective than other solutions based on signature techniques. Artificial Intelligence offers several advantages for virus detection such as increased accuracy, speed, cost reduction and adaptability. However, the effectiveness of Artificial Intelligence depends on the amount of training data and viruses may not be included in the training data.

4.4. Defense Techniques Against Man in The Middle Attack

Since the transmitted data can be intercepted and modified by attackers, the authors in [53] propose mitigation techniques based on policies and cryptography. In [29], the authors present three approaches to mitigate the Man in The Middle attack: embedded encryption, encryption performed by the hardware itself and application-level encryption. Wireless hardware tokens can be used to mitigate the risk of Man in The Middle attacks [54]. In the case of UAVs, these tokens act as a physical barrier between the UAV and the ground control station and provide an additional layer of authentication and encryption to the communication channel. IDS and multi-factor authentication contribute to the detection and mitigation of Man in The Middle attacks [55].

4.5. Defense Techniques Against GPS Spoofing Attack

In [56], the authors propose solutions for defending against cryptographic spoofing based on encryption keys or signature and the non-cryptographic defense solution. The methods of defense against the GPS spoofing attack are presented in [13]. The authors Meng et al., in [57], proposed a mitigation model for GPS identity attack. They used linear regression and proved it using the dynamic Stackelberg game. The same paper stipulates other methods such as the detection of the physical layer characteristics of the signal based on the signal characteristics to know the false signals and the real signals, and the verification detection based on cryptography. Khoei et al. propose in [58] several techniques for detecting GPS spoofing attacks.

Other techniques for defending against GPS spoofing in UAV systems have been proposed. For example, authors P.Dhomane and R. Mathew [30] have explored and compared countermeasures such as stackelberg game model and visual odometry to counter spoofing in UAVs. Using stackelberg game, the drone can take proactive measures to counter GPS spoofing attacks when acting as a leader. As a leader, and using anomaly detection techniques or by comparing different information from other sources, the drone can identify GPS spoofing signals. Using the visual odometry technique, the authors Varshosaz et al, in [34], proposed a method for detecting drone spoofing based on angular distance, Manhattan distance and the sum of Euclidean distances between corresponding points, enabling the spoofing location to be determined and limiting the drift error of visual odometry. Despite the advantages of these techniques, they do have their limitations, as shown in table 6.

Table 6 Comparison of Defense Techniques Against GPS Spoofing Attack

Techniques	**Advantages**	**Limitations**
Hybrid techniques [13]	-Combination of several defense approaches -Reduction of false alarms -Improved accuracy	-Complex to implement -High cost -Vulnerable to other types of attacks such as DoS
Stackelberg game techniques [30]	Sharing of information on anomalies detected and GPS signals received between UAVs in the region	It can be ineffective for a swarm of drones that are targets of several GPS spoofing attacks occurring at the same time.
Techniques of inertial navigation systems [58]	Provide position and speed information when GPS signals are unavailable	-Not applicable to small drones -Usable when the sensors are of high quality in terms of size and cost -Possibility of being affected by electromagnetic disturbances
Cryptographic techniques [58]	-Data encryption -Verification of the authenticity of received data	-They can be circumvented by sophisticated attackers by decrypting the keys -Not practical for civilian applications
Visual odometry technique [59]	- GPS spoofing attacks can be detected - Can be used in a variety of environments	-It can be ineffective if the attacker is able to manipulate the images; -Possibility of errors if the camera calculates its position from the captured images;

4.6. Defense Techniques Against DoS Attacks

To detect and mitigate DoS/DDoS attacks, [60] proposes the use of IDS, firewall. In [6], the authors propose the use of frequency hopping and frequency range variation between the UAV and the ground station. The fail-safe protocol which allows to minimize the consequences of DoS/DDoS attacks and the fail loud protocol aiming at preventing completely the malfunctioning have been suggested in [61].

Authors V. Tumen and K. Demir, in [62], have proposed a solution for mitigating DoS attacks in UAVs based on UDP port switching and using middleware. This solution enables UAVs using WiFi to communicate efficiently via TCP over UDP. Depending on the agreed sequence of confidential port numbers, the entities periodically change the open UDP ports to prevent the attacker from using them for a long time, which can render the attack ineffective. The results obtained from the tests carried out show that the system is 91.2% more resistant to DoS attacks. However, their solution is physically inefficient and also requires careful coordination when changing ports in synchronization. Another mechanism that can contribute to UAV security is the snort tool proposed by authors Mujeeb et al. in [63]. This tool was able to detect and identify malicious packets in the network. However, this tool was not compared with other tools in order to properly assess its effectiveness.

