Computer Networks 224 (2023) 109626

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Survey paper

A survey on security and privacy issues of UAVs

Yassine Mekdad [b,*], Ahmet Aris [b], Leonardo Babun [b], Abdeslam El Fergougui [a], Mauro Conti [c], Riccardo Lazzeretti [d], A. Selcuk Uluagac [b]

[a] Laboratory of Computer Networks and Systems, Moulay Ismail University of Meknes, Zitoune, Meknes, 11201, Morocco
[b] Cyber-Physical Systems Security Lab, Department of Electrical and Computer Engineering, Florida International University, Miami, 33174, FL, USA
[c] Department of Mathematics, University of Padua, Padua, 35121, Italy
[d] Department of Computer, Control, and Management Engineering "Antonio Ruberti", Sapienza University of Rome, Rome, 00185, Italy

ARTICLE INFO

Keywords:
Unmanned Aerial Vehicles
UAVs
Security
Privacy
Drones

ABSTRACT

In the 21st century, the industry of drones, also known as Unmanned Aerial Vehicles (UAVs), has witnessed a rapid increase with its large number of airspace users. The tremendous benefits of this technology in civilian applications such as hostage rescue and parcel delivery will integrate smart cities in the future. Nowadays, the affordability of commercial drones expands their usage on a large scale. However, the development of drone technology is associated with vulnerabilities and threats due to the lack of efficient security implementations. Moreover, the complexity of UAVs in software and hardware triggers potential security and privacy issues. Thus, posing significant challenges for the industry, academia, and governments.

In this paper, we extensively survey the security and privacy issues of UAVs by providing a systematic classification at four levels: Hardware-level, Software-level, Communication-level, and Sensor-level. In particular, for each level, we thoroughly investigate (1) common vulnerabilities affecting UAVs for potential attacks from malicious actors, (2) existing threats that are jeopardizing the civilian application of UAVs, (3) active and passive attacks performed by the adversaries to compromise the security and privacy of UAVs, (4) possible countermeasures and mitigation techniques to protect UAVs from such malicious activities. In addition, we summarize the takeaways that highlight lessons learned about UAVs' security and privacy issues. Finally, we conclude our survey by presenting the critical pitfalls and suggesting promising future research directions for security and privacy of UAVs.

1. Introduction

In the past decades, the global Unmanned Aerial Vehicles (UAVs) market has increased and gained more attention from governments and commercial industries due to its wide civilian and military applications such as traffic monitoring, search-and-rescue operations, surveillance, and biochemical sensing [1–3]. Currently, there is a socio-technical debate about the use of UAVs for passenger transportation, so-called "air taxis" that will replace commercial helicopters because of their electric Vertical Takeoff and Landing (eVTOL) capabilities [4]. A recent report shows that the commercial drone market revenue forecast will reach 129.33 billion dollars by 2025 [5]. According to the Federal Aviation Administration (FAA), the size of the commercial drone market could triple by 2023 [6]. Thus, the introduction of UAVs into the civilian market will increase the demand for their commercial use in different sectors. Nowadays, with the rise of drone technology, the industrial players have their interest investing in UAVs [7]. Therefore, the UAVs will represent an essential part of our technological society as their civilian popularity is significantly increasing.

Although the worldwide development of the drone business model and the benefits offered by commercial UAVs, a considerable number of drone incidents are reported every week [8]. Therefore, we need to prevent such incidents by providing appropriate mitigation strategies. To that end, one line of argument suggests detecting and identifying the UAV threats at their early phases [9]. This approach would provide the operator a reasonable amount of time to deploy the required tools to neutralize such threats. It is of utmost importance to consider the malicious use of such technology and its potential threats to civilian users. In fact, the exponential growth of UAVs triggers different vulnerabilities to their cyber and physical components [10]. The security and privacy aspects of UAV's deployment into the national airspace have become a significant concern for governments as the UAV threat landscape becomes wide. In addition, most of the existing commercial UAVs are

[*] Corresponding author.
E-mail addresses: ymekdad@fiu.edu (Y. Mekdad), aaris@fiu.edu (A. Aris), lbabu002@fiu.edu (L. Babun), a.elfergougui@umi.ac.ma (A.E. Fergougui), mauro.conti@math.unipd.it (M. Conti), lazzeretti@diag.uniroma1.it (R. Lazzeretti), suluagac@fiu.edu (A.S. Uluagac).

https://doi.org/10.1016/j.comnet.2023.109626
Received 3 November 2021; Received in revised form 3 July 2022; Accepted 7 February 2023
Available online 10 February 2023

not equipped with security mechanisms such as intrusion detection systems (IDS). Therefore, they present perfect targets for adversaries.

Recently, the world has witnessed a series of successful cyber attacks on UAVs [11]. Performing real-world cyber attacks against civilian UAVs has become a matter of national security. Upon integrating UAVs into the national airspace, their security issues have created a substantial discussion among governments and agencies in the public and private sectors. From a security point of view, the variety of existing cyber attacks demonstrates that UAVs are vulnerable at different levels. Indeed, malicious actors benefit from the ubiquity of drone usage in civilian applications. They exploit different vulnerabilities across commercial drones creating an active threat to the safety of people. Furthermore, drone manufacturers lack considering security and privacy concerns in the early phases of their production.

It is worth mentioning that the active use of civilian UAVs in many applications can pose new security and privacy challenges [12]. With this in mind, existing countermeasures to detect compromised drones and secure drone systems are weak. To that end, cyber attacks against UAVs are feasible due to the lack of implementing appropriate security measures that guarantee the classical CIA triad (Confidentiality, Integrity, and Availability) [13]. Hence, we need to investigate Unmanned Aerial Vehicles from a security and privacy perspective. On the other hand, integrating UAVs in the national airspace can also violate public users' privacy and sensitive facilities such as chemical industries and nuclear power plants. Indeed, most UAVs are equipped with onboard camera capabilities, which might potentially disclose sensitive details of human activities [14].

In general, we consider UAVs as complex aerial vehicles. A flying UAV operates under a set of onboard sensors (e.g., GPS, accelerometer) that provide sensor readings to the Flight Controller, which sends data through a communication channel to the operator. According to the received data, the operator sends the control signal to the Flight Controller. In this scenario, four fundamental components of the UAV system need to correlate and operate to maintain the desired state. These components are: the sensors, the hardware, the software, and the communication link.

Moreover, the potential failure of any components might result in grounding and crashing the UAV system. Motivated by this vision and from an adversarial perspective, we consider the abovementioned elements as critical attack points of the UAV system. Hence, we aim to investigate the security and privacy issues of UAVs according to these components that are organized into four levels: the *Sensor-level*, the *Hardware-level*, the *Software-level*, and the *Communication-level*.

1.1. Contributions

In this paper, we aim to provide a comprehensive survey targeting the security and privacy issues of Unmanned Aerial Vehicles and their related concepts. We summarize our main contributions as follows:

- We shed light on the background of UAVs, emphasizing the main components characterizing the UAV system, such as the hardware and software architecture, the communication principles, and the sensing technology;
- We provide the first comprehensive categorization of the security issues of UAVs into four different levels: the *Sensor-level*, the *Hardware-level*, the *Software-level*, and the *Communication-level*. For each level, we investigate common vulnerabilities, threats, attacks, and existing countermeasures. We believe that this categorization can provide a reference for future researchers to start investigating the UAV security;
- We systematically consider how commercial drones can affect people's privacy by discussing the primary privacy invasion attacks and possible countermeasures;
- Throughout our survey, we emphasize the quantitative results of the surveyed studies on the security and privacy issues of UAVs (e.g., computation cost, energy consumption, communication cost, latency). We believe these results will significantly help the researchers exercise better judgment when making choices.
- Finally, we discuss the lessons learned, pitfalls, and promising directions for future research in the field of security and privacy of UAVs.

1.2. Roadmap

The remainder of the article is structured as follows. Firstly, we provide an overview of related work in Section 2. Section 3 provides background on UAVs describing their general architecture, communication principles, and security requirements. In Section 4, we discuss the main security issues targeting UAVs. In particular, we classify these issues into four different levels: *Sensor-level*, the *Hardware-level*, the *Software-level*, and the *Communication-level*. For each level, we list the vulnerabilities and threats. Then, we discuss the potential attacks and existing countermeasures. In Section 5, we focus on the privacy issues of commercial UAVs, including existing defense mechanisms against privacy-invasion attacks. Section 6 discusses the lessons learned, pitfalls and future research directions. Finally, Section 7 concludes the survey.

