A Survey on Security of UAV Swarm Networks: Attacks and Countermeasures

XIAOJIE WANG, School of Communications and lnformation Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China
ZHONGHUI ZHAO, School of Communications and lnformation Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China
LING YI*, School of Communications and lnformation Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China
ZHAOLONG NING*, School of Communications and lnformation Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China
LEI GUO, School of Communications and lnformation Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China
F. RICHARD YU, Carleton University, Ottawa, Canada
SONG GUO, CSE, The Hong Kong University of Science and Technology, Kowloon, Hong Kong

The increasing popularity of **Unmanned Aerial Vehicle (UAV)** swarms is attributed to their ability to generate substantial returns for various industries at a low cost. Additionally, in the future landscape of wireless networks, UAV swarms can serve as airborne base stations, alleviating the scarcity of communication resources. However, UAV swarm networks are vulnerable to various security threats that attackers can exploit with unpredictable consequences. Against this background, this paper provides a comprehensive review on security of UAV swarm networks. We begin by briefly introducing the dominant UAV swarm technologies, followed by their civilian and military applications. We then present and categorize various potential attacks that UAV swarm networks may encounter, such as denial-of-service attacks, man-in-the-middle attacks and attacks against **Machine Learning (ML)** models. After that, we introduce security technologies that can be utilized to address these attacks, including cryptography, physical layer security techniques, blockchain, ML, and intrusion detection. Additionally, we investigate and summarize mitigation strategies addressing different security threats in UAV swarm networks. Finally, some research directions and challenges are discussed.

This work was supported by the Natural Science Foundation of China (62025105, 62272075, 62403092), by the National Natural Science Foundation of Chongqing (CSTB2024NSCQ-JQX0013), by the Science and Technology Research Program for Chongqing Municipal Education Commission (KJZD-M202200601, KJZD-K202300608), by the Hong Kong RGC Research Impact Fund (No. R5011-23F, No. R5060-19, No. R5034-18), and by the Collaborative Research Fund (No. C1042-23GF).
Authors' Contact Information: Xiaojie Wang, wangxj@cqupt.edu.cn, Zhonghui Zhao, S220101211@stu.cqupt.edu.cn, Ling Yi (corresponding author), yiling@cqupt.edu.cn, Zhaolong Ning (corresponding author), ningzl@cqupt.edu.cn, and Lei Guo, guolei@cqupt.edu.cn, School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China; Fei Richard Yu, richard.yu@carleton.ca, Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada; Song Guo, songguo@cse.ust.hk, Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong, China.

ACM 1557-7341/2024/11-ART
https://doi.org/10.1145/3703625

CCS Concepts: • **Security and privacy → Mobile and wireless security**; • **Networks → Ad hoc networks**; • **Computer systems organization** → *Robotics.*

Additional Key Words and Phrases: UAV swarm networks, security technologies, network attacks, security countermeasures

1 Introduction

The inception of the first **Unmanned Aerial Vehicle (UAV)** traces back to 1916, when a British engineer named Archibald Low developed a radio-controlled flying device. However, due to various technologies being in their nascent stage, the development of UAVs was severely restricted. This situation persisted until the outbreak of the Second World War. After that, UAVs entered the first phase of rapid development. Some countries began using UAVs for military purposes, including reconnaissance and bombing missions. However, after the end of World War II, the development of UAVs entered a relatively stagnant period.

In the 1990s, the rapid development of microelectronics and computer technology brought about a new opportunity for the second phase of UAV development. Small UAVs emerged and gradually entered the civilian sector. The flexibility and maneuverability of UAVs made them suitable for various applications, including agriculture [1], search and rescue operations [2], emergency communications [3], and natural disaster prevention [4]. However, when the demand for UAV applications increases, individual UAVs encounter certain limitations. For instance, during search and rescue missions, covering large areas may require multiple round trips or the coordination of multiple operators controlling separate UAVs, resulting in time and resource inefficiencies. Additionally, densely populated areas may require mobile **Base Stations (BSs)** to alleviate pressure on existing infrastructure. However, if a densely populated area is large enough to require more than one vehicle-mounted mobile BS, this can lead to a waste of resources. To resolve these challenges, UAV swarms emerge.

UAV swarm refers to a collection of UAVs connected through networking technologies and coordinated through collaborative control techniques to achieve intercommunication and data sharing. UAV swarms offer numerous advantages when executing complex tasks. First, there are multiple low-cost devices that cooperate to improve efficiency in the UAV swarm network; Second, data sharing among UAVs improves accuracy and coverage of task execution. Last, the failure of a few individual UAVs does not impact the overall performance of the swarm. These advantages lead to the widespread popularity of UAV swarms across various areas, including rescue [5], area coverage[6], and military attacks [7] and defense [8]. However, malicious attackers may employ various methods to obstruct, disrupt, and gain control over UAV swarms. Therefore, ensuring security of UAV swarms throughout all phases of their operations becomes an imperative requirement.

1.1 Related Surveys and Contributions

As a research field that has emerged in recent years, there has been significant attention given to issues related to the security of UAVs. Some surveys have been conducted on this topic.

There is research on UAV security. Authors in [9] address concerns at the physical layer, and discuss countermeasures such as trajectory design. Authors in [10, 11] focus on physical, application, and system layers of UAV security. The survey in [10] intricately examines the network security of **Unmanned Aircraft Systems (UASs)**. The paper [11] studies the network and physical security of the **Internet of Drones (IoDs)** and introduces the captivating concept of "impact chains".

Conversely, authors in [12–14] shed light on security aspects from physical, network, and application layers. The work in [12] underscores the challenges faced by safety-critical drones, summarizing **Blockchain (BC)** and **Machine Learning (ML)** solutions. Authors of [13] discuss security threats in drone communications, emphasizing physical and network layers. The work in [14] investigates security in centralized and distributed networks, advocating for BC solutions.

Table 1. Related survey.

Categories	Ref.	Contributions	Layered security				Architectural approach	
			Physical layer	Network layer	Application layer	System level	Centralized	Distributed
Traditional UAV networks	[9]	A survey on passive and active eavesdropping attacks in UAS, emphasizing defense techniques and their practical applications.	√	×	×	×	√	×
	[10]	A review on UAS security, categorizing threats into four areas and exploring cyber-attack and defense technologies.	√	×	√	√	√	×
	[11]	A comprehensive review of IoD's network and physical security, detailing threats, assets, and countermeasures.	√	×	√	√	√	×
	[12]	A review of drone security challenges, focusing on communication threats and emerging solutions.	√	√	√	×	√	×
	[13]	A review on UAV communication security, emphasizing challenges and countermeasures in physical and network layers.	√	√	√	×	√	×
	[14]	A survey on challenges and potential solutions of 5G UAV network security.	√	√	√	×	√	×
	[15]	A survey on UAV security and privacy, examining vulnerabilities, threats, attacks, and countermeasures.	√	√	√	√	√	×
	[16]	A review on UAV-based system vulnerabilities, charging attacks, and their mitigations.	√	√	√	√	√	×
	[17]	A review of cybersecurity for commercial UAVs, highlighting key threats and evolving countermeasures.	√	√	√	√	√	×
	[18]	A survey on UAV security in FANETs, analyzing threats and solutions via the OSI model's first four layers.	√	√	√	×	×	√
UAV swarm networks	Ours	A review on security issues, corresponding technologies, countermeasures and challenges of UAV swarm networks.	√	√	√	√	×	√

("√" if mention the corresponding content, "×" if not.)

Additionally, studies in [15–17] offer holistic insights into UAV network security from hardware to software. Authors in [15] conduct a thorough investigation into security and privacy issues of centralized UAV networks. In contrast, authors in [16] emphasize attacks on drone and charging systems. Authors in [17] present a comprehensive review of network security for commercial small drones, detailing key threats, vulnerabilities, and countermeasures. Finally, Tsao *et al.* in [18] delve deeply into the security of **Flying Ad-Hoc Networks (FANETs)** and IoD, referencing the OSI model.

The above surveys concentrate mainly on the security concerns of UAVs, and are limited to the security of networks or specific components of UAVs, UAS and IoDs. Even though the authors in [18] consider the security of self-organizing UAV swarm networks, they have not fully addressed the comprehensive security concerns of UAV swarms. In contrast, this survey concentrates on security issues of UAV swarm networks, and aims to provide readers with insights into corresponding attacks and potential security challenges. Additionally, readers can also thoroughly understand the latest developments of security countermeasures in UAV swarm networks. Table 1 showcases the reviews conducted in the field of UAV security.

To the best of our knowledge, ***we are the first to summarize security issues, corresponding technologies and solutions in UAV swarm networks.*** The main contributions of this article are as follows:

- We first survey technologies of UAV swarm networks and categorize related applications, which lay a solid foundation for understanding various security issues.
- We then discuss vulnerabilities in UAV swarm networks, followed by a comprehensive overview of security threats posed to communications, networks, data and ML models. Additionally, we summarize defense techniques employed to safeguard UAV swarm networks, including conventional cryptography, **Physical Layer Security (PLS)** and BC. Through these discussions, it provides a forward-looking knowledge for the subsequent mitigation measures.
- Finally, we investigate security countermeasures against various attacks in UAV swarm networks based on different security threats, and present open issues and research challenges.

1.2 Structure

The rest of this article is organized as follows. **Section 2** introduces the UAV swarm network and its applications in both civilian and military domains. **Section 3** discusses potential vulnerabilities and attacks on UAV swarm networks. **Section 4** first present technologies to ensure network security, and provides several countermeasures to against attacks on UAV swarm networks, corresponding to the identified attack categories. Research challenges and open issues are provided in **Section 5**. A summary of this survey is given in **Section 6**.

2 UAV Swarm Networks and Its Applications

In this section, we introduce key technologies and applications of UAV swarm networks.

2.1 UAV Swarm Networks

The successful operation of a UAV swarm network relies on several key aspects, including formation control, autonomous navigation, security and privacy [19]. In the following, we primarily discuss the architecture, communication networking, and navigation technologies of UAV swarm networks.

2.1.1 The Network Architecture. The structure of UAV swarm networks forms the foundation for swarm establishment, including communication and networking techniques.

Centralized control is one architecture used in UAV swarm networks. Here, a central controller governs all UAVs, but this method faces scalability limitations and a risk of single-point failures [20]. It's more common in traditional UAV networks due to its high computational and bandwidth demands.

In contrast, distributed architectures, where UAVs communicate among themselves and operate autonomously, are more prevalent in UAV swarms. These networks are resilient and adaptable, excelling in collaborative efficiency and broad-area coverage. They are preferred for their adaptability in dynamic environments and resource optimization capabilities but face challenges in communication and connectivity [21].

Hybrid architectures combine centralized and distributed frameworks' benefits, offering computational capabilities and broad coverage. This design is commonly adopted in UAV swarm networks to cater to diverse task requirements.

2.1.2 Communication and Networking Technologies. Once the architecture is determined, specific networking and communication techniques must be confirmed to meet the requirement of different tasks with in the UAV swarm.

There are several categories of communication technologies utilized for UAV swarm networks. The common method utilizes cellular networks, such as 4G and 5G, to enable connectivity with ground BSs [22, 23]. The second approach leverages satellite communication, offering extensive coverage, albeit potentially unsuitable for time-sensitive applications [22]. The third category utilizes Internet-based methods, such as WiFi 802.11, which boasts low costs and latency, making it practical for tasks like video streaming [22, 23]. Last, techniques such as MmWave, cognitive radio, and LoRa provide alternative solutions for specific scenarios within UAV swarm communications.

Once the networking technology is chosen, the corresponding routing protocols need to be determined. Based on descriptions in [24, 25], existing UAV swarm routing protocols can be categorized into the following categories:

Topology-based routing protocols: These protocols use the topology of moving nodes to exchange data packets. They can be further divided into flat-based and hierarchical protocols. The former utilizes planar addressing, with UAVs sharing similar roles [25], while the latter operates in clusters with communication mediated through a cluster head. An example is the mobility prediction clustering algorithm [25].

Location-based routing protocols: They make routing decisions based on the geographical position information of nodes, rather than relying on traditional IP addresses or node identifiers used in conventional networks, for example, mobility prediction-based geographic routing [25].

Swarm intelligence-based routing protocols: They draw inspiration from biological behavior, taking cues from the behavior of insects like bees, ants, and particle swarms. The ant-based geographical routing algorithm is an example of such a protocol [25].

2.1.3 Navigation Technologies. They play a vital role in ensuring the safe and coordinated flight of UAV swarms, and mainly comprise three aspects: localization, path planning, and collision avoidance and formation control.

Localization technologies: They serve as the foundation for UAV swarm navigation, determining the precise location of each UAV in **three-dimensional (3D)** space. Localization techniques typically rely on **Global Positioning Systems (GPSs)**, inertial navigation systems, and sensor-based positioning techniques (such as visual localization [26]).

Path planning: It primarily aims to determine the optimal flight paths and control a swarm of UAVs in real time, considering mission objectives, obstacle positions, and flight efficiency. A crucial concern in path planning is maximizing energy efficiency while ensuring collision avoidance and safety [21]. Common techniques employed include graph-based methods [27], artificial potential fields, ant colony optimization, and particle swarm optimization [28].

Collision avoidance and formation control: They are indispensable technologies for UAV swarm flight. Collision avoidance ensures safety during flight, while formation control ensures that multiple UAVs maintain predetermined relative positions and orientations during flight. A prevalent UAV collision avoidance approach is sensor-based detection, utilizing devices such as LiDAR, radar, and cameras [29]. Another technique is inspired by animal flocking behaviors, such as those simulating bird flock movements [30]. Additionally, there are methods that leverage ML techniques to enhance UAV flight [31].

All the aforementioned technologies pave the way for the widespread application and utilization of UAV swarms in various fields. With the continuous development and integration of these technologies, they are expected to further enhance the capabilities of UAV swarms, expand their applications, and improve the efficiency of UAV swarm operations.

2.2 Applications of UAV swarms

The application of UAV swarms can be divided into two main categories: civilian and military. Civilian UAV swarms are mainly utilized for work and daily life, such as disaster relief and information coverage enhancement. Military UAV swarms are primarily used for specific military tasks, such as reconnaissance and attack [8].

2.2.1 UAV Swarms in Civilian Applications. UAV swarm applications in civil settings can be broadly categorized into four major areas based on their performance functions: search and rescue [5], surveillance and monitoring (including area surveillance [6, 32], precision agriculture [33], area coverage [34, 35] and multi-user dynamic uninstallation [36–38]), transportation services [39], and construction and infrastructure inspection [40]. While these classifications do not encompass all possible applications, they provide a useful framework for understanding the diverse uses of UAV swarms.

Search and Rescue: UAV swarms offer vital communication services in disaster-stricken areas. UAVs, with their mobility and ability to bypass geographical constraints, can function as wireless communication bases, relays, or servers, providing crucial communication resources in emergencies [41]. They overcome challenges faced by rescue personnel in locating individuals and sharing information, especially when traditional communication infrastructure is damaged.

Surveillance and Monitoring: For surveillance and monitoring of public spaces, UAV swarms outperform traditional systems with fixed cameras that suffer from blind spots and limited deployment flexibility. Equipped with cameras, UAVs can be strategically placed to monitor vehicles, pedestrians, and provide cooperative perimeter surveillance [32].

Transportation Services: UAV swarms present a unique advantage by potentially replacing manual methods in the final leg of delivery, offering fast and cost-effective solutions, and alleviating manpower demands [42].

Construction and Infrastructure Inspection: In the construction industry, UAVs assist in aerial mapping, site monitoring, and integrity evaluations of projects [43]. They enable simultaneous oversight of multiple projects, leading to cost savings. Furthermore, UAVs enhance safety by conducting inspections of old buildings and infrastructure, mitigating risks for inspection personnel.

2.2.2 UAV Swarms in Military Applications. UAV swarms are difficult to detect by conventional radar systems due to their high maneuverability and small radar cross-section. At the same time, they have low manufacturing costs and high survivability. They are therefore considered to be highly effective and economical weapons [44]. Based on the functions they fulfill, UAV swarms primarily serve the following main purposes in warfare:

Infiltration reconnaissance: Small UAVs, hard to detect by radar due to size and stealth, enable extensive battlefield coverage. This facilitates significant real-time data collection, enhancing situational awareness with rapid data transmission to decision centers [45].

Offensive strikes: UAV swarms equipped with weapons can conduct surprise attacks and overwhelm enemy forces through their sheer numbers. By acting in concert, swarms can use collective firepower to eliminate hostile targets, e.g., Miramshah Airstrike, and Makin Airstrike [7].

Intercepting attacks: On the battlefield, the enemy may deploy radar-elusive weapons for attacks. Patrolling UAV swarms react when targets enter their blast range, launching explosives or self-destructing to neutralize threats [8].

Materiel transport: Traditional logistical operations often encounter difficulties in battlefield environments characterized by enemy defenses or restricted terrain. Fortunately, UAV swarms operating in the 3D space can overcome these limitations, by ensuring a continuous and uninterrupted supply of materiel to the battlefield.