The authors Ouiazzane et al. [64] proposed a new DoS attack detection model based on a multi-agent network for a fleet of AUVs. Their model is effective in detecting both known and unknown attacks. What's more, they achieved good results with a detection accuracy of 100%. However, implementation of the proposed system is complex and resource-intensive.

5. OTHER SOLUTIONS FOR IMPROVING CYBERSECURITY IN UAVs

In this section, new technologies that are currently being used to improve the reliability and security of drone communications are discussed.

5.1. Machine Learning Technology

Machine Learning is a branch of artificial intelligence that uses algorithms to learn and perform tasks without being explicitly programmed [65]. Machine Learning contributes to drone security by enabling rapid detection of the environment, thus avoiding collisions between drones. It also enables the detection of threats thanks to its algorithms, and reduces latency and increases the reliability of data transfers to the cloud. Machine learning algorithms can be used to detect unauthorized drones accessing a sensitive area. The detection of such drones is useful for preventing possible attacks or intrusions. Other algorithms are used to authorize drones to access this sensitive area. However, Machine Learning has its limits in terms of complexity, and deep learning algorithms require more training and testing [66].

In [67], the authors distinguish three main types of machine learning: supervised learning, unsupervised learning and reinforcement learning.

- Supervised learning: consists in making a computer learn from a set of labeled data comprising normal and abnormal data instances. In this type of learning, there are regression problems and classification problems. [68]. Supervised learning uses a number of algorithms such as Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Naïve Bayes (NB), Decision Tree (DT), etc.

- Unsupervised learning: unlike supervised learning, which deals with labeled data, unsupervised learning deals with unlabeled data. In this type of learning, the machine's task is to group unsorted data on the basis of similarities, patterns and differences, but without training the data. K-means and Density based clustering are examples of unsupervised learning;

- Reinforcement learning: this type of learning is different from the other two, as it allows an agent to interact with the environment to solve a given task. Q-learning and Temporal Difference (TD) learning are examples of reinforcement learning algorithms.

The table 7 lists the Summary of the analysis of existing works based on Machine Learning.

Table 7 Summary of the Analysis of Existing works based on Machine Learning

Ref	Learning algorithm	Simulation / dataset	Type of attack	Observation
[69]	LR, LDA, KNN, DT, GNB, SGD, KM	CICIDS2018	Botnet, DoS, Web attack, Infilteration, BruteForce, DDoS	-Compared with the other algorithms studied, DT performs better with a maximum accuracy rate of 99.99%. -Complexity of implementation -Lack of justification for dataset selection
[70]	K-NN, DT, LR	Simulation	DDoS : TCP-SYN flooding, UDP Flooding, Ping of death	- Good DDoS attack detection accuracy -Authors focus solely on DDoS attack detection - The authors have not dealt with the mitigation part
[71]	SVM, LR, DT, RF, NB	Dataset with GPS signal characteristics	GPS Spoofing	-The authors dealt with a single attack -Complexity of implementation and lack of information on the methodology used
[72]	DT	CICIDS2017	Brute force, DoS, Botnet attack, port scanning, SQL Injections, Cross Site Scripting (XSS),	-Very good detection accuracy (100%) -Complexity of the proposed approach

			Heartbleed	- Use of a single algorithm -No comparison with other algorithms
[73]	SVM, KNN, RF, GBDT, XGBoost	Dataset collected by sensors	GPS Spoofing	-The authors limited themselves to a single attack -The proposed model depends on sensor performance and accuracy. If one of the sensors fails, this may have an impact on the detection of the GPS Spoofing attack. -Their approach needs improvement
[74]	MLP, CNN, LSTM, CNN+LSTM	CICIDS2017	DDoS	- The proposed model is designed for regular networks, not drones - The authors focus solely on DDoS attacks

5.2. Blockchain Technology

Blockchain is the network system based on blocks linked together using cryptographic hash functions [75]. Currently, Blockchain technology is useful for drone safety, as drones can see where other drones are, avoiding collision between them thanks to public data. In addition, Blockchain can be used to store data transmitted to or from drones in encrypted form, meaning that data is stored transparently, immutably and resistant to tampering. What's more, the Blockchain-based identification system makes it possible to track previously registered drone flights while respecting the privacy of the drone user. However, it does have its limitations in terms of limited scalability and high energy consumption [66]. Table 8 lists the summary of analysis of existing blockchain based works.

