sciendo INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS

Article | DOI: 10.2478/ijssis-2023-0012 Issue 1 | Vol. 16 (2023)

Cybersecurity in Unmanned Aerial Vehicles: a Review

Wasswa Shafik[1,*], S. Mojtaba Matinkhah[2,*], Fawad Shokoor[2]

[1]Dig Connectivity Research Laboratory, PO Box 600040, Kampala, Uganda

[2]Department of Computer Engineering, Intelligent Connectivity, Research Laboratory, Yazd University, PO Box 89175-741, Yazd, Iran

*E-mails: wasswashafik@gmail.com, matinkhah@yazd.ac.ir

Received for publication May 20, 2022.

Abstract

Context: With the rapid advancement of unmanned aerial vehicle (UAV) technology, ensuring these autonomous systems' security and integrity is paramount. UAVs are susceptible to cyberattacks, including unauthorized access, control, or manipulation of their systems, leading to potential safety risks or unauthorized data retrieval. Moreover, UAVs encounter limited computing resources, wireless communication and physical vulnerabilities, evolving threats and techniques, necessity for compliance with regulations, and human factors.

Methods: This review explores the potential cyberthreats faced by UAVs, including hacking, spoofing, and data breaches, and highlights the critical need for robust security measures. It examines various strategies and techniques used to protect UAVs from cyberattacks, e.g., encryption, authentication, and intrusion detection systems using cyberthreat analysis and assessment algorithms. The approach to assess the UAVs' cybersecurity hazards included STRIDE (a model for identifying computer security-related threats) connected with the threats considered.

Findings: Emphasis was laid on the evaluation highly depending on the accuracy of UAV mission definition, potential intruders, and social and other human-related situations. The review discovered that most studies focused on possible intruders' portraits, which can be crucial when conducting a cybersecurity assessment. Based on a review, future research directions to mitigate cybersecurity risks are presented.

Significance: Protecting UAVs from cyberthreats ensures safe operations and data integrity and preserves public trust in autonomous systems.

Keywords

Cybersecurity, cyberattacks, drones, industry, innovation and Infrastructure, sustainable cities and communities, responsible consumption and production, unmanned aerial vehicles

1. Introduction

Cybersecurity has become an essential aspect of our increasingly digital world, encompassing various domains and technologies. Among these, unmanned aerial vehicles (UAVs), commonly known as drones, have emerged as a revolutionary technological tool with numerous applications in surveillance, delivery services, and disaster management. As UAVs evolve and become more autonomous, ensuring their cybersecurity becomes paramount. Cyberthreats pose significant risks to these UAVs' integrity, functionality,

Open Access. Published by Sciendo. CC BY-NC-ND
© 2023 Shafik et al. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License https://creativecommons.org/licenses/by-nc-nd/4.0/

and safety [1]. Therefore, robust measures must be implemented to protect UAVs from potential cyberattacks, safeguard sensitive data, and maintain public trust in their reliable and secure operation.

In recent years, the field of UAV cybersecurity has gained significant attention as the vulnerabilities and potential consequences of cyberattacks on these autonomous flying systems have become increasingly apparent. UAVs rely on complex software, wireless communication systems, and data exchange protocols, making them susceptible to cyberthreats. One of the primary concerns in UAV cybersecurity is the vulnerability to hacking. Malicious actors can attempt to gain unauthorized access to UAV systems, manipulate their flight controls, or compromise their onboard sensors and cameras [2]. Such unauthorized access can lead to severe consequences, including loss of control, property damage, or even endangerment of human lives.

Another challenge lies in the limited computing resources of UAVs. These systems are often designed with lightweight and energy-efficient hardware, which can pose constraints on implementing robust security measures. Balancing the need for strong security protocols while maintaining optimal performance and flight capabilities presents a unique challenge in UAV cybersecurity. Wireless communication vulnerabilities are also a critical concern. UAVs heavily rely on wireless protocols for communication with ground control stations and other connected devices. These wireless channels can be targeted by hackers for interception, eavesdropping, or jamming attacks [3]. Unauthorized access to these communication links compromises the confidentiality and integrity of the transmitted data and opens avenues for potential control manipulation or data theft.

Physical vulnerability is another aspect that must be considered in UAV cybersecurity. UAVs can be physically tampered with or stolen, providing unauthorized individuals with access to sensitive data or the ability to use the UAV for malicious purposes. Adequate physical security measures must be in place to prevent physical compromises and protect UAVs from unauthorized access. As the threat landscape constantly evolves, staying ahead of emerging cyberthreats and techniques is crucial. UAV cybersecurity measures must adapt and incorporate the latest advancements in encryption, authentication, and intrusion detection systems [4]. Continuous research and development are necessary to enhance the resilience of UAVs against evolving cyberthreats.

Furthermore, compliance with regulations and industry standards is a significant factor in UAV cybersecurity. UAVs often operate in regulated airspace and may be subject to specific security requirements. Adhering to these standards ensures that UAVs meet the necessary security protocols, mitigating potential risks to public safety and maintaining the trust of regulatory authorities and stakeholders. Notably, the human factor plays a crucial role in UAV cybersecurity. Human operators and stakeholders involved in UAV operations must be adequately trained and aware of cybersecurity best practices [5]. Weak passwords, susceptibility to social engineering attacks, and lack of proper security protocols can inadvertently introduce vulnerabilities into UAV systems. By addressing the human factor, organizations can reduce the risk of cyber breaches and enhance the overall security position of UAV operations.

Furthermore, the significance of cybersecurity in UAVs extends beyond the immediate operational and data protection concerns. The trust and public acceptance of UAV technology heavily rely on the assurance of robust cybersecurity measures. The general public and regulatory authorities must be confident that UAVs are not susceptible to malicious activities that could compromise privacy, national security, or public safety. Additionally, UAVs are increasingly being deployed in critical infrastructure sectors, such as transportation, energy, and emergency response. Cyberattacks on these UAVs could have far-reaching consequences, disrupting essential services and potentially causing significant economic and societal impacts [6]. Therefore, ensuring the cyber-resilience of UAVs becomes crucial for maintaining critical infrastructure systems' overall resilience and stability.

As UAVs are integrated into the airspace alongside semiautomatic aircraft, cybersecurity becomes a critical factor in maintaining the overall safety of aviation operations. A cyberattack on a UAV could potentially result in collisions or disruptions to air traffic control systems, posing risks to both UAVs and manned aircraft. By implementing robust cybersecurity measures, the aviation industry can effectively mitigate the risks and ensure the safe coexistence of UAVs and manned aircraft in shared airspace. Furthermore, the impact of cybersecurity in UAVs extends to various sectors and industries. In the commercial sector, businesses rely on UAVs for tasks such as aerial surveys, package delivery, and infrastructure inspection [7]. Any compromise in the cybersecurity of these UAVs could result in financial losses, theft of sensitive information, or disruption of business operations. Therefore, ensuring robust cybersecurity measures is essential for protecting companies' investments and intellectual property utilizing UAV technology.