With the development of technology, the scope of UAV swarm applications is expanding significantly. Concurrently, the increase in the use of UAV swarms brings concerns to security. The following section will outline current security challenges associated with UAV swarm networks and available security technologies.

3 Attacks in UAV Swarm Networks

In this section, we first discuss why UAV swarm networks are vulnerable. Next, we describe existing or potential attacks in UAV swarm networks and classify them based on the consequences they cause.

3.1 Vulnerabilities of UAV Swarm Networks

Compared to current communication networks with fixed architectures, UAV swarm networks lack several key components including a unified network architecture, an effective network security model, a behavioral assessment mechanism, a defense method for attacks, and proactive routing protocols [20]. We summarize these challenges in six aspects: communication, identity, resource, routing, data, and ML model.

3.1.1 Communication Vulnerabilities. The communications infrastructure for swarm networks relies on radio frequency technology and the Long Term Evolution standard, but these technologies have revealed several key vulnerabilities in practice. First, LTE technologies often run on top of so-called "commercial off-the-shelf" hardware and software, while cost-effective and ubiquitous, which may contain security vulnerabilities and provide potential entry points for cyber attackers [46]. Second, the open wireless channels that UAV swarms rely on can also be picked up by attackers due to their inherent broadcast nature, making them susceptible to eavesdropping; at the same time, this broadcast nature also makes the network susceptible to jamming, which can be used by illegal users to interrupt legitimate communication streams, posing a serious threat to UAV control and data transmission [47]. Currently, the communication bands used for UAVs are ultra-high frequency, L-band or C-band, and attackers can use tools, such as USRP developed by National Instruments, HackRF developed by Great Scott Gadgets, and software including GNU Radio and GQRX, to eavesdrop on the wireless signals or emit high-powered jamming signals. Additionally, since most jamming attacks act directly on the physical layer and there are relatively limited effective countermeasures against physical layer jamming, this poses a great challenge to traditional defense strategies [48]. To make matters worse, most UAVs on the market are not designed with anti-jamming features [49].

3.1.2 Identity Vulnerabilities. Identity-based attacks are one of the most serious threats to wireless networks [50]. Although modern encryption mechanisms provide strong data protection for UAV swarm networks, packets transmitted in wireless environments may still be at risk of being intercepted by third parties [51]. For example, an attacker could utilize advanced devices such as **software-defined radio (SDR)** devices (which have been developed by Rohde & Schwarz to capture data from wireless signals of UAVs) to listen in and capture wireless signals in a UAV network. Once attackers successfully intercept these signals and parse out identity information from them, they can potentially impersonate legitimate users and infiltrate the network. In this case, the attacker not only gains a comprehensive view of the network, but also performs malicious operations such as packet dropping, which can severely damage the integrity and availability of the network. Moreover, designing multi-factor user authentication schemes is challenging because wireless communication protocols face powerful adversaries and resource-constrained hardware [52].

In addition, rapid changes in the location of drones can lead to unstable network connectivity, which in turn affects the quality and reliability of data transmission [53]. In such cases, maintaining a stable link and accurately detecting the state of each node in the network becomes a challenging task [24], further exacerbating the complexity of the authentication and authorization processes.

3.1.3 Resource Vulnerabilities. UAV swarm networks are highly susceptible to resource exhaustion attacks due to their limited computational and communication resources. For example, attackers can use tools such as the 'aireplay-ng' module of Aircrack-ng to consume device resources by forcing UAV communications based on Wi-Fi to reconnect repeatedly, or they can use YateBTS to simulate a pseudo-base station to trick UAVs into connecting, thereby controlling their communications and further implementing attacks. These attacks can lead to bandwidth exhaustion and drone power depletion in the swarm network, which may ultimately trigger network service disruption or complete collapse, especially in latency-sensitive missions.

Additionally, attackers may plant 'sleeper' malware (e.g., Havex and Stuxnet), which may appear harmless in normal time, but can initiate destructive actions at specific moments or when triggered by remote commands. Since this 'sleep-activate' mode is difficult to detect and defend against, it further complicates the security threat of UAV swarm networks.

3.1.4 Routing Vulnerabilities. UAV swarm networks, due to their wide coverage and dynamically changing nature, need to rely on complex multi-hop routing mechanisms to ensure efficient data transmission. However, it's dynamic and highly dependent network structure becomes a potential weak point. Attackers can use tools such as AODV-UU, OMNeT++ and NS-3 to discover and exploit vulnerabilities in routing protocols. For example, by forging routing update messages, an attacker can trigger a black hole attack that results in packets being absorbed and dropped by malicious nodes. By tampering with routing information, an attacker can redirect packets to route along the wrong path or directly drop them, thus severely disrupting data transmission within the network.

Additionally, the attacker may also launch other attacks by forging routing information and creating optimal paths to direct data to malicious nodes. Under such attacks, communications among UAVs may be eavesdropped, tampered with, or blocked altogether, thus severely disrupting the connectivity and data integrity of the UAV swarm network.

3.1.5 Data Vulnerabilities. In the absence of effective data authentication mechanisms, UAV swarm networks face a serious challenge in ensuring data integrity and reliability of data sources. This absence makes the network highly vulnerable to various types of attacks. Attackers can exploit this vulnerability to tamper with or falsify critical data, such as UAV position information, sensor readings, and flight commands, which can lead to serious deviations in UAV operations. For example, by injecting false data packets, an attacker can mislead the UAV's navigation system, causing it to deviate from its intended trajectory; If the attacker tampers with sensor data, the UAV can even make incorrect judgements about environmental conditions, which in turn affects its decision-making process. Injecting false packets requires the previously mentioned identity attacks to be launched as a base, while tampering with sensor data does not. For example, the GPS-SDR-SIM developed by Takuji Ebinuma of Japan, used in conjunction with a number of SDR devices (ADALM-Pluto, BladeRF, HackRF and USRP), can lead to the tampering of UAV GPS sensor data [54]. All the above attacks not only threaten the safety of individual UAVs, but can also affect the coordination and cooperation of an entire fleet of UAVs, triggering a chain reaction that can lead to mission failure or physical damage.

3.1.6 ML Model Vulnerabilities. ML technology has been widely adopted in UAV swarm networks in a number of critical areas, such as power and energy transfer, communication resource allocation, flight path planning, target identification and monitoring [55–57]. However, with the increasing popularity of ML in UAV networks, its inherent security vulnerabilities have gradually surfaced as a problem that cannot be ignored. Attackers are able to take advantage of the inherent vulnerabilities of ML models, such as adversarial examples or data contamination during model training, to mislead the decision-making process of UAVs and severely weaken the overall operational effectiveness and reliability of the network.

To carry out these attacks, attackers can use a variety of existing tools. For example, Foolbox [58] and CleverHans [59] are capable of generating adversarial samples that could potentially lead UAVs to make erroneous decisions during target identification and path planning. The Adversarial Robustness Toolbox [60] offers a comprehensive suite of tools that not only generate adversarial samples but also perform model poisoning attacks, disrupting the model training process by tampering with training data. Additionally, DeepFool [61] specializes in creating minimally perturbed adversarial samples for vision models, which could significantly impair a UAV's ability to correctly recognize targets. HopSkipJumpAttack [62] can generate adversarial samples in a black-box environment, targeting models deployed on UAVs even when the model's internal details are undisclosed.

3.2 Attacks in UAV Swarm Networks

Based on the aforementioned overview, we classify attacks on UAV swarm networks into six categories: communication security, identity security, resource security, routing security, data security, and ML security. In real-world scenarios, attackers often utilize multiple attack methods simultaneously to achieve their objectives. In the following, we discuss these attacks in detail.

3.2.1 Communication Attacks for UAV Swarm Networks. Communication attacks in UAV swarm networks can be classified into two main categories: eavesdropping and jamming attacks [63]. The schematic diagram of communication attacks in UAV swarm networks is depicted in Fig. 1.

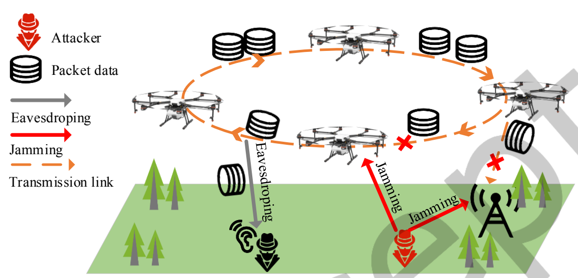

Fig. 1. Communication attacks.

Eavesdropping attacks: They refer to attackers' passive interception and decryption of wireless signals from legitimate UAVs. As shown in Fig. 1, the black attacker can intercept the transmitted information by eavesdropping on a wireless channel. Eavesdropping attacks are categorized into passive and active eavesdropping. Passive eavesdropping usually requires knowledge of perfect CSI information, and thus most eavesdropping is active eavesdropping attacks. An active eavesdropping attacker usually operates in a full-duplex mode to simultaneously receive confidential signals and send jamming signals. Jamming signals can reduce the data rate of a legitimate link, thus making eavesdropping feasible, even if the channel conditions of the eavesdropping link are worse than those of a suspect link without jamming. Authors in [47, 64, 65] describe active eavesdropping schemes in detail.

Jamming attacks: They refer to attackers deliberately transmitting noise to disrupt the receivers' ability to extract original information. Fig. 1 depicts a red attacker emitting jamming signals to interfere with a legitimate UAV's reception. Authors in [66] propose a defense concept that uses multiple legitimate UAVs to form a jamming tracking network, which actively locates and suppresses the malicious UAV's jamming source. However, an attacker could take the same steps to counter legitimate UAVs, using multiple malicious UAVs to simultaneously launch jamming on the communication links of legitimate UAVs, creating a situation that is difficult to defend against. In reality, there are various devices that can interfere with the communication frequency band of UAV swarm networks. For example, DroneDefender of Dedrone can generate targeted interference signals in the frequency band commonly used by UAVs, effectively interfering with their normal operation [67].

3.2.2 Identity-based Attacks. Weaknesses in identity security pose significant threats to the integrity and confidentiality of UAV swarm networks. Common attacks targeting UAV identities in UAV swarm networks include impersonation attacks, replay attacks, and **Man-in-the-Middle attacks (MITMs)**.

Impersonation attacks: They occur when an attacker forges an identity to act as a legitimate user in a network. The execution of such an attack may stem from the successful capture of a network node, which is a common way for attackers to obtain sensitive information and authentication credentials. Authors in [51] analyze 11 security vulnerabilities in typical user authentication protocols that enable attackers to exploit them to perform various types of attacks, such as impersonation. Particularly in UAV swarm networks, spoofing can lead to serious consequences. For example, legitimate UAVs are incorrectly quarantined due to conflicting identities, or critical communications being interrupted, thus seriously undermining trust and security within the network and affecting the efficiency of collaborative UAV swarm operations and mission execution.

Replay attacks: Attackers record packets and replay them continuously over a period of time without any modification. They are usually initiated during the authentication process to compromise the integrity of the system. Some common wireless network tools, such as Aircrack-ng and Kismet, can be used by attackers to obtain packets from wireless networks and then launch replay attacks. In addition, authors in [68] propose a tool called REPLIoT that is able to test the success of replay attacks without prior knowledge of the target device. Their results show that 75% of the devices are not able to defend against replay attacks.

MITM attacks: In MITM attacks, an attacker covertly inserts themselves into the communication link between the sender and the receiver, masquerading as a legitimate communication endpoint. As a result, they are able to intercept, listen to, and even tamper with packets. This process typically involves two key steps: first, the attacker intercepts signals and forces devices to connect to their spoofed node through technical means, e.g., exploiting wireless network vulnerabilities or deploying a mobile user identity capturer such as StingRay; subsequently, the attacker decrypts the communication content, potentially modifying it, and then re-encrypts and forwards it to the target, thereby maintaining interaction between the two parties. For example, for UAVs that rely on cellular networks, an attacker could use a device such as StingRay to launch an MITM attack to control or interfere with the UAV's command link.

Sybil attacks: The key to the effectiveness of UAV swarms is efficient collaboration and accurate information transfer among nodes, which requires that each legitimate node is able to receive and process reliable information from its peers. However, the vulnerability of this collaborative model is exposed in the face of threats such as witch attacks. In a witch attack, a malicious entity deceives legitimate network nodes by obfuscating them with multiple fake nodes. With destructiveness in a variety of contexts, this attack can interfere with data transmission, launch **Distributed Denial-of-Service (DDoS)** attacks using the created fake nodes, tamper with network routes, or even provide false sensor data that can lead to poor decision-making by a swarm of UAVs. In addition, attackers can manipulate voting and reputation systems within the network by generating a large number of virtual identities, thereby manipulating group behavior and disrupting overall collaboration [69]. Authors in [70] analyse the impact of the Sybil attack on P2P systems through a comprehensive simulation study. Similarly, the UAV swarm network can be considered as a type of P2P network and is threatened by similar attacks.

Remote-to-Local (R2L) and User-to-Root (U2R) attacks: They involve remote attackers exploiting vulnerabilities to gain unauthorized access to a system [71]. This type of attack is particularly common in **Internet of Things (IoT)** devices, which are sometimes equipped with default or weak passwords that make them easy to target, as exemplified by the Shodan search engine, which is capable of indexing publicly accessible IoT devices around the globe, including surveillance cameras, routers, and even industrial control systems. With Shodan, attackers can find these under-protected devices and then remotely access them using known vulnerabilities or default credentials to manipulate device functionality, such as changing settings, stealing data, and taking over the device altogether. For some commercial UAVs that are not protected by strict encryption, an attacker may be able to launch an R2L or U2R attack, which could lead to disruptions in UAV operations, thereby compromising data integrity and cybersecurity. For example, researchers from MIT used a network mapping tool to capture packets from the DJI Phantom 3 Standard and gained access to the root directory from its poor device password security [46].

3.2.3 Resource-based Attacks. In UAV swarm networks, network resource attacks primarily include **Denial of Service (DoS)** and DDoS attacks, Malware attacks, and hijacking attacks.

DoS attacks: Attackers often launch DoS attacks by exploiting weaknesses in network transport protocols, system vulnerabilities and service flaws. They use these vulnerabilities to send a large number of seemingly legitimate requests to the UAV swarm system, exhausting critical system resources and triggering buffer overflows. For example, authors in [72] and [73] experimentally evaluate the impact of DoS attack tools on UAV behaviour, and show that DoS attacks can lead to network availability issues that affect critical UAV applications, such as video streaming functionality and command delivery. Even DoS can cause CPU overload which can lead to UAV crashes [74].

DDoS attacks: They build upon DoS attacks, and coordinate a large number of computers (botnets) to launch DoS attacks. DDoS attacks typically operate in a client/server model, with the actual attackers hiding behind the scenes. While traditional DoS attacks focus on weaknesses in the protocol itself, DDoS attacks focus on weaknesses in the target infrastructure.

Malware attacks: They are an attack vector where the attacker injects malicious software (such as viruses, worms, Trojans, and spyware) into the target system or device to steal data, control systems, or disrupt device functionality [75]. Examples include Maldrone, and SkyJack [15]. Maldrone can open backdoors to give attackers access to sensors and drivers, while SkyJack exploits the weakly encrypted WiFi access points of civilian UAV systems, both of which are designed to manipulate devices or steal sensitive information without authorization.

Hijacking attacks: In hijacking attacks, the attacker infiltrates the communication network or controls system of the UAV swarm network to gain control over UAVs [76]. This type of attack aims to manipulate the behavior of the UAV swarm, and disrupt its functionalities. For example, hackers could use off-the-shelf hobby parts, a stock DJI Phantom drone, and some open source code to create a UAV that can take over other drones in flight [77].

3.2.4 Routing-based Attacks. They aim at maliciously manipulating or disrupting established routing schemes within the swarm network, including wormhole attacks, black hole attacks, and gray hole attacks. In comparison with traditional networks, these attacks pose a greater threat to UAV swarm networks [78].

Wormhole attacks: In wormhole attacks within UAV swarm networks, attackers create a virtual tunnel that rapidly transmits data packets to a different network location. This can mislead neighboring nodes into believing the wormhole tunnel offers the optimal transmission path [12]. Typically, the path length for routing is usually greater than the single-hop distance. But in a wormhole attack, an attacker is able to use virtual tunnelling to enable packets to be transmitted to other network participants, bypassing the normal path. Such attacks not only lead to severe packet loss, but also provide opportunities for other malicious activities such as data tampering. For example, authors in [79] show that simulations of wormhole attacks in IEEE 802.15.4-based wireless networks have revealed packet loss of up to about 50% of the entire network.

Black hole attacks: In UAV swarm networks, a black hole attack involves an attacker broadcasting false routing information, misleading other devices into routing their packets through the attacker's node. These black hole nodes then discard the packets. During such an attack, affected UAVs may lose prolonged contact with the swarm network, preventing them from receiving crucial decision-making commands and potentially leading to loss of control. Furthermore, black hole nodes might intercept and analyze packet contents, compromising sensitive information.

