A Comprehensive Analysis of Security Challenges and Solutions in the Internet of Drones: Recent Trends and Development

Amine Hedfi[1], Aida Ben Chehida Douss[2], Ryma Abassi[3], Mohamed Aymen Chalouf[4], Om Saad Hamdi[5]
University of Carthage-Higher School of Communications of Tunis,
LR11TIC03 Innov'COM Innovation of Communicant and Cooperative Mobiles Laboratory, Tunisia[1, 2, 3]
University of Tunis El Manar, National Engineering School of Tunis, El Manar, Tunisia[2]
University of Rennes, IRISA Laboratory, 22300 Lannion, France[4]
IEEE member, IMT Atlantique, 33500 Cesson Sevigne, France[5]

***Abstract*—The Internet of Drones (IoD) is a decentralized structure that links drones to regulate airspace and offer inter-location navigation services. With the increasing use of drones in both civilian and military applications, the importance of the IoD has grown significantly. It reshapes the current internet landscape, making it more extensive and all-encompassing. IoD establishes a connection between drones and the network, which exposes the IoD network to numerous privacy and security issues often associated with IoT ecosystems. To ensure optimal performance from IoD applications, it is crucial to maintain a secure environment devoid of privacy and security risks. Privacy and security concerns have obstructed the overall effectiveness of the IoD framework. This study conducts an extensive examination of security concerns and solutions related to IoD security. It delves into IoD-specific security requirements and sheds light on the latest developments in IoD security research. Hence, we first provide an overview of the overall context and structure of the IoD. We then identify the security issues linked to it. Afterward, we present the most recent security measures developed specifically for the IoD. Finally, we go through the challenges and potential areas for future research in the realm of IoD security.**

***Keywords*—Unmanned Aerial Vehicle; Internet of Drones; cybersecurity; attacks; threats**

I. Introduction

The recent progress in robotics and wireless communication has given rise to Unmanned Aerial Vehicle (UAV) technology. UAV, commonly known as a drone, is an aircraft that operates without a human pilot and is controlled remotely by a user or a control station [1]. Primarily, drones have found application in the military sector, where they are utilized for monitoring insurgents, conducting surveillance on terrorists, assisting in the rescue of injured personnel, etc. According to the E.U. Commission Delegated Regulation 2019/945 [2], a UAV consists of two primary components: an unmanned aircraft and a remote-control device.

Generally, UAV come outfitted with a Global Positioning System (GPS) and various sensors for data acquisition, with their storage and battery capabilities being relatively constrained [3]. Communication between UAVs and other entities, such as remote users or control stations, is established through wireless channels, forming the Internet of Drones network.

The Internet of Drones (IoD) is a subset of the Internet of Things (IoT) designed to facilitate communication and cooperation among UAVs. As a result, it inherits from the security vulnerabilities IoT networks. As the data exchanged within the IoD may contain sensitive and critical information, security is a major concern in this area [4]. This is because UAV are usually operated remotely and receive control and command signals from ground sites. These command-and-control signals are transmitted through different means of communication and with different transmission rates, which requires significant efforts to manage and control quality and security in a context of high mobility which could complicate these tasks (control and management). Critical data exchanged between UAV must not be disclosed or compromised in any way. Given the diversity of attacks that can target the IoD (Jamming, Flooding, Collision, Selective forwarding, replay, identity theft, tracing, etc.), it becomes essential to establish security measures by deploying protection mechanisms adapted to secure it [5][6]. Thus, confidentiality, integrity, availability, authenticity, and preservation of privacy represent the main security requirements of the IoD. Several research studies have focused on IoD security [5]. Despite the diversity (new authentication schemes, blockchain-based security, etc.) and relevance of existing solutions, we believe that much remains to be done in the field of IoD security. Indeed, the implementation of certain protection mechanisms can constitute an obstacle to the proper functioning of the IoD or, if necessary, cause the degradation of the performance and efficiency of the services provided by UAVs. For example, security has a potentially significant cost in terms of CPU, memory, and power consumption.

As UAVs are battery operated, battery life can be another constraint and a major problem, part of the solution of which can be the use of energy-efficient batteries (lithium-ion and hydrogen batteries [7]), the harvesting of (Energy Harvesting), the use of solar cells or wireless energy transfer [7]. Thus, it may be relevant to minimize the impact of security on the energy consumption of UAVs.

The primary objective of this study, which is described in Section I, is to offer a comprehensive and up-to-date survey of the fundamental concepts pertaining to communication within the IoD. In an era where UAVs are becoming increasingly integrated into our daily lives, understanding the intricacies of how these devices communicate and collaborate is of paramount importance. By exploring the latest advancements, protocols, and technologies employed in enabling seamless data exchange among drones and between drones and ground-based systems, this study attempts to provide a valuable reference for researchers, practitioners, and policymakers, addressing their needs and interests in Section II. In Section III of this study, we present a comprehensive examination of the security requirements and constraints that belong to the IoD (Confidentiality, Availability, Integration, etc.). Following our exploration of security requirements and constraints in the IoD, this study will shift its focus to hidden security vulnerabilities for IoD systems, as well as potential attack vectors targeting this emerging technology. Security vulnerabilities in the IoD environment can arise from a variety of sources. We will begin by identifying and examining common vulnerabilities associated with the communication infrastructure of IoD networks. These might include weaknesses in wireless communication protocols, flaws in encryption algorithms, or vulnerabilities in the underlying hardware and software of the drones themselves. By explaining these vulnerabilities, we provide a comprehensive view of the potential weaknesses that adversaries may exploit. Simultaneously, our discussion will encompass potential attack surfaces within IoD systems. This involves identifying and characterizing the various components and interfaces that can be targeted by malicious actors. Examples of attack surfaces in IoD may include command and control channels (C2), transmission links, and even the physical drones themselves. It is imperative to understand these attack surfaces to effectively mitigate and defend against potential threats. Finally, we undertake a comprehensive survey of recent advancements in the realm of existing security solutions designed to address and mitigate the diverse spectrum of attacks discussed earlier in Section IV. Among the various categories of available security solutions, we will showcase the most and widely adopted solutions in the IoD, including intrusion detection systems, cryptographic measures, authentication methods, and the utilization of the Blockchain mechanism. At the end of the study (Section V), recommendations and challenges are proposed to find possible solutions to secure the IoD.

This research aims to answer six research inquiries depicted in Fig. 1. While it's evident that numerous other questions could be raised, we support that these are adequate to inform a diverse spectrum of research within the examined domain.

RQ1: What are the fundamental principles concerning communication and classification in the context of the IoD, and what are the areas and sectors of application?

RQ2: What security prerequisites and limitations exist within the IoD?

RQ3: What are the security weaknesses present within an IoD network, and what are the possible consequences of assaults on drone systems?

RQ4: What are the attacks targeting the IoD network?

RQ5: What are the current countermeasures in place to mitigate these attacks?

RQ6: What are the recommendations and challenges to find possible solutions to secure the IoD?

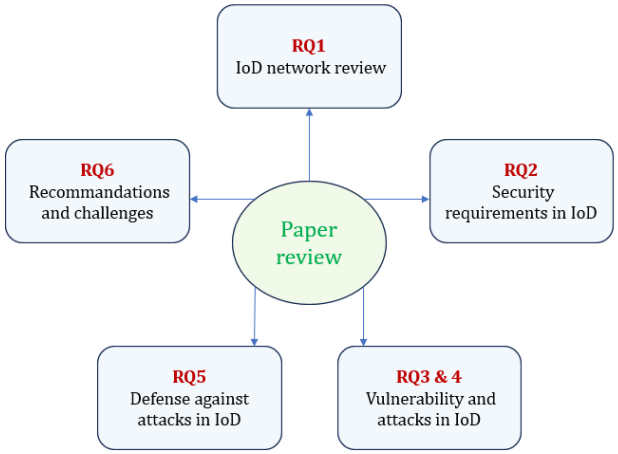

Fig. 1. Research inquiries of the study.

II. Unmanned Aerial Vehicles (UAV)

In recent years, UAVs have garnered considerable attention due to their versatility and autonomous capabilities. Recently, the United States' Federal Aviation Administration (FAA) has introduced fresh regulations permitting the utilization of drones for civilian and business applications. Consequently, the FAA anticipates that approximately seven million drones are presently in operation within the United States [8]. Drones can be remotely operated using a range of electronic devices, including microprocessors and sensors [9]. A key advantage of the drone is its ability to autonomously perform operations in hazardous environments where human intervention would be unsafe or impractical [10].

A. Architecture of Unmanned Aerial Vehicle Communication

As shown in Fig. 2 and described in [11, 12–14, 15-17], the typical representation of a UAV includes a UAV, flight controller, communication links, and either a ground command and control system or Ground Control Station (GCS) [15, 16, 18, 19]. Let us now provide a brief overview of each of these components:

- Flight controller: It is considered as the main processing unit of the drone. It can also be equipped with different sensors, like sensor units such as global positioning system (GPS) receivers, accelerometers, infrared cameras, gyroscope, magnetic orientation, and electro-optical sensors.
- Ground Control Station: It provides human operators with the tools they need to remotely control and monitor drones during missions.
- Data Link: It is used to communicate and control the data flow between the ground control station and the drone.

Drone communications can be classified into four distinct categories: Drone-To-Ground Station, Drone-To-Network, Drone-To-Satellite, and Drone-To-Drone (see Fig. 2). These categories represent different modes of communication that enable drones to establish connections with various entities. [17]

Drone-To-Ground Control Station: This method of communication uses well-known and standardized communication protocols such as Wireless communication (WiFi, Ad-Hoc, Satellite). However, most of these types of communications are public and unsecured, which exposes them to many types of attacks.

- Drone-To-Network: This method of communication allows users to select a network based on the level of security they require. Cellular communication can also be included.
- Drone-To-Satellite: The GPS network uses this type of communication to send coordinates in real-time. This allows any drone to be called back to its home station if it has wandered beyond the control line. Satellite communications are considered safe and reliable. However, they are expensive and require a lot of maintenance.
- Drone-To-Drone: It can be considered P2P (peer-to-peer) communication, which makes it prone to various P2P attacks.

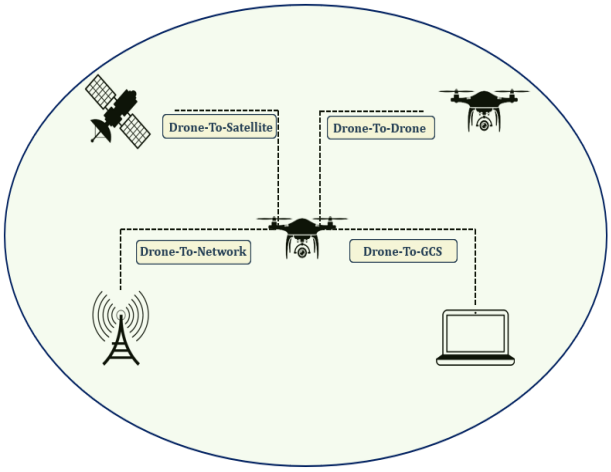

Fig. 2. Communication architecture for most UAVs.