In the military and defense sector, UAVs are crucial in surveillance, reconnaissance, and combat operations. The cybersecurity of military UAVs is paramount to protect classified information, prevent unauthorized access to sensitive systems, and maintain tactical advantage on the battlefield. The potential for cyberattacks on military UAVs raises concerns about national security and the potential compromise of military operations. Moreover, UAVs are increasingly being utilized in emergency response scenarios, such as search and rescue missions or disaster management. In these critical situations, the cybersecurity of UAVs becomes a matter of life and death [8]. Any interference or compromise of UAV systems could hinder emergency response efforts, jeopardizing the safety of responders and victims alike.

UAV cybersecurity is an important and current trend in the state-of-the-art industry due to the wide variety of UAV applications. The UAV has many advantages, such as its agility and ability to fly, which allow it to achieve momentum instantly; it can access hard-to-reach areas that might be hazardous for humans or that require an altitude [9]. The exponential growth in technology allows UAVs to be embedded with software, advanced sensors, and other gadgets and technologies that allow interdevice communication and connectivity to the Internet. This magnifies UAV users' cybersecurity and privacy concerns, mainly when used in the public domain [10]. Determining adequate algorithms for different security threats and attacks is needed to ensure the confidentiality, integrity, and availability (CIA) triad.

The significance of cybersecurity in UAVs is not limited to the present. As UAV technology advances and autonomous capabilities expand, the potential risks associated with cyberthreats also grow. Proactive measures and ongoing research in UAV cybersecurity are essential to stay ahead of emerging threats and ensure UAVs' long-term viability and safety. This review presents an overview of the cyberthreats faced by UAVs when these are applied in the public sphere. Other contributions of this review are as follows.

- The study presents background and technical terminologies used in this cyber domain, including the CIA triad; the model that considers spoofing, tampering, repudiation, information disclosure, denial of service (DoS), and elevation of privilege (STRIDE); and Process of Attack Simulation and Threat Analysis (PASTA) threat-based modeling.
- The study presents the currently proposed models for aiding cybersecurity in UAVs, demonstrating the type of threat, the proposed model, the solution description, and the application.
- The study further explores common UAV cybersecurity attacks, including eavesdropping, crashing, landing, media or file access, and hijacking. It illustrates the most common attack goals, such as password cracking and global positioning system (GPS) spoofing.
- The study investigates DoS attacks related to UAVs, including deauthentication attacks, deauthentication on CX-10W, man-in-the-middle attack on augmented reality (AR) drone, and unauthorized AR drone root control.
- Finally, the study presents future research directions in this research domain and lessons learned from the review.

The remainder of this study is structured as follows. In Section 2, a brief background is described, and the terminologies used, such as the STRIDE model, spoofing, tampering, repudiation, information disclosure, and DoS attacks, are described. Section 3 presents the related literature, detailing currently proposed models that aid cybersecurity in UAVs, demonstrating the type of threat, the proposed model, solution description, and application. Section 4 provides a detailed assessment of UAVs' common cybersecurity threats. Section 5 presents the future research direction and lessons from the study. Finally, Section 6 depicts the conclusion.

2. Background and Terminology

This section presents the background and terminologies used in the cyber domain concerning UAVs.

2.1. Background

UAV security attacks are prevalent as system vulnerabilities are exploited by cyberattackers for financial fulfillment or personal agenda [11]. Destruction of infrastructure and intellectual property theft are additional motives resulting from nation-state actors and industrial espionage [12, 13]. The most skilled attackers are sometimes employed by their state to secure the systems in case of any threats or targeted attacks. The time taken to detect a cybersecurity breach depends on several factors. Most currently, it has been discovered that cyberattacks in transmission layers

could compromise the network securities of entire control layers [14].

Cybersecurity invaders are aware of prevailing security threats and constantly enlighten possible attackers. Cyberattackers have various ranges of tools accessible, allowing them to bypass conventional security mechanisms [15]. For instance, the major task is to identify an appropriate feature to define the human's presence when images are taken by a UAV [16]. Studies are now implementing security learning algorithms within UAVs to strengthen cyber defense. Regulations and oversight (including cybersecurity) continue undeveloped, explicitly concerning the double use of civil UAVs that can be turned into armed drones for unlawful purposes [17].

Security holes are an unavoidable risk when it comes to UAVs. Initial detections are the superlative defensive mechanisms to survive an attack on the Internet of drones [18]. A security breach is any incident resulting in unlawful access to system data, networks, applications, and devices. Security professionals use UAV cybersecurity detection and prevention techniques to reduce the risk of cybersecurity breaches for UAV-enabled networks [19].

Techniques of detection are classified into two categories: anomaly based and signature based. Signature-based detection techniques monitor network traffic for current attacks [20]. Prevention techniques are emphasized to increase the difficulty of launching an attack. Prevention techniques include applying recent security updates, ascertaining a better security policy, launching influential user security literature, and avoiding default configurations [21].

2.2. Terminology

Several terminologies are used in the field of UAVs and cybersecurity aspects, which are defined herein.

2.2.1. CIA triad

The CIA Triad [22] represents confidentiality, integrity, and availability. The CIA Triad is a popular and respected model that forms the basis for developing security systems and policies. These are used to identify weaknesses and apply various methods to resolve problems and create effective security solutions. Confidentiality prevents unauthorized access to sensitive and personal information, while integrity focuses on detecting any modified data by any unauthorized party. In comparison, availability ensures that information is accessible to authorized users promptly when needed.

2.2.2. STRIDE model

The STRIDE model demonstrated in a previous paper [23] identifies computer security threats in six categories: spoofing, tampering, repudiation, information disclosure, DoS, and elevation of privilege. Every threat violates desirable properties in the system, including authenticity, integrity, nonrepeatability, confidentiality, availability, and authorization. A brief description of these threats is explained below.

2.2.2.1. Spoofing

An attack in which a program or person successfully identifies itself/himself/herself as another person by using falsified data to gain an illegitimate advantage. This security measure ensures that the exchanged message, document, or information is from the source it claims to be from.

2.2.2.2. Tampering

Usually, from a cybersecurity point of view, tampering refers to an intentional modification of data or products in a way that would make them harmful to the user.

2.2.2.3. Repudiation and information disclosure

This refers to the ability to deny the truth or the validity of something. For instance, nonrepudiation works by associating actions or changes with a unique individual. Information disclosure is the violation of confidentiality by privacy breaches or data leaks.

2.2.2.4. DoS attack

This works by flooding the targeted resource with requests with the aim of overloading it and preventing legitimate requests from being fulfilled.

2.2.2.5. Elevation of privilege (privilege escalation)

This happens through exploitation of a configuration oversight, design flaw, or a bug in an application or an operating system to gain elevated access to some resources that would generally be protected from this user or application.

2.2.3. Authorization

This security measure checks each user's privileges and access levels concerning the system resources.

The following section examines the state-of-art literature on the cybersecurity of UAVs and challenges. Summaries of these reviewed studies are presented in tabular format.