2. Related work

Unmanned Aerial Vehicles are considered a new emerging type of "flying IoT" devices [15]. They incorporate several applications. For example, drones can provide immediate assistance to patients, such as delivering blood and medical supplies. However, security and privacy challenges might occur when integrating UAVs into modern healthcare systems [16]. With the introduction of synchronized IT components in the Enterprise Architecture (EA) domain, commercial UAVs are extensively used for business development (e.g., safety inspection of critical infrastructures, aerial data collection). In contrast, the security implications of using UAVs within companies and organizations need to be properly considered [17]. In the past decade, the evolution of UAV technology has faced security and privacy issues. In this context, prior works have been published to cover different aspects of UAVs' security and privacy issues.

Security and Privacy Challenges of UAVs. Wang et al. [28] discussed the security and privacy challenges of UAV networks from a cyber–physical system (CPS) perspective. The authors considered the significant components of UAVs that are vulnerable to several cyber attacks either from the cyber or the physical domain. A similar work presented the security challenges of UAV communication networks and proposed their essential security requirements [29]. Shakhatreh et al. [23] reviewed UAVs' civil applications and their major key challenges. Krishna et al. [19] conducted a review on cybersecurity vulnerabilities of UAVs. The authors proposed a taxonomy to classify different types of UAV cyber attacks. Recently, a work by Shafique et al. [37] surveyed the security protocols and their vulnerabilities in UAVs. Syed et al. [34] surveyed the emerging technologies used in the literature to overcome the security and privacy challenges in UAVs. Their work primarily covers the application of Blockchain, Machine Learning (ML), and watermarking technologies.

Security and Privacy Issues of Commercial UAVs. In [18], the authors surveyed the security, privacy, and safety aspects of commercial drones. In particular, they identified the major vulnerabilities, cyber and physical threats, and potential attacks that can result in crashing the drone during a flight mission. Similarly, in [12], the authors investigated the emerging cyber attacks and challenges facing commercial drones. In [24], the authors reviewed the current threats and malicious use of drones in civilian applications. In their recent work, Nassi et al. [36] carried out a systematic literature review on the security and

Table 1
Comparison of our survey and existing surveys on security and privacy issues of UAVs.

Year	Work	Security issues																Privacy issues	
		Software-level				Hardware-level				Communication-level				Sensor-level					
		V	T	A	C	V	T	A	C	V	T	A	C	V	T	A	C	A	C
2016	Hayat et al. [1]	□	□	□	□	□	□	□	□	◪	◪	□	□	□	□	□	□	□	□
2017	Altawy et al. [18]	◪	◪	◪	◪	◪	◪	◪	◪	□	■	■	■	□	□	◪	◪	◪	◪
2017	Krishna et al. [19]	◪	□	◪	□	◪	□	□	□	■	◪	◪	◪	□	□	□	□	□	□
2017	Maxa et al. [20]	□	□	□	□	□	□	□	□	◪	◪	◪	◪	□	□	□	□	□	□
2018	Choudhary et al. [21]	□	□	◪	□	□	□	◪	□	◪	◪	■	□	□	□	□	□	◪	□
2018	Lin et al. [22]	□	□	□	□	□	□	□	□	□	□	□	◪	□	□	□	□	◪	◪
2019	Shakhatreh et al. [23]	□	□	□	□	□	□	□	□	□	□	■	■	□	□	◪	◪	□	□
2019	Nassi et al. [24]	□	□	◪	□	□	□	◪	◪	□	□	◪	◪	□	□	◪	◪	◪	◪
2019	Fotouhi et al. [25]	□	□	□	□	□	□	◪	□	◪	◪	◪	◪	□	□	□	□	□	□
2019	Chriki et al. [26]	□	□	□	□	□	□	□	□	□	□	◪	◪	□	□	□	□	□	□
2020	Yaacoub et al. [12]	◪	◪	◪	◪	◪	◪	◪	◪	◪	□	■	■	□	□	□	□	◪	◪
2020	Boccadoro et al. [27]	□	□	□	□	□	□	◪	◪	◪	◪	□	◪	□	□	□	□	◪	◪
2020	Wang et al. [28]	□	□	□	□	□	□	□	□	□	□	◪	□	□	□	◪	□	◪	□
2020	Hentati et al. [29]	□	□	□	□	□	□	□	□	□	□	◪	◪	□	□	◪	◪	□	□
2020	Zhi et al. [30]	□	□	◪	□	□	□	□	□	□	□	◪	□	□	□	◪	□	◪	□
2020	Sharma et al. [31]	□	□	□	□	□	□	□	□	◪	◪	◪	◪	□	□	□	□	□	□
2020	Noor et al. [32]	□	□	□	□	□	□	□	□	◪	◪	◪	□	□	□	□	□	□	□
2020	Mishra et al. [33]	□	□	□	□	□	□	□	□	◪	◪	□	□	□	□	□	□	□	□
2020	Syed et al. [34]	□	□	□	◪	□	□	□	◪	□	□	□	◪	□	□	□	◪	□	◪
2021	Yahuza et al. [35]	□	◪	◪	◪	□	◪	◪	◪	□	◪	■	◪	□	◪	□	□	◪	◪
2021	Nassi et al. [36]	□	□	◪	◪	□	□	◪	◪	◪	◪	◪	◪	□	□	◪	◪	◪	◪
2021	Shafique et al. [37]	◪	□	□	◪	◪	□	□	◪	◪	□	◪	◪	◪	□	□	◪	□	◪
2021	Hassija et al. [38]	□	□	□	□	□	□	□	□	◪	◪	◪	◪	□	□	□	□	◪	◪
2021	This work	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

■ = Survey the category, □ = Does not survey the category, ◪ = Partially survey the category
V = Vulnerabilities, T = Threats, A = Attacks, C = Countermeasures

privacy issues of commercial drones. In [30], the researchers analyzed the potential threats of wireless communications in commercial UAVs, such as Wi-Fi-based UAV communications. Further, they highlighted the privacy disclosure caused by UAVs through aerial photos.

Security and Privacy Issues of UAV Communications. Fotouhi et al. [25] surveyed the important security issues of UAV-assisted cellular communications. Mishra et al. [33] pointed out that the integration of UAVs to cellular networks such as 5G triggers security challenges that need to be thoroughly investigated by the research community. Hayat et al. [1] addressed the safety, security, and privacy issues of UAV networks from a communication viewpoint. In this study, the authors provided the general communication requirements of UAV networks to enable a safe, secure, and privacy-preserving deployment of UAVs. The authors in [31] provided a comprehensive review of the latest UAV communication technologies and the need to secure the collected and transmitted data to the Ground Control Station (GCS). Hassija et al. [38] presented a survey covering the major security issues in UAV communications and their potential vulnerabilities.

Security and Privacy Issues of UAV networks. Boccadoro et al. [27] provided a survey on the Internet of Drones (IoD). They discussed the security and privacy issues of the drone-2-drone communications and their existing solutions. They also considered the security aspects in specific application scenarios involved in the IoD architecture, such as public safety and smart farming. In another work, Noor et al. [32] considered the security and privacy challenges associated with the design of UAV networks. One of the main challenges is the communication among multiple UAVs in an ad hoc fashion. This type of communication is known as Flying Ad hoc Network (FANET). FANETs' security issues are also surveyed by Chriki et al. [26]. The authors discussed the need to develop robust security schemes before deploying FANETs in realistic scenarios. Additionally, Maxa et al. [20] surveyed the main security challenges of UAV routing protocols. Additionally, the work proposed by Sharma et al. [31] outlined the security mechanisms for communication and networking technologies of UAVs. In this context, the authors discussed the underlying security vulnerabilities and threats of UAVs communication protocols.

Differences from existing surveys. Different from prior works, our work aims to extensively survey the security and privacy issues of UAVs by categorizing them into different levels. Most existing surveys and tutorials in this line of research categorize UAVs' security and privacy issues in terms of attack vectors or according to the fundamental principles of information security. However, such categorization cannot fully explain the vulnerabilities, threats, attacks, and countermeasures of UAVs. Moreover, prior works consider analyzing specific components of the UAV system, such as communications and networking. Instead, our survey is focused on the security and privacy aspects of the complete drone system, covering the end-to-end components, including sensors, hardware, software, and communication. In our work, we survey the security and privacy issues of commercial UAVs. In particular, we dissect from a security perspective the vulnerabilities, threats, attacks, and existing countermeasures of commercial UAVs into four different levels: *(i) Sensor-level*, *(ii) Hardware-level*, *(iii) Software-level*, and *(iv) Communication-level*. These are the most important levels of the functionality of a UAV system. Moreover, we discuss the attacks targeting the privacy aspect of UAVs and their existing mitigation techniques. Throughout our survey, we offer readers a good understanding and visibility of UAVs' most current security and privacy issues at each level. To demonstrate the differences between existing surveys and our work, we compare our survey and existing surveys in the literature as shown in Table 1.