B. Unmanned Aerial Vehicle Classification

UAVs have several requirements, such as being able to deploy sensors having a global positioning system (GPS), a communication module, and efficient batteries. UAVs can be controlled autonomously without a pilot and can be controlled remotely [18]. UAVs come in a variety of configurations, equipment options, sizes, ranges, and shapes. Within the market, we can find UAVs with varying numbers of rotors or propellers, as detailed in Table I [19]. Moreover, UAVs have been designed with diverse engines and wing structures. In terms of communication capabilities, they can utilize both short and long-range wireless technologies. UAVs are also classified based on their size, ranging from nano to micro and large.

Moreover, different types of UAVs can be found in the literature: fixed-wing, single rotor, fixed-wing hybrid, and multirotor [20]. Fixed-wing UAVs [21] contain a main body, wings, a propeller and a motor. These UAVs are often used for aerial mapping and power line inspection and need special training to control, and they remain useless for aerial surveillance. Such drones are not capable of hovering or forward flight. However, single-rotor drones [22] are costly to produce and need skill training. These UAVs are mechanically difficult and susceptible to obstacles such as vibrations.

Furthermore, multirotor drones [23] are the most affordable and simple to build. These UAVs are often employed for image and video surveillance. The Hybrid-Wing drone [24] is a fixed-wing and rotating drone that has recently entered the market. This type of drone can quickly reach its target by gliding through the air and hovering with four rotors.

TABLE I. CATEGORIES OF DRONES BASED ON THE NUMBER OF PROPELLERS

Types of drones	Number of Propellers
Octo-copter	8
Hexa-copter	6
Quad-copter	4
Tri-copter	3

C. Communication Methods of Unmanned Aerial Vehicles

When discussing the communication aspect of UAVs, several crucial subcomponents come into focus, including communication protocols, network types, and the UAV model itself. It should be noted that changing the communication method can introduce variations in the number of components and alter the system architecture [25]. Various researchers have proposed different topologies and designs [26], with consideration for altitude range. The choice of communication module and protocol may vary depending on the mission and the nature of the task at hand [27]. Furthermore, the emergence of 5G networks has addressed several constraints such as data rate, latency, and coverage. This advancement in communication technology has not only improved these areas but also enhanced the positioning and control of UAVs in critical rescue and surveillance missions. Advanced flight controls, multiple sensors, camera placement, and different modes of control and communication based on altitude have been employed for these purposes.

D. Unmanned Aerial Vehicle in 5G and IoT Networks

With the rapid advancements in UAV technology, UAVs have established their significance in a wide range of applications, including environmental monitoring, wireless communication, and public safety. Moreover, UAVs have been extensively studied in conjunction with wireless networks and have shown promising potential for enhancing the energy and spectrum efficiencies of fifth generation (5G) wireless networks. They provide a flexible and on-demand platform for deploying aerial base stations. The unique attributes of UAVs, such as adaptive altitude, scalability, flexibility, mobility, high

resilience, high reliability, and low cost, make them suitable for various applications. The integration of UAVs into network systems is expected to achieve significant performance improvements compared to conventional terrestrial systems without UAVs. UAVs can be intelligently controlled and remotely operated as required. They offer a high probability of line-of-sight (LoS) communication, which greatly enhances transmission rates. The swift maneuverability of UAVs ensures reliable and broadband wireless coverage during live streaming events and natural disasters. As a result, UAVs can provide offloading services with strict requirements in emergency operations within 5G networks [28]. Given their capabilities, it is feasible to integrate UAVs into 5G networks. Extensive research efforts are underway to explore UAV-assisted 5G technology and reduce latency while extending network coverage, capacity, and energy efficiency. However, there are certain challenges to consider in this coexistence. UAVs are susceptible to interference, and the dynamic network topology and mobility of UAVs introduce spatial and temporal dynamics that can result in frequent intermittent connections or transmission failures [29]. Additionally, UAVs are utilized for wireless energy transfer (WET) and wireless information transfer (WIT) to power ground terminals such as IoT devices, which are integrated for developing flexible and sustainable 5G networks [30]. UAVs provide numerous advantages when integrated into IoT networks [31, 32, 33]:

- Enhanced maneuverability, autonomy, speed, flight time, and mechanical performance.
- Efficient data gathering from water, gas, and power meters.
- Real-time data collection on air quality in smart cities.
- Reliability, scalability, and agility for IoT initiatives.
- Mitigating connectivity issues and reducing IoT network overhead.
- Cost-effectiveness and suitability for emergency operations.
- A comprehensive study addressing these UAV-related challenges is presented in [34].
- Channel modeling challenges and the need for accurate channel state knowledge.
- Efficient energy management for IoT device batteries.
- Adaptation of communication strategies to dynamic sensing data.
- UAV maneuverability limitations and potential mission impact.
- Concerns related to sky pollution, physical collisions, safety, privacy, and regulations.

E. Unmanned Aerial Vehicle Application Areas

UAVs have demonstrated their potential across a wide range of applications, including personal use and military purposes. Equipping UAVs with cameras, smart sensors, and processors can enhance their efficiency in various missions. Researchers have identified over 100 different applications for drones [35]. Factors such as diligence, cost-effectiveness, mobility in inaccessible areas, payload options, and risk considerations drive the widespread adoption of UAVs. The design of UAVs is often tailored to the specific mission they will perform in the field [36]. Categorizing UAVs based on their domains helps in understanding their architecture better, as demonstrated in Fig. 3, where each domain has its own privacy and security requirements [36, 37]. In the rest of this subsection, the main UAV applications are presented.

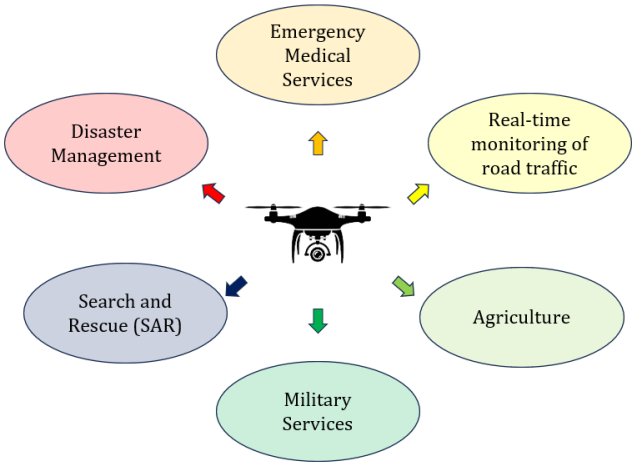

Fig. 3. UAV application areas.

1) Agriculture: UAVs have emerged as valuable tools in agriculture, providing real-time data and aiding farmers in making decisions. Equipped with advanced cameras, UAVs can deliver accurate information about soil conditions, crop health, and threats to crop yields. By analyzing this data, farmers can optimize the use of agricultural inputs to achieve higher crop yields. UAVs also offer early warning systems for threats such as wildlife or fires, allowing farmers to detect and mitigate these risks promptly. Researchers have highlighted the benefits of using UAVs in agriculture, including farm analysis, improved yields, monitoring, and spraying of pesticides. UAVs enable precise pesticide application by analyzing crop health and targeting infected areas, making spraying efforts safer and faster than manual methods [38, 39, 40].

2) Military: UAVs have found significant applications in the military sector, serving as a key component of the IoD. They are deployed in situations where manned flight is considered too risky or challenging. Military drones play crucial roles in combat operations, enemy surveillance, and target selection for military attacks [41]. They provide continuous aerial monitoring, offering troops a persistent eye in the sky. Kreps and Wallace [42] focused on the use of drones for counterterrorism, exploring the impact of international legal criticism on public support for drone strikes and the effectiveness of such strategies. Chand et al. developed a drone-based high-speed wireless mesh network, specifically designed for scenarios where no network infrastructure is available, such as disaster zones or military

conflicts. Their study demonstrates that drones can establish a wireless mesh network upon arrival, delivering Wi-Fi connectivity and real-time video streaming from an onboard camera. This network achieves wireless communication speeds of up to 160 Mbps within a range of approximately 200 meters.

3) Search and Rescue (SAR): With the increasing severity of climate change, natural disasters have become more frequent, emphasizing the crucial role of search and rescue operations. UAVs equipped with various sensors and cameras, including thermal sensors, have emerged as powerful tools in these missions. UAVs can effectively locate lost or injured individuals, even in challenging conditions or difficult terrain. Furthermore, UAVs can deliver essential supplies to inaccessible areas in war-torn or disaster-stricken regions. Cui et al. [43] addressed the use of UAVs in urban post-disaster search and rescue tasks and won the International Micro Air Vehicle Competition in 2014 by providing comprehensive solutions to key task components. Tilburg [44] reported two case studies showcasing the capabilities of UAVs in search and rescue missions, where UAVs assisted in locating a deceased person in a narrow valley at night and aided in obtaining images of challenging areas, facilitating successful rescue operations. Mayer et al. [45] discussed potential search and rescue scenarios for UAV deployment and highlighted the challenges and opportunities of human-machine interaction in these operations. Karaca et al. [46] utilized a simulation model to explore the use of UAVs in locating and searching for victims, as well as providing mobile transportation for search and rescue personnel in mountainous environments, particularly focusing on searching for unconscious victims on snow.

4) Disaster management: UAVs have the capability to access disaster-stricken areas that are hazardous for human intervention, whether the catastrophe is a result of human actions or natural disasters, such as terrorist attacks, tsunamis, or floods. Critical infrastructure like power, telecommunications, water utilities, and transportation systems are all susceptible to these calamities. UAVs play a crucial role in data collection, providing rapid responses, and maneuvering through debris. Equipped with sensors, radars, and high-resolution cameras, UAVs offer invaluable support to rescue teams in identifying damage, initiating urgent recovery operations, and delivering essential supplies, including first-aid kits and manned helicopters. UAVs contribute to disaster assessment, early warning systems, and the identification of preventive measures in real-time. In the case of wildfires, a swarm of drones outfitted with firefighting equipment can vigilantly monitor, analyze, and track affected areas without endangering human lives. Consequently, UAVs facilitate real-time surveillance over extensive regions while ensuring the safety and security of all involved parties. UAVs also play a vital role in locating and rescuing individuals and animals in distress.