Table 8 Summary of Analysis of Existing Blockchain based Works

Ref	Types of attacks	Benefit	Limits
[76]	DoS attacks Malware	-Data transmitted between UAVs is encrypted -The proposed system is effective against certain types of attack and malware	The system depends on the Blockchain. If the Blockchain encounters scalability or performance problems, this may affect the operation of the network.
[77]	Man in The Middle, DoS, replay, malicious, impersonation, de-synchronization attacks	The proposed scheme resists several common types of attack The authors use hyper-elliptic curve cryptography and Blockchain connected certification authority	-Implementing the proposed scheme can be complex -The proposed scheme applies only to the IoD network

[78]	Man in The Middle Replay GPS Spoofing	-The authors propose an access control protocol that resists several potential attacks in the context of military surveillance -The paper presents a detailed analysis of the proposed protocol -Command room registration and authentication of UAVs	-The article focuses solely on the military surveillance environment -With only unique identities, battlefield legitimacy for UAVs has not been effectively validated -Lack of activation of access control rules for UAVs Lack of traffic analysis
[79]	Malware Facility-related attack and Communication-related attack	Use of Blockchain to guarantee secure communications and data recording on Blockchain to facilitate traceability and auditing	Conventional Blockchain adoption limits with increased transaction time, less scalability and also vulnerable to attacks at 50%

6. REAL CYBERATTACKS AGAINST UAVs

Until 2007, the number of cyberattacks targeting UAV systems was small due to their limited use and lack of popularity. One incident was reported in 2009 when insurgents used SkyGrabber software to intercept UAV video feeds [15]. The insurgents were able to exploit a vulnerability because the video streams were not encrypted.

In 2011, the attack recognized in history was carried out by the Iranian army, resulting in the capture of an American Lockheed Martin RQ-170 Sentinel UAV, near the city of Kashmar, in northeastern Iran [80]. According to an Iranian engineer, the UAV was captured by disrupting satellite and ground control signals, followed by a GPS Spoofing attack that provided false location data to the UAV in order to land it in Iran [81].

In September 2011, a virus was introduced into the ground control station of the Predator and Reaper UAV communications network at Creech Air Force Base, Nevada. This type of malware, detected by the Army's IT security system, was considered to be a keylogger and its perpetrators were not identified, including its consequences [82]. In 2012, an unknown attack carried out by Iran targeted a ScanEagle drone manufactured by the American company Institute. The attack may have led to its capture [83].

7. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

- Advanced defense techniques : In order to enhance security in UAVs, researchers need to develop advanced defense techniques including machine learning;
- Vulnerabilities in wireless communication networks: UAVs are often connected to wireless networks, which are vulnerable to cyber-attacks. For this, researchers need to improve the most robust cryptographic techniques;
- Complexity and diversity of UAV systems: UAV systems are complex and diverse, making it difficult to apply uniform and consistent security measures. Researchers must strive to standardize UAVs and use security measures adapted to different types of UAV;
- Data availability in UAVs: To improve UAV safety, researchers need reliable data. However, access to this data is often limited because it is the intellectual property of the manufacturers. Collaboration between researchers and manufacturers is therefore needed to solve this problem;
- Given that Blockchain technology offers a means of decentralized data storage and processing, there is a need for in-depth research into Blockchain technology so that it can further enhance UAV cybersecurity;
- UAV vulnerability assessment: it is important to know the vulnerabilities in UAVs in order to better ensure their security. Penetration tests and assessments must be carried out to identify security flaws and propose security solutions to remedy them;
- Lightweight multi-factor authentication solutions: Since the use of a single factor is not sufficient to ensure adequate UAV security, it is important to improve lightweight multi-factor authentication solutions combining cryptographic and non-cryptographic techniques.

8. CONCLUSION

This article discussed the topic of cyber security in UAV systems. The taxonomy of cyberattacks in UAVs was used to classify the different attacks considering confidentiality, integrity and availability. The cyberattacks analyzed were grouped into three categories namely: data interception, data modification/fabrication, and data disruption. The defense techniques against these types of cyberattacks have been presented in this paper and include cryptography, firewall, cyberattack detection systems, access control, etc. In addition, technologies that can enhance the security of UAVs and improve their resilience to cyberattacks including Blockchain and Machine Learning were presented in this article. Thus, cybersecurity in UAV systems remains an area to be exploited by researchers given that cyberattacks have been increasing exponentially in recent years. Therefore, it is necessary for UAV designers, users and computer security researchers to be up to date on cybersecurity in order to take adequate security measures. Finally, research is needed to develop defense techniques and cybersecurity enhancement technologies for UAV systems.

REFERENCES

[1] W. Hayat Adnan and M. Fadly Khamis, “Drone Use in Military and Civilian Application: Risk to National Security,” *J. Media Inf. Warf.*, vol. 15, no. 1, pp. 60–70, 2022.