3. Background

In this section, we provide background information for Unmanned Aerial Vehicles. In our survey, our focus is only on commercial drones. Military drones are out of the scope of our work. In addition, for the rest of our paper, we use drones and Unmanned Aerial Vehicles interchangeably. In this section, we start by systematically introducing the hardware and software architecture of UAVs. Then, we highlight existing UAV communication capabilities and protocols. Afterward, we present the onboard sensing elements of UAVs that are part of the payload. Finally, we list the security and privacy requirements of the UAVs for mission-driven civilian applications.

3.1. General architecture of UAVs

The development of UAV technology has created various types of drones with different shapes and weights. To the best of our knowledge, there is no existing standard to classify UAVs. A UAV system generally consists of the *Unmanned Aircraft*, the *Ground Control Station* (GCS), and the *Communication Link* (CL). The *Unmanned Aircraft*, also known as UAV, constitutes the core of an Unmanned Aerial Vehicle system [18], and is monitored by the operator either through the GCS or using a *Remote Controller* (RC).

Hardware Architecture. The inner hardware architecture of an *Unmanned Aircraft* device includes: a *Flight Controller* (FC), *rechargeable batteries*, *actuators*, a set of *sensors* such as GPS and accelerometer, and a *wireless communication module*. A high-level architecture of an Unmanned Aerial Vehicle is depicted in Fig. 1.

- *The Flight Controller:* It serves as the central processing unit of the UAV that interfaces between the software and the onboard devices. It is a microcontroller board equipped with a computing and control unit and storage (e.g., Raspberry Pi [39], BeagleBoard [40]).
- *The rechargeable batteries:* Lithium polymer-based batteries that provide the power supply for the whole UAV.
- *The actuators:* They consist of the brushless motors and the propellers. Moreover, they produce the appropriate actuation needed for the UAV during the flight mission, thus ensuring high stability.
- *The sensors:* They are crucial parts of the UAV. They enable sensing functionalities by providing physical measurements of the surrounding environment, such as height, speed, and geospatial references. These measurements are translated into data that are processed by the Flight Controller, then transmitted to the operator.
- *The wireless communication module:* It is directly connected to the circuit board of the Flight Controller and includes a transmitter and a receiver. It is designed to send and receive signals from other devices such as the Remote Controller, the Ground Control Station, and nearby unmanned aircrafts.

The Ground Control Station (GCS) is a fundamental component of any UAV system. It allows to control and monitor the UAV remotely during the flight mission. The GCS hardware is a ground-based computer processing unit that controls and administers the flight mission [41]. It is equipped with a wireless data link module that: (1) generates and transmits control commands to the UAVs, and (2) receives real-time data from UAVs.

Software Architecture. The software architecture of the *Unmanned Aircraft* operates in a layered system. The integration between these layers constitutes the *flight stack*, and consists of three main layers: *the Firmware*, *the Middleware*, and *the Operating System*. Examples of open source flight stack are: Arducopter [42], Crazyflie 2.1 [43], and KKMultiCopter [44]. The firmware and the middleware are subject to real-time constraints.

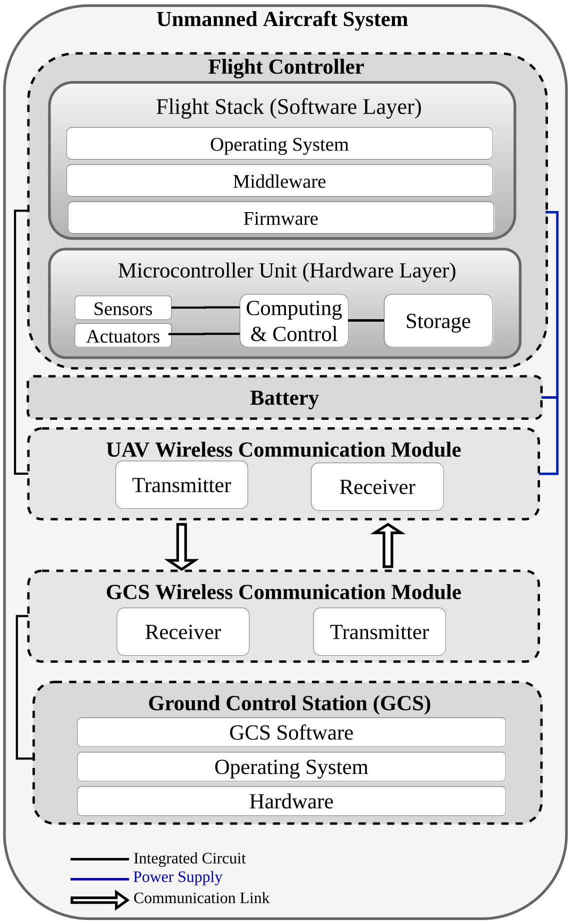


Fig. 1. General architecture of an Unmanned Aerial Vehicle.

- *The Firmware:* It is the lower layer of the flight stack and provides instructions from machine code to the Flight Controller's processor.
- *The Middleware:* It constitutes the layer responsible for proper control of the flight by managing the communication between the services such as guidance, navigation, and telecommunication. Thus, operating the UAV system as a distributed embedded system.
- *The Operating System:* It is the highest layer of the flight stack and, most of the time labeled as a Real-Time Operating System (RTOS). A Real-Time Operating System handles real-time data processing and enables the autopilot software to manage different processes such as flight operations, video recording, and path planning.

According to the recent FAA regulations, and with the integration of UAVs into the national airspace, all UAVs are required to have a Remote ID (or a System ID), which can be defined as the ability of a flying drone to provide its identification and location information to third parties such as law enforcement, and federal agencies [45].

The *Ground Control Station* software is also known as a mission planner. It includes a human–machine interface that displays the flight parameters and typically runs on laptops, tablets, or any devices in the field.

Communication Link. The communication link represents the wireless communication between the GCS and the UAV. It enables data transmission during the flight mission. However, due to the weather conditions and limited power supply, transmission frequencies and flight range may pose several challenges. We identify two types of communication streams: data communication and control communication.

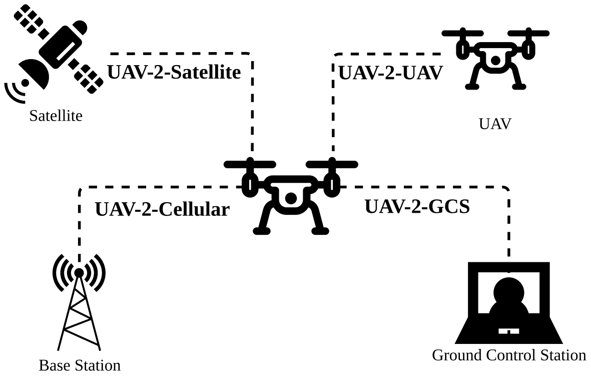


Fig. 2. UAV-2-X communication types.

In data communication, the UAV sends signals such as telemetry and status information to the GCS. While in control communication, the GCS sends commands and control signals to the UAV [46]. In what follows, we highlight the UAV communication principles.

3.2. Communication principles

UAV communications can occur between a UAV and another end point, which can be referred to as UAV-2-X communication. In this subsection, we first explain the UAV-2-X communications. Afterward, we explain the UAV communication architectures, networks of UAVs, as well as their routing protocols. Following that, we shed light on the well-known communication protocols.

3.2.1. UAV-2-X communication types

During a flight mission, a UAV communicates with several entities. As depicted in Fig. 2, we categorize four endpoints of UAV-2-X communications:

(i) *UAV-2-GCS communication*: It is the fundamental type of communication for UAVs. The GCS exchanges data with UAVs through uplinks and downlinks, enabling monitoring traffic and controlling the flight mission. We consider three classes of transmitted traffic in UAV-2-GCS communications: The control traffic, the coordination traffic, and the sensing traffic [47]. The control traffic encompasses controlling and monitoring commands. In particular, mission-specific commands and the real-time status of UAVs (e.g., telemetry data, battery level). The coordination traffic handles the collaboration between multiple UAVs during the flight mission and tasks performed independently from the GCS, such as collision avoidance processes. The sensing traffic encloses onboard sensor readings that are transmitted to the GCS. We mention that all different types of traffic in the UAV-2-GCS communications are based on wireless technologies with limited range, such as Bluetooth or Wi-Fi 802.11, and most of the time not secure [48]; thus, making them vulnerable to passive and active attacks.