5) Real-time monitoring of road traffic: The integration of UAVs with road traffic monitoring (RTM) systems is a subject of great interest. UAVs offer the potential for full automation of the transportation industry within the RTM sector [47], including functions performed by rescue teams, road surveyors, traffic officers, and on-site support personnel. These reliable and intelligent UAVs are instrumental in automating these operations. UAVs have proven to be effective tools for gathering data on road traffic conditions, outperforming traditional monitoring systems like surveillance cameras, ultrasonic sensors, and circuit analyzers [48]. Cost-effective drones can efficiently inspect extensive road sections. Local law enforcement agencies can leverage drones for comprehensive accident monitoring and security operations targeting illegal activities along highways, such as vehicle theft. Other applications include vehicle identification, pursuit of suspicious vehicles, tracking hijackers, and monitoring traffic rule violations [49]. UAVs can also monitor driving behavior and incidents inside vehicles, potentially mitigating traffic congestion and overcrowding. Furthermore, UAVs can contribute to monitoring road conditions, detecting fractures, and issuing early warnings to prevent accidents and reduce damage. Current road inspection methods rely on human-operated vehicles, highlighting the need for increased automation. The integration of road inspection technologies with UAVs holds the promise of significantly reducing road damage. UAVs can capture images of road fractures and use target detection algorithms to identify and assess these issues.

6) Emergency medical services: UAVs have demonstrated significant potential in the context of smart cities worldwide. These smart cities are equipped with advanced healthcare systems that rely on telemetry, implantable medical devices, and medical drones for the swift delivery of first-aid supplies. Notably, UAVs have effectively addressed the challenges posed by the COVID-19 pandemic in various countries. However, it is essential to highlight that the primary entities leading the response to COVID-19 are the national emergency medical services (EMS) institutions, working in conjunction with multiple stakeholders, including EMS personnel, nurses, and medical doctors. Additionally, policymakers are exploring various preventive measures to combat COVID-19, which encompass practices such as wearing surgical masks, refraining from touching one's face, practicing regular hand hygiene, implementing city lockdowns, avoiding high-risk areas, abstaining from social gatherings, and instituting health codes [50]. Policy makers should carefully consider the balance between economic concerns and public safety when contemplating the implementation of new measures. Currently, UAVs are being deployed for various tasks aimed at preventing the spread of COVID-19, such as: transport of patients, public announcements, crowd surveillance, spraying disinfection, mass screening, crown aerial monitoring and delivering vaccines and other medical supplies.

III. Cybersecurity Issues in UAVs

The advancement of UAV technology offers numerous benefits, including applications in agriculture, surveillance, infrastructure inspection, emergency response, and package delivery. However, these advancements also introduce concerns related to privacy, security, and safety [51, 52]. To address these issues, a comprehensive approach is required as drones become integral to various industries and daily life. This section focuses on the security prerequisites for UAVs in the IoD ecosystem, as well as essential security measures and strategies to safeguard UAV integrity and functionality, and the various types of threats that can target the IoD, spanning from physical hardware attacks to cyberattacks on communication systems and software.

A. Cybersecurity Requirements of UAVs

Due to the UAV's wireless communication system and its unmanned nature, it remains susceptible to security attacks and vulnerabilities, making the security issue even more critical. Both UAVs and the 5G network have encountered numerous security attack issues in recent years, drawing significant attention [53]. Consequently, UAVs are occasionally confronted with various types of security threats. The prevalence of this technology and the extensive use of UAVs in critical fields have given rise to security apprehensions, particularly concerning networked UAVs. These interconnected UAVs are exposed to diverse forms of malicious attacks through open-air communication channels. Fig. 4 shows the main components of a typical networked UAV system alongside a depiction of a cyberattack. Certainly, during the exchange of traffic between drones and the control station, the attacker can directly target the drone through specific attacks or focus on the communication network between the drones and the base station, or even direct their efforts towards the control station itself.

The extensive utilization of UAVs in civilian applications exposes them to numerous vulnerabilities [54]. To address this, several crucial attributes are necessary to safeguard UAVs against exposure, interference, alteration, and harm. To ensure the integrity of these attributes, we outline the key security and privacy prerequisites essential for establishing a secure UAV flight mission.

1) Confidentiality: To ensure adequate protection of information and data exchanges between UAVs and the GCS, several cryptographic security measures can be implemented. For instance, employing asymmetric encryption methods such as RSA or ECC would secure transmissions by rendering data unreadable to unauthorized individuals [55]. Furthermore, establishing secure VPN tunnels using protocols like IPSec or OpenVPN would ensure encrypted communication channels, preventing any unwanted interception of data in transit [56]. Implementing strong authentication protocols, such as the use of digital certificates or two-factor authentication keys, would verify the identity of UAVs and the GCS before any transmission of sensitive data [57]. By adopting security standards like TLS/SSL protocols to secure connections and adhering to reference recommendations from IEEE and NIST [58], it's possible to significantly bolster the security of exchanges between UAVs and the GCS. However, it's crucial to remain vigilant about technological advancements and new threats to continually adjust these protective measures and maintain an optimal level of security.

2) Integrity: Maintaining data integrity stands as a pivotal pillar for the seamless execution of UAV flight missions, serving not only as a fundamental necessity but also as a deterrent against potential adversarial interference within network traffic. The integrity of data is fundamental in preserving the unaltered state of telemetry information and control commands, crucial elements that dictate the UAV system's behavior. Any compromise in this integrity could lead to catastrophic mission failures or unpredictable behaviors in the UAVs. Thus, it becomes imperative to ensure that every communication exchange remains not only shielded from unauthorized access but also thoroughly verified. Employing authenticated encryption algorithms like AES-GCM or ChaCha20-Poly1305 [59] bolsters this safeguarding measure by not just encrypting the data but also providing authentication, ensuring that the received information remains unaltered and originates from legitimate sources. References from standards such as RFCs 4106 and 7539 outline the utilization of these algorithms, emphasizing their significance in maintaining the integrity of data during transmission. Additionally, insights from cybersecurity breaches, as documented in by Panko and case studies such as NASDAQ's cyber-attacks, underscore the catastrophic implications of compromised data integrity, further highlighting the criticality of robust protection mechanisms.

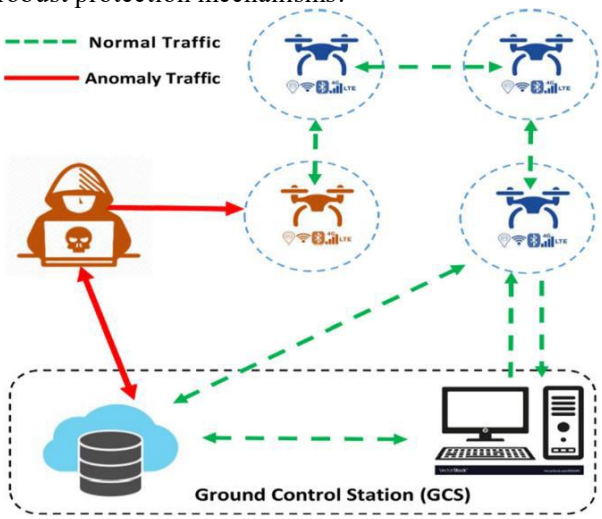

Fig. 4. Components of networked UAV and risk of a cybersecurity attack [54].

3) Availability: UAVs require uninterrupted operational continuity, free from intentional or inadvertent disruptions. In critical scenarios like search and rescue operations, their seamless operation is vital for constant surveillance of affected areas. Any failure, whether resulting from deliberate manipulation or unintended interruption, can significantly compromise critical operations. Similarly, in military contexts

[60] where UAVs play a pivotal role, any restricted access to necessary resources or unauthorized interruptions could impede mission success. Denial of Service (DoS) attacks pose a major threat [61], rendering UAVs inoperative by overwhelming their communication systems or disrupting connectivity. To counter such threats, the use of Intrusion Detection Systems (IDS) becomes imperative [62]. These systems monitor UAV networks, identifying abnormal activities and enabling swift responses to preserve their operational availability. They serve as essential mechanisms to ensure UAVs operate continuously and effectively, accessing necessary resources while remaining shielded from malicious interruptions or attacks targeting their availability.

4) Authenticity: Authentication plays a critical role in establishing secure communication within UAV systems, evident across various operational domains. In military applications [63], robust authentication protocols validate the legitimacy of each UAV involved in missions, ensuring that only authorized drones participate, safeguarding sensitive data, and preventing potential disruptions from unauthorized sources. Similarly, within commercial UAV networks [64], authentication procedures authenticate drones before granting access to logistical systems, maintaining the integrity of delivery routes, and protecting cargo from unauthorized access. In collaborative swarm operations [65], authentication serves to verify the identity of each drone, mitigating risks of infiltration by rogue elements, preventing collisions, and ensuring coordinated task execution. Moreover, authentication acts as a frontline defense against cyber threats targeting UAV networks, thwarting attempts by adversaries to impersonate legitimate nodes and compromise system control or data integrity. Across these diverse contexts, authentication not only confirms the credibility of individual UAVs but also fortifies the overall security posture of the system, shielding against potential adversarial intrusion and ensuring a trusted and controlled UAV environment.

5) Privacy: Privacy remains a critical concern within IoT systems, particularly in the realm of UAVs. The complex nature of these interconnected systems demands strict measures to ensure unauthorized access is barred from both the UAVs and any personal information they might possess. While this sharing enhances operational efficacy, it poses a significant privacy risk. If this information fell into malicious hands, it could facilitate tracking or surveillance of individuals, compromising their privacy. Moreover, the collection of personal data, such as images or videos, during surveillance missions demands increased protection to prevent unwarranted access or misuse [66]. The risk amplifies when considering potential interception or manipulation of shared information within a network of UAVs [67]. Safeguarding against these threats necessitates robust encryption, secure communication channels, strict access controls, and authentication mechanisms. Table II outlines the essential security requirements specific to UAVs.

TABLE II. ESSENTIAL SECURITY REQUIREMENTS OF UAVS

Security requirement	Description
Confidentiality	Only authorized people can have access to the sensitive data.
Integrity	The data are not modified when transferring.
Availability	The services provided are operational.
Authenticity	The receiver can confirm that the message was sent by a legitimate sender.
Privacy	The information of each entity is confidential.

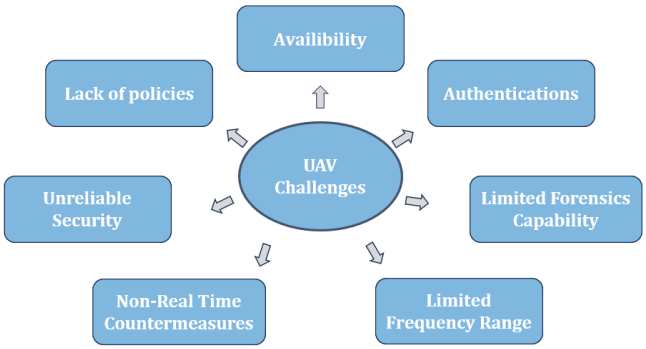

Fig. 5. Challenges in the adoption and execution of security measures for UAVs [68].