[2] A. Hamza, U. Akram, A. Samad, S. N. Khosa, R. Fatima, and M. F. Mushtaq, “Unmaned Aerial Vehicles Threats and Defence Solutions,” *Proc. - 2020 23rd IEEE Int. Multi-Topic Conf. INMIC 2020*, 2020, doi: 10.1109/INMIC50486.2020.9318207.

[3] E. G. JELER, “Military and civilian applications of UAV systems,” *Strateg. XXI Int. Sci. Conf. Complex Dyn. Nat. Secur. Environ.*, vol. 1, no. November 2017, pp. 379–386, 2019.

[4] A. Utsav, A. Abhishek, P. Suraj, and R. K. Badhai, “An IoT Based UAV Network for Military Applications,” *2021 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2021*, pp. 122–125, 2021, doi: 10.1109/WiSPNET51692.2021.9419470.

[5] M. Sivakumar and T. Y. J. Naga Malleswari, “A literature survey of unmanned aerial vehicle usage for civil applications,” *J. Aerosp. Technol. Manag.*, vol. 13, pp. 1–23, 2021, doi: 10.1590/jatm.v13.1233.

[6] J. P. Yaacoub, H. Noura, O. Salman, and A. Chehab, “Security analysis of drones systems: Attacks, limitations, and recommendations,” *Internet of Things (Netherlands)*, vol. 11, p. 100218, 2020, doi: 10.1016/j.iot.2020.100218.

[7] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta, and M. Guizani, “A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques,” *Ad Hoc Networks*, vol. 111, p. 102324, 2021, doi: 10.1016/j.adhoc.2020.102324.

[8] O. M. Alhawi, M. A. Mustafa, and L. C. Cordiro, “Finding Security Vulnerabilities in Unmanned Aerial Vehicles Using Software Verification,” *Proc. - 2019 Int. Work. Secur. Internet Things, SIoT 2019*, pp. 1–17, 2019, doi: 10.1109/SIOT48044.2019.9637109.

[9] C. Yinka-Banjo and O. Ajayi, “Sky-Farmers: Applications of Unmanned Aerial Vehicles (UAV) in Agriculture,” *Auton. Veh.*, 2020, doi: 10.5772/intechopen.89488.

[10] Y. Yazid, I. Ez-Zazi, A. Guerrero-González, A. El Oualkadi, and M. Arioua, “Uav-enabled mobile edge-computing for iot based on ai: A comprehensive review,” *Drones*, vol. 5, no. 4, 2021, doi: 10.3390/drones5040148.

[11] M. Gašparović and D. Gajski, “Unmanned Aerial Photogrammetric Systems in the Service of Engineering Geodesy,” *SIG 2016 - Int. Symp. Eng. Geod.*, no. May, pp. 561–572, 2016.

[12] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, “Cyber security threat analysis and modeling of an unmanned aerial vehicle system,” *2012 IEEE Int. Conf. Technol. Homel. Secur. HST 2012*, no. November, pp. 585–590, 2012, doi: 10.1109/THS.2012.6459914.

[13] M. Riahi Manesh and N. Kaabouch, “Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions,” *Comput. Secur.*, vol. 85, pp. 386–401, 2019, doi: 10.1016/j.cose.2019.05.003.

[14] H. Benkraouda, E. Barka, and K. Shuaib, “Cyber-Attacks on the Data Communication of Drones Monitoring Critical Infrastructure,” pp. 83–93, 2018, doi: 10.5121/csit.2018.81708.

[15] N. A. Khan, S. N. Brohi, and N. Jhanjhi, *UAV’s Applications, Architecture, Security Issues and Attack Scenarios: A Survey*, vol. 118. Springer Singapore, 2020. doi: 10.1007/978-981-15-3284-9_86.

[16] M. Cosar, “Cyber attacks on unmanned aerial vehicles and cyber security measures,” *Eurasia Proc. Sci. Technol. Eng. Math.*, vol. 21, pp. 258–265, 2022, doi: 10.55549/epstem.1226251.

[17] P. Y. Kong, “A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles,” *IEEE Access*, vol. 9, pp. 148244–148263, 2021, doi: 10.1109/ACCESS.2021.3124996.

[18] X. Tang, P. Ren, Y. Wang, and Z. Han, “Combating full-duplex active eavesdropper: A hierarchical game perspective,” *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1379–1395, 2017, doi: 10.1109/TCOMM.2016.2645679.

[19] Y. Zeng and R. Zhang, “Active eavesdropping via spoofing relay attack,” *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, vol. 2016-May, pp. 2159–2163, 2016, doi: 10.1109/ICASSP.2016.7472059.