In addition, some studies show that when a mobile self-organising network is subjected to a black hole attack, which not only leads to a dramatic increase in the packet loss rate, but also has a significant increase in the end-to-end delay [80].

Gray hole attacks: They can be considered as a variant of black hole attacks, but differ from black hole attacks in that they only drop a portion of data packets, rather than all packets that pass through them. These packets may be of a specific type, or from certain IP addresses. Due to their unique attack mechanism, identifying gray hole nodes in UAV swarm networks is a challenging task [13]. Authors in [81] evaluate the impact of grey-hole attacks on wireless networks in the NS-2 simulation tool, and show that grey-hole attacks can severely degrade the throughput and energy efficiency of communication protocols, as well as increase network latency.

3.2.5 Data Attacks for UAV Swarm Networks. UAV swarm networks involve the transmission and storage of a significant amount of sensitive data and control commands. If attackers gain access to the data, they can manipulate legitimate data and inject malicious codes to take control of the UAV swarm network easily. In the following discussion, we explore attacks on data in UAV swarm networks and provide an illustration in Fig. 2.

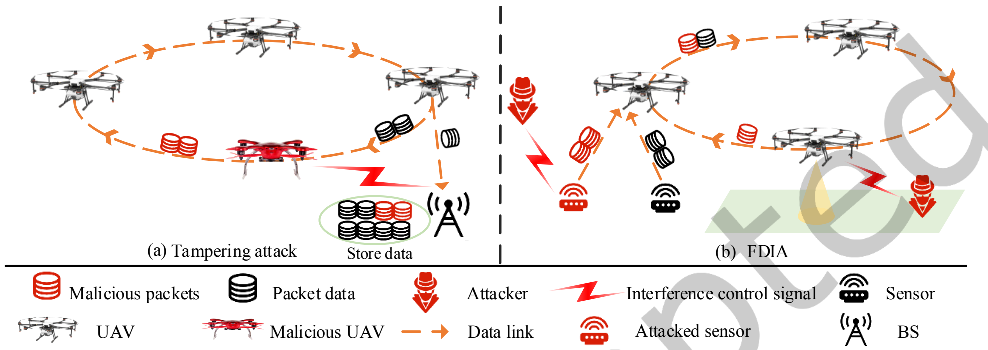

Fig. 2. Data attacks.

Data tampering attacks: As depicted in Fig. 2(a), data tampering attacks refer to the unauthorized alteration, manipulation, and disruption of data during transmission and storage processes within UAV swarm networks. Such tampering significantly impacts the performance and stability of the entire system [11]. Specifically, an attacker may use wireless network listening tools to intercept wireless packets, and subsequently exploit weaknesses in these packets to decrypt the authentication information of devices as an entry point for intrusion. Once successfully infiltrated, an attacker can tamper with sensor data, and this falsified data can mislead the UAV swarm's sensing and decision-making mechanisms, causing the system to make decisions based on incorrect information, and thus perform improper or harmful operations.

This type of attack not only destroys data integrity, but can also cause chain reactions, such as causing coordination failures among UAVs, affecting mission execution, and even posing a threat to the safety of people and property.

False Data Injection Attacks (FDIAs): As depicted in Fig. 2(b), within the context of UAV swarm networks, there are two main means by which an attacker can interfere with the normal operation of the UAV: one is to tamper with sensor readings and generate misleading data, and the second is to directly inject false information into the data stream. Both approaches lead to the UAV receiving erroneous sensory data, which in turn affects its decision-making process and may ultimately result in the UAV performing wrong tasks or behaviours. Authors in [82] find that the attack significantly increases the estimation error by modelling the effect of a fully covert FDIA on the state estimation of a networked control system.

GPS spoofing: It is an example of FDIA, and attackers transmit false coordinates and timing information to the target UAV, aiming to gain control over it [83]. For example, four researchers at the University of Texas at Austin took over a publicly accessible UAV by transmitting spoofed GPS signals. Their attack strategy consists of capturing real signals from GPS satellites with a spoofing device. The spoofing device then generates a series of fake signals to convince the drone receiver to report false position and velocity data [46]. Additionally, attackers can employ high-power amplifiers and GPS signal simulators, such as rogue BSs and SDRs, to broadcast GPS signals that effectively interfere with genuine GPS signals [84]. In many commercial UAVs, the received GPS signals are not encrypted, making them susceptible to such attacks.

3.2.6 ML Attacks for UAV Swarm Networks. Attacks on ML in UAV swarm networks can be classified into two categories: model attacks and privacy attacks.

Model attacks: They include adversarial attacks, backdoor attacks, and data poisoning attacks. Adversarial attacks aim to deceive the ML model by injecting malicious perturbations into the input data, leading to incorrect outputs [11]. Backdoor attacks enable the model to function normally with regular inputs but produce attacker-desired outputs when triggered by specific inputs [85]. Data poisoning attacks insert incorrect or biased data samples to manipulate the model's training process and decision boundaries [86]. If attackers launch the aforementioned attacks against ML models employed by a UAV swarm, it can easily result in the loss of control during their operation. For example, authors in [87] demonstrate the harm of adversarial attacks for DL in UAV swarm networks.

Data privacy attacks: They primarily involve inference attacks and membership inference attacks. The former exploits the model's output and gradient information to infer sensitive information about the training data. The latter aims to determine if specific data points are used in the model training process by analyzing the model's output and the training dataset [88]. For example, an attacker could use PrivacyRaven to develop new privacy metrics and attacks, and repurpose the attacks to data sources and other use cases [89]. Consequently, when ML models are utilized, UAV swarms might inadvertently expose data privacy, potentially allowing attackers to access sensitive information.

In addition, traditional cloud-centric ML technologies, hindered by latency and resource burdens [90], are often unsuitable for UAV swarm networks. **Federated Learning (FL)**, as a distributed ML algorithm, offers solutions like privacy protection, local model training, and reduced network load [91]. However, in UAV swarm networks, FL still faces risks from the dynamic and heterogeneous nature of UAVs, their limited computational and communication capabilities, and new attack types during model parameter sharing. For example, model aggregation attacks aim to compromise FL models by uploading malicious parameters [92], and model privacy attacks target the privacy of FL through inference on aggregated parameters and data during training. Authors in [93] propose a RL-based attack framework that learns to identify and exploit weaknesses in the FL system. This suggests that an attacker could further threaten the security of a UAV swarm network by building a framework specifically designed to attack FL models.

4 Security Countermeasures for UAV Swarm Networks

In this section, we conduct a thorough review of current security techniques and countermeasures against attacks in UAV swarm networks. We organize these security measures into six aspects: communication security, identity security, resource security, routing security, data security, and ML security, based on the previous attack classifications.

4.1 Security Technologies for UAV Swarm Networks

In this part, we introduce technologies that can be used to ensure the security of UAV swarm networks, including cryptography, PLS technology, ML, BC, and **Intrusion Detection Systems (IDS)**.

4.1.1 Cryptography. It plays a crucial role in ensuring data and identity security in UAV swarms by offering algorithms and protocols for confidentiality, integrity, authentication, and digital signatures [94]. There are three main types of encryption schemes, i.e., symmetric encryption, asymmetric encryption and hash functions. Symmetric encryption, which uses the same key for both encryption and decryption, ensures data confidentiality and integrity but faces challenges in key sharing. Asymmetric encryption, utilizing separate public and private keys, excels in identity authentication but is computationally complex and slow. Finally, hash functions are vital for data integrity checks and password storage, generating a unique and irreversible hash from input data.

4.1.2 Physical Layer Technologies. In the last decade, traditional cryptography-based security methods are effective but face challenges in key management and maintenance in complex networks like UAV swarm networks [95]. To address these issues, PLS technology has become a popular complement in enhancing UAV swarm network security [96]. PLS technologies focus on developing transmission schemes that exploit wireless channel characteristics, such as noise and interference, to widen the performance gap between legitimate receivers and attackers, thereby improving security [95].

Physical Unclonable Function (PUF): It leverages the inherent inconsistencies and randomness that arise during the hardware manufacturing process, making each piece of hardware unique [97]. Consequently, even with identical inputs, different devices produce unique outputs. This characteristic makes PUFs valuable for identity verification and cryptographic key generation [97].

Secure channel coding: Error control codes play a crucial role in establishing reliable and secure systems, especially when attackers face more channel degradation than legitimate users. Therefore, researchers focus on developing and designing channel coding techniques [95].

Artificial Noise (AN): UAV swarm networks can transmit information by emitting AN signals to interfere with eavesdroppers and reduce their channel quality. Even if the eavesdropper's location is unknown, this method can effectively mitigate eavesdropping attacks [98].

Beamforming: It can be essentially regarded as a spatial filtering operation, which utilizes the antenna array at the transmitter or receiver to capture or radiate energy in a specific direction [99]. The various antenna elements in the array can be weighted accordingly to signal enhancement in a specific direction with signal attenuation in other directions. UAVs with multiple antennas can use beamforming technology to focus the signal in a specific direction to improve communication security and reduce interference [100]. **Intelligent Reflecting Surface (IRS)** is a typical application of beamforming. In addition, the signal strength of a single UAV is limited, and thus **Collaborative Beamforming (CB)** technology can be used to improve signal quality [101]. However, beamforming requires knowing the **Channel State Information (CSI)** of the receiving UAV to optimize the antenna transmission mode, but the CSI of an UAV in flight is unstable and requires a lot of energy to calculate [100].

4.1.3 ML. ML models, categorized into various types based on feedback received during training, are essential in enhancing UAV swarm networks security. Supervised learning models, which rely on labeled data, are adept at predicting outputs for new and unlabeled data. Unsupervised learning uncovers hidden patterns in data without labels, while semi-supervised learning utilizes both labeled and unlabeled data. **Reinforcement Learning (RL)**, involves an agent learning to maximize rewards through environment interaction [102].

In the context of UAV swarm networks, these ML methods are invaluable. For example, supervised learning can detect unauthorized UAV activities using historical data. RL can be used to plan UAV flight paths or modulate transmission power. These various types of ML algorithms provide a range of tools to enhance the security of UAV swarm networks.

4.1.4 BC. It combines cryptography, mathematics, and networking technologies to create a decentralized ledger vital for data management [103]. It comprises blocks connected by cryptographic hashes, each containing transaction data, timestamps, and hash values. Key characteristics of blockchain include decentralization, immutability, and transparency. Decentralization ensures that no single entity controls the blockchain in a UAV swarm network. Immutability, provided by hash values, safeguards data and identity information from tampering. Transparency allows for the visibility of transactions, enabling the detection and tracing of false information in the UAV swarm network.

4.1.5 IDS. It is a security mechanism used to identify malicious behaviors [13]. It monitors the operation of UAV swarm networks according to certain security detection policies, to ensure confidentiality, integrity, and availability of the system. From a functional perspective, IDS detection methods can be categorized into three types. The first type is anomaly-based detection, which differentiates between normal and abnormal behaviors through statistical behavior modeling. This is crucial in UAV swarm networks as it promptly identifies UAVs that deviate from expected flight patterns. The second type is signature or rule-based detection, leveraging known attack patterns for detection. The third type is specification-based detection, which establishes a set of standards and constraints that define the correct operation of protocols [104].

4.1.6 Security Techniques for UAV Swarm Networks ML. Since ML technologies have many security and privacy vulnerabilities, it is possible to enhance its security and privacy by BC and cryptography techniques, as well as encryption and **Differential Privacy (DP)** techniques.

Encryption can be primarily categorized into **Homomorphic Encryption (HE)** and **Secure Multi-party Computation (SMC)**. HE allows computations on encrypted data without decryption, protecting against parameter tampering and safeguarding training data. SMC enables collaborative computation among multiple entities without exposing individual data, allowing ML models to evolve without accessing base training data [105]. However, HE and SMC introduce extra computational and communication demands.

DP provides robust privacy by adding noise to sensitive data, ensuring consistent query results regardless of specific data points [105]. This makes deducing data challenging for adversaries, thus securing the privacy of parameters and training data in ML models used in UAV swarms. However, the accuracy of ML models may be compromised due to the noise introduced by DP [106].

4.2 Communication Security Countermeasures for UAV Swarm Networks

The primary communication threats within UAV swarm networks are network eavesdropping and interference attacks. In the following, we focus on security strategies against these two threats. Furthermore, technologies, approaches, optimization targets, and limitations employed by different security countermeasures are summarized in Table 2.

Security Countermeasures for Eavesdropping. In order to address eavesdropping attacks during UAV-assisted communication, authors in [101] and [107] explore the use of UAV-supported virtual antenna arrays and CB technology. In [101], authors optimize the UAV's hovering position, propulsion current weighting, and communication scheduling with remote ground users to mitigate the impact of eavesdroppers while minimizing propulsion energy consumption. Sun *et al.* optimize the UAV's position, energy consumption, excitation current weighting, and the selection of BSs [107]. However, these articles consider that some eavesdroppers can be detected, whereas in reality, eavesdroppers are often unknown.

AN can be also applied to prevent eavesdropping attacks. Zhang *et al.* propose a method where UAV jammers transmit AN signals to eavesdroppers, while UAV transmitters send confidential information to legitimate users [108]. They employ multi-agent deep RL to optimize UAV trajectory, transmission power, and jamming power. However, UAVs are energy-constrained devices, and the long-term emission noise may affect the operation of the entire UAV swarm. Recognizing this limitation, authors in [109, 110] consider applying collaborative UAVs within a swarm to confuse malicious eavesdroppers, by transmitting interference signals while employing wireless Energy Harvesting (EH) techniques to assist communications. Authors in [109] determine the optimal heights of UAV relays and UAV jammers to maximize secrecy performance and extrapolates the probability of the eavesdropper being detected. Authors in [110] optimize both the EH time and the number of UAVs in the swarm to achieve a specific level of secrecy protection and derive the probability of covert message interruption.

Table 2. Countermeasures for communication security in UAV swarm networks.

Attacks	Ref.	Technologies	Purposes	Defects
Eavesdropping attacks	[101]	CB	Minimizing energy consumption and eavesdropper impacts by an improved multi-objective dragonfly algorithm.	The assumption that some eavesdroppers can be detected.
	[107]	CB	Maximizing secrecy rates by an improved multi-objective salp swarm algorithm.	The assumption that some eavesdroppers can be detected.
	[108]	AN, CB, Deep RL	Optimizing UAV trajectory and transmit power for system secrecy rate maximization.	Without the consideration of energy consumption.
	[109]	AN, EH	A communication protocol with dual phases for UAV eavesdropper detection.	Without the consideration of communication interfe-rence when detecting.
	[110]	AN, EH	A three-phase UAV swarm protocol for secure signal relay and concurrent eavesdropper jamming.	Without the consideration of trajectory optimization.
	[111]	Channel coding, RL	Optimizing grid coding for enhancing anti-eavesdropping performance.	Without the consideration of energy consumption.
	[112]	Channel coding, DL	Enhancing secure data transmission by lowering bit error rates and security gaps for UAVs in 5G and beyond.	The assumption that receiver's CSI is known.
	[113]	IRS, Beam-forming	Joint optimization of UAV transmit power and beamforming for average secrecy rate maximization.	The assumption that all CSI is known.
Jamming attacks	[114]	CB	Non-convex optimization in UAV hovering altitudes and satellite beamforming against jamming.	The assumption of perfect CSI of all links.
	[115]	Multi-agent RL	Optimizing UAV relay selection and transmit power allocation for improved anti-jamming performance.	The assumption of a line-of-sight link bet-ween the jammer and the UAV swarm.
	[116]	RL	Defense against intelligent jamming in UAV networks.	Performance degradation caused by discretization of training data.
	[117]	IRS, Beam-forming	Optimizing beamforming for interference immunity, independent of known or unknown interferer CSI.	Without the consideration of the IRS phase shift and amplitude refle-ction correlation.

However, Tran *el al.* assume that all CSI is known [109], and Dang-Ngoc *et al.* consider fixed eavesdroppers, which is not realistic [110].

Channel coding is also used to prevent eavesdropping attacks. An RL-based random linear network coding scheme for UAV-assisted cellular systems is proposed in [111] to address eavesdropping issues. The computational complexity of RL is typically high, yet the authors accelerate policy exploration speeds and improve communication efficiency through a hierarchical architecture. Similar to [111], authors in [112] propose a method to enhance wireless communication security among UAVs by providing an additive Gaussian white noise channel, even in the presence of eavesdroppers. However, the assumption that the transmitter is aware of the receiver's CSI may not be realistic in dynamic UAV scenarios.

Furthermore, authors in [113] use IRSs to reconfigure the propagation environment, with the purpose of mitigating the presence of eavesdroppers. The authors jointly optimize the transmit power, active beamforming, and passive beamforming for the 3D trajectory of UAVs. However, it should be noted that the approach presented in [113] may lack generalizability to other scenarios.