Challenges persist in the adoption and execution of inflexible security measures for UAVs, as illustrated in Fig. 5. The limitations in UAV security [68–70] are described below:

- Limited Forensics Capability: In case of a harmful event, the limited availability of forensic tools and methods makes it difficult to identify the malicious operator of the UAV involved in the dangerous act.
- Limited Frequency Range: The UAVs are being operated within a limited range of frequencies. Making them an easy target for jamming-based attacks.
- Non-Real-Time Countermeasures: Due to a lack of standardization for design and operational software, the current UAV does not have real-time protection during flight. If a UAV is compromised during flight, it cannot be retained by the original owner.
- Lack of policies: Standardization and policies are absent for UAV operations and operators. In some countries, policies are defined for UAV flying in proximity to sensitive areas. However, a general set of operating policies for a UAV is still not available.
- Unreliable Security: Based on the hostile operational environment of UAVs, the default security measures are not suitable. Due to the harsh operating environment of UAVs, a robust security protocol is necessary. But due to design and resource limitations, improving security measures is very challenging.

Most of these limitations can be surmounted through the establishment of standardized UAV designs, communication protocols, and fundamental factory default security measures.

B. Cybersecurity Attacks of UAVs

In the context of the IoT, security breaches can manifest in various ways, affecting several critical system components. These primary targets encompass IoD sensors, hardware, software, networking infrastructure, and the transmission communication that enable data exchange within the drone ecosystem. The security landscape for UAVs is multifaceted, and as such, a range of different attacks can be directed at these UAVs. These attacks may encompass both hardware and software components, each with the potential to compromise the integrity, availability, and confidentiality of UAV operations. Therefore, in the following sub-section, we will delve into some of these diverse attack vectors that can target UAVs, shedding light on the specific vulnerabilities and consequences associated with each. By understanding the nature of these threats, we can better formulate strategies and defenses to safeguard the rapidly evolving and vital field of drone technology.

1) Hardware-based attacks: At the hardware level, irrespective of the specific make and features of various commercial UAVs, including firmware and hardware variations, UAV hardware may be susceptible to targeting during the manufacturing phase or before and during flight missions. These situations are reasonable due to vulnerabilities that can arise in UAV firmware and the absence of encryption in custom chipsets. Given the widespread use and variety of existing UAVs, it is crucial to establish a consistent hardware security approach aimed at safeguarding UAVs from hardware-based attacks [71].

a) Supply chain attack: As the drone industry continues to expand, potential adversaries have a larger opportunity to compromise UAVs through supply chain attacks. This form of attack involves taking advantage of vulnerabilities in an organization's supply chain process, with a focus on components that are less secure and more sensitive, such as propellers, airframes, and actuators. Consequently, the final product delivered to the customer is already compromised. Belikovetsky et al. [72] have demonstrated a practical supply chain attack on UAVs using Additive Manufacturing (AM). This attack involves sabotaging a specific UAV by remotely manipulating the design files for its propellers. The adversary effectively reduces the fatigue life of the 3D printed propeller and creates delayed damage during a flight mission. This research illustrates that detecting sabotage attacks in additive manufacturing systems remains a complex research challenge.

b) Radio frequency modules attacks: Radio Frequency (RF) modules serve the purpose of transmitting and receiving radio signals between two distinct devices. In the context of UAVs, an operator typically employs a standard remote controller or the GCS to transmit control signals to the airborne UAVs. In this scenario, a potential adversary has the capability to interfere with the control signals, effectively disrupting the communication between the UAV and GCS, which leads to a situation where the UAVs lose their communication. In [73], the authors illustrated a replay attack targeting the XBee 868LP protocol, which is a low-power radio frequency module used for UAV-to-GCS communications. In this attack, the adversary manipulates the UAV-to-GCS communication by employing a third XBee chip. Specifically, the attacker compromises the security of the primary XBee communication channel by utilizing the chip's existing features to gain access to the address of the XBee communication channel.

c) Battery attack: Commonly, UAVs are powered by rechargeable Lithium-Ion batteries, and these batteries rely on the Battery Management System (BMS) to ensure a consistent energy supply to various UAV components. Nevertheless, there exists a vulnerability where an adversary can exhaust the battery's energy deliberately, a tactic known as a potential battery exhaustion attack [74]. This type of attack can lead to a malfunction of the UAV system, subsequently compromising the availability, integrity, and confidentiality of the batteries [75]. One method by which an attacker can compromise the availability of UAV batteries is by physically tampering with or swapping genuine batteries with faulty ones, thus causing the UAV system to fail. Another potential attack vector involves deep discharging of the batteries, which could be achieved by compromising other UAV components, such as manipulating sensors or injecting malicious software. This could ultimately lead to the exhaustion of UAV batteries [75].

2) Software-based attacks: Regarding software aspects, adversaries can exploit both zero-day vulnerabilities and existing software weaknesses within the flight stack and the GCS software to compromise the success of a flight mission. The importance of software attacks underscores the necessity to create strong defense mechanisms for UAV software security [76]. Nevertheless, existing UAV manufacturers tend to refrain from integrating software security measures into their products primarily for performance-related considerations. Consequently, adversaries can capitalize on this gap to develop malicious software, examples being Maldrone [77], Snoopy [78], and SkyJack [79].

a) Tampering attacks: Attackers deliberately engage in destruction, unauthorized manipulation, or alteration of data through IoD channels. Information, whether in motion or stationary, could be vulnerable to interception and unauthorized alterations. For example, if an unprotected data packet is transmitted over an IoD channel, the attacker might intercept the packet, modify its content, and change its intended destination address [80].

b) Operating system attack: Possible threats to civilian or military missions may manifest through vulnerabilities in the Flight Controller's system software. Consequently, the compromise of the system software can result in the loss of both UAVs and their payloads. An illustration of this risk is evident in the case of Amazon's Prime Air service's parcelcopters, which are civilian applications susceptible to attacks on their operating systems [81]. An attack on the delivery system has the potential to disrupt the delivery package for the intended recipient, subsequently causing the drone to crash. Attacks on UAV operating systems involve the remote injection of malicious software into UAVs, such as in the case of Maldrone, which is then followed by the takeover

of the drone's system. In doing so, the adversary can access the Flight Controller's cryptographic key and steal unencrypted data stored there.

3) Sensor-based attacks: When it comes to sensors, their variety and complexity onboard UAVs (including chemical, physical, mechanical, and others) render them attractive targets for adversaries. Furthermore, the current defenses against spoofing, sniffing, or jamming of these onboard sensors are constrained by the distinctive attributes of UAVs. While existing security research addresses threats and attacks related to sensors, in the context of UAVs, it is imperative to consider supplementary factors such as the legitimacy of sensor data readings and the energy and computational overhead involved in safeguarding sensed data against malicious actors.

a) Falsified data injection attack: Introducing erroneous sensor data readings into the Flight Controller has the potential to compromise external sensors like electro-optical and infrared sensors [82]. This form of attack disrupts the stabilization of the UAV. An attacker can carry out this attack by manipulating the sensor readings in multiple ways. They may gain access to the onboard Flight Controller system or modify sensor data via system calls. Alternatively, the attacker can directly transmit fraudulent signals to the sensors, thereby compromising the UAV's flight. A well-known instance of such an attack is GPS spoofing. Given that GPS signal broadcasts are often unencrypted and lacking authentication, attackers execute spoofing attacks on GPS by generating false signals, which can subsequently manipulate the UAV's GPS receiver [83]. As a result, the attacker can take control of the UAV.

b) Sensor communication channel attack: UAVs rely on a range of sensors, where their sensory channels, such as infrared, acoustic, and light, can potentially be exploited as a pathway for attacks. In [84], the authors provide evidence that UAVs equipped with Micro-Electro-Mechanical Systems (MEMS) gyroscopes can experience failure due to deliberate acoustic interference. This research reveals that MEMS gyroscopes resonate at frequencies within the audible range. Another investigation has demonstrated that optical flow camera sensors, employed to stabilize UAVs, can be rendered ineffective by manipulating the conditions in the surrounding environment [85].

4) Communication-based attacks: In the context of Communication-level considerations, the development of a multi-UAV network necessitates careful attention to potential security challenges aligned with the chosen network topology [86]. Numerous UAV protocols currently lack adequate security measures, presenting significant vulnerabilities. As communication constitutes an essential component of the UAV system, we maintain that the development of standardized UAV protocols that ensure both reliability and security is imperative. Many of the existing communication protocols employed in UAVs lack encryption or possess only limited cryptographic capabilities, thereby exposing communication channels to potential compromise by adversaries. Furthermore, the existing security measures designed to safeguard civilian UAVs from malicious users are primarily tailored to single UAV systems [87]. Hence, there is an imperative need to devise countermeasures suitable for scenarios involving multiple UAVs.

a) Hijacking attacks: When a wireless link is hijacked, the intruder obtains full access to that link. For example, the access and communication links between UAV nodes and GCS are established through Wi-Fi communication. Adversaries may initially employ de-authentication management frames to disconnect a drone from its associated GCS, initiating a hijacking attempt. Subsequently, they can remotely manipulate the drone using IEEE 802.11 protocols. Several security measures can be implemented to counteract de-authentication attacks. This includes practical detection algorithms and the encryption of transmitted frames. In [88], it is suggested that WPA2 encryption (802.11i 2004) with an appropriate key length can serve as a countermeasure to hijacking. Additionally, [89] has shown that encryption with dynamic secret keys provides an extra layer of defense against attackers. Moreover, safeguarding Wi-Fi-connected UAVs can involve limiting access points concealed by MAC addresses, while preventing intruders from accessing Wi-Fi links by not broadcasting SSIDs.

b) Jamming attack: The jamming attack disrupts legitimate communication links and hinders the exchange of information between authorized nodes by emitting interference or jamming signals [90]. In this scenario, the attacker creates interference signals and sends them within the same frequency band, leading to a degradation in Signal-to-Interference-plus-Noise Ratio (SINR) at the intended destination node. This, in turn, affects the reception of the original data and results in a delay in acknowledging the response. The A2G (Air-to-Ground) link of UAVs, which is easily accessible and has a broad coverage area, can be exploited by malicious intruders, whether they are airborne or terrestrial, to jam the communication link. An incident involving GPS jamming is documented in [91], where a small drone crashed in 2012. Initially, the legitimate user was suspected, but later the guilty was identified. Various algorithms have been developed to estimate the likelihood of intrusions and their impact on received data. Enhancing the Signal-to-Noise Ratio (SNR) serves as an effective initial defense against jamming. However, the energy constraints of UAVs limit the transmitted signal power and the practical receiver algorithms that can reduce noise at the receiver.

c) Collusion attacks: When two or more drones operate on the identical frequency, it results in information collisions, leading to an unstable network operation. These collisions are typically a consequence of the limited communication capabilities and constrained computing resources of the IoD network [93].

d) Spoofing attacks: Spoofing attackers introduce falsified identity information into legitimate communication links to manipulate or gain unauthorized access to data. They use misleading signals with elevated power levels to gain control over the source nodes. Common spoofing attacks

encompass activities such as email and phone call interception, IP address spoofing, and cache poisoning of the address resolution protocol. Additionally, GPS spoofing is prevalent in UAVs, involving the transmission of unauthorized high-power signals within the operational frequency band. Consequently, a malicious actor can access personal information, manipulate GPS locations, or propagate a virus within the system through GPS spoofing.