[20] W. Wu, Y. Wang, J. Mo, and J. Liu, “Robust proactive eavesdropping in UAV-enabled wireless communication networking,” *Eurasip J. Wirel. Commun. Netw.*, vol. 2019, no. 1, 2019, doi: 10.1186/s13638-019-1599-6.

[21] A. Shen, J. Luo, J. Ning, Y. Li, Z. Wang, and B. Duo, “Safeguarding UAV Networks against Active Eavesdropping: An Elevation Angle-Distance Trade-Off for Secrecy Enhancement,” *Drones*, vol. 7, no. 2, pp. 1–18, 2023, doi: 10.3390/drones7020109.

[22] Y. Ahmed and A. Abdullahi, “Mitigating of Malicious Insider Keylogger Threats,” *Researchgate.Net*, no. February 2013, 2016, [Online]. Available: https://www.researchgate.net/profile/Yahye_Abukar2/publication/301197154_Mitigating_of_Malicious_Insider_Keylogger_Threats/links/570b696e08aea660813881c4/Mitigating-of-Malicious-Insider-Keylogger-Threats.pdf

[23] C. Drive, “of SINGAPORE Security Analysis of Unmanned Aircraft Systems Manh-Dung Nguyen , Naipeng Dong and Abhik Roychoudhury,” no. January, 2017.

[24] M. Software, “Chapter 7,” pp. 183–184, 2021.

[25] J. H. Wang, P. S. Deng, Y. S. Fan, L. J. Jaw, and Y. C. Liu, “Virus detection using data mining techinques,” *IEEE Annu. Int. Carnahan Conf. Secur. Technol. Proc.*, pp. 71–76, 2003, doi: 10.1109/ccst.2003.1297538.

[26] C. Gudla, M. Shohel Rana, and A. H. Sung, “Defense Techniques Against Cyber Attacks on Unmanned Aerial Vehicles Malware Detection View project E-Learning View project Defense Techniques Against Cyber Attacks on Unmanned Aerial Vehicles,” no. October, 2018, [Online]. Available: https://www.researchgate.net/publication/328135272

[27] R. Zhang, “Intrusion Detection System In A Fleet Of Drones,” 2022.

[28] O. Westerlund and R. Asif, “Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things,” *2019 1st Int. Conf. Unmanned Veh. Syst. UVS 2019*, no. c, pp. 1–10, 2019, doi: 10.1109/UVS.2019.8658279.

[29] N. M. Rodday, R. O. De Schmidt, and A. Pras, “Exploring security vulnerabilities of unmanned aerial vehicles,” *Proc. NOMS 2016 - 2016 IEEE/IFIP Netw. Oper. Manag. Symp.*, no. Noms, pp. 993–994, 2016, doi: 10.1109/NOMS.2016.7502939.

[30] P. Dhomane and R. Mathew, “Counter-measures to spoofing and jamming of drone signals,” *SSRN Electron. J.*, pp. 1–10, 2021, doi: 10.2139/ssrn.3774955.

[31] S. M. Giray, “Anatomy of unmanned aerial vehicle hijacking with signal spoofing,” *RAST 2013 - Proc. 6th Int. Conf. Recent Adv. Sp. Technol.*, pp. 795–800, 2013, doi: 10.1109/RAST.2013.6581320.

[32] E. Basan, O. Makarevich, M. Lapina, and M. Mecella, “Analysis of the Impact of a GPS Spoofing Attack on a UAV,” *CEUR Workshop Proc.*, vol. 3094, pp. 6–16, 2022.

[33] S. Mahfoudhi, M. A. Khodja, and F. O. Mahroogi, “A second-order sliding mode controller tuning employing particle swarm optimization,” *Int. J. Intell. Eng. Syst.*, vol. 13, no. 3, pp. 212–221, 2020, doi: 10.22266/IJIES2020.0630.20.

[34] M. O. Demir, G. K. Kurt, and A. E. Pusane, “On the Limitations of GPS Time-Spoofing Attacks,” *2020 43rd Int. Conf. Telecommun. Signal Process. TSP 2020*, pp. 313–316, 2020, doi: 10.1109/TSP49548.2020.9163444.

[35] S. Behal and K. Kumar, “Characterization and comparison of DDoS attack tools and traffic generators - a review,” *Int. J. Netw. Secur.*, vol. 19, no. 3, pp. 383–393, 2017, doi: 10.6633/IJNS.201703.19(3).07.