Security Countermeasures for Jamming. Addressing intentional or unintentional interference in satellite and UAV communications, authors in [114] introduce a two-level anti-jamming scheme. In the first stage, low-altitude satellites in low Earth orbit send group instruction information to all UAV groups. In the second stage, the leading UAV in the swarm calculates the optimal beamforming vector and height, which are then broadcasted to other UAVs.

RL is also frequently utilized against jamming attacks. For instance, authors in [115] introduce an anti-jamming UAV swarm communication scheme based on multi-agent RL. This scheme leverages shared communication experiences and observations among neighboring UAVs to enhance the anti-jamming performance of group communications. However, the above scheme assumes that the network and interference models are known, which may not hold in practical scenarios. Although RL techniques can assist UAV swarms to counter jamming attacks, the limited computational resources of UAVs make the algorithms challenging to converge. To address this issue, Li *et al.* propose a knowledge-based RL approach to mitigate the impact of smart jammers on UAV networks [116]. This algorithm utilizes domain knowledge to compress the agent's exploration of the state space, thus improving the convergence speed of the algorithm.

IRS is also used against jamming attacks. Authors in [117] investigate robust beamforming in a multi-user anti-interference communication system based on IRS. They propose a general model for joint optimization of BS's active transmit beamforming and IRS's passive reflect beamforming, aiming to minimize total transmit power while satisfying QoS requirements. The study addresses both scenarios with and without statistical interference CSI, and also leverages effective optimization techniques to handle uncertainty and non-convexity in the process of beamforming.

Different from above strategies, game theory has also been used to enhance the anti-jamming ability of UAV swarms. Authors in [118] propose a game-theoretic approach for deploying UAV swarms to perform reconnaissance missions in harsh interference environments. This approach allows UAVs within the swarm to compete with each other and independently adjust their positions while avoiding jamming.

Lesson 1: Eavesdropping and jamming attacks pose critical threats to the physical layer of wireless communications. Addressing these challenges necessitates a foundational focus on the physical layer. Techniques like beamforming can be utilized to amplify signal strength for authorized users, thereby mitigating the risks of eavesdropping and jamming. Meanwhile, strategies such as trajectory planning and power control can assist in alleviating physical layer attacks. However, it's paramount to note that many contemporary research assumptions, like knowing an attacker's location and CSI, may not be practical in real-world scenarios.

4.3 Identity Security Countermeasures for UAV Swarm Networks

Identity attacks aim to impersonate legitimate users to gain unauthorized access. Cryptography is a good choice based on the experience of identity security countermeasures in traditional networks. A lightweight cryptography-based user authentication and key negotiation scheme for IoD deployments is proposed in [119]. This approach solely employs efficient one-way cryptographic hash functions and bitwise exclusive OR for authentication, making it particularly suitable for resource-constrained UAVs.

In addition to lightweight cryptographic authentication schemes, PUF is commonly used. For instance, Alladi *et al.* present a mutual authentication protocol for **Software-Defined Networking (SDN)**-based UAV swarm networks [120]. This protocol utilizes question-response pairs generated by PUF chips embedded in UAVs, to eliminate the need for storing keys in the physical memory of UAV nodes. Each round of authentication generates a unique session key, which aims to prevents identity attacks. Similarly, authors in [121] propose a PUF-based authentication protocol for UAV swarm networks, to defend against MITM attacks, replay attacks, and other identity attacks. Compared to [120], it also offers improved computational efficiency. However, both protocols do not consider the interference of noise on PUF responses. Authors in [122] address this issue by using a fuzzy extractor to reduce the noise of PUF responses and utilizing PUF responses for authentication.

Furthermore, BC has also emerged as a significant technology to ensure identity security in UAV swarm networks. For example, authors in [123] propose a BC-based identity verification protocol. It establishes session keys between UAVs and ground stations to verify identities of UAVs and ensure secure communications. However, the protocol does not account for scenarios where certain nodes may not receive keys due to the unreliable nature of wireless channels. In contrast, authors in [124] address this limitation by proposing a BC-based mutual recovery group key distribution scheme. Furthermore, Tan *et al.* argue that managing keys through ground stations can become a target for attacks or increase the communication overhead for UAVs [83]. To overcome these challenges, they propose a BC-based distributed key management scheme for heterogeneous FANETs. In this scheme, the UAV swarm is divided into different groups, each comprising a powerful leader UAV and regular UAVs, allowing each group to manage its own keys. Additionally, each UAV possesses its own "transaction chain" to ensure the authenticity of its identity.

The aforementioned BC-based identity verification scheme is mainly implemented within the same region. However, when UAV swarms engage in cooperative tasks across different regions, the authentication of UAVs becomes challenging. To address this, authors in [125] propose a BC-based cross-domain authentication scheme, which uses multiple signatures based on threshold sharing to create identity federations for collaborating regions. The scheme utilizes smart contracts for authentication to enable reliable communications among cross-domain devices. However, it introduces additional latency. Different from this, authors in [126] consider both the problem of cross-domain authentication for UAVs and the reduction of authentication latency. Their proposed UAV security authentication scheme employs UAV controller in each region, which is responsible for authenticating and saving UAV identities within the region. When a UAV needs to migrate to another region, it only requires the UAV controller to check the BC information.

Additionally, researchers often discuss R2L and U2R attacks together in the context of network security. For example, authors in [71] and [127] discuss the utilization of ML-based IDSs to mitigate R2L and U2R attacks. In [71], a two-layer dimensionality reduction module and a two-layer detection module are used to detect R2L and U2R attacks. Different from [71], authors in [127] propose a layered random forest attack detection algorithm based on random search cross validation. Due to resource constraints, they also employ a feature selection algorithm based on the Pearson correlation coefficient to reduce the computational complexity of the model.

Besides the measures mentioned above that simultaneously prevent various types of identity attacks, specific security countermeasures have been proposed to target certain attacks. For example, authors in [128] propose an intelligent Sybil attack detection method for the FANET-based IoT. This method exploits the physical layer properties of radio signals emitted by UAVs and utilizes ML to classify the signals. Authors in [129] use the time series of **Received Signal Strength Indicator (RSSI)** as a feature to detect the mutation points in the RSSI time series using Bernaola Galván segmentation algorithm to identify the power control behaviour of illegal nodes. But its effectiveness is limited to specific attack types.

Lesson 2: Clearly, these countermeasures either aim to ensure that identity information is immutable (such as security strategies based on PUFs and BC) or consider to analysis the identity and behavior information of UAVs (such as security strategies based on ML and IDS). In addition, it is crucial to consider that resource-constrained UAV swarm networks require lightweight authentication protocols and detection schemes.

4.4 Network Resource Security Countermeasures for UAV Swarm Networks

The purpose of network resource attacks is to exploit various resources, such as network bandwidth resources and UAV computational resources, to steal data and gain control over UAV swarm networks. In the following, we review security measures for network resources in UAV swarm networks and provide a summary in Table 3.

Security Countermeasures for DoS/DDoS. The goal of DoS and DDoS is to flood a network with a large volume of malicious data packets, depleting network resources and disrupting network services. Therefore, most mitigation strategies for DoS and DDoS attacks focus on detecting and mitigating abnormal network traffic.

For DoS attacks, Zhang *et al.* propose an effective approach to design state feedback controllers against DoS attacks [130]. The approach involves introducing a logic processor embedded in the controller to capture information on the duration time of each DoS attack. By modeling the closed-loop system as an aperiodic sampled-data control system dependent on the maximum and minimum duration time of DoS attacks, resilient controllers can be designed using linear matrix inequalities with tuning parameters. Similarly, a software framework to provide DoS-resilient control for real-time UAS is proposed in [131]. They defend against DoS attacks primarily targeting at the CPU, memory, and communication channels by constraining resource usage.

For DDoS attacks, Safavat *et al.* propose a ML-based approach to enhance security of UAV networks controlled by an SDN controller [132]. Their method utilizes principal component analysis and linear discriminant analysis techniques to identify features associated with DDoS attacks. Subsequently, they employ a feedforward neural network classifier to classify normal and abnormal network traffic data from UAVs. Similarly, an ML-based approach for defending against DDoS attacks is proposed in [133]. The method uses synthetic minority oversampling technique to make a distinction between normal and abnormal data.

In addition to ML algorithms, researchers often employ IDS techniques to detect DDoS attacks. For instance, a hybrid approach based on spectral traffic analysis is proposed in [134]. The method utilizes wavelet-based data spectrum multifractal analysis to differentiate normal and abnormal traffic. Unlike ML or IDS-based research, Mairaj *et al.* discuss the use of game theory to prevent DDoS attacks on UAVs [135]. They propose five non-cooperative game scenarios for two DDoS attack variants and introduce the quantum response equilibrium concept to account for participants' mistakes and evolving behavioral patterns. Both Nash equilibria and quantum response equilibrium information are utilized to provide UAV operators with enhanced insights.

Security Countermeasures for Malware. Malware aims to disrupt availability, integrity, and functionality of software within UAV networks. Software behavior-based anomaly detection is a common approach to Malware attacks in UAV swarm networks. Authors in [136] use the timing information of subcomponents during software operations as features for detecting anomalies. They introduce anomaly detection techniques based on ranges, multidimensional euclidean distances, and single-class support vector machine classification.

Carreon *et al.* propose a statistical-based method for Malware detection [137]. The authors utilize the cumulative distribution function of timing data to capture the system behavior of applications. They also employ a probabilistic estimation approach to determine the presence of malware in individual operations and operation sequences within the software execution paths, while establishing the detection thresholds.

Authors in [138] point out that existing UAV malware detection techniques primarily analyze the malicious behavior occurring during communications between malware and control servers. However, these methods may not effectively detect advanced persistent threats that employ low-traffic attack patterns. To address this, the authors propose an Internet UAV malware detection method based on domain name system traffic. This method employs ML techniques to detect malware traffic, while also utilizing Fourier transform-based detection methods to identify domains associated with malware. In contrst, authors in [139] introduce a robust DL detection method based on device opcode sequences. The authors utilize a deep feature space to effectively differentiate between malicious and benign applications.

Security Countermeasures for Hijack. Hijacking attacks aim to compromise hardware resources within UAV swarm networks. Authors in [140] propose a method for detecting hijacked UAVs in UAV networks by corroborating event information from different sources. The method utilizes secure asymmetric encryption along with a pre-shared list of official UAVs to ensure authenticity and integrity of UAVs. Additionally, a trust policy inspired by BC principles is employed to identify infected UAVs.

Table 3. Summary of security countermeasures for network resources.

Attacks	Ref.	Technologies	Description
DoS	[130]	Logic processor	Designing resilient controllers to ensure system stability.
	[131]	Container	DoS attack resilience for real-time UAV systems.
DDoS	[132]	ML	Balancing load and detecting DDoS attacks in SDN-based environments for maximum throughput and security.
	[133]	DL	Detecting and identifying DDoS attacks to enhance network security.
	[134]	IDS	Detecting and analyzing various types of DDoS attacks.
	[135]	Game theoretic	Mitigating DDoS attacks by dynamic and static models for attackers and UAVs.
Malware	[136]	Timing anomaly detection	Data-driven anomaly detection based on temporal features in embedded systems.
	[137]	Anomaly detection	Detecting malware in embedded systems by analyzing timing data with an optimization approach.
	[138]	String matching, Fourier transform	Detecting malware to discover temporal correlations among domain name system requests from monitored devices.
	[139]	DL	Enhancing identification accuracy and resilience against junk code attacks in military IoT devices.
Hijack	[140]	Cryptography, Trust strategy	Detecting compromised UAVs by information verification and secure encryption methods.
	[141]	Anomaly detection	Detecting non-random behavior in robot swarms and isolating compromised robots.

Conversely, authors in [141] explore the detection of non-random behavior based on signs. They propose a runtime monitoring framework that utilizes the signed residual, which is the difference between expected and received information, for identifying and isolating unexpected non-random patterns in multirobot systems. They also introduce a technique called the cumulative sign detector that tracks fluctuations in the signed values of the residual, aiming to detect inconsistencies and initiate alarms upon detecting potential attacks.

Lesson 3: ML or IDSs are commonly employed to mitigate DoS or DDoS attacks within UAV swarm networks. For malware attacks, researchers typically focus on either detecting anomalies in software execution or monitoring data transmitted by the software. In the case of hijacking attacks, the primary focus lies in analyzing the behavior of UAVs or establishing a reputation mechanism to ascertain the normalcy of UAVs. However, almost all the research focus on accuracy, without considering the relationship between algorithm complexity and energy consumption.

4.5 Routing Security Countermeasures for UAV Swarm Networks

In UAV swarm networks, attackers conducting network routing attacks redirect data traffic to nodes under their control, aiming to steal sensitive information, disrupt network services, or engage in other malicious activities. Implementing secure routing measures is crucial to ensure the safety of UAV swarm networks. Therefore, we introduce mitigation measures for routing attacks in UAV swarm networks, and provide a brief summary of methods and approaches in Table 4.

Security Countermeasures for Wormhole. To counteract wormhole attacks, Teng *et al.* propose a detection algorithm integrated with the node trust optimization model [142]. The algorithm first adds nodes in the network with the number of neighbors exceeding the threshold to the suspicious list. If the route between the suspicious node and the neighbor node exceeds the wormhole threshold, then the path is marked as a test path and the trust level of the node is evaluated.

Similar to [142], authors in [143] propose an SDN-based wormhole analysis approach by using the neighbor similarity as a new wormhole countermeasure in software-defined **Mobile Ad Hoc Networks (MANETs)**. It uses an improved K-means algorithm to analyze the similarity index of adjacent nodes on a centralized SDN controller, and marks nodes that exceed the threshold. If the number of nodes' neighbors is much more than that before, it can be determined as a wormhole node. In addition, the algorithm does not require specific location information to detect wormholes.

Security Countermeasures for Black Hole. To counter black hole attacks, authors in [144] propose a BC based mechanism for UAVs, integrating a BC broadcast module with the routing protocol for low confirmation latency and high scalability. This mechanism employs BC consensus for behavior validation and a time-to-live forwarding rule against black hole attacks. Another study introduces a dynamic threshold-based protocol [145] to mitigate these attacks, calculating standard deviations of sequence numbers from response packets to identify malicious nodes using sequence number thresholds and hop counts. However, this approach increases routing overhead.

In contrast to the passive defense mentioned above, authors in [146, 147] adopt active defense approaches. Authors in [146] utilize data control packets to inspect nodes on the selected paths and utilize an extended data routing information table to detect and eliminate malicious nodes. Authors in [147] employ active detection techniques to identify and avoid suspicious nodes. They utilize multiple detection paths to detect anomalies in the network and ensure reliable data transmission.

Table 4. Summary of security countermeasures for routing.

Attacks	Ref.	Technologies	Description
Worm-hole	[142]	Anomaly detection	Detecting wormhole attacks in wireless sensor networks to conserve network energy.
	[143]	Anomaly detection	Detecting and countering wormhole attacks without location information in MANETs.
Black hole	[144]	BC	Trusted self-organizing in UAV swarms, focusing on secure data transmission and decision making.
	[145]	Anomaly detection	Detecting and preventing black hole attacks in MANETs to improve network security.
	[146]	Anomaly detection	Enhancing the detection and elimination of cooperative black hole attacks based on an extended data routing information table.
	[147]	Anomaly detection	Secure routing in wireless sensor networks to enhance data transmission success.
Gray hole	[148]	IDS	Detecting and defending against gray hole attacks by G-IDS nodes.
	[149]	Reputation system	Increasing packet delivery success and overall network performance by identifying and avoiding malicious nodes.

Security Countermeasures for Gray Hole. As mentioned earlier, gray hole attacks are challenging to trace, since the data packets are selectively discarded during the attack. Therefore, more complex and sophisticated strategies are required to detect and prevent such attacks in UAV swarm networks.

Authors in [148] deploy special **Gray hole Intrusion Detection System (G-IDS)** nodes in the network to monitor neighboring nodes' transmission. When a G-IDS node detects significant data packet loss beyond a threshold, it broadcasts an alert with the identity and addresses of the gray hole node to isolate it. A drawback is that G-IDS nodes can only detect their immediate neighbors.

Authors in [149] discuss the use of reputation-based mechanisms to secure MANETs by identifying and avoiding malicious nodes. The authors explore the effect of reputation on the throughput of a MANET by simulating four different scenarios. They further note that applying reputation to complete routing, rather than just neighboring nodes, results in successful packet transmission in adversarial networks.

Lesson 4: To ensure routing security in UAV swarm networks, extensive research has been conducted on reputation-based IDSs, BC techniques, and detection mechanisms. These methods aim to identify malicious nodes or routes and protect the integrity of routing within the system. However, these methods often overlook resource consumption within the network, which can be an important consideration for the overall system performance improvement.

4.6 Data Security Countermeasures for UAV Swarm Networks

In this section, we review the security strategies adopted by UAV swarms to mitigate data tampering attacks and FDIAs. We also summarize the countermeasures against data tampering attacks in Table 5 and provide a comprehensive summary of strategies against FDIAs in Table 6.