5) Network-based attacks: Maxa et al. surveyed the main security challenges of UAV routing protocols. Additionally, the work proposed by Sharma et al. outlined the security mechanisms for communication and networking technologies of UAVs.

a) Man-In-The-Middle attack: Adversaries have the capability to position malicious UAVs within operational networks, resulting in data breaches, service disruptions, and various security issues. Furthermore, they can intercept communications between a UAV and its GCS, impersonate the GCS, issue misleading directives to terminate an ongoing mission, or potentially take control of the UAVs [94].

b) Denial of Service (DoS) attack: DoS attackers seek to hinder legitimate service users from accessing essential resources. The attacker can flood the server with a substantial volume of requests, leading to network congestion and subsequently preventing legitimate users from accessing services [95].

c) Eavesdropping attack: Eavesdropping attack represents a common security threat in which either aerial or terrestrial intruders covertly intercept confidential information being exchanged between two legitimate nodes. This type of security threat has repercussions on the confidentiality of the information being leaked and grants unauthorized access to both the source and destination nodes, including personal data like access codes, control commands, navigational details, and more. For instance, systems like FANETS and cellular communications are susceptible to attacks by nearby intruders who might be challenging to detect as they do not emit any signals, thus posing a significant security risk to the communication network [96]. Implementing more advanced Physical security mechanisms can serve as a general solution, while additional encryption can provide protection against eavesdropping.

d) Flooding attacks: One primary goal of malicious UAVs is to overwhelm real UAVs with substantial volumes of original or duplicated data packets. This form of assault can exhaust the limited resources of UAVs, such as communication bandwidth and storage capacity, leading to significant network congestion and a surge in traffic across the IoD network [97]. The discussion on cyber-attack types for UAV components will delve into a detailed examination of various forms of cyber threats and vulnerabilities that can potentially target the different components of UAVs in Table III.

TABLE III. CYBERATTACK TYPES FOR UAV COMPONENTS

Attack Component	Attack Type	Security Services
Hardware attack	Supply chain attack	Integrity
	Battery attack	Integrity / availability
	Radio frequency attack	Integrity / availability
Software attack	Operating system attack	Confidentiality / integrity
	Tampering attack	Integrity
	Maldrone attack	Confidentiality / integrity
Sensors attacks	Sensor Communication Channel attack	Confidentiality
	Falsified Data Injection Attack	Integrity
Communication attacks	Jamming Attack	Availability
	GPS Spoofing Attack	Availability/Integrity/Confidentiality
	GCS MITM Attack	Confidentiality/Integrity
	Hijacking Attack	Confidentiality/Integrity
Network attack	MITM Attack	Confidentiality/Integrity
	DoS Attack	Availability
	Brute Force Attack	Confidentiality/Integrity
	SYN Flood Attack	Availability
	Eavesdropping Attack	Confidentiality

The rise of UAV technology created an overflow of cyber attacks. Protecting the flight mission requires a comprehensive defense-in-depth approach. Our finding results from different research indicate that UAVs are vulnerable to a variety of attacks across different levels of security. This vulnerability may arise because manufacturers prioritize improving the performance of their commercial products over security issues. Additionally, the implementation of security measures may potentially face additional costs for manufacturers. Therefore, it is advisable for existing UAV manufacturers to incorporate security and privacy considerations throughout all phases of the supply chain when developing their products.

IV. CURRENT APPROACHES AND DEFENSE STRATEGIES FOR UAV SECURITY

In this section, different existing countermeasures that secure UAVs, against damage from the threats and attacks discussed in the previous section are discussed.

A. Data Protection Using Cryptography

Cryptographic techniques are essential for securing UAV data, including text, images, and video, transmitted over unsecured communication channels such as GPS and Wi-Fi. Encrypting data exchanged through these vulnerable links ensures confidentiality, integrity, and availability. Yoon et al. [98] proposed an asymmetric authentication scheme to verify data authenticity, based on public and private key pairs. In this approach, the UAV encrypts a random sequence with a public key and sends it to the Ground Control Station (GCS), which decrypts and re-encrypts the data before returning it to the UAV. By comparing the received sequence with the original one, the UAV can detect potential security threats. If the link is

secure, commands are accepted; otherwise, the connection is terminated. Despite its effectiveness, this method may incur high bandwidth overhead when handling large data volumes.

Steinmann et al. [99] proposed a security mechanism based on asymmetric cryptography in which encryption keys are dynamically and randomly refreshed, thereby strengthening both data confidentiality and key robustness. Encrypted messages are transmitted together with a hash value, which is validated after decryption using the private key; inconsistencies between the computed and received hashes indicate malicious activity. To reduce computational complexity, Lin et al. [100] introduced a lightweight symmetric encryption scheme that uses a shared secret key for both encryption and decryption, ensuring data confidentiality even if transmissions are intercepted. Sharma et al. investigated functional encryption for UAV networks, enabling selective decryption so that only authorized data components are revealed without exposing the entire message. Moreover, [101] presented a command authentication protocol based on digital signatures, allowing UAVs to execute control instructions solely when verified by the Ground Control Station (GCS); otherwise, the UAV automatically switches to return-to-launch (RTL) mode. Despite their security benefits, many conventional encryption-based solutions remain challenging for real-time UAV operations due to processing delays, computational overhead, and complex key management, which can degrade communication efficiency.

B. Blockchain-Enabled Security Approaches

Blockchain is a shared ledger that uses cryptographic techniques to secure shared data. Along with enhancing UAV security and transparency, and guarantee the integrity of the data.

Ge et al. [102] proposed a distributed blockchain-based framework to secure UAV communications during data collection and transmission, while reducing the risk of attacks caused by compromised or malicious UAVs. Since conventional blockchain solutions impose high computational and bandwidth demands that exceed the limited storage and processing capabilities of UAVs, the authors introduced a lightweight blockchain design that preserves security and privacy with significantly lower overhead. The framework defines multiple transaction types to represent diverse data access operations and employs a novel reputation-driven consensus mechanism to enhance trust within the decentralized network. This architecture enables UAV-enabled applications to securely manage sensor data and support real-time data acquisition while satisfying key security requirements, including integrity, confidentiality, and availability.

Ch et al. [103] introduced a blockchain-driven framework aimed at improving data privacy, secure storage, and distributed access for UAV systems. The proposed solution leverages a cloud infrastructure to store operational commands, UAV feedback, authentication records, and integrity-related metadata. Data confidentiality is ensured through the use of pentatope-based elliptic curve cryptography combined with the SHA hashing protocol. Subsequently, the secured data are recorded on an Ethereum-based public blockchain to support transparent and efficient transactions. Experimental results indicate that the proposed architecture effectively safeguards UAV data against a wide range of cyber threats.

Garcia-Magariño et al. [104] presented a blockchain-based security framework that employs asymmetric cryptography to identify falsified data produced by compromised UAVs. Within this model, an attacked UAV may generate incorrect alerts or fail to report valid observations. However, system robustness is preserved through collaboration among neighboring UAVs, which can detect anomalies and mitigate the impact of malicious nodes. This resilience is supported by a secure digital signature mechanism that ensures data authenticity and trustworthiness. Experimental evaluations confirmed that the proposed approach maintains reliable performance even when a limited number of UAVs are compromised.

Khan et al. [105] introduced a blockchain-enabled framework that integrates machine learning for collaborative intrusion detection. The proposed system follows a two-phase process: initially, each network node independently applies an ML-based detector, after which the locally trained models are shared and combined across the blockchain network using a stacking strategy. Experimental results demonstrated that this collaborative model aggregation significantly enhances overall intrusion detection accuracy.

C. Rules-Based UAV Security

In rule-based methods, engineers establish a set of predefined rules and monitor UAV behavior, checking for deviations that may indicate potential threats. Nevertheless, this approach has seen limited adoption in recent years compared to other security strategies.

Sedjelmaci et al. [106] proposed a rule-based approach to distinguish between authenticated and unauthenticated signals. The method compares signal values against a predefined threshold derived from established rules: signals below the threshold indicate normal UAV operation, while those exceeding it signal potential threats. This technique allows UAVs to detect GPS spoofing and jamming attacks that could jeopardize system availability and data confidentiality. However, the reliance on a fixed threshold limits its effectiveness in dynamic or complex environments.

Lee et al. [107] developed a rule-based system to detect cyberattacks affecting the availability, confidentiality, and integrity of UAV operations. When a rule threshold is exceeded, the system triggers an appropriate defense mechanism. Although a large rule set can increase processing time and potentially delay detection, it helps lower the false negative rate. Similarly, [108] proposed a framework to identify cyber-physical attacks on small unmanned aerial systems (UASs) by analyzing UAV sensors and establishing rules to determine which sensors are most vulnerable to threats that could compromise UAV integrity.

However, rule-based approaches have inherent limitations in detection capabilities and require ongoing maintenance to remain effective. They are often unable to identify complex or novel threats that fall outside the predefined rules, making it necessary to continuously update the rule set to address emerging and evolving attacks.

D. Supervised ML Approaches for UAV Security

Supervised learning is a machine learning (ML) approach that trains models using labeled data to predict or classify new instances, making the quality of training critical for effective threat detection. Manesh et al. applied an artificial neural network (ANN) to safeguard UAV systems against GPS spoofing attacks. Their model utilizes GPS signal features such as Doppler shift, pseudorange, and signal-to-noise ratio (SNR) as inputs, achieving high accuracy in detecting spoofed signals according to experimental results.

Greco et al. [109] developed a supervised learning framework to defend UAV networks against jamming attacks, employing decision trees (DT) and multilayer perceptrons (MLP) as the primary ML techniques. The framework analyzes network metrics such as throughput, received signal strength indicator (RSSI), and packet delivery rate (PDR). It operates in two stages: first, packet sequences are processed to extract relevant features; second, each feature is evaluated independently to enable accurate detection and classification of potential jamming events.