(ii) *UAV-2-Satellite communication*: In the Beyond Line-of-Sight (BLOS) missions, the operator needs to locate UAV's position for safe navigation. Therefore, UAVs can establish a satellite communication link to gather their real-time GPS location, then transmit it back to the GCS through the satellite. Furthermore, satellite communications are useful at long distances without fixed infrastructure and provide reliable communication with high transmission bandwidth. Moreover, we can leverage commercial satellite communications to control UAVs [49]. However, they are energy-consuming and expensive in terms of maintenance costs, and can introduce high latency issues.

(iii) *UAV-2-Cellular communication*: At high altitudes in urban or rural environments, UAVs guarantee a wide coverage area and incorporate cellular networks with the coexistence of ground users to provide reliable wireless communication [25]. In this integration, the UAVs operate either as aerial User Equipments (UEs) or as aerial Base Stations (BSs) [29]. When they act as User Equipments, also known as *cellular-connected UAVs*, they establish a UAV-2-Cellular communication with the terrestrial base station, and the ground pilot can directly control UAVs through cellular networks. Differently, UAVs as aerial Base Stations are complementary to ground base stations. They provide reliable and cost-effective wireless cellular networks to cover areas where ground base stations are inaccessible. Although given the advantages of using UAVs in cellular networks in both scenarios, their real-world deployments face several challenges, such as limited performance and energy-efficiency [50].

(iv) *UAV-2-UAV communication*: Referred to as Air-to-Air communications, and takes place during flight missions that require multiple UAVs. In such scenarios, UAVs collaborate and coordinate over wireless technologies with low-power consumption (e.g., Bluetooth, Zigbee) to exchange information directly or through multi-hop wireless links. In this case, a single UAV operates within a network of UAVs to share data and accomplish the desired flight mission. However, UAV-2-UAV communications have a very low throughput and transmission bandwidth.

3.2.2. UAV-2-X communication architecture

UAV-2-X communications operate under a layered architecture and include the physical & MAC layer, the network layer, and the transport layer. Unfortunately, implementing security solutions for these layers is challenging due to UAV's characteristics, such as battery life, insufficiency of resources, real-time computation, and autonomous control. This problem triggers various vulnerabilities at the communication level.

Physical & MAC Layer. The physical & MAC layer defines the communication between the UAV and the transmission medium. In the Physical & MAC layer of UAV-2-X communications, UAVs utilize different wireless communication technologies such as Wi-Fi, Zigbee, and Bluetooth.

Network Layer. In multi-UAV systems, UAV communication networks are aerial, notably different from the mobile ad hoc, and vehicular ad hoc networks in terms of node mobility and topology change [2]. The unique properties and challenges of these networks create a new category of ad hoc networks, namely flying ad hoc networks (FANETs) [51]. In Multi-UAV operations, the features and the nature of FANETs make them vulnerable to various cyber attacks [26]. Indeed, challenging issues arise in multi-UAV systems due to their very low node density, topology change, and architectural design [2]. As shown in Fig. 3, we distinguish two broad categories of UAV communication network architectures: centralized architecture and decentralized architecture [52].

In the centralized architecture, UAVs transmit to and receive data and control commands from a single GCS that serves as a central station. The centralized architecture is applicable in small and straightforward missions. An example of this type of communication is in crowd surveillance applications in urban areas [53]. In such a network architecture, any UAV-2-UAV communication must go through the GCS. This routing results in a delay in data transmission. Therefore, the centralized architecture is not suitable for long-distance communications, especially for resource-constrained UAVs.

In contrast, the decentralized architecture enables UAV-2-UAV communications without routing information to the GCS. We consider two sub-types of decentralized UAV network architectures: single backbone UAVs and multiple backbone UAVs. For both scenarios, a single UAV or multiple UAVs operate as a gateway node and transmit exchanged data to the GCS directly or through another networking infrastructure such

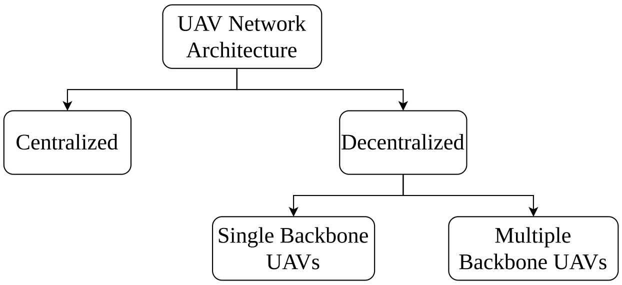


Fig. 3. UAV communication network architectures.

as cellular-based or satellite-based systems. In a single backbone UAV ad hoc network, UAVs form a connection group, and only one backbone UAV serves as a gateway between the GCS and the other UAVs. However, the single backbone UAV architecture may not be practical for flight missions that require a significant number of UAVs. In this case, we rely on two types of multiple backbone UAV architectures. Namely, the swarm of UAVs architecture and the mixed UAVs architecture. In the first type, multiple groups of UAVs in a collective behavior form a swarm, such that each group consists of a single backbone UAV architecture. The mixed UAVs architecture consists of grouping all single backbone UAVs of all groups. Each group can transmit data to the other group without being routed through the GCS, and only one backbone UAV exchanges data with the GCS. We note that all the abovementioned UAV network architectures have strengths and limitations regarding communication needs, autonomy, and scalability. Therefore, the appropriate type of architecture to deploy depends on the flight mission requirements. For example, in Search And Rescue (SAR) missions where time is crucial, the decentralized architecture is more efficient than the centralized one due to the collaboration and coordination between multiple UAVs.

In multi-UAV networks, routing protocols are essential to provide a reliable end-to-end data transmission between UAV nodes [54]. Several routing protocols have been proposed in the literature with different classifications [54–56]. One approach classifies these protocols either on the network architecture or data forwarding [57]. Another approach suggests classifying UAV routing protocols according to their design constraints, such as dynamic topology, energy consumption, scalability, security, and allocated bandwidth [55]. However, given UAV's unique characteristics, all these protocols cannot fulfill UAV's security requirements.

Transport Layer. The transport layer provides reliable data transfer between end-to-end components. Two well-known examples of UAV communication protocols at the transport layer include the MAVLink protocol and the UranusLink protocol.

MAVLink Protocol. The Micro Air Vehicle Link (as known as MAVLink) protocol is a lightweight point-to-point networking protocol primarily used in UAV-2-GCS communications to exchange control and telemetry data [58]. It uses bidirectional communication between UAVs and GCS over wireless channels for real-time applications. Its transmissions can be performed through different wireless mediums, such as Wi-Fi and Bluetooth, with sub-GHz frequencies. MAVLink protocol comes in two versions: v1.0 and v2.0. *MAVLink v2.0* is currently the recommended one. It is a backward-compatible and improved version compared to *MAVLink v1.0*. *MAVLink v2.0* protocol header contains new features and adds new fields to the existing structure of MAVLink messages, such as message extensions and packet-signing. Commercial UAVs extensively use *MAVLink v2.0* since it provides reliable communication and packet-signing. However, only a few studies addressed security implementations of the MAVLink communication protocol. Therefore, MAVLink protocol is prone to several attacks such as flooding and packet injection [59].

UranusLink Protocol. UranusLink is a packet-oriented protocol for wireless UAV-2-GCS communications [60]. Its design satisfies radio communication requirements such as data throughput and low latency, making it useful for aerospace and robotic applications. UranusLink operates in a half-duplex mode under 2.4 GHz frequency and with a maximal throughput of 250 kbps. It is suitable for UAVs with small overheads. Although UranusLink employs an integrity protection scheme, it does not encrypt message payloads that can result in replay attacks [61].

3.3. Sensing technology

UAVs possess a wide range of sensors to accomplish their flight missions. These sensors represent critical components for the functionality of the UAV system, and they are designed to measure physical quantities of the surrounding environment, such as altitude, speed, and GPS location. The outputs of these quantities are then directly transferred to the Flight Controller to decide the appropriate actuation/action. In Table 2, we present the well-known sensors of most of the commercial UAVs. We mention that a corresponding set of onboard sensors exists for each type of UAV application. It is also worth mentioning that the Flight Controller cannot distinguish between legitimate or malicious sensor inputs, even with the robust design of UAV sensors.

3.4. Security and privacy requirements

The wide use of UAVs in civilian applications raises a large number of vulnerabilities [19]. To that end, different features are essential to protect UAVs from disclosure, disruption, modification, and destruction [18]. To guarantee these properties, we identify the following major security and privacy requirements needed to establish a secure UAV flight mission.