Security Countermeasures for Tampering. For data tampering attacks, researchers primarily leverage BC as a mitigation strategy. For example, Aggarwal *et al.* design a system that utilizes a public BC distributed network based on Ethereum for secure data transmission and collection [150]. BC stores the data collected by UAVs and updates the information to a distributed ledger, ensuring the security of both data and identities simultaneously. Similarly, Singh *et al.* also protect data dissemination by creating tamper-proof and transparent transaction records using BC [151].

However, these methods overlook the trustworthiness of miner nodes in the UAV swarm network. In contrast, authors in [152, 153] consider both secure data sharing using BC in the UAV swarm network and the honesty of nodes among network miners. Authors in [152] introduce credit as a metric for selecting miner nodes and evaluate miners using a highly accurate quadruple subjective logic model. The highest-credited node is chosen as the miner, and credits are recorded in a decentralized and tamper-proof manner to achieve secure data sharing. In contrast, authors in [153] propose a BC-based crowdsourcing framework with a reputation-based incentive mechanism to address the selfishness issue of untrusted UAVs. It aids task publishers in choosing UAVs with strong reputations, while the BC-based data transmission scheme ensures secure data sharing.

Table 5. Summary of security countermeasures for tampering attacks.

Ref.	Description	Consensus mechanisms	Reliable nodes	Lightweight framework
[150]	A BC-based scheme is proposed for enabling secure data dissemination.	Proof of stake	×	×
[151]	A BC-based security framework to ensure secure transmission of information.	Proof of work	×	×
[152]	A permission-based BC for data sharing in UAV networks.	Practical byzantine fault tolerance	√	×
[153]	A BC-based collaborative framework for securing data sharing between UAVs and task publishers.	Proof of work	√	×
[154]	A scheme for secure data sharing in UAV-assisted disaster relief.	Byzantine fault tolerant	√	√
[155]	A credit-based consensus algorithm to securely track UAV and vehicle misbehavior.	Delegated proof of stake	√	√

("√" if the solution satisfies the property, "×" if not.)

However, the aforementioned studies may overlook the issue of resource limitations. Authors in [154, 155] focus on data security and node honesty, while also considering energy-constrained scenarios. In Wang *et al.'s* research, they propose a lightweight BC framework that integrates reputation-based consensus protocols and an off-chain mechanism based on vehicular fog computing [154]. The lightweight implementation allows resource-constrained devices to store only block headers, while resource-intensive tasks are offloaded to ground vehicles. Additionally, the authors utilize RL-based algorithms to optimize payment and compute resource-sharing strategies during offloading to ensure secure data transmission. Similarly, a lightweight BC-based framework for secure data sharing is proposed in [155]. Authors develop a credit-based delegated proof of stake algorithm to enhance consensus efficiency. Similar to [154], the lightweight implementation allows resource-constrained devices to store only block headers, and RL techniques are applied to provide optimal strategies during the data sharing process.

Table 6. Summary of countermeasures for FDIA.

Ref.	Technologies	Description	Defects
[156]	ML	Detecting FDIAs in drone-collected images to enhance data security of UAVs.	The data type is too monolithic.
[157]	Anomaly detection	Detecting FDIAs in the cyber-physical system.	No compensation is made to the system.
[158]	Anomaly detection	Detecting FDIAs and interferences in UAS, ensuring UAV control safety.	The noise of the environment is not considered.
[159]	Anomaly detection, ML	Real-time detection and estimation for FDIAs in network control systems with noise.	Excessive computational complexity.
[160]	Anomaly detection	A distributed tracking algorithm to detect and identify GPS spoofing attacks.	Not suitable for places with few GPS devices.
[161]	DL	UAV GPS spoofing detection through analysis of path loss statistics.	Without the consideration of resource consumption.

Security Countermeasures for FDIAs. As mentioned earlier, apart from data tampering attacks, FDIAs is another significant data security threat in UAV swarm networks. To counter FDIAs, several mitigation strategies have been proposed.

For instance, authors in [156] present a DL-based technique to detect FDIAs in images acquired by UAVs. Images are initially preprocessed and then classified by a convolutional neural network. Nearest neighbor interpolation is employed to adjust the image size, followed by normalization using the min-max method. Subsequently, the Mahalanobis distance is utilized to assess the presence of FDIAs. However, their focus is primarily on FDIAs for images, neglecting system-specific FIDAs considerations. In contrast, authors in [157] present a specialized FDIAs detector designed to address environmental white noise. This detector collects current and historical information to reveal potential threats. Additionally, the false positive rate can be adjusted by selecting an appropriate threshold.

Unlike the work in [157], authors in [158] consider system compensation in addition to FDIAs detection. They introduce a multi-feature fusion-based attack detection mechanism, which utilizes average received signal power and estimation errors of injected virtual system verification signals to identify attacks. However, the above studies only focus on detecting FDIAs in a noisy environment or compensating for the attacked system, without considering the both at the same time. Sargolzaei *et al.* study FDIAs in a noisy environment and compensate for the attacked system [159]. They design a real-time FDIAs monitoring scheme that employs a linear Kalman filter in conjunction with a three-layer feedforward neural network observer.

GPS spoofing is an attack on positioning systems that can lead to uncontrolled behavior in UAV swarms not equipped with encrypted GPS systems. Researchers have proposed two main categories of countermeasures against GPS spoofing: passive defense and active detection [162]. Passive defense methods primarily involve encrypted GPS signals. However, encrypted GPS signals either necessitates the update of the existing GPS infrastructure or the modification of the GPS signal structure. Therefore, defense methods involving GPS signal encryption are typically employed in military activities and are not suitable for civilian UAVs [162]. In contrast, active detection of GPS spoofing is the main method in UAV swarm networks.

Active detection methods can utilize surrounding devices that provide GPS signals to detect and defend against GPS spoofing attacks. For example, in [160], authors utilize distributed radar ground stations equipped with local trackers to detect GPS spoofing attacks on UAVs. In addition to utilizing surrounding devices, ML algorithms can also be employed. Different from [160], an ML-based method is proposed in [161] to detect GPS spoofing attacks even with a single base station. The authors analyze the statistical features of path loss between UAVs and BSs to determine if UAVs are under GPS spoofing. They deploy six types of DL models on edge computing servers to integrate the results of multilayer perceptrons.

Lesson 5: From the above review of data security measures for UAV swarm networks, the main focus is to utilize the characteristics of BC to prevent data tampering attacks. As for FDIAs mitigation strategies, most researchers focus on utilizing ML or IDSs to design detection mechanisms based on data authentication. However, BC-based security measures have limited considerations for lightweight implementations. Similarly, ML or IDS detection mechanisms also need to take account of energy consumption caused by high computational complexity.

4.7 Security and Privacy Protection Countermeasures for Machine Learning in UAV Swarm Networks

As previously mentioned, ML is not inherently secure. Therefore, trustworthy ML countermeasures are essential to maintain security and reliability of UAV swarm networks. In the following, we review security and privacy protection strategies for ML in UAV swarm networks and summarize them in Table 7.

Security Countermeasures for ML Models. For UAV swarms, if the underlying ML models are compromised without detection, this may result in the loss of UAV control.

One common method to compromise ML models is through adversarial attacks, often executed by adding perturbations along the largest gradient. Common mitigation strategies against these attacks include adversarial training, although this approach is computationally intensive. To conserve computational resources, authors in [163] investigate the causal relationships among samples, outputs, and actual labels under adversarial conditions as a means to mitigate these attacks. Notably, this method also provides portability.

Compared to ML, FL is more commonly applied in UAV swarm networks, leading to an increased focus on security solutions of FL models. For the model-safe aggregation problem in FL, an SMC based global model aggregation method is introduced in [164], to ensure the absence of malicious local models during the aggregation process. The method sends a query to all users during the aggregation process and generates a response in each iteration to verify whether the user has malicious purposes.

Wang *et al.* construct multiple explainable models and backdoor classifiers on the server, randomly sent to the agent during training. This prevents the agent from sending malicious parameters to the server [165]. For suspicious backdoor data, the authors use a blur-label-flipping strategy to clean them and restore data availability.

Nguyen *et al.* use noise to eliminate backdoor attacks in aggregation[166]. However, noise injection based on DP excitation degrades the performance of the aggregation model. Therefore, authors provide boundary proofs for the injected noise and use model clustering and weight pruning methods to select the submission parameters to mitigate the effect of noise.

In addition to the methods mentioned above, there is also the approach using statistics and weight shares to achieve secure aggregation of models. Authors in [167] propose a mitigation method based on zero-knowledge clustering. During the aggregation iteration, if a node is identified as malicious and differs from normal nodes in statistical characteristics, its weight is reduced.

Furthermore, authors in [170, 171] use BC to ensure the security of participants, thereby safeguarding the security of FL aggregation. BC is employed to verify the legitimacy of participants in FL model aggregation [170, 171]. In contrast, in [172], BC is utilized to ensure the security of local data, thereby protecting the security of aggregated parameters.

Table 7. Summary of countermeasures for ML security.

Attacks	Ref.	Technologies	Description
Adversarial	[163]	Causal Theory	A gradient-based approach to maintain detection model accuracy.
Back door	[165]	ML	A federated filter-based algorithm to protect applications from malicious data.
	[166]	Anomaly detection	A defense framework to detect and remove high-impact anomalous models.
Model aggregation	[167]	ML	A zero-knowledge clustering algorithm to enhance the robustness of FL systems.
Membership inference	[168]	SMC	A FL framework for private and accurate data sharing in edge computing scenarios.
FL model privacy	[169]	AN	A UAV-assisted covert FL algorithm to reduce convergence time and energy consumption of devices.
Poisoning, Membership inference	[170]	BC, SMC, HE	A BC-based FL algorithm for UAVs to enhance data privacy.
Model aggregation and FL model privacy	[164]	SMC	A FL scheme for defense against poisoning attacks.
	[171]	DP, BC	An algorithm to achieve trustworthy privacy-preserving ML.
	[172]	ML, DP	An intrusion detection algorithm for UAV networks, addressing data imbalance and privacy challenges.

Privacy Protection Countermeasures for ML Models. There are also privacy attacks directed towards ML models. If the underlying ML privacy is compromised, it can potentially lead to the leakage of confidential information within the network.

Regarding the privacy issue of the FL training process, Li *et al.* propose an FL framework based on SMC techniques to protect data privacy during model sharing [168]. Participants are organized into a chain-like structure. Each participant in a chain generates output by adding masking information to their gradient. The output of a parent participant is used as masking information by its descendant participants to protect the gradient. The final participant sends its output as the aggregated gradient of all participants in the chain back to the server. This way, adversaries cannot extract privacy-sensitive information from the participants' outputs.

For the problem of parameter eavesdropping during the FL model aggregation process, authors in [169] present a solution in which UAVs not only participate in training during the FL aggregation process but also emit AN interference against eavesdroppers. It is worth noting that if the privacy problems faced by FL models during aggregation are related to the physical layer, the security measures adopted in UAV swarm communications can be used as references.

Furthermore, to prevent parameter inference during the aggregation of FL models, authors in [171, 172] use DP to ensure the privacy of participants when uploading their local parameters. In contrast, authors in [164, 170] use SMC to aggregate the models without revealing any information about the parameters of the aggregated model. They also use masking to protect the privacy of local models.

Lesson 6: BC, HE, DP, and SMC are commonly used techniques to mitigate security and privacy attacks for ML in UAV swarm networks. However, existing mitigation measures often target specific security or privacy attacks within ML, and do not fully consider the possibility of the coexistence of multiple attacks. Furthermore, they do not take into account the resource constraints and the diversity of scenarios related to UAV swarm networks.

5 Research Challenges and Open Issues

Because the applications of UAV swarms continue to expand, the security concerns in this field have gained significant attention. While numerous security countermeasures are available currently, several challenges and open issues still need to be addressed, which are discussed below.

5.1 Resource Constraints in UAV Swarm Networks

The security of UAV swarm networks is difficult to guarantee, since limited network resources pose a major challenge to the design of effective security measures. Solutions based on BC, cryptography, and ML require significant energy support, which may be impractical for resource-constrained UAVs. Therefore, there is an urgent need for lightweight algorithms that can balance security and resource consumption.

In addition to studying lightweight algorithms to save the energy of UAV swarm networks, there are other methods to mitigate the problem of energy constraints in UAV swarm networks, such as wireless charging. It can ensure that UAVs have sufficient power to perform tasks. Previous studies [109] and [110] both mention the application of wireless charging technology in UAVs. However, dedicated research on wireless charging for UAV swarms is still relatively limited. Future research should further explore the potential of these technologies in UAV swarms.

5.2 The Joint Software and Hardware Design for Secure UAV Swarm Networks

In the Cybersecurity of UAV swarm networks, most researchers focus on studying security algorithms implemented at the software level, such as encryption, authentication, and authorization. However, software and hardware are interdependent. In addition to considering secure algorithms, how to ensure the security of UAV swarm networks from a perspective of software-hardware integration is essential. SDN technology is a typical example that encompasses both software and hardware. The software control plane of SDN achieves centralized control and management of the network, while the hardware of SDN provides data processing and forwarding capabilities. Through the integration of software and hardware, SDN effectively accomplishes functions such as centralized control, dynamic configuration, and programmability.

Integrating SDN into UAV swarm networks can provide security for the data within the network. This is because all data is routed through a central controller, allowing centralized analysis to identify and filter out anomalous data. Furthermore, SDN can facilitate network slicing in UAV swarm networks, isolating external access. While SDN offers advantages in network management and data forwarding, it also exposes potential security vulnerabilities, such as DDoS and replay attacks. Additionally, SDN controller in UAV swarm networks is susceptible to single points of failure. Lastly, the high mobility of UAVs may pose connectivity challenges with SDN controllers. Therefore, integrating SDN into UAV swarm networks presents several challenges.

5.3 3D Placement of UAV Swarm Networks

Currently, there are some studies on the 3D positioning of individual UAVs. For instance, studies like [173] and [174] propose models that provide 3D modeling of UAV motion, effectively preventing eavesdropping attacks. Although research on the 3D trajectories of UAVs has made some progress, such as significantly improving average secrecy rates compared to 2D schemes, there is currently a lack of dedicated research focusing on 3D trajectories for UAV swarms. One of the main reasons is that planning the 3D trajectories for UAV swarms is more complex and dynamic than those for individual UAVs. However, appropriate planning of the 3D positions for UAV swarms can save energy for the entire UAV swarm network and enhances the overall system security. While the applications of UAV swarms continue to expand, the 3D trajectory planning of UAV group has become a key problem that must be solved.

5.4 Artificial Intelligence-based Secure Routing Protocols in UAV Swarm Networks

Traditional routing protocols can provide basic communication support for UAV swarms; however, they lack security when facing routing attacks such as black holes and grey holes, and their performance may degrade in adverse environments. Considering the immense potential demonstrated by **Artificial Intelligence (AI)** in other applications of UAV swarm networks, AI may offer new solutions for secure routing. Nevertheless, the trustworthiness of AI must be taken into account [175]. Researchers have already explored AI-based routing protocols, such as topology prediction and adaptive learning-based methods, but AI-based secure routing protocols specifically tailored for UAV swarm networks remain unexplored.

Furthermore, due to the diverse applications of UAV swarms, it is necessary to investigate secure routing protocols suitable for different scenarios and attack patterns. At the same time, AI-based secure routing protocols often require high computational and communication resources to detect and respond to network attacks in realtime, which may harm the overall performance and efficiency of UAV swarms. Therefore, appropriate measures need to be taken to make a trade-off between performance and security.

5.5 The Application of Quantum Cryptography in UAV Swarm Networks

With the emergence of quantum computers, encryption-based security solutions, even those with high mathematical complexity, may be vulnerable to quantum attacks [95]. With resource-constrained devices, UAV swarm networks' encryption schemes are even more susceptible to potential breaches. Therefore, new technologies are needed to safeguard the security of UAV swarm networks.

Quantum cryptography presents new countermeasures for enhancing the security of UAV swarm networks. First, quantum cryptography can utilize encryption methods based on quantum properties to ensure data security. Second, quantum key distribution can be employed to establish secure keys, enhancing communication privacy among UAVs and protecting data transmission within UAV swarms.

However, integrating quantum cryptography into UAV swarm networks also has significant challenges. First, quantum cryptography is complex, requiring extensive technical support when incorporated into UAV swarm networks. Second, cost may pose obstacles to the adoption of quantum-secure communication, given the typically expensive hardware and infrastructure investments associated with this technology. Additionally, addressing the management of quantum keys, especially in large-scale UAV swarm networks, remains a challenge. Last, UAVs are resource-constraint devices, necessitating appropriate solutions that balance security and performance.