3. Related Literature

Cybersecurity in UAVs is of paramount importance across a wide range of sectors. It affects businesses, critical infrastructure, national security, emergency response, and future technological advancements. However, several issues challenge it, and some efforts have been undertaken, as presented below.

Cybersecurity and related attacks are prevalent when system vulnerabilities are exploited through cyberattackers for several purposes such as financial fulfillment [22]. Cybersecurity invaders know the prevailing security protocols and constantly enlighten possible attackers, and the latter have various ranges of tools accessible, allowing them to bypass conventional security mechanisms. Cybersecurity emphasizes the practical enforceability of cybersecurity policies, and the devices that get connected must be able to comply with these policies [23].

Cybersecurity attack recognition is one of the techniques used in modern UAVs and detections. Attack detections are classified into two categories: anomaly-based detection and signature-based detection. Such cybersecurity detections provide respectable protection against unknown threats. Networked traffic for current attacks is monitored through signature-based detection techniques but diminishes zero-attack detection. Even though 10 cybersecurity threat modeling approaches were examined during the study, different sources and target parts were not demonstrated. No single cybersecurity threat model method is recommended for a decision regarding the modeling methods, which should be based on the cybersecurity needs [24, 25].

Some UAVs extensively use global navigation satellite systems for locating targets. During the connection of UAVs to these satellites, some studies have demonstrated that cybersecurity attacks tend to occur due to their capacity to reach hard-to-reach areas. Besides their positives, several cybersecurity attacks, such as spoofing, exist on these UAVs, which reduces the efficiency of drone technology [26]. The study concludes by assessing the combination of artificial intelligence and drones, reviewing the current cybersecurity threat landscape, and UAV vulnerabilities regarding cyberattack techniques.

Evaluation of the cybersecurity control channels of the UAV was done using an illustration of DJI Tello. The DJI Tello is a consumer-based UAV targeting global consumer utilization [27]. According to the study's findings, a security strategy like deauthentication or dissociation frames was suggested. The maximum cybersecurity protection for UAVs comprises reactive detection and adaptive cybersecurity mitigation procedures [28].

A unique algorithm was provided for robust spherical object detection under different illumination conditions for situations such as cybersecurity threats. Invalidating the purported landing system and detection algorithm, eight flight tests were performed using a successful DJI Tello drone with an average height position error of 3 cm. The study never depicted anything about cybersecurity concerns, even though it is related to UAV security. When it comes to nodes within the network, cybersecurity classically involves the use of classical tools, e.g., firewalls, intrusion detection systems, and intrusion prevention systems, among others.

Due to technological advancement requirements, alternative security mechanisms, based on received signal strength indications and trilateration methods, are needed. However, a study demonstrated that it is quite complex to distinguish between malicious and regular traffics because of the advancement in cybersecurity attack techniques. The provided approach of the two-stage hybrid method to iron this cybersecurity issue focused on using the ensemble classifier and decision trees. The accuracy achieved was reported to be close to 99.9% over 10-fold cross-validation utilizing a multiclass approach, and further, a clear distinction between the cybersecurity threats was provided [29].

A bioinspired combination with game theory-centered flight control algorithms for a swarm for consumer-based UAVs was proposed. The proposed approach was centered on blocking networks on the primary channel while certifying that the transmitter is authentic based on its location [30]. The central drone connected by the two UAVs exchanges the essential information with them to compute the transmitter's location using the proposed models. Table 1 summarizes the surveyed literature and contains the challenges (issues) of cybersecurity, the methods, frameworks or algorithms, solution description, and technologies used during the experiment.

Based on the literature, most current approaches to UAV cybersecurity challenges are based on federated learning. One study used the federated

Table 1. Cybersecurity issues and proposed solutions

Issues	Method	Solution Description	Application	Reference
Intrusion detection in vehicular environments	Game theory-based approach	Detecting intruders generally, and nearby in the Vehicular ad hoc network (VANET) environment	Vehicular ad hoc network	[22]
Cybersecurity, privacy, and public safety	Enhancement in functionalities of unmanned aerial vehicles (UAVs)	Framework's overviews, followed in determining maturity at the international, regional, and national levels	Unmanned aircraft systems (UASs)/ UAVs	[23]
Traffic issues, and smart advancement	Surveillance cameras and sensor application	Efficient connected and autonomous vehicles need to exercise caution in the context of privacy and security	UAVs	[24]
Nonsecure communication	Machine learning	An edge-aided secure lightweight guarantee technique for safe interaction	Internet of drones	[25]
Infection monitoring and facial recognition	Pandemic situations (Covid-19)	Indisputably enhances drone design	Autonomous UAV deployment	[26]
Cyberattacks and counterattacks at airports	UAV deployment	Installing drone-supported facilities near areas such as airports	Drone-sensing technologies	[27]
Precise landing	A robust spherical-object detection algorithm	Installation of a camera on the platform controls the macro drones near the landing area	A DJI Tello drone	[28]
Intrusion detection	Advanced machine learning	A two-stage hybrid approach to regulating attack	Internet of things (IoT) networks	[29]
Effectiveness, flexibility, and vigor	Bio-inspired routing	Heterogeneous UAS swarm networking	UAVs	[30]
UAV authentication	Deep neural networks	Proposed a federated learning-based UAV authentication approach	UAVs	[31]

learning-aided UAV verification model with UAVs' radiofrequency features on Internet of things (IoT)-based networks, e.g., drone authentication [31]. Deep neural schemes are implemented for UAV authentication in conjunction with a gradient descent optimization accomplished in the vicinity of drones. The results demonstrated that the drone-based authentication approaches minimize computation compared to other authentication approaches [32, 33]. The study demonstrated that the cybersecurity hacker could cause irreparable damage and take complete control over the UAVs simply by compromising the communication network between the operator and the UAV. Table 1 summarizes some of the reviewed literature.

4. Common UAV Cybersecurity Attacks

In this section, we present some of the identified critical threats related to UAVs. Hijacking, crashing, or landing on demand are depicted to be the ultimate common targets for cybersecurity attacks.

Second is hijacking, which is prevalent in spoofing attacks, and DoS attacks involving crashing or landing are the most rampant. A simple demonstration of the attack targets using the STRIDE model (see Table 2) depicts the distribution of the attack targets, and Table 3 demonstrates the most common attack goals [23].

4.1. Password cracking attack

Cyberattacks against passwords have demonstrated an increase in more connected devices. Password cracking in commercial UAVs, as a simple example of UAV control and disclosed positive security flaws, is an authentication intrusion, and this attack can be known as identity spoofing. In the attack, the violators use intercommunication mechanism vulnerabilities to get into the device and use the control tools of the robot's functioning scheme [34].

4.2. Parrot Bebop 2 and DJI Phantom 4

Drone such as DJI's Phantom 4 Pro and Parrot's Bebop 2 have been vulnerable to many cyberattacks. Especially, the Phantom 4 Pro has two threats: DJI software development kit (SDK) and GPS spoofing [35].