- **Confidentiality.** It is crucial to protect private information and data exchange between UAVs and the GCS from unauthorized access, as it could be a source of sensitive information leakage of the flight mission, such as telemetry data and control commands. Additionally, we need to consider implementing robust cryptographic solutions to prevent the adversary from obtaining such information.
- **Integrity.** Preserving data integrity is of utmost importance. It is a requirement for the success of a flight mission, and it prevents adversaries from forging the network traffic. Compromising the integrity could change the behavior of the UAV system and lead to a mission failure. Hence, any communication has to be protected and verified. We can guarantee this requirement through authenticated encryption algorithms [18].
- **Availability.** UAVs must be operational without intentional or unintentional interruptions. All the resources needed for a flight mission must be available for authorized users. Moreover, it is required from the UAV system to resist Denial of Service (DoS) attacks that are compromising its availability. Such attacks can be mitigated using IDS [62].
- **Authenticity.** The authentication process is a fundamental step toward establishing secure communication between different components of the UAV system. It verifies the authenticity and identity of UAVs participating in the flight mission. We ensure the trustworthiness of each UAV through authentication, and only authenticated UAVs can participate in the flight mission. Moreover, the authentication protects the UAV network from adversaries that are spoofing the legitimate nodes.
- **Non-Repudiation.** The users cannot deny their actions (e.g., transmitting or receiving data) within UAV networks. Otherwise, we may deal with accountability issues in case of a mission failure. This property prevents the denial of the user's operations. Furthermore, the UAV system has to develop proper mechanisms ensuring non-repudiation, such as the digital signature of the exchanged messages.

Table 2
Sensors of unmanned aerial vehicles.

Components	Functionality
GPS	Many UAVs use Global Positioning System in outdoor applications to determine geospatial references from the satellite within its range.
3D Accelerometers	Three accelerometer sensors are used to provide the non-gravitational acceleration of UAVs for each axis X, Y, and Z. They rely on the piezoelectric effect and handle the hover capability of UAVs.
3D gyroscopes	3D Gyroscopes can measure or maintain orientation and angular velocity in pitch, roll, and yaw. They are essential for navigation and provide orientation stability of UAVs. Moreover, they collaborate with 3D accelerometers to handle rotational and linear movements.
Magnetometers	Magnetometers provide additional geographical direction of UAVs using the magnetic field. However, these sensors might be defective when placed together with motors and electrical devices.
Infrared cameras	Also known as thermographic cameras, they provide detailed images using infrared energy of objects even in the darkness. Mainly used in military UAV applications. This type of camera could potentially spy on people in challenging environments (e.g., forest, private houses).
Gas sensors	Gas sensors can detect different gasses such as toxic or explosive gasses and measure their concentrations. They have many industrial and military applications.
Radiation sensors	Very useful in nuclear industries. UAVs can be equipped with radiation sensors to determine radiation levels and provide gamma radiation readings for large areas.
Cameras	Crucial devices of UAVs. A wide range of cameras for UAVs exist with different types and sizes. With many civilian and military applications, they can capture images and record videos. Moreover, they help the pilot to navigate in indoor missions. However, the zoom function of these cameras triggers privacy challenges.
Microphones	Practical for search and rescue operations or spying missions, microphones can record audio and gather information remotely. However, using microphones can violate personal privacy.
Biosensors	Biosensors are electrochemical sensing technologies mainly used to detect airborne biological hazards.
Pressure sensors	Pressure sensors aim to detect the atmospheric pressure and convert it into altitude. They provide UAV's altitude stabilization.
LiDAR sensors	Light detection and ranging sensors provide a high-resolution map with laser light. They have several applications such as archeology, agriculture, and landscaping.

- **Authorization.** Data exchange in the UAV system must be shared only with authorized users. We note that unauthorized users are not allowed to perform any action in the UAV network. Besides, the UAV system has to specify what resources an authorized user can access. Granting access to such resources has to be monitored through access control policies.
- **Non-disclosure.** In addition to the abovementioned security requirements, we consider the non-disclosure property in the privacy requirements for UAV systems. Indeed, sensitive information exchanged between the GCS and the UAV, such as captured images and video footage, should not be disclosed to a third party [58].

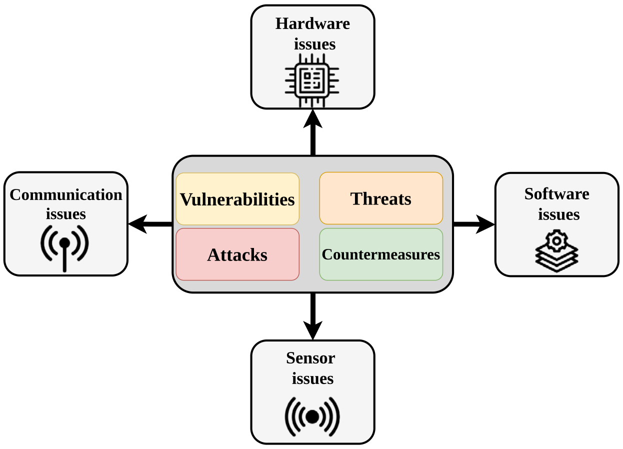


Fig. 4. Taxonomy of UAV security issues.

4. Security issues of UAVs

Security issues associated with UAVs in the national airspace greatly increase the likelihood of performing passive and active attacks. In this section, we categorize the security issues of UAVs into four different levels: *Sensor-level*, *Hardware-level*, *Software-level*, and *Communication-level*. As shown in Fig. 4, we provide a detailed overview about the threats and vulnerabilities targeting UAVs for each level. Then, we review the attacks and their existing countermeasures.

4.1. Sensor-level issues

UAVs rely on sensors to gather data about the surrounding environment. These data are sensitive and need to be protected from malicious actors. Under adversarial conditions, compromising UAV sensors might cause the UAV system to fail. In what follows, we provide different sensor-level vulnerabilities, threats, and potential attacks against UAVs. Afterward, we highlight existing countermeasures against sensor-based attacks on UAVs.

4.1.1. Sensor vulnerabilities and threats

UAVs are extremely sensor-driven devices. They are equipped with various sensors such as cameras, GPS, and accelerometers. Therefore, they rely on sensor readings to operate efficiently. However, these sensors handle sensitive information and could be used by a malicious operator to compromise the flight mission. For example, civil GPS signals are unencrypted and unauthenticated. Therefore, an adversary can exploit this vulnerability by simulating a GPS signal to delude the operator. From an attacker's perspective, exploiting the onboard sensors' real-time data may cause the UAV system to malfunction. This exploit could happen because the Flight Controller does not evaluate the authenticity of sensor readings. The introduction of sensor vulnerabilities into the UAV system can also be performed through malicious software. Due to the practicality of sensory-channel attacks in real-world scenarios, this class of vulnerabilities exposes a new attack vector for the adversary to fully control commercial UAVs [63,64].

4.1.2. Sensor-based attacks

Sensor-based attacks include GPS data jamming, false sensor data injection, and sensory-channel attacks.

GPS data jamming. During a flight mission, the onboard GPS receiver gathers its GPS location from the satellite and sends it to the GCS. GPS data jamming attack occurs when the adversary blocks the navigation feed of the GPS signals, forcing the UAV into a disoriented mode [65]. Performing such attacks results in losing control of the UAV, and therefore possible hijacking of the drones.

Table 3
Summary of sensor-level security issues, existing countermeasures and their limitations.

Sensor-based attacks/threats	Countermeasures	Limitations
Sensory channel attacks [63]	-Physical isolation for acoustic sensory channels to shield the sound noise [70]. -Building robust optical flow algorithms for optical flow sensors [71].	-A large number of sensory channels to consider.
GPS data spoofing [68,69]	-Implementing anti-GPS-spoofing methods into the Flight Controller [72–74]. -The use of collaborative data attestation approach that verifies the correctness of GPS coordinates [75]. -The adoption of authenticated schemes for GPS signals. -Detection of unusual signal power changes that indicates the beginning of a spoofing attack.	-Authenticated GPS signals require additional changes in the infrastructure of the satellite.
GPS data jamming [65]	-Enabling the autonomous navigation without GPS signal [76]. -The use of additional sensors for alternative navigation [77]. -Adopting machine learning-based IDS to detect sensor-based attacks [78] [79].	-Limited energy and computation costs for realistic implementations.
False sensor data injection [66]	-Modeling UAV's physical properties [80]. -Securing sensor readings in the presence of physical invariants [81]. -Cross-verification of data by gathering sensor readings from an alternative set of sensors.	-Adopting the existing solutions to other types of on-board sensors is still unknown.
MEMS gyroscopes attacks [82]	-Physical isolation for acoustic sensory channels to shield the sound noise [70].	-The physical isolation could increase the temperature and cause a malfunctioning of the UAVs.
Optical flow camera sensor attack [83]	-Building robust optical flow algorithms for optical flow sensors [71].	-Practical limits of the optical flow estimation due to its inherent noisy nature.