6 Conclusion

We conduct a comprehensive survey on security of UAV swarm networks. First, we briefly introduce the three key aspects of UAV swarm networks and outline corresponding applications. Next, we discuss and categorize existing and potential security threats in UAV swarm networks based on their consequences. Regarding the threats, we also discuss existing security-based techniques. Additionally, we summarize mitigation strategies adopted by UAV swarm networks for different types of attacks. Finally, we explore current challenges faced by UAV swarm networks and suggest future research directions. We believe that this survey can help researchers in understanding and studying UAV swarm networks.

References

[1] Panagiotis Radoglou-Grammatikis, Panagiotis Sarigiannidis, Thomas Lagkas, and Ioannis Moscholios. 2020. A compilation of UAV applications for precision agriculture. *Computer Networks* 172 (2020), 107148.

[2] Jiong Dong, Kaoru Ota, and Mianxiong Dong. 2021. UAV-Based Real-Time Survivor Detection System in Post-Disaster Search and Rescue Operations. *IEEE Journal on Miniaturization for Air and Space Systems* 2, 4 (2021), 209–219. DOI: http://dx.doi.org/10.1109/JMASS.2021.3083659

[3] Zhuohui Yao, Wenchi Cheng, Wei Zhang, Tao Zhang, and Hailin Zhang. 2022. The Rise of UAV Fleet Technologies for Emergency Wireless Communications in Harsh Environments. *IEEE Network* 36, 4 (2022), 28–37.
[4] Milan Erdelj, Michał Król, and Enrico Natalizio. 2017. Wireless sensor networks and multi-UAV systems for natural disaster management. *Computer Networks* 124 (2017), 72–86.
[5] Muhammad Atif, Rizwan Ahmad, Waqas Ahmad, Liang Zhao, and Joel J. P. C. Rodrigues. 2021. UAV-Assisted Wireless Localization for Search and Rescue. *IEEE Systems Journal* 15, 3 (2021), 3261–3272. DOI: http://dx.doi.org/10.1109/JSYST.2020.3041573
[6] Hailong Huang and Andrey V. Savkin. 2021. Navigating UAVs for Optimal Monitoring of Groups of Moving Pedestrians or Vehicles. *IEEE Transactions on Vehicular Technology* 70, 4 (2021), 3891–3896. DOI: http://dx.doi.org/10.1109/TVT.2021.3065102
[7] Vinay Chamola, Pavan Kotesh, Aayush Agarwal, Navneet Gupta, Mohsen Guizani, et al. 2021. A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. *Ad hoc networks* 111 (2021), 102324.
[8] Chengcai Wang, Ao Wu, Yueqi Hou, Xiaolong Liang, Luo Xu, and Xiaomo Wang. 2023. Optimal deployment of swarm positions in cooperative interception of multiple UAV swarms. *Digital Communications and Networks* 9, 2 (2023), 567–579.
[9] Xiaofang Sun, Derrick Wing Kwan Ng, Zhiguo Ding, Yanqing Xu, and Zhangdui Zhong. 2019. Physical Layer Security in UAV Systems: Challenges and Opportunities. *IEEE Wireless Communications* 26, 5 (2019), 40–47. DOI: http://dx.doi.org/10.1109/MWC.001.1900028
[10] Zhaoxuan Wang, Yang Li, Shihao Wu, Yuan Zhou, Libin Yang, Yuan Xu, Tianwei Zhang, and Quan Pan. 2023. A survey on cybersecurity attacks and defenses for unmanned aerial systems. *Journal of Systems Architecture* 138 (2023), 102870.
[11] Abdelouahid Derhab, Omar Cheikhrouhou, Azza Allouch, Anis Koubaa, Basit Qureshi, Mohamed Amine Ferrag, Leandros Maglaras, and Farrukh Aslam Khan. 2023. Internet of Drones Security: Taxonomies, Open Issues, and Future Directions. *Vehicular Communications* 39 (2023), 100552.
[12] Vikas Hassija, Vinay Chamola, Adhar Agrawal, Adit Goyal, Nguyen Cong Luong, Dusit Niyato, Fei Richard Yu, and Mohsen Guizani. 2021. Fast, reliable, and secure drone communication: A comprehensive survey. *IEEE Communications Surveys & Tutorials* 23, 4 (2021), 2802–2832.
[13] Li Wang, Yu Chen, Pu Wang, and Zheng Yan. 2021. Security Threats and Countermeasures of Unmanned Aerial Vehicle Communications. *IEEE Communications Standards Magazine* 5, 4 (2021), 41–47. DOI: http://dx.doi.org/10.1109/MCOMSTD.0001.2000078
[14] Parimal Mehta, Rajesh Gupta, and Sudeep Tanwar. 2020. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Computer Communications* 151 (2020), 518–538.
[15] Yassine Mekdad, Ahmet Aris, Leonardo Babun, Abdeslam El Fergougui, Mauro Conti, Riccardo Lazzeretti, and A Selcuk Uluagac. 2023. A survey on security and privacy issues of UAVs. *Computer Networks* 224 (2023), 109626.
[16] Fadhila Tlili, Lamia Chaari Fourati, Samiha Ayed, and Bassem Ouni. 2022. Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures. *Ad Hoc Networks* 129 (2022), 102805.
[17] Alessio Rugo, Claudio A Ardagna, and Nabil El Ioini. 2022. A security review in the UAVNet era: Threats, countermeasures, and gap analysis. *Comput. Surveys* 55, 1 (2022), 1–35.
[18] Kai-Yun Tsao, Thomas Girdler, and Vassilios G Vassilakis. 2022. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks* 133 (2022), 102894.
[19] Patrick McEnroe, Shen Wang, and Madhusanka Liyanage. 2022. A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges. *IEEE Internet of Things Journal* 9, 17 (2022), 15435–15459. DOI: http://dx.doi.org/10.1109/JIOT.2022.3176400
[20] Wu Chen, Jiajia Liu, Hongzhi Guo, and Nei Kato. 2020. Toward Robust and Intelligent Drone Swarm: Challenges and Future Directions. *IEEE Network* 34, 4 (2020), 278–283. DOI: http://dx.doi.org/10.1109/MNET.001.1900521
[21] Reza Shakeri, Mohammed Ali Al-Garadi, Ahmed Badawy, Amr Mohamed, Tamer Khattab, Abdulla Khalid Al-Ali, Khaled A Harras, and Mohsen Guizani. 2019. Design challenges of multi-UAV systems in cyber-physical applications: A comprehensive survey and future directions. *IEEE Communications Surveys & Tutorials* 21, 4 (2019), 3340–3385.
[22] Haifa Touati, Amira Chriki, Hichem Snoussi, and Farouk Kamoun. 2021. Cognitive Radio and Dynamic TDMA for efficient UAVs swarm communications. *Computer Networks* 196 (2021), 108264.
[23] Anna Maria Vegni, Valeria Loscri, Carlos T Calafate, and Pietro Manzoni. 2021. Communication Technologies Enabling Effective UAV Networks: a Standards Perspective. *IEEE Communications Standards Magazine* 5, 4 (2021), 33–40.
[24] Amira Chriki, Haifa Touati, Hichem Snoussi, and Farouk Kamoun. 2019. FANET: Communication, mobility models and security issues. *Computer Networks* 163 (2019), 106877.
[25] Demeke Shumeye Lakew, Umar Sa'ad, Nhu-Ngoc Dao, Woongsoo Na, and Sungrae Cho. 2020. Routing in flying ad hoc networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials* 22, 2 (2020), 1071–1120.
[26] Andy Couturier and Moulay A Akhloufi. 2021. A review on absolute visual localization for UAV. *Robotics and Autonomous Systems* 135 (2021), 103666.
[27] Momena Monwar, Omid Semiari, and Walid Saad. 2018. Optimized Path Planning for Inspection by Unmanned Aerial Vehicles Swarm with Energy Constraints. In *Proc. IEEE GLOBECOM.* 1–6. DOI: http://dx.doi.org/10.1109/GLOCOM.2018.8647342
[28] Alejandro Puente-Castro, Daniel Rivero, Alejandro Pazos, and Enrique Fernandez-Blanco. 2022. A review of artificial intelligence applied to path planning in UAV swarms. *Neural Computing and Applications* (2022), 1–18.

[29] A. N. Wilson, Abhinav Kumar, Ajit Jha, and Linga Reddy Cenkeramaddi. 2022. Embedded Sensors, Communication Technologies, Computing Platforms and Machine Learning for UAVs: A Review. *IEEE Sensors Journal* 22, 3 (2022), 1807–1826. DOI: http://dx.doi.org/10.1109/JSEN.2021.3139124

[30] Jia Wu, Chunbo Luo, Yang Luo, and Ke Li. 2022. Distributed UAV Swarm Formation and Collision Avoidance Strategies Over Fixed and Switching Topologies. *IEEE Transactions on Cybernetics* 52, 10 (2022), 10969–10979. DOI: http://dx.doi.org/10.1109/TCYB.2021.3132587

[31] Zhiqing Wei, Zeyang Meng, Meichen Lai, Huici Wu, Jiarong Han, and Zhiyong Feng. 2022. Anti-Collision Technologies for Unmanned Aerial Vehicles: Recent Advances and Future Trends. *IEEE Internet of Things Journal* 9, 10 (2022), 7619–7638. DOI: http://dx.doi.org/10.1109/JIOT.2021.3135578

[32] Derek Kingston, Randal W. Beard, and Ryan S. Holt. 2008. Decentralized Perimeter Surveillance Using a Team of UAVs. *IEEE Transactions on Robotics* 24, 6 (2008), 1394–1404. DOI: http://dx.doi.org/10.1109/TRO.2008.2007935

[33] Wouter H Maes and Kathy Steppe. 2019. Perspectives for remote sensing with unmanned aerial vehicles in precision agriculture. *Trends in plant science* 24, 2 (2019), 152–164.

[34] Jianguo Sun, Wenshan Wang, Sizhao Li, Qingan Da, and Lei Chen. 2023. Scheduling optimization for UAV communication coverage using virtual force-based PSO model. *Digital Communications and Networks, DOI:https://doi.org/10.1016/j.dcan.2023.01.007* (2023).

[35] Zhaolong Ning, Hao Hu, Xiaojie Wang, Qingqing Wu, Chau Yuen, F. Richard Yu, and Yan Zhang. 2024. Joint User Association, Interference Cancellation and Power Control for Multi-IRS Assisted UAV Communications. *IEEE Transactions on Wireless Communications, DOI:10.1109/TWC.2024.3401152* (2024).

[36] Zhaolong Ning, Yuxuan Yang, Xiaojie Wang, Lei Guo, Xinbo Gao, Song Guo, and Guoyin Wang. 2023. Dynamic Computation Offloading and Server Deployment for UAV-Enabled Multi-Access Edge Computing. *IEEE Transactions on Mobile Computing* 22, 5 (2023), 2628–2644. DOI: http://dx.doi.org/10.1109/TMC.2021.3129785

[37] Zhaolong Ning, Peiran Dong, Miaowen Wen, Xiaojie Wang, Lei Guo, Ricky Y. K. Kwok, and H. Vincent Poor. 2021. 5G-Enabled UAV-to-Community Offloading: Joint Trajectory Design and Task Scheduling. *IEEE Journal on Selected Areas in Communications* 39, 11 (2021), 3306–3320. DOI: http://dx.doi.org/10.1109/JSAC.2021.3088663

[38] Xiaojie Wang, Zhaolong Ning, Song Guo, Miaowen Wen, Lei Guo, and H. Vincent Poor. 2023. Dynamic UAV Deployment for Differentiated Services: A Multi-Agent Imitation Learning Based Approach. *IEEE Transactions on Mobile Computing* 22, 4 (2023), 2131–2146. DOI: http://dx.doi.org/10.1109/TMC.2021.3116236

[39] Behzad Shirani, Majdeddin Najafi, and Iman Izadi. 2019. Cooperative load transportation using multiple UAVs. *Aerospace Science and Technology* 84 (2019), 158–169.

[40] Samira Hayat, Evşen Yanmaz, and Raheeb Muzaffar. 2016. Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint. *IEEE Communications Surveys & Tutorials* 18, 4 (2016), 2624–2661. DOI: http://dx.doi.org/10.1109/COMST.2016.2560343

[41] Zhaolong Ning, Yuxuan Yang, Xiaojie Wang, Qingyang Song, Lei Guo, and Abbas Jamalipour. 2024. Multi-Agent Deep Reinforcement Learning Based UAV Trajectory Optimization for Differentiated Services. *IEEE Transactions on Mobile Computing* 23, 5 (2024), 5818–5834.

[42] Kevin Dorling, Jordan Heinrichs, Geoffrey G Messier, and Sebastian Magierowski. 2016. Vehicle routing problems for drone delivery. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 47, 1 (2016), 70–85.

[43] Idris Jeelani and Masoud Gheisari. 2021. Safety challenges of UAV integration in construction: Conceptual analysis and future research roadmap. *Safety science* 144 (2021), 105473.

[44] Daojing He, Guang Yang, Hongyi Li, Sammy Chan, Yao Cheng, and Nadra Guizani. 2021. An Effective Countermeasure Against UAV Swarm Attack. *IEEE Network* 35, 1 (2021), 380–385. DOI: http://dx.doi.org/10.1109/MNET.011.2000380

[45] Wei Wu, Fuhui Zhou, Baoyun Wang, Qihui Wu, Chao Dong, and Rose Qingyang Hu. 2022. Unmanned aerial vehicle swarm-enabled edge computing: Potentials, promising technologies, and challenges. *IEEE Wireless Communications* 29, 4 (2022), 78–85.

[46] Katharina Ley Best, Jon Schmid, Shane Tierney, Jalal Awan, Nahom M. Beyene, Maynard A. Holliday, Raza Khan, and Karen Lee. 2020. *How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools.* RAND Corporation, DOI: 10.7249/RR2972, Santa Monica, CA. DOI: http://dx.doi.org/10.7249/RR2972

[47] Yitao Han, Lingjie Duan, and Rui Zhang. 2019. Jamming-Assisted Eavesdropping Over Parallel Fading Channels. *IEEE Transactions on Information Forensics and Security* 14, 9 (2019), 2486–2499.

[48] Hossein Pirayesh and Huacheng Zeng. 2022. Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials* 24, 2 (2022), 767–809. DOI: http://dx.doi.org/10.1109/COMST.2022.3159185

[49] Center for the Study of the Drone. 2019. Countering Unmanned Aircraft Systems: Second Edition. (Dec. 2019). https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf Accessed December 2019, from Bard College.

[50] Kai Zeng, Kannan Govindan, Daniel Wu, and Prasant Mohapatra. 2011. Identity-based attack detection in mobile wireless networks. In *Proc. IEEE INFOCOM.* 1880–1888.

[51] Dragos Mocrii, Yuxiang Chen, and Petr Musilek. 2018. IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things* 1-2 (2018), 81–98.

[52] Chenyu Wang, Ding Wang, Yi Tu, Guoai Xu, and Huaxiong Wang. 2022. Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks. *IEEE Transactions on Dependable and Secure Computing* 19, 1 (2022), 507–523.

[53] Fei Xiong, Aijing Li, Hai Wang, and Lijuan Tang. 2019. An SDN-MQTT Based Communication System for Battlefield UAV Swarms. *IEEE Communications Magazine* 57, 8 (2019), 41–47. DOI: http://dx.doi.org/10.1109/MCOM.2019.1900291

[54] Osqzss. 2023. GPS-SDR-SIM: A software-defined radio simulator for GPS signals. GitHub, Online: https://github.com/osqzss/gps-sdr-sim. (2023).

[55] Zhaolong Ning, Hao Hu, Xiaojie Wang, Lei Guo, Song Guo, Guoyin Wang, and Xinbo Gao. 2023. Mobile Edge Computing and Machine Learning in the Internet of Unmanned Aerial Vehicles: A Survey. *ACM Comput. Surv.* 56, 1, Article 13 (2023), 31 pages.

[56] Harrison Kurunathan, Hailong Huang, Kai Li, Wei Ni, and Ekram Hossain. 2024. Machine Learning-Aided Operations and Communications of Unmanned Aerial Vehicles: A Contemporary Survey. *IEEE Communications Surveys & Tutorials* 26, 1 (2024), 496–533.

[57] Xiaojie Wang, Jiameng Li, Jun Wu, Lei Guo, and Zhaolong Ning. 2024. Energy Efficiency Optimization of IRS and UAV-Assisted Wireless Powered Edge Networks. *IEEE Journal of Selected Topics in Signal Processing, DOI:10.1109/JSTSP.2024.3452501* (2024), 1–14.

[58] Roland Zimmermann. 2024. Foolbox: A Python toolbox to generate adversarial perturbations for deep neural networks. GitHub, Online: https://github.com/bethgelab/foolbox. (2024).

[59] Nicolas Papernot. 2024. CleverHans: A software library for adversarial machine learning. GitHub, Online: https://github.com/cleverhans-lab/cleverhans. (2024).