4.2.1. SDK threat

The attackers track user authentication information and modify specific codes to allow malicious users to execute the operations of legitimate UAV users. This approach allows individuals to take pictures and videos to monitor the device [35]. This represents an attack on privilege escalation by allowing access to inaccessible features for unauthorized users.

4.2.2. GPS spoofing

The GPS is used in phantom models and is not encrypted. In addition, private GPS can be easily set. For this, the invader cracks the UAVs in the opponent's GPS parody and exchanges a fake GPS code with the UAV flight controller. The UAV remains under the complete control of the attacker in case the attacker succeeds. This attack could be carried out on a UAV without a device for detecting spoofing using the LabSat3 GPS simulator [35]. This is a noticeable STRIDE spoofing attack. There are also three specific Bebop 2 attacks, including open Wireless Fidelity (WiFi) and deauthorization.

4.2.3. Open WiFi

The Bebop UAVs have free WiFi, which gives many users access to the network. With this access, the team successfully hijacks the drone. We also found that the device allows multiple user connections so that multiple unauthenticated users can control the drone. After that, there is no way to verify the drone's owner [35].

4.2.4. Deauthentication

The system is disturbed by the unauthorized user by continuously sending deauthentication packets to the UAV, which block the entire network in turn. It further prohibits communication with other users except for enemies who can hijack the UAV [36]. A "*" denotes the type of cybersecurity attacks; spoofing and DoS are indeed prevalent types of UAV attacks, and there is no repudiation case in the literature assessment. This is a DoS attack to control the UAVs.

4.2.5. Telnet

If the intruder is using Telnet, the intruder will have direct access to the drone system. The intruder can manipulate

Table 2. Distribution of the cybersecurity attack targets

Attack	S	T	R	I	D	E
Eavesdropping	3	-	-	-	-	-
Crashing	3	-	-	-	4	-
Landing	1	-	-	-	4	-
Media or file access	-	-	-	1	-	1
Hijacking	6	1	-	1	1	-

STRIDE, spoofing, tampering, repudiation, information disclosure, denial of service (DoS), and elevation of privilege.

Table 3. Most common attack goals

Attack	S	T	R	I	D	E
Eavesdropping	2	-	-	-	-	-
Crash/land	3	-	-	-	4	-
Media or file access	-	-	-	1	-	1
Hijacking	5	1	-	1	1	-

STRIDE, spoofing, tampering, repudiation, information disclosure, denial of service (DoS), and elevation of privilege.

critical system files and shellcode scripts with Parrot to destroy the system [26]. In certain situations, an intruder can completely restart the drone; deactivating the motor will cause it to fall to the ground [37].

4.3. Man-in-the-middle attack

The UAV address can be reached by using a wireless network to transmit a packet with an acknowledgment from the UAV. A study hacked the connection by remotely changing the destination high (DH) and destination low (DL) parameters. The authors managed to hijack the connection between the UAV and the remote controller. They also reversed the flight computer and control program, set the envelope, and injected it into the flight machine [38].

4.4. DoS communication system

A study [39] was done on cybersecurity in a Parrot AR drone, which used a DoS intrusion tool for UAV communication. During the attempt, the author interrupted the user by sending a deauthentication key, and then a UAV memory filled the control. The controller avoided reconnecting to the system, and the UAV crashed. The study used the air-cracking script to perform the attack [39]. It is a DOS attack that crashes the UAV in a STRIDE configuration.

4.5. DoS attacks

This is a way to disconnect two network devices using all the bandwidth that the two network devices provide. The goal is to break into a particular service and deny access. Typically, it overloads the device's computing power or uses available bandwidth to prevent authorized users from doing so [40].

4.6. Parrot AR Drone 2.0 and Cheerson CX-10W

A survey on Cheerson CX-10W and Parrot AR Drone 2.0 was carried out; many hacking techniques were run in separate tests. Six successful attacks were reported. Both attacks used a network mapper (Nmap) scanner to collect reachable target devices [41].

4.6.1. Deauthentication attack

The attack is directed at the control system, and the device sends a deauthentication packet before the driver stops responding, signaling that the attack was successful. If the UAV's relationship with the transmitter is broken, the controller will receive a warning that the connection has been lost, and the UAV will stop at its current position [41]. This attack is a form of spoofing because an intruder can attack an authorized user and reconnect to the network after deauthentication.

4.6.2. Deauthentication on CX-10W

As mentioned earlier, an attack on the CX-10W with the same method was also launched. If the UAV and the transmitter are missing, the UAV crashes automatically [42]. It is also a spoofing attack.

4.6.3. Man-in-the-middle attack on AR Drone

The authors monitored the AR drone connection because they were targeting man-in-the-middle attacks using WiFi Nano Pineapple. The WiFi system was checked for access points, and it mimicked the point of contact of a pineapple instead of a UAV. User commands were sent to the UAV so that an attacker could monitor the user's actions without being recognized. Any other unsafe user-driven actions, such as Hypertext Transfer Protocol HTTP websites, can be tracked instead of a better-protected Hypertext Transfer Protocol Secure (HTTPS) alternative, making the application, similar to the UAV, vulnerable in case it is used in a man-in-the-middle attack [43].

4.6.4. Man-in-the-middle attack on CX-10W

The CX-10W is also targeted using the same attack approach. Thus, it is also a spoofing threat. The AR drone is marginally less susceptible than this system because the controller software is not linked to the network [44].

4.6.5. Unauthorized AR Drone root control

Two protocols were used for this study, such as File Transfer Protocol (FTP) and Telnet. The UAV was deactivated by accessing the operating system file system via Telnet (Busy Box). The user ID and password and many drone executables identified the data. This attack demonstrates an interruption as an attempt to divulge information as sensitive data are collected and sent to the attacker by an authorized user to hijack the UAV [44].

4.6.6. AR Drone packet spoofing

The spoofing node that is used in the AR drone's Python script mimics a UAV controller, and the author tracks the vehicle. First, the script is used to check the UAV controller's compatibility, examine the data packet, and identify the packet. Then, the hackers use another script to emulate the media access control (MAC) and Internet protocol (IP) addresses of the device. In case the IP and MAC addresses are correct, the drone will accept the attacker's command, so every detail is needed to force a UAV [45]. Packet spoofing attacks can be classified as spoofing threats with the STRIDE feature.

4.7. Bebop assault

Parrot Bebop drone has three vulnerabilities: buffer overflows, DoS, and address resolution protocol (ARP) cache poison attacks. A study used Nmap to evaluate Wireshark's network traffic, looking for available ports before the attack. These measures provided the author of the study with the media access control and IP addresses of the devices that the system would use to query the UAV controller [46].

4.7.1. Buffer overflow

In another study, the UAV's central processing unit (CPU) and memory consumption dropped to about 10 s. This indicates that the navigation system has collapsed, stopped, and crashed in the air [47]. This attack causes UAV memory overload and prevents users from accessing the system.

4.7.2. DoS assault

The study performed a DoS intrusion by submitting a UAV request that should be processed continuously. Up to 1000 submissions were rendered at the same time. Like a buffer overflow attack, UAVs collapse in navigation applications [48].