Fenga et al. [110] introduced a two-step GPS spoofing detection approach that combines a Genetic Algorithm (GA) with XGBoost, leveraging data from both the inertial measurement unit (IMU) and GPS. In their experiments, spoofing attacks were simulated using a device that transmitted counterfeit GPS signals, causing the UAV to misinterpret them as authentic. The proposed method achieved a detection accuracy of 96.3%, demonstrating its effectiveness against GPS spoofing.

Shafique et al. [111] proposed a GPS spoofing detection method for UAVs based on analyzing GPS signal features. Incoming signals are classified as authentic or spoofed using various algorithms, including Naive Bayes (NB), linear regression (LR), decision trees (DT), random forest (RF), and support vector machines (SVM), with K-fold cross-validation to determine the most effective classifier. The study reported that SVM with a polynomial kernel achieved the highest accuracy of 98%. Similarly, Manesh et al. [112] explored ML-based techniques to detect jamming attacks on ADS-B receivers. They trained and compared supervised models such as artificial neural networks (ANN), SVM, K-nearest neighbors (KNN), and DT using features like energy statistics, bit error rate, and bad packet ratio, enabling effective differentiation between jamming and authentic signals.

E. UAV Security via Unsupervised Learning

Unsupervised learning is a machine learning approach that identifies patterns or clusters in unlabeled data, addressing a key challenge in UAV intrusion detection systems (IDS) where labeled datasets are often unavailable. This technique can detect both known and unknown cyberattacks, which is critical given that many threats remain undiscovered. However, unsupervised methods often generate a high rate of false alarms. Park et al. [113] developed an IDS using a one-class linear autoencoder trained exclusively on normal flight data. Abnormal UAV behavior was detected by analyzing reconstruction loss, with higher loss values signaling potential intrusions. The study emphasized feature extraction principles based on hardware generality and sensor stability and applied feature engineering to reconcile differences in feature scales and sampling periods. Despite being trained only on benign data, the model successfully identified GPS spoofing and denial-of-service (DoS) attacks during validation.

Panice et al. [114] proposed a GPS spoofing detection method for UAVs that combines machine learning with state estimation. The approach employs a support vector machine (SVM) integrated into a GPS–inertial navigation system (INS) hybrid framework. By analyzing discrepancies between INS and GPS readings, the system identifies abnormal signals and potential intrusions. Key parameters, including window length, threshold, and attack duration, are adjusted to enhance performance and predict the UAV's future sensor values and location. UAV status is classified as normal or abnormal using state estimation as a primary feature. Validation using simulated post-mission data with injected spoofed GPS signals showed a maximum true positive rate of 95%.

Whelan et al. [115] introduced a novelty-based IDS to overcome the lack of labeled UAV-IDS datasets by using unsupervised machine learning classifiers, including one-class SVM (OC-SVM), autoencoder neural networks, and local outlier factor (LOF). Each classifier analyzes data from individual sensors to detect attacks, including previously unseen ones, and to identify the targeted sensor. Models are trained solely on normal UAV behavior, with deviations considered potentially malicious. Experimental results indicated that the autoencoder achieved the highest performance with an F1 score of 94.81%, followed by OC-SVM at 81.17%, while LOF showed the lowest performance with an F1 score of 58.93%.

F. Reinforcement Learning–Based Methods

Reinforcement learning (RL) allows an agent to learn from interactions with its environment through trial and error, identifying actions that lead to positive or negative outcomes. This makes RL particularly suitable for detecting and classifying attacks on UAVs.

Bouhamed et al. [116] proposed a cost-effective intrusion prevention and detection system for UAV swarms, combining deep reinforcement learning (DRL) on UAVs with offline periodic learning at the Ground Control Station (GCS). A deep Q-network (DQN) multiclass classifier was trained using stored normal and intrusion cases, allowing the system to update knowledge without forgetting prior information. Using a customized reward function improved detection of minor classes, achieving 99.7% accuracy, 0.95 precision, 0.97 recall, and a 0.96 F1-score.

Xiao et al. [117] proposed a deep Q-network (DQN)– based power allocation strategy for UAVs to defend against attacks, optimizing safe transmission rate and secrecy capacity. The interaction between UAV and attacker is modeled as a smart attack game, with Nash equilibrium (NE) and prospect theory (PT) guiding optimal responses. The approach achieved a 93% safe transmission rate and a 16% improvement in secrecy capacity over standard Q-learning methods.

Elnaggar and Bezzo [118] applied inverse reinforcement learning (IRL) to predict sensor spoofing attacks in autonomous vehicles. The method estimates the attacker's

intent and identifies compromised sensors, then uses Bayesian IRL (BIRL) to restore system integrity by analyzing measurements and control inputs. The approach leverages optimal Markov decision processes (MDPs) to enhance system security. The authors validated the method through simulations of three UAV navigation scenarios in stochastic environments.

Praveena et al. proposed a deep reinforcement learning (DRL)–based method optimized with the Black Widow Optimization (BWO) algorithm, termed DRL-BWO, for intrusion detection in UAV networks. The approach employs an enhanced deep belief network (DBN) within the DRL framework to identify intrusions, while BWO optimizes DRL hyperparameters to improve performance. Experiments demonstrated high effectiveness, achieving 98% precision, 99% recall, 98% F1-score, and 98% accuracy.

Fei et al. proposed a reinforcement-learning-based flight recovery method for UAVs under cyber-physical attacks. The RL policy works alongside the flight controller, making minimal adjustments during normal operation and rapidly modifying actuator commands during attacks to maintain stability and path tracking. Results showed effective UAV stabilization under attack conditions.

Wang et al. proposed a reinforcement-learning-based energy-efficient anti-jamming relay (REAR) scheme, allowing UAVs to optimize relay power and strategies without prior knowledge of the network or channel model. A hot-starting technique was used to accelerate learning. Simulations with five UAVs under random jamming attacks showed improved communication reliability and reduced energy consumption.

Table IV highlights a taxonomy of the common cyberattacks, the security requirements affected and the methods proposed to defend the UAVs against such attacks.

TABLE IV. OVERVIEW OF SECURITY REQUIREMENTS AFFECTED BY CYBERATTACKS AND CORRESPONDING COUNTERMEASURES

Cyber-Attack	Security requirement affected	Countermeasures	
CPS spoofing	Availability, integrity	Rule- based approach	[106]
		Supervised learning	[109,110,111]
		Unsupervised learning	[113,114]
		Reinforcement learning	[117,118]
Jamming	Integrity	Rule-based approach	[106,107]
		Supervised learning	[109,112]
		Unsupervised learning	[115]
		Reinforcement learning	[117,118]
Eavesdropping	Confidentiality	Cryptographic approach	[100]
		Reinforcement learning	[117]
DoS	Availability	Cryptographic approach	[98]
		Blockchain approach	[105]
		Unsupervised learning	[113]
		Reinforcement learning	[116,118]
Black hole	Availability	Availability	[106]
Grey hole	Availability	Rule-based approach	[106]
MiTM	Authentication, confidentiality and integrity	Cryptographic approach	[101]
		Blockchain approach	[104]
DDOS	Availability	reinforcement learning	[116]

V. CONCLUSION

The surge and rapid expansion in the utilization of UAVs are ushering in an era dominated by self-governing aerial vehicles. UAVs bring forth a multitude of benefits spanning civilian and military domains alike and other application domains. However, this escalating utilization and accessibility have given rise to substantial apprehensions concerning security and privacy. The adaptability, cost-effectiveness, swift deployment, and portability of these Wencheng Yang, Song Wang, Xuefei Yin, Xu Wang, Jiankun Hu, “A Review on Security Issues and Solutions of the Internet of Drones”, IEEE Open Journal of the Computer Society, IEEE, Pages: 96-110, June 2022, transformed them into valuable implements for malicious endeavors. Despite the existence of numerous countermeasures to thwart the malevolent use of UAVs, their efficacy in executing harmful activities remains pronounced. Equally significant are the privacy quandaries intertwined with UAVs. In this era of technology, privacy stands as a prominent concern for both individuals and organizations.

In this study, we have tried to cite the different categories of security solutions for the IoD by highlighting the multifaceted challenges. Authentication-based solutions highlight the critical need to strengthen the security of communications between drones while efficiently managing cryptographic keys, ensuring interoperability, defending against targeted attacks, and scaling against a growing number of devices and users. Encryption-based solutions face challenges in preserving user anonymity, protecting personal data, ensuring interoperability, and maintaining network performance while preserving privacy. Blockchain-based solutions have highlighted the complex challenges of integrating with IoT and 5G, with a focus on coordination, security robustness, and educational adoption. Privacy-based

solutions require addressing vulnerabilities, user awareness, and resource constraints, while balancing security and usability. Intrusion detection systems must adapt to SDN architectures, balance efficiency and accuracy, integrate seamlessly into diverse networks, and scale to combat evolving threats in dynamic drone environments. Addressing these challenges requires innovative, adaptable, and interdisciplinary approaches merging technical prowess, user training, and resource-efficient methodologies to ensure the robustness, longevity, and security of IoD networks.

REFERENCES

[1] Kang, J.H.; Park, K.J.; Kim, H.: in: 2015 International conference on information and communication technology convergence (ICTC) (IEEE, 2015), pp. 533–538

[2] Commission delegated regulation (EU) 2019/945, 2019, Official Journal of the European Union, 12th, Mar.2019, URL https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=CELEX%3A32019R0945.

[3] Mitka, E.; Mouroutsos, S.G.: Classification of drones. Amer. J. Eng. Res 6, 36–41 (2017).

[4] Arslan Shafique, Abid Mehmood, Mourad Elhadef, "Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles", IEEE Access, Volume 9, Page: 46927-46948, March 2021.

[5] Wencheng Yang, Song Wang, Xuefei Yin, Xu Wang, Jiankun Hu, "A Review on Security Issues and Solutions of the Internet of Drones", IEEE Open Journal of the Computer Society, IEEE, Pages: 96-110, June 2022 .

[6] Bora Ly, Romny Ly, "Cybersecurity in unmanned aerial vehicles (UAVs)", Journal of Cyber Security Technology, Vol 5, No.2, Page: 120-137, 2021.

[7] Teng Long, Mustafa Ozger, Oktay Cetinkaya, Ozgur B. Akan, "Energy Neutral Internet of Drones", IEEE Communications Magazine, Volume 56, Issue, Page: 22-28, January 2018.