[36] G. Vasconcelos, G. Carrijo, R. Miani, J. Souza, and V. Guizilini, “The Impact of DoS Attacks on the AR.Drone 2.0,” *Proc. - 13th Lat. Am. Robot. Symp. 4th Brazilian Symp. Robot. LARS/SBR 2016*, pp. 127–132, 2016, doi: 10.1109/LARS-SBR.2016.28.

[37] J. Feng and J. Tornert, “Denial-of-service attacks Denial-of-service attacks against the Parrot ANAFI drone,” 2021, [Online]. Available: https://kth.diva-portal.org/smash/get/diva2:1601435/FULLTEXT01.pdf

[38] S. Sharma, “Cryptography : An Art of Writing a Secret Code,” *Int. J. Comput. Sci. Technol.*, vol. 8491, no. 1, pp. 26–30, 2017.

[39] A. Liu, P. Ning, H. Dai, Y. Liu, and C. Wang, “Defending DSSS-based broadcast communication against insider jammers via delayed seed-disclosure,” *Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC*, pp. 367–376, 2010, doi: 10.1145/1920261.1920315.

[40] Q. Wang, “Defending wireless communication against eavesdropping attacks using secret spreading codes and artificial interference,” *Comput. Secur.*, vol. 103, pp. 1–14, 2021, doi: 10.1016/j.cose.2020.102175.

[41] W. Stallings, *Cryptography and Network Security: Principles and Practice 7th Global Edition*. 2017.

[42] T. M. Hoang, N. M. Nguyen, and T. Q. Duong, “Detection of Eavesdropping Attack in UAV-Aided Wireless Systems: Unsupervised Learning with One-Class SVM and K-Means Clustering,” *IEEE Wirel. Commun. Lett.*, vol. 9, no. 2, pp. 139–142, 2020, doi: 10.1109/LWC.2019.2945022.

[43] R. S. Sreenivas and R. Anitha, “Detecting keyloggers based on traffic analysis with periodic behaviour,” *Netw. Secur.*, vol. 2011, no. 7, pp. 14–19, 2011, doi: 10.1016/S1353-4858(11)70076-9.

[44] A. Bhardwaj and S. Goundar, “Keyloggers: silent cyber security weapons,” *Netw. Secur.*, vol. 2020, no. 2, pp. 14–19, 2020, doi: 10.1016/S1353-4858(20)30021-0.

[45] S. Chahrvin, “Keyloggers - your security nightmare?,” *Comput. Fraud Secur.*, vol. 2007, no. 7, pp. 10–11, 2007, doi: 10.1016/S1361-3723(07)70090-8.

[46] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, “Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review,” *J. Cybersecurity Priv.*, vol. 2, no. 3, pp. 527–555, 2022, doi: 10.3390/jcp2030027.

[47] Z. Yangchun, Y. Zhao, and J. Yang, “New Virus Infection Technology and Its Detection,” *Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS*, vol. 2020-Octob, pp. 388–394, 2020, doi: 10.1109/ICSESS49938.2020.9237708.

[48] Institute of Electrical and Electronics Engineers, “2017_Haris-A.-Khan_Computer Virus and Protection Methods Using Lab Analysis,” pp. 882–886, 2017.

[49] H. Kasban, O. Zahran, S. M. Elaraby, M. El-Kordy, and F. E. Abd El-Samie, “A comparative study of Virus detection techniques,” *Sens. Imaging*, vol. 11, no. 3, pp. 89–112, 2010, doi: 10.1007/s11220-010-0054-x.

[50] A. Thengade, A. Khaire, D. Mitra, and A. Goyal, “Virus Detection Techniques and Their Limitations,” *Int. J. Sci. Eng. Res.*, vol. 5, no. 10, pp. 1334–1337, 2014.

[51] S. Chakraborty, “A Comparison study of Computer Virus and Detection Techniques,” *Res. J. Eng. Technol.*, vol. 8, no. 1, p. 49, 2017, doi: 10.5958/2321-581x.2017.00008.3.

[52] O. Asiru, M. Dlamini, and J. Blackledge, “Application of artificial intelligence for detecting derived viruses,” *Eur. Conf. Inf. Warf. Secur. ECCWS*, pp. 647–655, 2017.

[53] B. B. Madan, M. Banik, and D. Bein, “Securing unmanned autonomous systems from cyber threats,” *J. Def. Model. Simul.*, vol. 16, no. 2, pp. 119–136, 2019, doi: 10.1177/1548512916628335.

[54] A. Ben-david, O. Berkman, Y. Matias, and S. Patel, “Contextual OTP : Mitigating Emerging Man-in-the-Middle Attacks,” *Lncs 7341. Acns 2012*, pp. 30–47, 2012.