4.7.3. Cache poison

The communication signals are endlessly transmitted to the UAV channel during a cache poison attack. The message is impersonated by the IP and MAC address of the authorized controller at the first level. The UAV recognizes the valid and intruder signals: inconsistencies and interruptions. The communication. The UAV separates after 1 min [49]. It is a spoofing invasion as the intruder interacts with the UAV to emulate the device's signal.

4.8. Maldrone hacking

Maldrone is a software vulnerability explicitly developed for UAVs. The blog writer who hijacked DJI Phantom and Parrot AR Drone 2.0, during the attack, put Maldrone in the middle of the drone. This allows an individual to control the drone's launch location and cause malfunctions if necessary [50]. An overview of the current cybersecurity attacks in the STRIDE categories is demonstrated in Table 4.

Comprehensively structured methods for detection of device threats and prioritizing susceptibilities of the highest degree have been studied. Numerous illustrations include STRIDE and attack trees (conceptual illustrations demonstrating how an asset, in this case, cybersecurity, may be targeted or attacked [51]). abuser stories [52], cyber operations

Table 4. Overview of current cybersecurity attacks in the STRIDE categories

UAV Cybersecurity	S	T	R	I	D	E
Cybersecurity 4.1	*	-	-	-	-	-
Cybersecurity 4.2.1	-	-	-	-	-	*
Cybersecurity 4.2.2	*	-	-	-	-	-
Cybersecurity 4.2.3	*	-	-	-	-	-
Cybersecurity 4.2.4	-	-	-	-	*	-
Cybersecurity 4.2.5	-	-	-	-	*	-
Cybersecurity 4.3	*	-	-	-	-	-
Cybersecurity 4.4	-	-	-	-	*	-
Cybersecurity 4.5	-	-	-	-	*	-
Cybersecurity 4.6.1	*	-	-	-	-	-
Cybersecurity 4.6.2	*	-	-	-	-	-
Cybersecurity 4.6.3	*	-	-	-	-	-
Cybersecurity 4.6.4	*	-	-	-	-	-
Cybersecurity 4.6.5	-	-	-	*	-	-
Cybersecurity 4.7.1	-	-	-	-	*	-
Cybersecurity 4.7.2	-	-	-	-	-	-
Cybersecurity 4.7.3	*	-	-	-	-	-
Cybersecurity 4.8	-	*	-	-	-	-

STRIDE, spoofing, tampering, repudiation, information disclosure, denial of service (DoS), and elevation of privilege.

rapid assessment (CORAS) [53], and Common Vulnerability Scoring System [54]. Table 5 summarizes the goals and gears for any spoofing group attack and DoS.

5 Future Research Directions and Lessons Learned

In this section, notable research directions in the field of cybersecurity in UAVs, which are crucial to address emerging threats, improve existing security measures, and adapt to the evolving landscape of UAV technology, and the lessons learned are presented.

5.1. Future research directions

As the capabilities and applications of UAVs continue to expand, researchers and industry professionals are actively exploring innovative approaches to enhance cybersecurity in this domain; the following research is likely to shape the application.

To appreciate the current efforts that have been done to mitigate UAV cybersecurity threats: Cybersecurity frequently incorporates various skills to protect UAV cyber data security and privacy. The cybersecurity procedures involve numerous duties such as regulation creation, policy enforcement, and drafting procedures to secure UAV data governance [35]. During this global coronavirus disease-2019

Table 5. Goals and gears for any spoofing group attack and DoS

UAV Cybersecurity Attacks	Targets	Some Gear Any spoofing group attack	DoS	Tampering
Attack 4.1	Hacking	Adapter, joystick, ROS, WiFi network	-	-
Attack 4.2.1	Hacking	LabSat3 global positioning system (GPS) simulator	DJI software development kit (SDK)	-
Attack 4.2.2	Hacking	Unknown	-	-
Attack 4.2.3	Eavesdropping	Adapter, Xbee, universal serial bus (USB) to RS232, Python interpreter	DJI SDK	-
Attack 4.2.4	Eavesdropping	Xbee, Python interpreter	SDK	
Attack 4.2.5	Eavesdropping	868LP chip, Python interpreter	-	-
Attack 4.3	Crashing	WiFi network adapter, virtual machine (VM)	Hping3, Network, and LOIC	-
Attack 4.4	Hacking	Air-cracking	-	-
Attack 4.5	Crashing	-	Telnet	-
Attack 4.6.1	Landing	Air-cracking	-	-
Attack 4.6.2	Crashing	-	Air-cracking	-
Attack 4.6.3	Eavesdropping	WiFi pineapple nano	-	-
Attack 4.6.4	Eavesdropping	WiFi pineapple nano	-	-
Attack 4.6.5	Hacking	Not specified	-	-
Attack 4.7.1	Landing	Not specified	Not specified	-
Attack 4.7.2	Crashing	Not specified	Not specified	-
Attack 4.7.3	Crashing	Not specified	Not specified	-
Attack 4.8	Hacking	Maldrone software tool	-	None Specified

(COVID-19) pandemic, the Internet has revolutionized more businesses and social life habits regardless of the benefits. This conversion has resulted from connecting information and IoT-like UAVs into a network to connect people [36]. This increases the cybersecurity attacks since the majority are not aware of how to implement security within the business systems and, worst of all, on their portable devices, even if the security parameters are available though not activated.

In forthcoming years, UAV cybersecurity will be just as significant as it is today, if not more than today. The expanding Internet connectivity rate and complexities in modern systems' infrastructures are being manipulated with cybersecurity threats [35]. In the long run, these cybersecurity threats summarized in Table 3 put the economies, public cyber securities, commerce, and businesses at risk. Cybersecurity risk effects, such as reputational and financial risks, touch a company's bottom line, affecting revenue and driving up costs. Consequently, cybersecurity threats can limit the capability of organizations to revolutionize, contend, and enhance the reputation of their devices, such as UAVs. There is likely to be an increase in ransomware attacks due to monitoring of monetization [36]. Cryptocurrencies and the emergence of ransomware have made it easier for individuals to commit a crime and get away with it because they can get paid in untraceable ways.

5.1.1. Lightweight and adaptive encryption techniques

Future research should focus on developing lightweight encryption algorithms designed explicitly for resource-constrained UAVs. These algorithms should aim to provide robust security while minimizing computational overhead. Additionally, researchers are exploring adaptive encryption techniques that can dynamically adjust encryption parameters based on UAV system conditions, such as available resources and network conditions [37]. This research direction ensures secure and efficient communication between UAVs and ground control stations, protecting the confidentiality and integrity of data. Secure communication protocols and encryption techniques will protect sensitive information transmitted between UAVs and ground control stations, prevent unauthorized access, and safeguard data confidentiality during critical operations, such as surveillance, package delivery, and infrastructure inspections [39].