[8] Atherton, K.D.: The FAA says there will be 7 million drones flying over America by 2020. Pop. Sci. (2016)

[9] Nourmohammadi A, Jafari M, Zander TO (2018) A survey on unmanned aerial vehicle remote control using brain–computer interface. IEEE Trans Hum-Mach Syst 48(4):337–348

[10] Kanellakis C, Nikolakopoulos G (2017) Survey on computer vision for UAVs: current developments and trends. J Intell Rob Syst 87(1):141–168

[11] A. Riham, A.M. Youssef, Security, privacy, and safety aspects of civilian drones: A survey, ACM Trans. Cyber-Phys. Syst. 1 (2) (2016).

[12] T.F. Villa, F. Salimi, K. Morton, L. Morawska, F. Gonzalez, Development and validation of a UAV based system for air pollution measurements, Sensors 16 (12) (2016).

[13] M. Aljehani, M. Inoue, A. Watanbe, T. Yokemura, F. Ogyu, H. Iida, UAV communication system integrated into network traversal with mobility, SN Appl. Sci. 2 (2020) 1057.

[14] D. Giordan, M.S. Adams, I. Aicardi, M. Alicandro, P. Allasia, M. Baldo, P.D. Berardinis, D. Dominici, D. Godone, P. Hobbs, V. Lechner, T. Niedzielski, M. Piras, M. Rotilio, R. Salvini, V. Segor, B. Sotier, F. Troilo, The use of unmanned aerial vehicles (UAVs) for engineering geology applications, Bull. Eng. Geol. Environ. 79 (2020) 3437–3481

[15] A. Chriki, H. Touati, H. Snoussi, F. Kamoun, FANET: Communication, mobility models and security issues, Comput. Netw. 163 (2019) 106877

[16] Unmanned aerial systems (UAS), 2020, SKYbrary, 8 December 2020, URL https://www.skybrary.aero/articles/unmanned-aerial-systems-uas

[17] Y.Mekdad et al. A survey on security and privacy issues of UAVs, Computer Networks: The International Journal of Computer and Telecommunications NetworkingVolume 224Issue CApr

[18] Aljehani, M.; Inoue, M.; Watanbe, A.; Yokemura, T.; Ogyu, F.; Iida, H. UAV communication system integrated into network traversal with mobility. SN Appl. Sci. 2020, 2, 2749.

[19] Different Types of Drones. Available online: https://dronepedia.xyz/5-different-types-of-drones/ (accessed on 1 April 2022).

[20] Tahir A, Böling J, HaghbayanMH, Toivonen HT, Plosila J (2019) Swarms of unmanned aerial vehicles—a survey. J Ind Inf Integr 16:100106

[21] Thato Elijah, Rodrigo S Jamisola, Zeundjua Tjiparuro, and Molaletsa Namoshe. A review on control and maneuvering of cooperative fixed-wing drones. Int. Jour. of Dynamics and Control, 9 (3) :1332–1349, 2021

[22] Sheng WEN, Jie HAN, Yubin LAN, Xuanchun YIN, Yuhua LU (2018) Influence of wing tip vortex on drift of single rotor plant protection unmanned aerial vehicle. Nongye Jixie Xuebao/Trans Chin Soc Agric Mach 49(8)

[23] Ahmed Bahabry, Xiangpeng Wan, Hakim Ghazzai, Gregg Vesonder, and Yehia Massoud. Collision-free navigation and efficient scheduling for fleet of multi-rotor drones in smart city. In 2019 IEEE 62nd Int. Midwest Symposium on Circuits and Systems (MWSCAS), pages 552–555. IEEE, 2019.

[24] Davide Todeschini, Lorenzo Fagiano, Claudio Micheli, and Aldo Cattano. Control of vertical take-off, dynamic flight and landing of hybrid drones for airborne wind energy systems. In 2019 American control conference (ACC), pages 2177–2182. IEEE, 2019

[25] Pilot, What's the Difference Between Drones, UAV, and UAS? Definitions and Terms. Pilot Institute. 22 March 2020. Available online: https://pilotinstitute.com/drones-vs-uav-vs-uas/ (accessed on 18 August 2022).

[26] Ghulam E. Mustafa et al. Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats, Journal Drones, Volume 6, Issue number 10, Oct 2022

[27] Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges. IEEE Commun. Surv. Tutorials 2019, 21, 3417–3442

[28] El Haber, E.; Alameddine, H.A.; Assi, C.; Sharafeddine, S. UAV-aided ultra-reliable low-latency computation offloading in future IoT networks. IEEE Trans. Commun. 2021, 69, 6838–6851.

[29] Wang, L.; Che, Y.L.; Long, J.; Duan, L.; Wu, K. Multiple access mmWave design for UAV-aided 5G communications. IEEE Wirel. Commun. 2019, 26, 64–71

[30] Che, Y.; Lai, Y.; Luo, S.; Wu, K.; Duan, L. UAV-aided information and energy transmissions for cognitive and sustainable 5G networks. IEEE Trans. Wirel. Commun. 2020, 20, 1668–1683

[31] Fotouhi, A.; Ding, M.; Hassan, M. Understanding autonomous drone maneuverability for Internet of Things applications. In Proceedings of the 2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Macau, China, 12–15 June 2017; pp. 1–6

[32] Giyenko, A.; Im Cho, Y. Intelligent UAV in smart cities using IoT. In Proceedings of the 2016 16th International Conference on Control, Automation and Systems (ICCAS), Gyeongju, Korea, 16–19 October 2016; pp. 207–210.

[33] Feng, W.; Wang, J.; Chen, Y.; Wang, X.; Ge, N.; Lu, J. UAV-aided MIMO communications for 5G internet of things. IEEE Internet Things J. 2018, 6, 1731–1740.

[34] Motlagh, N.H.; Taleb, T.; Arouk, O. Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives. IEEE Internet Things J. 2016, 3, 899–922.

[35] Sharma, A.; Vanjani, P.; Paliwal, N.; Basnayaka, C.M.; Jayakody, D.N.K.; Wang, H.-C.; Muthuchidambaranathan, P. Communication and networking technologies for UAVs: A survey. J. Netw. Comput. Appl. 2020, 168, 102739

[36] Ullah, H.; Nair, N.G.; Moore, A.; Nugent, C.; Muschamp, P.; Cuevas, M. 5G Communication: An Overview of Vehicle-to-Everything, Drones, and Healthcare Use-Cases. IEEE Access 2019, 7, 37251–37268

[37] Luo, C.; Miao, W.; Ullah, H.; McClean, S.; Parr, G.; Min, G. Unmanned aerial vehicles for disaster management. In Geological Disaster Monitoring Based on Sensor Networks; Springer: Singapore, 2019; pp. 83–107.

[38] V. Puri, A. Nayyar, and L. Raja, "Agriculture drones: A modern breakthrough in precision agriculture," Journal of Statistics and Management Systems, vol. 20, no. 4, pp. 507–518, 2017.

[39] U. R. Mogili and B. Deepak, "Review on application of drone systems in precision agriculture," Procedia computer science, vol. 133, pp. 502–509, 2018.

[40] S. Ahirwar, R. Swarnkar, S. Bhukya, and G. Namwade, "Application of drone in agriculture," International Journal of Current Microbiology and Applied Sciences, vol. 8, no. 01, pp. 2500–2505, 2019

[41] S. E. Kreps and G. P. Wallace, "International law, military effectiveness, and public support for drone strikes," Journal of Peace Research, vol. 53, no. 6, pp. 830–844, 2016

[42] G. S. L. K. Chand, M. Lee, and S. Y. Shin, "Drone based wireless mesh network for disaster/military environment," Journal of Computer and Communications, vol. 6, no. 04, p. 44, 2018.

[43] J. Q. Cui, S. K. Phang, K. Z. Ang, F. Wang, X. Dong, Y. Ke, S. Lai, K. Li, X. Li, and F. Lin, "Drones for cooperative search and rescue in post-disaster situation," in 2015 IEEE 7th international conference on cybernetics and intelligent systems (CIS) and IEEE conference on robotics, automation and mechatronics (RAM). IEEE, 2015, Conference Proceedings, pp. 167–174.

[44] C. Van Tilburg, "First report of using portable unmanned aircraft systems (drones) for search and rescue," Wilderness environmental medicine, vol. 28, no. 2, pp. 116–118, 2017

[45] S. Mayer, L. Lischke, and P. W. Wo´zniak, "Drones for search and rescue," in 1st International Workshop on Human-Drone Interaction, 2019, Conference Proceedings

[46] Y. Karaca, M. Cicek, O. Tatli, A. Sahin, S. Pasli, M. F. Beser, and S. Turedi, "The potential use of unmanned aircraft systems (drones) in mountain search and rescue operations," The American journal of emergency medicine, vol. 36, no. 4, pp. 583–588, 2018

[47] Menouar H, Guvenc I, Akkaya K, Uluagac AS, Kadri A, Tuncer A (2017) UAV-enabled intelligent transportation systems for the smart city: applications and challenges. IEEE Commun Mag 55(3):22–28

[48] Shakhatreh H, Sawalmeh AH, Al-Fuqaha A, Dou Z, Almaita E, Khalil I et al (2019) Unmanned aerial vehicles (UAVs): a survey on civil applications and key research challenges. IEEE Access 7:48572–48634

[49] Elloumi M, Dhaou R, Escrig B, Idoudi H, Saidane LA (2018) Monitoring road traffic with a UAV-based system. In: 2018 IEEE wireless communications and networking conference (WCNC). IEEE, pp 1–6.

[50] Pulsiri N, Vatananan-Thesenvitz R (2021) Drones in emergency medical services: a systematic literature review with bibliometric analysis. Int J Innov Technol Manag 18(04):2097001

[51] Hosseini, N.; Jamal, H.; Haque, J.; Magesacher, T.; Matolak, D.W. UAV Command and Control, Navigation and Surveillance: A Review of Potential 5G and Satellite Systems. In Proceedings of the 2019 IEEE Aerospace Conference, Big Sky, MT, USA, 2–9 March 2019; pp. 1–10.

[52] IvyPanda, Unmanned Aerial Vehicles Essay. 13 January 2020. Available online: https://ivypanda.com/essays/unmanned aerialvehicles- essay/ (accessed on 20 December 2020).

[53] M. Krichen et al. Security Challenges for Drone Communications: Possible Threats, Attacks and Countermeasures, 2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH), 04 August 2022

[54] Q. Abu Al-Haija, A. Al Badawi, High-performance intrusion detection system for networked UAVs via deep learning, Neural Computing and Applications (2022) 34:10885–10900, 21 February 2022.

[55] Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126

[56] D. Harkins, D. Carrel. (2005). The Internet Key Exchange (IKE). RFC 4306.

[57] Dierks, T., & Rescorla, E. (2008). The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246

[58] IEEE 802.11 Working Group. [Online] Available: https://standards.ieee.org/committee/802.11.html

[59] N. Ahmad1, L. Mei Wei1, M. Hairol Jabbar, Advanced Encryption Standard with Galois Counter Mode using Field Programmable Gate Array, 1st International Conference on Green and Sustainable Computing (ICoGeS) 2017.