False sensor data injection. Injecting false sensor data readings in the Flight Controller can compromise external sensors such as electro-optical and infrared sensors [66]. This attack leads to an imbalance in UAV's stability. An attacker can inject false sensor data into UAVs by accessing the onboard Flight Controller system or by altering the sensor readings through system calls. Otherwise, he can directly transmit fake signals to the sensors, thereby compromising the flying UAV. A well-known example of false sensor data injection attacks is GPS spoofing. Since GPS signal broadcasts are most of the time unencrypted and unauthenticated, the attacker performs a spoofing attack on the GPS by faking the generated signal, which can eventually alter the UAV's GPS receiver [67]. Consequently, the attacker gains control over the UAV. In [68,69], the authors demonstrate a GPS spoofing attack on UAVs. The GPS spoofing attack forces the drone to respond to fake signals, consequently affecting its navigation system.

Sensory-channel attacks. UAVs use a set of sensors in which their sensory channels (e.g., infrared, acoustic, light) serve as a vector for attacks. In [82], the authors demonstrate that UAVs equipped with Micro-Electro-Mechanical Systems (MEMS) gyroscopes can fail using intentional sound noise. The study shows that MEMS gyroscopes resonate at audible frequencies. Another study has shown that optical flow camera sensors that are used to stabilize UAVs can be compromised by influencing the surrounding environment [83].

4.1.3. *Countermeasures for sensor-based attacks*

To mitigate GPS jamming attacks, the authors in [76] provided a solution enabling autonomous navigation when the Flight Controller does not receive GPS signals. Other approaches rely on ML-based IDS to detect known and unknown sensor-based attacks [78,79]. The solution provided by Whelan et al. [78] collects training datasets from onboard components of the UAVs (e.g., flight logs, sensors readings) and demonstrates its effectiveness across different UAV platforms with an F1 score of 99.73% for malicious sensor readings. However, real-world implementation is challenging due to the limited energy and computation resources of the UAVs. In another work, Wu et al. [77] proposed using additional sensors as an alternative navigation solution when GPS signals are unavailable. The authors used a monocular camera visual sensor combined with an Inertial Measurement Unit (IMU) sensor to enable the autonomous flight of UAVs in a loss-of-GPS scenario.

To prevent injecting falsified Flight Controller sensors data, we can cross-verify the data by gathering readings from an alternative set of sensors. Another solution to detect external sensor attacks is by modeling UAV's physical properties through a control invariant approach [80]. The control invariant approach checks the consistency of the UAV's physical state with its expected state, which is identified by its control model. The evaluation of the approach for several quadrotors shows that the proposed scheme can detect sensor attacks in 100 ms [80]. Similarly, in [81], the authors presented an architecture to secure sensor readings in the presence of physical invariants. Physical invariants of the UAVs are unique features that can be modeled to predict sensor measurements according to their behavior. These features consist of nonlinear differential equations that model a UAV's speed, angles, position, and angular speed. The study shows that the use of well-known physical invariants provides learning of their parameters, which can detect sensor-based stealthy attacks in less than 100 ms and with a false alarm rate below 2%.

Preventing the adversary from performing a GPS spoofing attack could be achieved by detecting unusual signal power changes, which indicates the beginning of a spoofing attack. In Multi-UAVs scenarios, the authors in [75] proposed a collaborative data attestation framework based on a Control Flow Graph (CFG) that verifies the correctness of shared information such as GPS coordinates and detects GPS spoofing attacks. The performance of the framework on PixHawk drone's GPS sensor shows that for a CFG size of 2922, the required time to generate the attestation report and the verification time is 835 ms and 849 ms, respectively.

In [84], the authors proposed an information fusion method to detect GPS spoofing attacks for UAVs using a monocular camera and an IMU sensor. The experimental results show that the detection method is successful after 2046 ms when considering the x-axis during the flight and 23,311 ms when using only the y-axis. Another countermeasure against GPS spoofing attacks is by adopting GPS signal authentication schemes with classical cryptographic approaches. However, implementing such solutions requires additional changes in the infrastructure of the satellite [18]. We also note that some anti-GPS-spoofing methods are suitable to be implemented into the Flight Controller, enabling an efficient hijacking detection solution [72–74]. For instance, Feng et al. [72] proposed a GPS spoofing detection method that utilizes GPS and IMU data. This approach implements a two-step machine learning model combined with a genetic algorithm (i.e., GA-XGBoost). First, the model is pre-trained off-board the drone to reduce the computation cost. Then, the model is trained on the drone to achieve a high detection rate. The experimental results demonstrate the prediction accuracy of 96.3% and 100% for the hijacked and non-hijacked cases, respectively.

A set of countermeasures have been proposed in the literature to mitigate each type of sensory-channel attack. Acoustic sensory channels are protected by the physical isolation that can shield the sound noise [82]. Optical flow sensors rely on optical flow algorithms, which are utilized to measure visual motion. Building robust optical flow algorithms such as the RANSAC algorithm [71] constitutes a defense-in-depth mechanism for spoofing optical flow sensors.

The attacker's capabilities to compromise UAV sensors are outlined in Table 3. The reported sensor-based attacks aim to compromise the sensory channel, GPS signals, and also inject false sensor data. The solutions proposed in the existing literature are specific for each type of sensor. For example, implementing anti-GPS-spoofing methods or using a collaborative data attestation approach to verify the correctness of GPS coordinates helps prevent GPS data spoofing. The cross-verification of data by gathering sensor readings from different sensors protects the UAVs from gathering false sensor data. However, we also need to consider that the proposed countermeasures for sensor-based attacks have primary shortcomings. For instance, realistic implementations to prevent GPS jamming attacks will increase the computation costs. Moreover, given many sensory channels, providing a set of alternative sensors for each sensory channel is not efficient.

4.2. Hardware-level issues

The adversaries consider UAVs as a potential means to conduct physical attacks in the national airspace. The hardware components of a UAV system consist of the onboard Flight Controller and the Ground Control Station. Both hardware devices are subject to security issues that can potentially lead to cyber or physical attacks. In this subsection, we present the vulnerabilities that an adversary can exploit to compromise the Hardware-level of a UAV system. Then, we provide existing defense mechanisms to mitigate hardware-based attacks.

4.2.1. Hardware vulnerabilities and threats

Hardware-level vulnerabilities and threats include hardware trojans, physical UAV collision, hardware failures, and flying skills issues.

Hardware trojans. Hardware trojans involve the modifications of the electronic hardware (e.g., tampering with the hardware circuit, changing the logic gate) [85]. In particular, hardware trojans target the Flight Controller, making the UAV system vulnerable to several attacks. The hardware trojans are maliciously embedded by a non-trusted third party in the semiconductor supply chain of the Flight Controller [86]. The adversary leverages these modifications to compromise the functionalities and security features of the FC's Integrated Circuit (IC) (e.g., decreasing the rotation speed of the propellers, leaking the cryptographic keys of the Flight Controller). An example of a trojan was found in the Actel ProASIC chip of the Boeing 787 jet [87]. The backdoor allowed the attacker to monitor the avionics system and control the aircraft, therefore jeopardizing the safety of the flight mission.

Physical UAV collision. During a flight mission that requires the cooperation and collaboration between multiple UAVs, physical collisions could happen, resulting in crashing the drones. To prevent such collisions in the civilian airspace, the UAVs rely heavily on Collision Avoidance Systems (CAS) [88]. However, these systems do not encompass built-in security features and cannot satisfy the collision avoidance threat caused by malicious actors [89].

Hardware failures. UAVs can go through malfunctioning of their hardware components, such as battery life or motor issues. These technical failures constitute a threat to the flight mission and could lead to an unsafe landing of the UAVs in an unexpected location [90]. In this case, if the UAVs store unencrypted data, the adversary can disclose sensitive mission-related information and violate the flight mission's confidentiality.

Flying skills issues. These issues occur when human operators remotely control non-autonomous or semi-autonomous UAVs, especially those that are very sensitive under wind disturbance due to their complex dynamics and size [91]. They require flying skills such as remote control of the speed, height, and orientation of the UAV. In such scenarios, the operator's lack of these technical skills might crash the drone and cause an operational failure. Consequently, the UAVs can be easily exposed to physical theft.

4.2.2. Hardware-based attacks

Hardware-based attacks include hijacking, supply chain attacks, battery attacks, and radio frequency module attacks. Other types of attacks consist of performing a hardware reverse engineering to understand the inner composition and properties of the UAV hardware chip [92].