5.1.2. Enhanced authentication and access control mechanisms

Future research aims to develop advanced authentication and access control mechanisms tailored specifically for UAV systems. These mechanisms verify the identity and integrity of UAVs, ground control stations, and connected devices, preventing unauthorized access and reducing the risk of impersonation attacks [40]. This research direction ensures secure interactions within the UAV ecosystem, mitigating the potential for malicious activities and unauthorized control. Strong authentication and access control mechanisms will safeguard UAV operations by ensuring that only authorized entities can interact with the UAV system [41]. This is particularly important in critical applications, such as military operations and emergency response, where the integrity and reliability of UAV systems are crucial.

5.1.3. Intrusion detection and prevention systems

This approach involves innovation that focuses on developing sophisticated intrusion detection and prevention systems for UAVs [42]. These systems use machine learning and artificial intelligence techniques to detect anomalous behavior, identify unauthorized access attempts, and respond in real time. Intrusion prevention mechanisms, such as firewalls and intrusion response systems, are also being integrated into UAV systems to block and neutralize threats actively [43]. Intrusion detection and prevention systems will enhance the resilience of UAVs against cyberattacks, providing real-time threat detection and response [44]. This is vital when UAVs operate in sensitive environments or handle classified information, such as military surveillance or critical infrastructure inspections.

5.1.4. Secure wireless communication protocols and antijamming techniques

Future research should focus on developing secure wireless communication protocols for UAVs, which are resistant to interception, eavesdropping, and jamming attacks [45]. These protocols should use adaptive modulation and coding techniques, frequency hopping mechanisms, and advanced signal-processing algorithms to ensure reliable and

secure communication between UAVs and ground control stations, even in hostile environments. Secure wireless communication protocols and antijamming techniques will safeguard the integrity and availability of UAV communication links [46]. This is crucial in scenarios where UAVs operate in remote areas or in the presence of potential adversaries, maintaining reliable connectivity and protecting against unauthorized access or interference.

5.1.5. Resilient and self-healing UAV systems

Research should also focus on developing resilient UAV systems that can detect and mitigate cyberthreats autonomously. These systems incorporate self-diagnostic mechanisms, redundancy measures, and adaptive response capabilities to maintain system integrity and functionality even during cyberattacks [47]. This research direction aims to build UAVs with inherent resilience against cyberthreats, thus ensuring operation continuity and maintaining mission-critical capabilities in the face of cyberattacks [48]. This is particularly relevant in scenarios such as emergency response, where UAVs play a vital role in search and rescue missions or disaster management.

5.1.6. Human-centric approaches to cybersecurity

This includes developing training programs, security awareness campaigns, and guidelines for UAV operators and stakeholders to educate them on best practices, emphasizing the importance of strong passwords, secure configurations, and adherence to security protocols [49]. This research direction emphasizes the role of human operators and stakeholders in maintaining the security of UAV operations. Human-centric approaches to cybersecurity will minimize the risk of human-induced vulnerabilities and ensure that UAV operators and stakeholders actively contribute to maintaining secure UAV operations [50]. This is essential for preventing common pitfalls such as weak passwords, social engineering attacks, or negligence in security practices.

5.1.7. Threat intelligence and forensics for UAVs

This involves collecting and analyzing data on emerging cyberthreats targeting UAV systems, understanding attack vectors, and developing countermeasures [51]. Additionally, forensic analysis techniques for UAV systems are being explored to investigate and attribute cyberattacks, aiding in postincident analysis and recovery [52]. Threat intelligence and forensics for UAVs will enable proactive defense against emerging cyberthreats and facilitate identifying and mitigating attacks. It also helps provide evidence and insights for legal proceedings in the case of cyberattacks on UAV systems.

5.1.8. Compliance with regulations and standards

Future research should emphasize the importance of compliance with regulations and industry standards in UAV cybersecurity. Researchers are developing frameworks and guidelines that align with existing regulations and promote industrywide adoption of security best practices [53]. Compliance with regulations ensures that UAVs meet the necessary security protocols, mitigating potential risks to public safety and maintaining trust from regulatory authorities and stakeholders. This is crucial for maintaining the trust of stakeholders, adhering to legal requirements, and fostering a secure and reliable UAV ecosystem [54]. These future research directions in cybersecurity for UAVs focus on lightweight encryption, authentication, intrusion detection, wireless communication, resilience, human-centric approaches, threat intelligence, forensics, and compliance. The applications of these research directions span various sectors, including commercial applications, critical infrastructure, military operations, emergency response, and regulatory compliance, ultimately ensuring UAVs' security, reliability, and trustworthiness in the face of evolving cyberthreats [55].

5.2. Lessons learned from the review

These lessons provide valuable insights into the key challenges and considerations in UAV cybersecurity. As summarized herein, by addressing these lessons and implementing appropriate security measures, stakeholders can enhance the resilience and protection of UAV systems against cyberthreats.

5.2.1. Vulnerabilities in communication channels

Most studies have highlighted the susceptibility of UAV communication channels to interception and unauthorized access. It has been observed that weak encryption, lack of authentication protocols, and

insufficient access controls can expose UAV systems to cyberthreats. Lesson learned: robust encryption, authentication mechanisms, and secure communication protocols are essential to protect UAV communication channels from unauthorized access and data interception.

5.2.2. Firmware and software security

UAV surveys have revealed vulnerabilities in firmware and software components. Outdated software, unpatched vulnerabilities, and insecure coding practices can create entry points for cyberattackers. The surveys demonstrate that regular firmware and software updates, adherence to secure coding practices, and vulnerability management are crucial to minimizing the risk of cyberattacks on UAV systems.

5.2.3. Physical access and tampering

The review has shown that physical access to UAVs can lead to tampering and compromise of the system. Unauthorized individuals gaining physical access to UAVs can manipulate hardware components, inject malicious code, or extract sensitive information. Implementing physical security measures such as tamperproof designs, secure storage facilities, and restricted access protocols is essential to prevent physical tampering and unauthorized modifications to UAVs.

5.2.4. Lack of security awareness

Studies have highlighted the lack of security awareness among UAV operators and stakeholders. Many operators may not fully understand the potential cyber risks associated with UAVs, leading to inadvertent security lapses. Thus, conducting security awareness programs and training sessions and providing guidelines on secure practices can improve the overall security position of UAV systems by raising awareness and promoting responsible behavior among operators and stakeholders.

5.2.5. Integration with existing cybersecurity infrastructure

The review has identified challenges in integrating UAVs into existing cybersecurity infrastructures. UAV systems often require unique security solutions due to their distinct characteristics and operational requirements. Compatibility issues, lack of interoperability, and limited integration with existing security frameworks have been reported. Consequently, developing standardized security frameworks and protocols that specifically address the unique requirements of UAVs can facilitate seamless integration and improve overall cybersecurity in UAV operations.

5.2.6. Insider threats

Surveys have highlighted the potential risks posed by insider threats in UAV operations. Insiders with authorized access to UAV systems, such as operators or maintenance personnel, may intentionally or unintentionally engage in malicious activities that compromise the security of the UAVs. Lesson learned: implementing access controls, user activity monitoring, and periodic security audits can help detect and prevent insider threats, ensuring the integrity and security of UAV systems.