[60] Ö. KANAT, The Significance of Unmanned Aerial Vehicles (UAVs) in Strategic Contexts, Journal of Anadolu Strategy, 26.12.2023

[61] G. Bertoli, L.A. Pereira, O.Saotome, Classification of Denial of Service Attacks on Wi-Fi-based Unmanned Aerial Vehicle, 2021 10th Latin-American Symposium on Dependable Computing (LADC), 17 January 2022

[62] R. Fotohi, Securing of Unmanned Aerial Systems (UAS) Against Security Threats Using Human Immune System, Reliability Engineering and System Safety ,Volume 193, January 2020, 106675

[63] K. Yongho et al. Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone, Sensors (Basel), 2021 Mar 15;21(6):2057. doi: 10.3390/s21062057.

[64] M. Rodrigues et al. Authentication Methods for UAV Communication, 2019 IEEE Symposium on Computers and Communications (ISCC), June 2019

[65] Y. Aydin et al. Authentication and Handover Challenges and Methods for Drone Swarms, IEEE JOURNAL OF RADIO FREQUENCY IDENTIFICATION, January 2022

[66] H. Jalil Al hadi *et al*. A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs, Journal of Network and Computer Applications, Volume 213, April 2023, 103607.

[67] E. Ntizikira *et al*. Secure and Privacy-Preserving Intrusion Detection and Prevention in the Internet of Unmanned Aerial Vehicles, Sensors 2023, *23*(19), 8077; 25 September 2023

[68] G. Choudhary, V. Sharma, T. Gupta, J. Kim, I. You, Internet of Drones (IoD): Threats, Vulnerability, and Security Perspectives, in MobiSec 2018: The 3rd International Symposium on Mobile Internet Security, Cebu, Philippines, 2018

[69] H. N.Noura, O. Salman, A. Chehab and R. Couturier, DistLog: A distributed logging scheme for IoT forensics, Ad Hoc Netw., 98 (2020), 102061. https://doi.org/10.1016/j.adhoc.2019.102061

[70] R. S. Cohen, The Drone Zappers, Air Force Magazine, 22 March 2019. Available: https://www.airforcemag.com/article/the-drone-zappers

[71] O.Ceviz, P. Sadioglu, S. Sen, Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions, eprint arXiv:2306.14281, June 2023.

[72] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, Y. Elovici, dr0wned-Cyber-Physical Attack with Additive Manufacturing, in: 11th USENIX Workshop on Offensive Technologies (WOOT 17), 2017

[73] N. Rodday, Hacking a Professional Drone, Black Hat Asia. URL https://www.blackhat.com/docs/asia-16/materials/ asia-16-Rodday-Hacking-A-Professional-Drone.pdf

[74] V. Desnitsky, I. Kotenko, Simulation and assessment of battery depletion attacks on unmanned aerial vehicles for crisis management infrastructures, Simulation Modelling Practice and Theory 107. doi: 10.1016/j.simpat.2020.102244.

[75] A. B. Lopez, K. Vatanparvar, A. P. Deb Nath, S. Yang, S. Bhunia, M. A. Al Faruque, A security perspective on battery systems of the internet of things, Journal of Hardware and Systems Security 1 (2) (2017) 188–199.

[76] O.Ceviz, P. Sadioglu, S. Sen, Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions, eprint arXiv:2306.14281, June 2023

[77] P. Paganini, A hacker developed maldrone, the first malware for drones, (Online; Accessed 2 April 2022) (2015). URL https://securityaffairs.co/wordpress/32767/hacking/ maldrone-malware-for-drones.html

[78] (Online; Accessed 2 April 2022). URL https://money.cnn.com/2014/03/20/technology/security/ drone-phone/index.html

[79] J. Crook, Infamous Hacker Creates SkyJack To Hunt, Hack, And Control Other Drones, Tech. rep. (2013).

[80] E. Deligne, Ardrone corruption, Journal in Computer Virology 8 (1) (2012) 15–27.

[81] Amazon.com Inc., Revising the Airspace Model for the Safe Integration of Small Unmanned Aircraft Systems, NASA UTM 2015: The Next Era of Aviation (1) (2015) 2–5.

[82] E. Deligne, "ARDrone corruption," Journal in Computer Virology, vol. 8, no. 1-2, pp. 15–27, 2012

[83] K. Wesson and T. Humphreys, "Hacking drones," Scientific American, vol. 309, no. 5, pp. 54–59, 2013

[84] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," Proceedings of the 24th USENIX Security Symposium, pp. 881–896, 2015

[85] D. Davidson, H. Wu, R. Jellinek, T. Ristenpart, and V. Singh, "Controlling UAVs with sensor input spoofing attacks," 10th USENIX Workshop on Offensive Technologies, WOOT 2016, 2016

[86] [86] O.Ceviz, P. Sadioglu, S. Sen, Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions, eprint arXiv:2306.14281, June 2023

[87] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and Privacy Issues of UAV: A Survey," Mob. Networks Appl., vol. 25, no. 1, pp. 95–101, 2020

[88] D. He, S. Chan, and M. Guizani, ``Communication security of unmanned aerial vehicles," IEEE Wireless Commun., vol. 24, no. 4, pp. 134_139, Aug. 2017

[89] C. Javali, G. Revadigar, M. Ding, and S. Jha, ``Secret key generation by virtual link estimation," in Proc. 10th EAI Int. Conf. Body Area Network

[90] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, ``A survey on jamming attacks and countermeasures in WSNs," IEEE Commun. Surveys Tuts., vol. 11, no. 4, pp. 42_56, 4th Quart., 2009

[91] C. G. L. Krishna and R. R. Murphy, ``A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in Proc. IEEE Int. Symp. Saf., Secur. Rescue Robot. (SSRR), Oct. 2017, pp. 194_199.

[92] A. Kumar, R. Krishnamurthi, A. Nayyar, A. K. Luhach, M. S. Khan, and A. Singh, "A novel software-defined drone network (SDDN)-based collision avoidance strategies for on-road traffic monitoring and management," Veh. Commun., vol. 28, 2021, Art. no. 100313

[93] M. H. Yilmaz and H. Arslan, ``A survey: Spoo_ng attacks in physical layer security," in Proc. IEEE 40th Local Comput. Netw. Conf.Workshops (LCN Workshops), Oct. 2015, pp. 812_817.

[94] Y. Li and C. Pu, "Lightweight digital signature solution to defend micro aerial vehicles against man-in-the-middle attack," in Proc. IEEE 23rd Int. Conf. Comput. Sci. Eng., 2020, pp. 92–97

[95] A. Fotouhi et al., "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," IEEE Commun. Surv. Tuts., vol. 21, no. 4, pp. 3417–3442, Oct.–Dec. 2019.

[96] N.Wang, P.Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, ``Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," IEEE Internet Things J., vol. 6, no. 5, pp. 8169_8181, Oct. 2019.

[97] C. Pu and P. Zhu, "Defending against flooding attacks in the internet of drones environment," in Proc. IEEE Glob. Commun. Conf., 2021, pp. 1–6.

[98] M. Yahuza et al., "Internet of drones security and privacy issues: Taxonomy and open challenges," IEEE Access, vol. 9, pp. 57243–57270, 2021

[99] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks," IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2017.

[100] M. A. Siddiqi, W. Pak, Optimizing Filter-Based Feature Selection Method Flow for Intrusion Detection System, Electronics, 9 (2020), 2114. https://doi.org/10.3390/electronics9122114

[101] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the security: An ECC-based authentication scheme for internet of drones," IEEE Syst. J., vol. 15, no. 3, pp. 4431–4438, Sep. 2021.

[102] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A provably secure and lightweight authentication scheme for internet of drones for smart city surveillance," J. Syst. Architecture, vol. 115, 2021, Art. no. 101955.

[103] N. Zhang, Q. Jiang, L. Li, X. Ma, and J. Ma, "An efficient three-factor remote user authentication protocol based on BPV-FOURQ for internet of drones," Peer-to-Peer Networking and Applications, vol. 14, no. 5, pp. 3319–3332, 2021.

[104] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for internet of drones," Comput. Commun., vol. 154, pp. 455–464, 2020

[105] Lindqvist J, et al. Privacy-preserving 802.11 access-point discovery. In: Proceedings of the second ACM conference on wireless network security, 2005, pp.123–130.

[106] Herbadji, A.; Goumidi, H.; Harbi, Y.; Medani, K.; Aliouat, Z.: Blockchain for internet of vehicles security. Blockchain Cybersecur. Priv.: Archit. Chall. Appl. 1, 159–197 (2020)

[107] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchainbased access control scheme in IoT-enabled internet of drones deployment," Comput. Commun., vol. 153, pp. 229–249, 2020

[108] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5Genabled internet of drones," IEEE Internet Things J., vol. 9, no. 8, pp. 6224–6238, Apr. 2022.

[109] Wang, W.; Huang, H.; Zhang, L.; Su, C. Secure and efficient mutual authentication protocol for smart grid under blockchain. Peer-to-Peer Netw. Appl. 2020, 14, 2681–2693

[110] Zhang, L.; Zhang, Z.;Wang,W.; Jin, Z.; Su, Y.; Chen, H. Research on a Covert Communication Model Realized by Using Smart Contracts in Blockchain Environment. IEEE Syst. J. 2021, 16, 2822–2833

[111] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for AODV," in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003, pp. 125–134.

[112] V. Vaidya, "Dynamic signature inspection-based network intrusion detection," Aug. 2001, US Patent 6,279,113.

[113] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Computer networks, vol. 51, no. 12, pp. 3448–3470, 2007

[114] M. A. Aydın, A. H. Zaim, and K. G. Ceylan, "A hybrid intrusion detection system design for computer network security," Computers & Electrical Engineering, vol. 35, no. 3, pp. 517–526, 2009.

[115] E. Biermann, E. Cloete, and L. M. Venter, "A comparison of intrusion detection systems," Computers & Security, vol. 20, no. 8, pp. 676–683, 2001.

[116] G. Choudhary, V. Sharma, I. Chen, J. Cho, Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey, 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), 30 August 2018.

[117] L. Kou, S. Ding, T. Wu, W, Dong, Y. Yin, An Intrusion Detection Model for Drone Communication Network in SDN Environment, *Drones* 2022, *6*(11), 342; 4 November 2022.

[118] R. Shrestha, A. Omidkar, S. Roudi, R. Abbas, S. Kim, Machine-Learning-Enabled Intrusion Detection System for Cellular Connected UAV Networks, *Electronics* 2021, *10*(13), 1549; 26 June 2021