Hijacking. Due to the nature of UAVs, they are visible at a low altitude, making them the perfect targets for hijacking. The adversary hijacks a flying drone either directly or remotely through malicious software. The straightforward technique to disable and hijack UAVs is by using the anti-drone rifles [93]. They are usually in possession by law enforcement to protect malicious UAVs hovering in restricted flight areas. Nevertheless, the attacker can also use the same rifle to ground the drones and hijack them.

Supply chain attacks. With the drone industry's growth, the adversaries have a wider window to compromising the UAVs through supply chain attacks. This type of attack consists of exploiting the vulnerabilities in the supply chain process of an organization by targeting the less-secure and sensitive components such as the propellers, airframes, and actuators. Consequently, the end product that is delivered to the customer is already compromised. A practical supply chain attack against UAVs is demonstrated by Belikovetsky et al. [94]. The researchers conducted a physical supply chain attack for UAVs with Additive Manufacturing (AM). The attack consists of sabotaging a given UAV by remotely manipulating the design files of the propellers. The adversary reduces the 3D printed propeller's fatigue life and creates delayed damage during a flight mission. This study shows that sabotage attack detection for additive manufacturing systems remains a challenging research problem.

Battery attacks. Prevalent UAVs are powered with Lithium-Ion rechargeable batteries. These batteries are supported by the Battery Management System (BMS) to provide reliable energy to different components of the UAV system. However, an adversary can exhaust the battery's energy by performing potential battery depletion attacks [95], which results in a malfunctioning of the UAV system, and consequently compromising the availability, integrity, and confidentiality of the batteries [96]. The attacker compromises the availability of UAV batteries by physically tampering or swapping legitimate batteries with faulty ones to fail the UAV system. Another possible attack may occur when the adversary generates a deep discharging of the batteries. This type of attack could happen by compromising other components of UAVs, such as spoofing the sensors or injecting malicious software, leading to exhausting the UAV batteries [96]. Attacking the integrity of UAV batteries includes modifying real battery information for the operator through the UAV-2-GCS data transmission. Furthermore, the confidentiality of UAV batteries can be compromised by leaking sensitive battery-related data such as the State-of-Charge (SoC), which represents the ratio of available charge to the UAV battery capacity.

Radio Frequency modules attacks. Radio Frequency modules (RF) are used to transmit and receive radio signals from two different devices. In the context of UAVs, an operator might use a typical remote controller or the GCS to send control signals to the flying drones. In this case, the adversary can jam the control signals and disable the UAV-2-GCS communication, resulting in the drones' lost-link state. In [97], the authors demonstrated a replay attack on the XBee 868LP protocol, a low power radio frequency module used for UAV-2-GCS communications. In this attack, the adversary alters the UAV-2-GCS communication using a third XBee chip. In particular, the attacker compromises the security of the communication channel of the main XBee by combining existing features of the chip to access the address of the XBee communication channel.

4.2.3. Countermeasures for hardware-based attacks

Given the physical vulnerabilities and threats of UAVs, physical protection approaches should be considered and enhanced to address those threats. To guarantee a trojan-free drone, possible mitigation of hardware trojans consists of building ML-based IDSs to detect such hardware attacks [86]. Detecting the presence of tampered data or commands using IDS solutions is achieved by: (1) learning the model based on the average data generated by the Pulse Width Modulation (PWM) signals. These signals are commonly used in the IC of UAVs. (2) training the model with malicious data. These data are generated by compromising the firmware or injecting hardware trojans. Thus, affecting the PWM signals. Another mitigation technique consists of performing a fine-grained circuit analysis to enable the detection of hardware trojans [98]. In this case, the trojan detection under various settings can be achieved with a probability greater than 0.99.

Securing both the GCS and UAVs from illegal access using authenticated encryption, and keeping them malware-free will significantly prevent malicious actors from taking over and hijacking the flying UAV. Further, changing the flight paths could prevent the adversary from identifying the flight pattern, thus making the target more difficult for physical theft. In [99], the authors proposed a hijacking detection method for UAVs based on a statistical analysis of standard flight patterns. The simulation of different hijacking scenarios shows the effectiveness of their detection algorithm against 20 potential hijacking cases over 50 generated baseline flights. However, their algorithm fails when simulation parameters such as control instability are changed, which motivates further testing and improvement of the quality of the simulation data.

Supply chain attacks can be mitigated by managing the supply chain's security during the manufacturing process to avoid using compromised UAV components [18,100]. Besides, tamper-proofing solutions (e.g., tamper-proof microprocessors, anti-tamper software) will disable unauthorized physical or logical modifications that could sabotage the authenticity of the UAV's critical components.

Existing countermeasures to mitigate battery depletion attacks include using safety circuits in the Battery Management System that ensures physical battery protection for UAVs [96]. Moreover, a pre-flight diagnosis of the UAV batteries would be an equitable procedure to guarantee a safe flight mission. For instance, the experimental results were performed on the Parrot AR.Drone 2.0 regarding the battery replacement attacks shows a significant difference in the real lifespan between the faulty batteries (2.9 min) and the normal ones (10.8 min) [95]. Another solution could also detect depletion attacks during the flight mission, which consists of real-time monitoring of the battery discharging process. However, if the UAV-2-GCS data transmission is unauthenticated, the adversary may counterfeit the transmission and display an incorrect battery level to the operator. Therefore, we need to adopt cryptographic solutions to secure the UAV-2-GCS data transmission. Further, we can leverage machine learning techniques to detect UAV battery depletion attacks automatically, and can be achieved using the features extracted from simulated battery depletion attacks [95].

To mitigate the radio frequency module attacks, the manufacturer can adopt the onboard encryption of the chip. However, this solution remains limited because it decreases the bandwidth and increases the latency of the chip. In this case, the authors in [97] suggested possible outsourcing of the encryption to a second separate chip. Although this remediation guarantees the confidentiality of the data sent over the radio channel, it would not prevent the adversary from executing remote commands since they are sent directly to the chip. Therefore, the adversary can perform a DoS attack by setting random values to destination addresses. Another approach considers encrypting the Radio Control (RC) link. In [101], the authors implemented an encrypted RC link based on Galois Embedded Crypto (GEC) library [102], which is compatible with resource-constrained devices. The proposed design enables secure communication between the UAV and the RC transmitter. To avoid physical attacks for UAVs with dynamic objects, Garg et al. [103] presented a prototype to identify projectiles thrown at the direction of UAVs using a microphone-based acoustic sensing mechanism. The solution considers a Short-Term-Fourier-Transform (STFT) algorithm capable of detecting approaching objects in 100 ms, and which enables dodging capabilities for the UAVs.

Hardware-level security issues, their countermeasures, and limitations are summarized in Table 4. As outlined in Table 4, the existing attacks against UAVs on the Hardware-level include the supply chain attacks, the battery depletion attacks, the use of hijacking techniques, and attacks on Radio Frequency Modules. The security measures proposed by the research community include developing defense mechanisms at the Hardware-level. For instance, managing the supply chain's security during the manufacturing process, performing a fine-grained circuit analysis, and using safety circuits in the Battery Management System. Although the existing countermeasures aim to protect UAVs from hardware-based attacks, limitations still need to be considered. For example, the hardware obfuscation techniques can hinder the fine-grained circuit analysis; the onboard encryption on the Radio Frequency Modules decreases the bandwidth and increases the latency of the chip. Furthermore, the development of Collision Avoidance Systems does not consider security implementations.

4.3. Software-level issues

Having discussed the Hardware-level issues, we introduce the Software-level issues by presenting the vulnerabilities, threats, and attacks targeting the software-level of UAVs. Afterward, we provide existing defense mechanisms to protect against such attacks.

4.3.1. Software vulnerabilities and threats

Software-level vulnerabilities and threats on UAVs consist of malicious software and zero-day vulnerabilities.

Malicious software. The Ground Control Station and the Flight Controller are prone to malicious software. The threats posed by UAV malware can lead to the loss of sensitive data and control of the operated UAV system. The accessibility of an attacker to the UAV's flight stack could potentially lead him to shut down the UAV system, which results in a denial-of-service and consequently disrupts the flight mission. Embedding such malware into UAVs can significantly compromise their security and privacy. For instance, Maldrone is a virus infecting the Flight Controller, enabling the attacker to control the UAV [107]. It behaves as a proxy for the drone's Flight Controller and sensor communications, thus making the compromised drone land at any chosen location. SkyJack is a hijacking malware that can be implanted on a malicious drone [108]. It can wirelessly take over other legitimate drones through the Wi-Fi de-authentication attack and compromise the whole system. Snoopy is a spyware that can be equipped on a drone with the ability to steal personal information from public users [109]. It uses impersonation techniques to trick the users into joining a fake Wi-Fi network. Afterward, Snoopy tracks its users and harvests their personal information. Recently, there has been an emerging type of malware that consists of encrypting a user's data or locking the system, and holding it encrypted or locked until the user pays a ransom to the adversary. This type of malware is known as ransomware [110]. To the best of our knowledge, ransomware attacks have not targeted UAVs yet.