5.2.7. Regulatory compliance

Studies have emphasized the importance of regulatory compliance in UAV cybersecurity. UAV operations are subject to regulations and standards that aim to ensure the safety and security of operations. Failure to comply with these regulations can result in vulnerabilities and increased risks. Adhering to relevant regulations, standards, and industry best practices is crucial to maintaining high cybersecurity in UAV systems. Compliance helps mitigate risks, ensures accountability, and promotes a security culture within the UAV industry.

6. Conclusions

This study presented several cybersecurity vulnerabilities for contemporary UAVs. These vulnerabilities are more vivid in communication, control, surveillance, and navigation of equipment of present-day UAVs. A few cyberthreat analyses and assessment algorithms were presented. The approach used to assess the UAV's cybersecurity hazards was the STRIDE model (the model popular for identifying computer security-related threats) connected with the considered threats. Emphasis was laid further on the evaluation depending on the accuracy in cybersecurity mission definition, potential intruders, and social and other human-related situations. The study discovered that newer devices get connected to the Internet without activating cybersecurity parameters, and that greater level of cybersecurity breach is evidenced in the

global Internet village. Nowadays, the majority are either delightfully unaware of the cybersecurity threats from cyberattacks or have acknowledged the consequences of putting their whole lives into a digital environment. Publicity regarding personality theft, information (data) breaches, and leaking of sensitive data and photos do not seem to have transformed our enthusiasm to store our most sensitive information in the cloud. The certainty is that cybersecurity offenders are aware of this and this will boost how they manipulate humanity without caring whether they damage us. Studies have provided valuable insights into the vulnerabilities and lessons learned in UAV cybersecurity, highlighting the need for robust encryption, secure communication protocols, firmware and software updates, physical security measures, security awareness programs, integration with existing cybersecurity infrastructure, mitigation of insider threats, and adherence to regulatory compliance. By incorporating these lessons and implementing appropriate security measures, we can enhance UAV systems' resilience, integrity, and trustworthiness, ensuring their safe and secure operation in the face of evolving cyberthreats.

References

[1] T. Vyas, and H. R. Varia, "Impact of Construction Work Zone on Urban Traffic Environment," International Journal on Smart Sensing and Intelligent Systems, 2023, vol. 16, no. 1.

[2] S. Lee, H. Yeo, and M. Kang, "Biometric authentication sensor with an encryption module for prevention of h/w hacking in digital custody services," International Journal on Smart Sensing and Intelligent Systems, 2023, vol. 16, no. 1.

[3] W. Shafik, "Cyber Security Perspectives in Public Spaces: Drone Case Study," In Handbook of Research on Cybersecurity Risk in Contemporary Business Systems, 2023, pp. 79–97. IGI Global.

[4] A. K. Arora, S. Mahajan, M. Verma, and D. Haridas, "Study of structural and morphological properties of RF-sputtered SnO thin films and their effect on gas-sensing phenomenon," International Journal on Smart Sensing and Intelligent Systems, 2023, vol. 16, no. 1.

[5] W. Shafik, "A Comprehensive Cybersecurity Framework for Present and Future Global Information Technology Organizations," In Effective Cybersecurity Operations for Enterprise-Wide Systems, 2023, pp. 56–79. IGI Global.

[6] A. Yudhana, A. D. Cahyo, L. Y. Sabila, A. C. Subrata, and I. Mufandi, "Spatial distribution of soil nutrient content for sustainable rice agriculture using geographic information system and Naïve Bayes classifier," International Journal on Smart Sensing and Intelligent Systems, 2023, vol. 16, no. 1.

[7] S. N. Alaziz, B. Albayati, AAAH El-Bagoury, and W. Shafik, "Clustering of COVID-19 Multi-Time Series-Based K-Means and PCA With Forecasting," International Journal of Data Warehousing and Mining (IJDWM), 2023, vol. 19, no. 3, pp. 1–25.

[8] W. Shafik, "Making Cities Smarter: IoT and SDN Applications, Challenges, and Future Trends," In Opportunities and Challenges of Industrial IoT in 5G and 6G Networks, 2023, pp. 73–94. IGI Global.

[9] R. Majeed, N. Abdullah and M. Mushtaq, "IoT-based cyber-security of drones using the naïve bayes algorithm," International Journal of Advanced Computer Science and Applications, 2021, vol. 12, pp. 422–427.

[10] W. Shafik, S. M. Matinkhah, and M. N. Sanda, "Network resource management drives machine learning: a survey and future research direction," Journal of Communications Technology, Electronics and Computer Science, 2020, pp. 1–15.

[11] Y. Jun, A. Craig, W. Shafik, and L. Sharif, "Artificial intelligence application in cybersecurity and cyberdefense," Wireless Communications and Mobile Computing, 2021, pp. 1–10.

[12] E. Basan, A. Basan, A. Nekrasov, C. Fidge, J. Gamec et al., "A self-diagnosis method for detecting UAV cyberattacks based on analysis of parameter changes," Sensors, 2021, vol. 21, no. 2.

[13] A. Abdelmaboud, "The internet of drones: requirements, taxonomy, recent advances, and challenges of research trends," Sensors, 2021, vol. 21, no. 17.

[14] B. Ly and R. Ly, "Cybersecurity in unmanned aerial vehicles (UAVs)," Journal of Cyber Security Technology, 2021, vol. 5, no. 2, pp. 120–137.

[15] Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam et al., "Cybersecurity attacks in vehicular sensors," IEEE Sensors Journal, vol. 20, no. 22, pp. 13752–13767, 2020.

[16] M. Ghasemi, M. Varshosaz, S. Pirasteh and G. Shamsipour, "Optimizing sector ring histogram of oriented gradients for human injured detection from drone images," Geomatics, Natural Hazards and Risk, 2021, vol. 12, no. 1, pp. 581–604.

[17] K. Kim, J. S. Kim, S. Jeong, J. H. Park and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," Computers & Security, 2021, vol. 103, pp. 102150.

[18] L. Abualigah, A. Diabat, P. Sumari and A. H. Gandomi, "Applications, deployments, and integration of internet of drones (IoD): a review," IEEE Sensors Journal, 2021, vol. 21, no. 22, pp. 25532–25546.

[19] I. U. Khan, A. Abdollahi, R. Alturki, M. D. Alshehri, M. A. Ikram et al., "Intelligent detection system enabled attack probability using markov chain

in aerial networks," Wireless Communications and Mobile Computing, 2021, pp. 1–9.

[20] M. R. Khosravi and S. Samadi, "Mobile multimedia computing in cyber-physical surveillance services through UAV-borne Video-SAR: A taxonomy of intelligent data processing for IoMT-enabled radar sensor networks," Tsinghua Science and Technology, 2021, vol. 27, no. 2, pp. 288–302.

[21] G. Lykou, D. Moustakas and D. Gritzalis, "Defending airports from UAS: a survey on cyber-attacks and counter-drone sensing technologies," Sensors, 2020, vol. 20, no. 12.