[60] Maria-Irina Nicolae, Mathieu Sinn, Minh Ngoc Tran, Beat Buesser, Ambrish Rawat, Martin Wistuba, Valentina Zantedeschi, Nathalie Baracaldo, Bryant Chen, Heiko Ludwig, Ian M. Molloy, and Ben Edwards. 2019. Adversarial Robustness Toolbox v1.0.0. *arXiv preprint* (2019). arXiv:1807.01069 https://arxiv.org/abs/1807.01069

[61] Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, and Pascal Frossard. 2015. DeepFool: A Simple and Accurate Method to Fool Deep Neural Networks. *Proc. IEEE CVPR* (2015), 2574–2582. https://api.semanticscholar.org/CorpusID:12387176

[62] Jianbo Chen, Michael I. Jordan, and Martin J. Wainwright. 2020. HopSkipJumpAttack: A Query-Efficient Decision-Based Attack. In *Proc. IEEE SP*. 1277–1294. DOI: http://dx.doi.org/10.1109/SP40000.2020.00045

[63] Yang Wu, Xinrong Guan, Weiwei Yang, and Qingqing Wu. 2021. UAV swarm communication under malicious jamming: Joint trajectory and clustering design. *IEEE Wireless Communications Letters* 10, 10 (2021), 2264–2268.

[64] Haiyang Zhang, Lingjie Duan, and Rui Zhang. 2020. Jamming-Assisted Proactive Eavesdropping Over Two Suspicious Communication Links. *IEEE Transactions on Wireless Communications* 19, 7 (2020), 4817–4830.

[65] Haiquan Lu, Haiyang Zhang, Haibo Dai, Wei Wu, and Baoyun Wang. 2019. Proactive Eavesdropping in UAV-Aided Suspicious Communication Systems. *IEEE Transactions on Vehicular Technology* 68, 2 (2019), 1993–1997.

[66] Panayiota Valianti, Savvas Papaioannou, Panayiotis Kolios, and Georgios Ellinas. 2022. Multi-Agent Coordinated Close-in Jamming for Disabling a Rogue Drone. *IEEE Transactions on Mobile Computing* 21, 10 (2022), 3700–3717.

[67] DeDrone. Online: https://www.dedrone.com/white-papers/counter-uas. Counter-UAS: What you need to know to protect against drone threats. (Online: https://www.dedrone.com/white-papers/counter-uas). https://www.dedrone.com/white-papers/counter-uas

[68] Sara Lazzaro, Vincenzo De Angelis, Anna Maria Mandalari, and Francesco Buccafurri. 2024. Is Your Kettle Smarter Than a Hacker? A Scalable Tool for Assessing Replay Attack Vulnerabilities on Consumer IoT Devices. In *Proc. IEEE PerCom*. 114–124.

[69] J. Newsome, E. Shi, D. Song, and A. Perrig. 2004. The Sybil attack in sensor networks: analysis & defenses. In *Proc. IEEE IPSN*. 259–268.

[70] O. Jetter, J. Dinger, and H. Hartenstein. 2010. Quantitative Analysis of the Sybil Attack and Effective Sybil Resistance in Peer-to-Peer Systems. In *Proc. IEEE ICC*. 1–6.

[71] Hamed Haddad Pajouh, Reza Javidan, Raouf Khayami, Ali Dehghantanha, and Kim-Kwang Raymond Choo. 2019. A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks. *IEEE Transactions on Emerging Topics in Computing* 7, 2 (2019), 314–323. DOI: http://dx.doi.org/10.1109/TETC.2016.2633228

[72] Gabriel Vasconcelos, Gabriel Carrijo, Rodrigo Miani, Jefferson Souza, and Vitor Guizilini. 2016. The Impact of DoS Attacks on the AR.Drone 2.0. In *Proc. IEEE LARS/SBR*. 127–132.

[73] Gabriel Vasconcelos, Rodrigo Miani, Vitor Guizilini, and Jefferson Souza. 2019. Evaluation of DoS attacks on commercial Wi-Fi-based UAVs. *International Journal of Computer Network and Information Security* 11 (04 2019), 212.

[74] Anthony C. Tang. 2020. A Review on Cybersecurity Vulnerabilities for Urban Air Mobility. *AIAA Scitech 2021 Forum* (2020). https://api.semanticscholar.org/CorpusID:234312401

[75] Harun Oz, Ahmet Aris, Albert Levi, and A Selcuk Uluagac. 2022. A survey on ransomware: Evolution, taxonomy, and defense solutions. *Comput. Surveys* 54, 11s (2022), 1–37.

[76] R Lakshmana Kumar, Quoc-Viet Pham, Firoz Khan, Md Jalil Piran, and Kapal Dev. 2021. Blockchain for securing aerial communications: Potentials, solutions, and research directions. *Physical Communication* 47 (2021), 101390.

[77] Chris Arnold . Online: https://airpower.airforce.gov.au/sites/default/files/2022-04/BP16723318.pdf, 2021-05. Swarms of Trouble: The Hidden Threat of Consumer UAVs. (Online: https://airpower.airforce.gov.au/sites/default/files/2022-04/BP16723318.pdf, 2021-05).

[78] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, and Abbas Jamalipour. 2007. A survey of routing attacks in mobile ad hoc networks. *IEEE Wireless Communications* 14, 5 (2007), 85–91.

[79] Pericle Perazzo, Carlo Vallati, Dario Varano, Giuseppe Anastasi, and Gianluca Dini. 2018. Implementation of a wormhole attack against a rpl network: Challenges and effects. In *Proc. IEEE WONS*. 95–102.

[80] Andrew Fiade, Afie Yudha Triadi, Ahmad Sulhi, Siti Ummi Masruroh, Velia Handayani, and Hendra Bayu Suseno. 2020. Performance Analysis of Black Hole Attack and Flooding Attack AODV Routing Protocol on VANET (Vehicular Ad-Hoc Network). In *Proc. IEEE CITSM*. 1–5.

[81] Priya Chawla and Monika Sachdeva. 2018. Detection of Selective Forwarding (Gray Hole) Attack on LEACH in Wireless Sensor Networks. *Next-Generation Networks* (2018), 389–398.

[82] Yifa Liu and Long Cheng. 2023. Completely Stealthy FDI Attack Against State Estimation in Networked Control Systems. *IEEE Transactions on Circuits and Systems II: Express Briefs* 70, 3 (2023), 1114–1118. DOI:http://dx.doi.org/10.1109/TCSII.2022.3217132

[83] Yawen Tan, Jiajia Liu, and Nei Kato. 2021. Blockchain-Based Key Management for Heterogeneous Flying Ad Hoc Network. *IEEE Transactions on Industrial Informatics* 17, 11 (2021), 7629–7638. DOI:http://dx.doi.org/10.1109/TII.2020.3048398

[84] Peng Jiang, Hongyi Wu, and Chunsheng Xin. 2022. DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network. *Digital Communications and Networks* 8, 5 (2022), 791–803.

[85] Chuanshuai Chen and Jiazhu Dai. 2021. Mitigating backdoor attacks in LSTM-based text classification systems by Backdoor Keyword Identification. *Neurocomputing* 452 (2021), 253–262. DOI:http://dx.doi.org/10.1016/j.neucom.2021.04.105

[86] Yuanyuan Sun, Jiajia Liu, Jiadai Wang, Yurui Cao, and Nei Kato. 2020. When Machine Learning Meets Privacy in 6G: A Survey. *IEEE Communications Surveys & Tutorials* 22, 4 (2020), 2694–2724. DOI:http://dx.doi.org/10.1109/COMST.2020.3011561

[87] Jiwei Tian, Buhong Wang, Rongxiao Guo, Zhen Wang, Kunrui Cao, and Xiaodong Wang. 2022. Adversarial Attacks and Defenses for Deep-Learning-Based Unmanned Aerial Vehicles. *IEEE Internet of Things Journal* 9, 22 (2022), 22399–22409. DOI:http://dx.doi.org/10.1109/JIOT.2021.3111024

[88] Hongsheng Hu, Zoran Salcic, Lichao Sun, Gillian Dobbie, Philip S. Yu, and Xuyun Zhang. 2022. Membership Inference Attacks on Machine Learning: A Survey. *Comput. Surveys* 54, 11s (2022), 37.

[89] James Olds. 2023. PrivacyRaven. GitHub, Online: https://github.com/trailofbits/PrivacyRaven. (Month 2023). https://github.com/trailofbits/PrivacyRaven

[90] Yuben Qu, Haipeng Dai, Yan Zhuang, Jiafa Chen, Chao Dong, Fan Wu, and Song Guo. 2021. Decentralized Federated Learning for UAV Networks: Architecture, Challenges, and Opportunities. *IEEE Network* 35, 6 (2021), 156–162. DOI:http://dx.doi.org/10.1109/MNET.001.2100253

[91] Wei Yang Bryan Lim, Sahil Garg, Zehui Xiong, Yang Zhang, Dusit Niyato, Cyril Leung, and Chunyan Miao. 2021. UAV-Assisted Communication Efficient Federated Learning in the Era of the Artificial Intelligence of Things. *IEEE Network* 35, 5 (2021), 188–195. DOI:http://dx.doi.org/10.1109/MNET.002.2000334

[92] Xiaoyuan Liu, Hongwei Li, Guowen Xu, Zongqi Chen, Xiaoming Huang, and Rongxing Lu. 2021. Privacy-Enhanced Federated Learning Against Poisoning Adversaries. *IEEE Transactions on Information Forensics and Security* 16 (2021), 4574–4588. DOI:http://dx.doi.org/10.1109/TIFS.2021.3108434

[93] Henger Li, Xiaolin Sun, and Zizhan Zheng. 2022. Learning to Attack Federated Learning: A Model-based Reinforcement Learning Attack Framework. In *Advances in Neural Information Processing Systems*, S. Koyejo, S. Mohamed, A. Agarwal, D. Belgrave, K. Cho, and A. Oh (Eds.), Vol. 35. Curran Associates, Inc., 35007–35020. https://proceedings.neurips.cc/paper_files/paper/2022/file/e2ef0cae667dbe9bfdbcaed1bd91807b-Paper-Conference.pdf

[94] Alfred Menezes and Douglas Stebila. 2021. Challenges in Cryptography. *IEEE Security & Privacy* 19, 2 (2021), 70–73. DOI:http://dx.doi.org/10.1109/MSEC.2021.3049730

[95] Jehad M. Hamamreh, Haji M. Furqan, and Huseyin Arslan. 2019. Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials* 21, 2 (2019), 1773–1828. DOI:http://dx.doi.org/10.1109/COMST.2018.2878035

[96] Xiaoming Chen, Derrick Wing Kwan Ng, Wolfgang H. Gerstacker, and Hsiao-Hwa Chen. 2017. A Survey on Multiple-Antenna Techniques for Physical Layer Security. *IEEE Communications Surveys & Tutorials* 19, 2 (2017), 1027–1053. DOI:http://dx.doi.org/10.1109/COMST.2016.2633387

[97] Fahem Zerrouki, Samir Ouchani, and Hafida Bouarfa. 2022. A survey on silicon PUFs. *Journal of Systems Architecture* 127 (2022), 102514.

[98] Yan Huo, Yuqi Tian, Liran Ma, Xiuzhen Cheng, and Tao Jing. 2018. Jamming Strategies for Physical Layer Security. *IEEE Wireless Communications* 25, 1 (2018), 148–153. DOI:http://dx.doi.org/10.1109/MWC.2017.1700015

[99] Shajahan Kutty and Debarati Sen. 2016. Beamforming for Millimeter Wave Communications: An Inclusive Survey. *IEEE Communications Surveys & Tutorials* 18, 2 (2016), 949–973. DOI:http://dx.doi.org/10.1109/COMST.2015.2504600

[100] Yamen Alsaba, Sharul Kamal Abdul Rahim, and Chee Yen Leow. 2018. Beamforming in Wireless Energy Harvesting Communications Systems: A Survey. *IEEE Communications Surveys & Tutorials* 20, 2 (2018), 1329–1360. DOI:http://dx.doi.org/10.1109/COMST.2018.2797886

[101] Geng Sun, Jiahui Li, Aimin Wang, Qingqing Wu, Zemin Sun, and Yanheng Liu. 2022. Secure and Energy-Efficient UAV Relay Communications Exploiting Collaborative Beamforming. *IEEE Transactions on Communications* 70, 8 (2022), 5401–5416. DOI:http://dx.doi.org/10.1109/TCOMM.2022.3184160

[102] Joost Verbraeken, Matthijs Wolting, Jonathan Katzy, Jeroen Kloppenburg, Tim Verbelen, and Jan S Rellermeyer. 2020. A survey on distributed machine learning. *Comput. Surveys* 53, 2 (2020), 1–33.
[103] Zigui Jiang, Kai Chen, Hailin Wen, and Zibin Zheng. 2022. Applying blockchain-based method to smart contract classification for CPS applications. *Digital Communications and Networks* 8, 6 (2022), 964–975.
[104] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar. 2014. A Survey of Intrusion Detection Systems in Wireless Sensor Networks. *IEEE Communications Surveys & Tutorials* 16, 1 (2014), 266–282. DOI:http://dx.doi.org/10.1109/SURV.2013.050113.00191
[105] Bo Liu, Ming Ding, Sina Shaham, Wenny Rahayu, Farhad Farokhi, and Zihuai Lin. 2021. When machine learning meets privacy: A survey and outlook. *Comput. Surveys* 54, 2 (2021), 1–36.
[106] Xiaokang Zhou, Wei Liang, Kevin I-Kai Wang, Zheng Yan, Laurence T. Yang, Wei Wei, Jianhua Ma, and Qun Jin. 2023. Decentralized P2P Federated Learning for Privacy-Preserving and Resilient Mobile Robotic Systems. *IEEE Wireless Communications* 30, 2 (2023), 82–89. DOI:http://dx.doi.org/10.1109/MWC.004.2200381
[107] Geng Sun, Xiaoya Zheng, Zemin Sun, Qingqing Wu, Jiahui Li, Yanheng Liu, and Victor C.M. Leung. 2023. UAV-enabled Secure Communications via Collaborative Beamforming with Imperfect Eavesdropper Information. *IEEE Transactions on Mobile Computing* (2023), 1–18. DOI:http://dx.doi.org/10.1109/TMC.2023.3273293
[108] Yu Zhang, Zhiyu Mou, Feifei Gao, Jing Jiang, Ruijin Ding, and Zhu Han. 2020. UAV-enabled secure communications by multi-agent deep reinforcement learning. *IEEE Transactions on Vehicular Technology* 69, 10 (2020), 11599–11611.
[109] Hung Tran, Chakchai So-In, et al. 2021. Enhanced intrusion detection system for an EH IoT architecture using a cooperative UAV relay and friendly UAV jammer. *IEEE/CAA Journal of Automatica Sinica* 8, 11 (2021), 1786–1799.
[110] Hanh Dang-Ngoc, Diep N Nguyen, Khuong Ho-Van, Dinh Thai Hoang, Eryk Dutkiewicz, Quoc-Viet Pham, and Won-Joo Hwang. 2022. Secure swarm UAV-assisted communications with cooperative friendly jamming. *IEEE Internet of Things Journal* 9, 24 (2022), 25596–25611.
[111] Liang Xiao, Hongyan Li, Shi Yu, Yi Zhang, Li-Chun Wang, and Shaodan Ma. 2022. Reinforcement learning based network coding for drone-aided secure wireless communications. *IEEE Transactions on Communications* 70, 9 (2022), 5975–5988.
[112] Himanshu Sharma, Neeraj Kumar, Raj Kumar Tekchandani, and Nazeeruddin Mohammad. 2022. Deep Learning enabled Channel Secrecy Codes for Physical Layer Security of UAVs in 5G and beyond Networks. In *Proc. IEEE ICC*. 1–6.
[113] Tianhao Cheng, Buhong Wang, Kunrui Cao, Runze Dong, and Danyu Diao. 2023. IRS-Enabled Secure G2A Communications for UAV System With Aerial Eavesdropping. *IEEE Systems Journal* 17, 3 (2023), 3670–3681.
[114] Jihong Yu, Yue Gong, Jinhui Fang, Rongrong Zhang, and Jianping An. 2022. Let Us Work Together: Cooperative Beamforming for UAV Anti-Jamming in Space–Air–Ground Networks. *IEEE Internet of Things Journal* 9, 17 (2022), 15607–15617.
[115] Zefang Lv, Liang Xiao, Yousong Du, Guohang Niu, Chengwen Xing, and Wenyuan Xu. 2023. Multi-Agent Reinforcement Learning Based UAV Swarm Communications Against Jamming. *IEEE Transactions on Wireless Communications* 22, 12 (2023), 9063–9075. DOI:http://dx.doi.org/10.1109/TWC.2023.3268082
[116] Zhiwei Li, Yu Lu, Xi Li, Zengguang Wang, Wenxin Qiao, and Yicen Liu. 2021. UAV networks against multiple maneuvering smart jamming with knowledge-based reinforcement learning. *IEEE Internet of Things Journal* 8, 15 (2021), 12289–12310.
[117] Yifu Sun, Kang An, Junshan Luo, Yonggang Zhu, Gan Zheng, and Symeon Chatzinotas. 2022. Outage Constrained Robust Beamforming Optimization for Multiuser IRS-Assisted Anti-Jamming Communications With Incomplete Information. *IEEE Internet of Things Journal* 9, 15 (2022), 13298–13314. DOI:http://dx.doi.org/10.1109/JIOT.2022.3140752
[118] Chen Han, Aijun Liu, Kang An, Gan Zheng, and Xinhai Tong. 2021. Distributed UAV deployment in hostile environment: A game-theoretic approach. *IEEE Wireless Communications Letters* 11, 1 (2021), 126–130.
[119] Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Athanasios V Vasilakos, and Joel JPC Rodrigues. 2018. Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of drones deployment. *IEEE Internet of Things Journal* 6, 2 (2018), 3572–3584.
[120] Tejasvi Alladi, Vinay Chamola, Neeraj Kumar, et al. 2020. PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks. *Computer Communications* 160 (2020), 81–90.
[121] Gaurang Bansal and Biplab Sikdar. 2021. S-MAPS: Scalable mutual authentication protocol for dynamic UAV swarms. *IEEE Transactions on Vehicular Technology* 70, 11 (2021), 12088–12100.
[122] Chuang Tian, Qi Jiang, Teng Li, Junwei Zhang, Ning Xi, and Jianfeng Ma. 2022. Reliable PUF-based mutual authentication protocol for UAVs towards multi-domain environment. *Computer Networks* 218 (2022), 109421.
[123] Muhammad Arslan Akram, Hira Ahmad, Adnan Noor Mian, Anca Delia Jurcut, and Saru Kumari. 2023. Blockchain-based privacy-preserving authentication protocol for UAV networks. *Computer Networks* 224 (2023), 109638.
[124] Xinghua Li, Yunwei Wang, Pandi Vijayakumar, Debiao He, Neeraj Kumar, and Jianfeng Ma. 2019. Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network. *IEEE Transactions on Vehicular Technology* 68, 11 (2019), 11309–11322.
[125] Chaosheng Feng, Bin Liu, Zhen Guo, Keping Yu, Zhiguang Qin, and Kim-Kwang Raymond Choo. 2021. Blockchain-based cross-domain authentication for intelligent 5G-enabled Internet of drones. *IEEE Internet of Things Journal* 9, 8 (2021), 6224–6238.