[55] M. A. Siddiqi, C. Iwendi, K. Jaroslava, and N. Anumbe, “Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations,” *Math. Biosci. Eng.*, vol. 19, no. 3, pp. 2641–2670, 2022, doi: 10.3934/MBE.2022121.

[56] T. E. Humphreys, “Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and other Systems to Civil Gps Spoofing Submitted to the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security,” pp. 1–16, 2012.

[57] L. Meng *et al.*, “An Approach of Linear Regression-Based UAV GPS Spoofing Detection,” *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/5517500.

[58] T. Talaei Khoei, S. Ismail, and N. Kaabouch, “Dynamic Selection Techniques for Detecting GPS Spoofing Attacks on UAVs,” *Sensors*, vol. 22, no. 2, 2022, doi: 10.3390/s22020662.

[59] M. Varshosaz, A. Afary, B. Mojaradi, M. Saadatseresht, and E. G. Parmehr, “Spoofing detection of civilian UAVs using visual odometry,” *ISPRS Int. J. Geo-Information*, vol. 9, no. 1, 2019, doi: 10.3390/ijgi9010006.

[60] Y. Mekdad *et al.*, “A survey on security and privacy issues of UAVs,” *Comput. Networks*, vol. 224, p. 109626, 2023, doi: 10.1016/j.comnet.2023.109626.

[61] R. Altawy and A. M. Youssef, “Security, privacy, and safety aspects of civilian drones: A survey,” *ACM Trans. Cyber-Physical Syst.*, vol. 1, no. 2, 2017, doi: 10.1145/3001836.

[62] K. D. Vedat TÜMEN1*, “A Defense Mechanism Against DoS Attacks on Unmanned Aerial Vehicle Communication,” vol. 17, no. 2, pp. 233–239, 2022.

[63] S. Mujeeb, S. K. Chowdhary, A. Srivastava, R. Majumdar, and M. Kumar, “Unmanned Aerial Vehicle Attack Detection using Snort,” no. Icicis 2021, pp. 18–24, 2022, doi: 10.5220/0010789700003167.

[64] S. Ouiazzane, M. Addou, and F. Barramou, “A Multiagent and Machine Learning Based Denial of Service Intrusion Detection System for Drone Networks,” *Adv. Sci. Technol. Innov.*, no. January, pp. 51–65, 2022, doi: 10.1007/978-3-030-80458-9_5.

[65] Z. Baig, N. Syed, and N. Mohammad, “Securing the Smart City Airspace: Drone Cyber Attack Detection through Machine Learning,” *Futur. Internet*, vol. 14, no. 7, pp. 1–19, 2022, doi: 10.3390/fi14070205.

[66] M. Krichen, W. Y. H. Adoni, A. Mihoub, M. Y. Alzahrani, and T. Nahhal, “Security Challenges for Drone Communications: Possible Threats, Attacks and Countermeasures,” *Proc. - 2022 2nd Int. Conf. Smart Syst. Emerg. Technol. SMARTTECH 2022*, no. May, pp. 184–189, 2022, doi: 10.1109/SMARTTECH54121.2022.00048.

[67] O. Simeone, “A Very Brief Introduction to Machine Learning with Applications to Communication Systems,” *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 4, pp. 648–664, 2018, doi: 10.1109/TCCN.2018.2881442.

[68] S. K. Sahu, A. Mokhade, and N. D. Bokde, “An Overview of Machine Learning, Deep Learning, and Reinforcement Learning-Based Techniques in Quantitative Finance: Recent Progress and Challenges,” *Appl. Sci.*, vol. 13, no. 3, 2023, doi: 10.3390/app13031956.

[69] R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim,

“Machine-learning-enabled intrusion detection system for cellular connected uav networks,” *Electron.*, vol. 10, no. 13, pp. 1–28, 2021, doi: 10.3390/electronics10131549.

[70] A. Shrivastava and K. Sharma, “DDoS Detection for Amateur Internet of Flying Things using Machine Learnings,” *SSRN Electron. J.*, no. Aece, pp. 124–133, 2022, doi: 10.2139/ssrn.4159111.

[71] A. Shafique, A. Mehmood, and M. Elhadef, “Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models,” *IEEE Access*, vol. 9, pp. 93803–93815, 2021, doi: 10.1109/ACCESS.2021.3089847.

[72] S. Ouiazzane, F. Barramou, and M. Addou, “Towards a Multi-Agent based Network Intrusion Detection System for a Fleet of Drones,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 10, pp. 351–362, 2020, doi: 10.14569/IJACSA.2020.0111044.