[22] K. Fenrich, "Securing your control system: the" CIA triad" is a widely used benchmark for evaluating information system security effectiveness" Power Engineering, 2008, vol. 112, pp. 44–49.

[23] S. Hussain, A. Kamal and S. Ahmad, "Threat modeling methodologies: a survey," Science International, 2014, vol. 26. No. 4, pp. 1607–1609.

[24] N. Shevchenko, T. A. Chick and P. O'riordan, "Threat modeling: a summary of available methods," 2018.

[25] M. Mahuza, M. Y. Idris, A. W. Wahab, T. Nandy, I. B. Ahmedy et al., "An edge assisted secure lightweight authentication technique for safe communication on the Internet of drones network," IEEE Access, 2021, vol. 9, pp. 31420–31440.

[26] U. J. Butt, W. Richardson, M. Abbod, H. M. Agbo and C. Eghan, "The deployment of autonomous drones during the covid-19 pandemic," Cybersecurity, Privacy and Freedom Protection in the Connected World, 2021, pp. 183–220.

[27] A. Almulhem, "Threat modeling of a multi-UAV system," Transportation Research Part A: Policy and Practice, 2020, vol. 142, pp. 290–295.

[28] D. Lee, W. Park and W. Nam, "Autonomous landing of micro unmanned aerial vehicles with landing-assistive platform and robust spherical object detection," Applied Sciences, 2021, vol. 11, no. 18, pp. 8555.

[29] T. Saba, T. Sadad, A. Rehman, Z. Mehmood and Q. Javaid, "Intrusion detection system through advance machine learning for the internet of things networks," IT Professional, 2021, vol. 23, no. 2, pp. 58–64.

[30] J. Wang, Y. Liu, S. Niu, H. Song, "Bio-inspired routing for heterogeneous unmanned aircraft systems (UAS) swarm networking," Computers & Electrical Engineering, 2021, vol. 95, pp. 107401.

[31] A. Yazdinejad, R. M. Parizi, A. Dehghantanha and H. Karimipour, "Federated learning for drone authentication," Ad Hoc Networks, 2021, vol. 120, pp. 102574.

[32] G. S. Ilgi and Y. Kirsal Ever, "Chapter Eleven - Critical analysis of security and privacy challenges for the Internet of drones: a survey," Drones in Smart-Cities, 2020, pp. 207–214.

[33] A. Javaid, "Cyber security threat analysis and attack simulation for unmanned aerial vehicle network," Doctoral dissertation, University of Toledo, 2015.

[34] C. Rani, H. Modares, R. Sriram, D. Mikulski and F. L. Lewis, "Security of unmanned aerial vehicle systems against cyber-physical attacks," Journal of Defense Modeling and Simulation, 2016, vol. 13, no. 3, pp. 331–42.

[35] A. Shafique, A. Mehmood and M Elhadef, "Survey of security protocols and vulnerabilities in unmanned aerial vehicles," IEEE Access, 2021, vol. 9, pp. 46927–46948.

[36] S. P. Arteaga, L. A. M. Hernández and G. S. Pérez, "Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo," IEEE Access, 2019, vol. 7, pp. 51782–51789.

[37] K. Afzal, R. Tariq, F. Aadil, Z. Iqbal, N. Ali et al., "An Optimized and Efficient Routing Protocol Application for IoV," Mathematical Problems in Engineering, 2021.

[38] Y. Xu, G. Deng, T. Zhang, H. Qiu and Y. Bao, "Novel denial-of-service attacks against cloud-based multi-robot systems," Information Sciences, 2021, vol. 576, pp. 329–344.

[39] J. Tian, B. Wang, R. Guo, Z. Wang, K. Cao et al., "Adversarial Attacks and Defenses for Deep Learning-based Unmanned Aerial Vehicles," IEEE Internet of Things Journal, 2021, vol. 9, no. 22, pp. 22399–22409.

[40] T. A. Youssef, G. A. Francia III and H. E. Sevil, "Data Collection and Generation for Radio Frequency Signal Security," Advances in Security, Networks, and Internet of Things, 2021, pp. 745–758.

[41] W. Shafik, S. M. Matinkhah, and M. Ghasemzadeh, "Internet of things-based energy management, challenges, and solutions in smart cities," Journal of Communications Technology, Electronics and Computer Science, 2020, vol. 27, pp. 1–11.

[42] A. Graham, H. Kutzli, T. C. Kulig and F. T. Cullen, "Invasion of the drones: a new frontier for victimization," Deviant Behavior, 2021, vol. 42, no.3, pp. 386–403.

[43] A. Shoufan, C. Yeun, C. Yeob and B. Taha, "eSIM-Based authentication protocol for UAV remote identification," Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications, 2021, pp. 91–122.

[44] I. W. Alluhybi and H. O. H. Alhazmi, "Towards a threat model for unmanned aerial vehicles," Intelligent Computing and Innovation on Data Science. Springer, Singapore, 2021, pp. 319–328.

[45] G. Christophe, M. Royer and N. Larrieu, "Machine learning and software defined network to secure communications in a swarm of drones," Journal of Information Security and Applications, 2021, vol. 61 pp. 102940.

[46] M. H. Ismael "Authentication and encryption drone communication by using HIGHT lightweight

algorithm." Turkish Journal of Computer and Mathematics Education, 2021, pp. 5891–5908.

[47] K. Bong-Han, "Implementing a fuzzing agent to dectect buffer overflow vulnerability," Journal of the Korea Convergence Society, 2021, vol. 12, pp. 11–17.

[48] K. V. Raghavender and P. Premchand, "Accurate and reliable detection of DDoS attacks based on ARIMA-SWGARCH model," International Journal of Information and Computer Security, 2021, pp. 118–135.

[49] A. V. Priya and H. K. Singh, "Mitigation of ARP Cache Poisoning in software-defined networks," Advances in Smart System Technologies, 2021, pp. 85–94.

[50] H. P. D. Nguyen and D. D. Nguyen, "Drone application in smart cities: The general overview of security vulnerabilities and countermeasures for data communication," Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead, 2021, pp. 185–210.

[51] B. Kordy, L. Piètre-Cambacédès and P. Schweitzer, "DAG-based attack and defense modeling: don't miss the forest for the attack trees," Computer Science Review, 2014, pp. 1–38.

[52] A. Singhal and H. Banati, "Fuzzy logic approach for threat prioritization in agile security framework using the DREAD model, Defence Technology, 2021.

[53] M. S. Lund, B. Solhaug and K. Stølen, "Model-driven risk analysis: the CORAS approach," Springer Science & Business Media, 2010.

[54] P. Johnson, R. Lagerström and M Ekstedt, "Can the common vulnerability scoring system be trusted? A Bayesian analysis," IEEE Transaction on Dependable Secure Computer, vol. 15, no. 6, 2016, pp. 1002–1015.

[55] R. Von Solms and J. Van Niekerk, "From information security to cyber security," Computers & Security, 2013, vol. 38, pp. 97–102.