[126] Abbas Yazdinejad, Reza M Parizi, Ali Dehghantanha, Hadis Karimipour, Gautam Srivastava, and Mohammed Aledhari. 2020. Enabling drones in the Internet of things with decentralized blockchain-based security. *IEEE Internet of Things Journal* 8, 8 (2020), 6406–6415.
[127] Vivian Ukamaka Ihekoronye, Simeon Okechukwu Ajakwe, Dong–Seong Kim, and Jae Min Lee. 2022. Hierarchical Intrusion Detection System for Secured Military Drone Network: A Perspicacious Approach. In *Proc. IEEE MILCOM*. 336–341. DOI: http://dx.doi.org/10.1109/MILCOM55135.2022.10017532
[128] Donpiti Chulerttiyawong and Abbas Jamalipour. 2023. Sybil Attack Detection in Internet of Flying Things-IoFT: A Machine Learning Approach. *IEEE Internet of Things Journal* (2023).
[129] Yuan Yao, Bin Xiao, Gaofei Wu, Xue Liu, Zhiwen Yu, Kailong Zhang, and Xingshe Zhou. 2019. Multi-Channel Based Sybil Attack Detection in Vehicular Ad Hoc Networks Using RSSI. *IEEE Transactions on Mobile Computing* 18, 2 (2019), 362–375.
[130] Xian-Ming Zhang, Qing-Long Han, Xiaohua Ge, and Lei Ding. 2020. Resilient Control Design Based on a Sampled-Data Model for a Class of Networked Control Systems Under Denial-of-Service Attacks. *IEEE Transactions on Cybernetics* 50, 8 (2020), 3616–3626. DOI: http://dx.doi.org/10.1109/TCYB.2019.2956137
[131] Jiyang Chen, Zhiwei Feng, Jen-Yang Wen, Bo Liu, and Lui Sha. 2019. A Container-based DoS Attack-Resilient Control Framework for Real-Time UAV Systems. In *Proc. IEEE DATE*. 1222–1227. DOI: http://dx.doi.org/10.23919/DATE.2019.8714888
[132] Sunitha Safavat and Danda B Rawat. 2022. OptiML: An Enhanced ML Approach Towards Design of SDN based UAV Networks. In *Proc. IEEE ICC*. 1–6.
[133] Saif ur Rehman, Mubashir Khaliq, Syed Ibrahim Imtiaz, Aamir Rasool, Muhammad Shafiq, Abdul Rehman Javed, Zunera Jalil, and Ali Kashif Bashir. 2021. DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU). *Future Generation Computer Systems* 118 (2021), 453–466.
[134] Jean-Philippe Condomines, Ruohao Zhang, and Nicolas Larrieu. 2019. Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation. *Ad Hoc Networks* 90 (2019), 101759.
[135] Aakif Mairaj and Ahmad Y Javaid. 2022. Game theoretic solution for an Unmanned Aerial Vehicle network host under DDoS attack. *Computer Networks* 211 (2022), 108962.
[136] Sixing Lu and Roman Lysecky. 2019. Data-driven anomaly detection with timing features for embedded systems. *ACM Transactions on Design Automation of Electronic Systems* 24, 3 (2019), 1–27.
[137] Nadir A Carreon, Sixing Lu, and Roman Lysecky. 2021. Probabilistic estimation of threat intrusion in embedded systems for runtime detection. *ACM Transactions on Embedded Computing Systems* 20, 2 (2021), 1–27.
[138] Weina Niu, Xiyue Zhang, Xiaosong Zhang, Xiaojiang Du, Xiaoming Huang, Mohsen Guizani, et al. 2020. Malware on Internet of UAVs detection combining string matching and fourier transformation. *IEEE Internet of Things Journal* 8, 12 (2020), 9905–9919.
[139] Amin Azmoodeh, Ali Dehghantanha, and Kim-Kwang Raymond Choo. 2019. Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning. *IEEE Transactions on Sustainable Computing* 4, 1 (2019), 88–95. DOI: http://dx.doi.org/10.1109/TSUSC.2018.2809665
[140] Iván García-Magariño, Raquel Lacuesta, Muttukrishnan Rajarajan, and Jaime Lloret. 2019. Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. *Ad Hoc Networks* 86 (2019), 72–82.
[141] Paul J Bonczek, Rahul Peddi, Shijie Gao, and Nicola Bezzo. 2022. Detection of Nonrandom Sign-Based Behavior for Resilient Coordination of Robotic Swarms. *IEEE Transactions on Robotics* 38, 1 (2022), 92–109. DOI: http://dx.doi.org/10.1109/TRO.2021.3139592
[142] Zhijun Teng, Chunqiu Du, Meng Li, Hengjia Zhang, and Weihua Zhu. 2022. A Wormhole Attack Detection Algorithm Integrated With the Node Trust Optimization Model in WSNs. *IEEE Sensors Journal* 22, 7 (2022), 7361–7370. DOI: http://dx.doi.org/10.1109/JSEN.2022.3152841
[143] Faheed AF Alenezi, Sejun Song, and Baek-Young Choi. 2021. SWANS: SDN-based Wormhole Analysis using the Neighbor Similarity for a Mobile ad hoc network (MANET). In *Proc. IFIP/IEEE IM*. IEEE, 653–657.
[144] Jian Yang, Xun Liu, Xiaofeng Jiang, Yaohui Zhang, Shuangwu Chen, and Huasen He. 2023. Toward Trusted Unmanned Aerial Vehicle Swarm Networks: A Blockchain-Based Approach. *IEEE Vehicular Technology Magazine* 18, 2 (2023), 98–108. DOI: http://dx.doi.org/10.1109/MVT.2023.3242834
[145] Shashi Gurung and Siddhartha Chauhan. 2019. A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET. *Wireless Networks* 25 (2019), 1685–1695.
[146] Ali Dorri. 2017. An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. *Wireless Networks* 23, 6 (2017), 1767–1778.
[147] Yuxin Liu, Mianxiong Dong, Kaoru Ota, and Anfeng Liu. 2016. ActiveTrust: Secure and trustable routing in wireless sensor networks. *IEEE Transactions on Information Forensics and Security* 11, 9 (2016), 2013–2027.
[148] Shashi Gurung and Siddhartha Chauhan. 2018. A novel approach for mitigating gray hole attack in MANET. *Wireless Networks* 24 (2018), 565–579.
[149] Abdulaziz S Almazyad. 2018. Reputation-based mechanisms to avoid misbehaving nodes in ad hoc and wireless sensor networks. *Neural Computing and Applications* 29 (2018), 597–607.
[150] Shubhani Aggarwal, Mohammad Shojafar, Neeraj Kumar, and Mauro Conti. 2019. A new secure data dissemination model in Internet of drones. In *Proc. IEEE ICC*. 1–6.

[151] Maninderpal Singh, Gagangeet Singh Aujla, and Rasmeet Singh Bali. 2020. A deep learning-based blockchain mechanism for secure Internet of drones environment. *IEEE Transactions on Intelligent Transportation Systems* 22, 7 (2020), 4404–4413.
[152] Jiawen Kang, Zehui Xiong, Dusit Niyato, Shengli Xie, and Dong In Kim. 2021. Securing data sharing from the sky: Integrating blockchains into drones in 5G and beyond. *IEEE Network* 35, 1 (2021), 78–85.
[153] Liang Xie, Zhou Su, Nan Chen, and Qichao Xu. 2021. Secure data sharing in UAV-assisted crowdsensing: Integration of blockchain and reputation incentive. In *Proc. IEEE GLOBECOM*. 1–6.
[154] Yuntao Wang, Zhou Su, Qichao Xu, Ruidong Li, and Tom H Luan. 2021. Lifesaving with RescueChain: Energy-efficient and partition-tolerant blockchain based secure information sharing for UAV-aided disaster rescue. In *Proc. IEEE INFOCOM*. 1–10.
[155] Zhou Su, Yuntao Wang, Qichao Xu, and Ning Zhang. 2020. LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue. *IEEE Transactions on Dependable and Secure Computing* 19, 1 (2020), 19–32.
[156] Farid Naït-Abdesselam, Chafiq Titouna, and Ashfaq Khokhar. 2022. Detecting False Data Injections in Images Collected by Drones: A Deep Learning Approach. In *Proc. IEEE GLOBECOM*. 263–268.
[157] Dan Ye and Tian-Yu Zhang. 2019. Summation detector for false data-injection attack in cyber-physical systems. *IEEE Transactions on Cybernetics* 50, 6 (2019), 2338–2345.
[158] Yapei Gu, Xiang Yu, Kexin Guo, Jianzhong Qiao, and Lei Guo. 2021. Detection, estimation, and compensation of false data injection attack for UAVs. *Information Sciences* 546 (2021), 723–741.
[159] Arman Sargolzaei, Kasra Yazdani, Alireza Abbaspour, Carl D Crane III, and Warren E Dixon. 2019. Detection and mitigation of false data injection attacks in networked control systems. *IEEE Transactions on Industrial Informatics* 16, 6 (2019), 4281–4292.
[160] Bethi Pardhasaradhi and Linga Reddy Cenkeramaddi. 2022. GPS spoofing detection and mitigation for drones using distributed radar tracking and fusion. *IEEE Sensors Journal* 22, 11 (2022), 11122–11134.
[161] Yongchao Dang, Chafika Benzaïd, Bin Yang, Tarik Taleb, and Yulong Shen. 2022. Deep-Ensemble-Learning-Based GPS Spoofing Detection for Cellular-Connected UAVs. *IEEE Internet of Things Journal* 9, 24 (2022), 25068–25085. DOI:http://dx.doi.org/10.1109/JIOT.2022.3195320
[162] Nian Xue, Liang Niu, Xianbin Hong, Zhen Li, Larissa Hoffaeller, and Christina Pöpper. 2020. DeepSIM: GPS spoofing detection on UAVs using satellite imagery matching. In *Proc. ACM ACSAC*, Vol. 16. 304–319. DOI:http://dx.doi.org/10.1145/3427228.3427254
[163] Rong Huang and Yuancheng Li. 2023. Adversarial Attack Mitigation Strategy for Machine Learning-Based Network Attack Detection Model in Power System. *IEEE Transactions on Smart Grid* 14, 3 (2023), 2367–2376. DOI:http://dx.doi.org/10.1109/TSG.2022.3217060
[164] Jingjing Guo, Haiyang Li, Feiran Huang, Zhiquan Liu, Yanguo Peng, Xinghua Li, Jianfeng Ma, Varun G Menon, and Konstantin Kostromitin Igorevich. 2022. ADFL: A poisoning attack defense framework for horizontal federated learning. *IEEE Transactions on Industrial Informatics* 18, 10 (2022), 6526–6536.
[165] Boyu Hou, Jiqiang Gao, Xiaojie Guo, Thar Baker, Ying Zhang, Yanlong Wen, and Zheli Liu. 2022. Mitigating the Backdoor Attack by Federated Filters for Industrial IoT Applications. *IEEE Transactions on Industrial Informatics* 18, 5 (2022), 3562–3571. DOI:http://dx.doi.org/10.1109/TII.2021.3112100
[166] Thien Duc Nguyen, Phillip Rieger, Huili Chen, Hossein Yalame, Helen Möllering, Hossein Fereidooni, Samuel Marchal, Markus Miettinen, Azalia Mirhoseini, Shaza Zeitouni, Farinaz Koushanfar, Ahmad-Reza Sadeghi, and Thomas Schneider. 2022. FLAME: Taming Backdoors in Federated Learning. In *Proc. USENIX Security Symposium*. 1415–1432. https://www.usenix.org/conference/usenixsecurity22/presentation/nguyen
[167] Zheyi Chen, Pu Tian, Weixian Liao, and Wei Yu. 2020. Zero knowledge clustering based adversarial mitigation in heterogeneous federated learning. *IEEE Transactions on Network Science and Engineering* 8, 2 (2020), 1070–1083.
[168] Yong Li, Yipeng Zhou, Alireza Jolfaei, Dongjin Yu, Gaochao Xu, and Xi Zheng. 2021. Privacy-Preserving Federated Learning Framework Based on Chained Secure Multiparty Computing. *IEEE Internet of Things Journal* 8, 8 (2021), 6178–6186. DOI:http://dx.doi.org/10.1109/JIOT.2020.3022911
[169] Xiangwang Hou, Jingjing Wang, Chunxiao Jiang, Xudong Zhang, Yong Ren, and Mérouane Debbah. 2023. UAV-Enabled Covert Federated Learning. *IEEE Transactions on Wireless Communications* 22, 10 (2023), 6793–6809. DOI:http://dx.doi.org/10.1109/TWC.2023.3245621
[170] Chaosheng Feng, Bin Liu, Keping Yu, Sotirios K. Goudos, and Shaohua Wan. 2022. Blockchain-Empowered Decentralized Horizontal Federated Learning for 5G-Enabled UAVs. *IEEE Transactions on Industrial Informatics* 18, 5 (2022), 3582–3592. DOI:http://dx.doi.org/10.1109/TII.2021.3116132
[171] Pathum Chamikara Mahawaga Arachchige, Peter Bertok, Ibrahim Khalil, Dongxi Liu, Seyit Camtepe, and Mohammed Atiquzzaman. 2020. A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. *IEEE Transactions on Industrial Informatics* 16, 9 (2020), 6092–6102. DOI:http://dx.doi.org/10.1109/TII.2020.2974555
[172] Xiaoqiang He, Qianbin Chen, Lun Tang, Weili Wang, and Tong Liu. 2022. CGAN-Based Collaborative Intrusion Detection for UAV Networks: A Blockchain-Empowered Distributed Federated Learning Approach. *IEEE Internet of Things Journal* 10, 1 (2022), 120–132.
[173] Pankaj K Sharma and Dong In Kim. 2019. Random 3D mobile UAV networks: Mobility modeling and coverage probability. *IEEE Transactions on Wireless Communications* 18, 5 (2019), 2527–2538.
[174] Pankaj K Sharma and Dong In Kim. 2020. Secure 3D mobile UAV relaying for hybrid satellite-terrestrial networks. *IEEE Transactions on Wireless Communications* 19, 4 (2020), 2770–2784.

[175] Xiaojie Wang, Beibei Wang, Yu Wu, Zhaolong Ning, Song Guo, and Fei Richard Yu. 2024. A Survey on Trustworthy Edge Intelligence: From Security and Reliability To Transparency and Sustainability. *IEEE Communications Surveys & Tutorials, DOI:10.1109/COMST.2024.3446585* (2024), 1–1.

Received 13 December 2023; revised 8 September 2024; accepted 3 November 2024