[73] X. Wei, Y. Wang, and C. Sun, “PerDet: Machine-Learning-Based UAV GPS Spoofing Detection Using Perception Data,” *Remote Sens.*, vol. 14, no. 19, pp. 1–20, 2022, doi: 10.3390/rs14194925.

[74] M. Roopak, G. Yun Tian, and J. Chambers, “Deep learning models for cyber security in IoT networks,” *2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019*, pp. 452–457, 2019, doi: 10.1109/CCWC.2019.8666588.

[75] V. Hassija *et al.*, “Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey,” *IEEE Commun. Surv. Tutorials*, vol. 23, no. 4, pp. 2802–2832, 2021, doi: 10.1109/COMST.2021.3097916.

[76] M. Dave, K. Chauhan, H. Sachdeva, S. Gupta, and A. Misra, “Privacy and Security Improvement in UAV Network using Blockchain,” *Int. J. Commun. Networks Distrib. Syst.*, vol. 1, no. 1, p. 1, 2023, doi: 10.1504/ijcnds.2023.10048925.

[77] S. Javed *et al.*, “An Efficient Authentication Scheme Using Blockchain as a Certificate Authority for the Internet of Drones,” *Drones*, vol. 6, no. 10, pp. 1–15, 2022, doi: 10.3390/drones6100264.

[78] B. Bera, A. K. Das, S. Garg, M. Jalil Piran, and M. S. Hossain, “Access Control Protocol for Battlefield Surveillance in Drone-Assisted IoT Environment,” *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2708–2721, 2022, doi: 10.1109/JIOT.2020.3049003.

[79] K. Gai, Y. Wu, L. Zhu, K. K. R. Choo, and B. Xiao, “Blockchain-Enabled Trustworthy Group Communications in UAV Networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4118–4130, 2021, doi: 10.1109/TITS.2020.3015862.

[80] K. Hartmann and C. Steup, “The vulnerability of UAVs to cyber attacks - An approach to the risk assessment,” *Int. Conf. Cyber Conflict, CYCON*, 2013.

[81] E. Yağdereli, C. Gemci, and A. Z. Aktaş, “A study on cyber-security of autonomous and unmanned vehicles,” *J. Def. Model. Simul.*, vol. 12, no. 4, pp. 369–381, 2015, doi: 10.1177/1548512915575803.

[82] C. G. Leela Krishna and R. Murphy, “A review on cybersecurity vulnerabilities for unmanned aerial vehicles,” *Auvsi Xponential 2018*, pp. 0–5, 2018.

[83] L. He, W. Li, C. Guo, and R. Niu, “Civilian unmanned aerial vehicle vulnerability to GPS spoofing attacks,” *Proc. - 2014 7th Int. Symp. Comput. Intell. Des. Isc. 2014*, vol. 2, pp. 212–215, 2015, doi: 10.1109/ISCID.2014.131.

Authors

Simon Niyonsaba is a PhD student in computer science at Cheikh Anta Diop University of Dakar (UCAD), Senegal. He does his research in network security. He completed his Master's studies in Computer Security and Telecom Network respectively at Supdeco and the Higher Institute of Computer Science of Dakar. His research interests are cybersecurity, computer security, Machine Learning, intrusion detection/prevention systems and cryptography.

Karim Konate received a Ph.D. degree in Engineering Sciences (High-performance and Fault-tolerant Computers and Systems) in January 1997 from the Supreme Attestation Commission of Ukraine, upon the recommendation of Vinnytsia State Technical University, Vinnytsia, Ukraine. He received M. S. degree in Electronics and Systems Engineering from Vinnytsia Polytechnical Institute, Ukraine, USSR. From 1999 to 2001 he was a Network and Telecommunications Administrator at Fondation Trade Point Senegal. He is currently an Associate Professor in Mathematics and Computer Science Department at Université Cheikh Anta Diop, Dakar, Senegal. His research interests include wireless communications and networking, computer systems and architecture, cryptography and network security, compilers and parallelism.

Dr. Moussa Moindze Soidridine obtained his PhD in Telecommunication at Cheikh Anta Diop University, Dakar in 2018. He is currently a Research Professor at Cheikh Anta Diop University. He is also a consultant in Network and Computer Security. Moindze has published several articles and his research interests are in network security, telecommunications, IoT and artificial intelligence.

How to cite this article:

Simon Niyonsaba, Karim Konate, Moussa Moindze Soidridine, “A Survey on Cybersecurity in Unmanned Aerial Vehicles: Cyberattacks, Defense Techniques and Future Research Directions”, International Journal of Computer Networks and Applications (IJCNA), 10(5), PP: 688-705, 2023, DOI: 10.22247/ijcna/2023/223417.