Table 4
Summary of hardware-level security issues, existing countermeasures and their limitations.

Hardware-based attacks/threats	Countermeasures	Limitations
Hardware trojans [85]	-Building ML-based IDSs to detect hardware trojans [86]. -Performing a fine-grained circuit analysis [98].	-Hardware obfuscation techniques can bypass the existing detection methods.
Physical collisions [104]	-The development of Collision Avoidance Systems [88].	-Collision Avoidance Systems do not implement security features.
Hardware failures [90]	-Adopting encryption techniques on the flying UAVs prevent the adversary from capturing the stored data in the case of hardware failures [37].	-Data encryption might prevent forensics analysts from recovering evidence about the hardware failures.
Hijacking [93]	-Secure the GCS and UAVs from unauthorized access using authenticated encryption [105]. -Consistent change of the flight path to avoid the adversary from identifying the flight pattern [99].	-The use of counter-drone technology from malicious users to hijack legitimate UAVs.
Supply chain attacks [94]	-Managing the supply chain's security during the manufacturing process [100]. -Adopting tamper-protected devices [106].	-Internal attacks during the manufacturing process.
Battery depletion attacks [95]	-The use of safety circuits in the Battery Management System [96]. -Pre-flight diagnosis of the UAV batteries. -Monitoring the real-time battery discharging process [95].	-For unauthenticated communications, the adversary can display incorrect battery levels to the operator.
Attacks on Radio Frequency Modules [97]	-Encryption of the Radio Control link [101]. -Onboard encryption of the Flight Controller.	-Onboard encryption decreases the bandwidth and increases the latency of the chip.

Table 5
Summary of Software-level security issues, existing countermeasures and their limitations.

Software-based attacks/threats	Countermeasures	Limitations
Malicious software [107–109]	-Firewall implementations. -The use of antivirus and IDS solutions.	-Real-time detection of malware increases the computation costs.
Zero days vulnerabilities [48]	-Periodic system update.	-Some manufacturers can release the patches weeks after the zero-day disclosures.
Operating systems attacks [107]	-Adopting the authorization mechanisms for UAV system resources. -Software-based attestation approaches [113] [114].	-In a multi-UAVs network, managing authorizations for a swarm of UAVs is challenging.
Tampering captured videos [66]	-Firewall implementations. -Software-based attestation approaches [113] [114].	-Even with proper security measures, a legitimate user who joins the UAV network can still tamper the captured videos.
System ID spoofing [21]	-Periodic system update. -Firewall implementations.	-The use of social engineering techniques can reveal the System ID of UAVs since their manufacturers provide them.

However, it is essential to consider that future ransomware might target UAVs, given their popularity and civilian applications.

Zero-day vulnerabilities. Unknown vulnerabilities may exist in the UAV's flight stack or the GCS software (e.g., buffer overflow, DoS). These vulnerabilities are unknown to the UAV's manufacturers and can present critical threats to the operators. The adversaries can continuously exploit zero-day vulnerabilities until the UAV's manufacturers release appropriate patches. However, the operators need to update their UAV systems for every patch released.

4.3.2. Software-based attacks

Software-based UAV attacks include operating system attacks, tampering captured videos, and system ID spoofing. A supplementary attack relies on reverse engineering the software system of the UAVs in order to reveal its architecture and functionalities [111].

Operating systems attacks. Potential attacks against civilian or military missions could happen through the Flight Controller's system software. As a result, the compromised system software will lead to the loss of the UAVs and their payloads. Parcel-copters of the Prime Air service developed by Amazon is an example of the civilian applications that can be subject to operating system attacks [112]. Attacking the delivery system can potentially bring down the delivery package for the recipient and consequently crash the drone. Attacking UAV operating systems consists of remotely injecting malicious software to UAVs such as Maldrone [107], then hijacking the drone by taking control of the system. To that end, the adversary can extract the FC's cryptographic key and steal the stored unencrypted data.

Tampering captured videos. To guarantee safe navigation and avoid collisions during a flight mission, the operating system uses system calls that enable capturing the videos from the onboard camera [66]. However, a knowledgeable adversary with the system parameters can intercept the issued system calls to hijack UAVs. The adversary might also combine the tampering attack with a GPS spoofing attack to control the flying drone. Unlike the operating system attacks, the adversary's primary goal is to compromise the navigation's safety and produce collisions.

System ID spoofing. According to the FAA's regulations [45], UAVs should provide their System ID and location to third parties such as federal agencies and law enforcement when required. However, since most existing UAVs do not implement encryption mechanisms, the attacker can impersonate a third-party and execute an *identity spoofing attack* to compromise the communication link and get the System ID of a UAV [21].

4.3.3. Countermeasures for software-based attacks

A regular operating system update can prevent compromising the UAVs and their payloads. In addition, firewall implementations on the GCS can block sending malicious traffic to the UAVs. Also, software-based solutions such as antivirus and IDSs can monitor the network traffic and secure UAVs against malicious activities. Sedjelmaci et al. [9] presented an intrusion detection system for UAV networks. Although the simulation results demonstrate a high detection accuracy of over 93% with a low false positive rate around 3%, increasing the number of UAVs would significantly increase the false negative rate as well as the energy consumption, which can directly impact the network's scalability. Further, enabling the authorization mechanisms for UAV system resources can help protect malicious code from execution. A promising solution against software-based attacks is the use of software-based attestation approaches. They ensure the integrity of software running on the flight stack [113]. Remote attestation solutions are low-cost, and they provide a strong legitimacy of the software stack. In [114], the authors proposed SARA: a Secure Asynchronous Remote Attestation protocol that performs attestation over a large number of IoT devices. Through realistic simulation, the authors demonstrated that SARA has a low storage overhead of 3.03 KB, a runtime of 19 s for 250 services, and low energy consumption of 0.196 mJ.

At the Software-level, the adversary leverages malicious software and zero-days to infect the flight stack. Moreover, the adversary can tamper with the captured videos to mislead the operator. These software-based attacks are mitigated by adopting antivirus and IDS solutions. Furthermore, the operator should keep his operating system up to date and implement software-based attestation solutions to verify the legitimacy of the code running on the operating system. However, it is worth mentioning that the provided defense mechanisms against software-based attacks cannot fully protect the flight stack from malicious activities. The patching process can take several weeks for disclosed zero-day vulnerabilities. Thus, making the UAVs vulnerable to adversaries. Furthermore, using IDS solutions or firewall implementations on the GCS can increase the computation costs and cause latency issues. Table 5 summarizes the software security issues of UAVs, their existing countermeasures, and limitations.

4.4. Communication-level issues

Communication is the critical component of the UAV system for flight control and data transmission. Most UAVs use wireless communication for data and command exchange with the GCS. In this section, we provide the communication-level vulnerabilities, threats, and attacks against UAVs that compromise confidentiality, integrity, authenticity, and availability.

4.4.1. Communication vulnerabilities and threats

Communication-level vulnerabilities and threats can be categorized based on the communication layers as follows.

Physical & MAC Layer Vulnerabilities and Threats. The complexity of the UAV-2-GCS wireless communication network opens potential vulnerabilities. In [48] the authors demonstrated three different zero-day attacks affecting commercial Wi-Fi-based UAVs such as Parrot Bebop UAV [115]. These attacks are (1) Buffer overflow attack, (2) DoS attack, and (3) ARP cache poisoning attack. The buffer overflow attack on Parrot Bebop UAV consists of sending large connection request packets for the UAV. The DoS attack relies on sending simultaneous requests to the Parrot Bebop UAV. In this case, the drone is under a denial of service since it cannot handle more than 1000 simultaneous requests. For the ARP cache poisoning attack, the adversary sends continuously spoofed ARP replies to fool the UAV's wireless network. The experimental results reveal massive security issues in UAV-2-GCS wireless communications. Choosing the correct type of wireless communication technology depends on the specification of the mission requirements (e.g., transmission range, operating frequency, category). However, this choice does not guarantee the flight's success since we have to consider the security issues of each type of wireless communication technology. Therefore, the fundamental question that remains unanswered is which type of wireless communication technology achieves a high level of security for UAVs for each application domain.

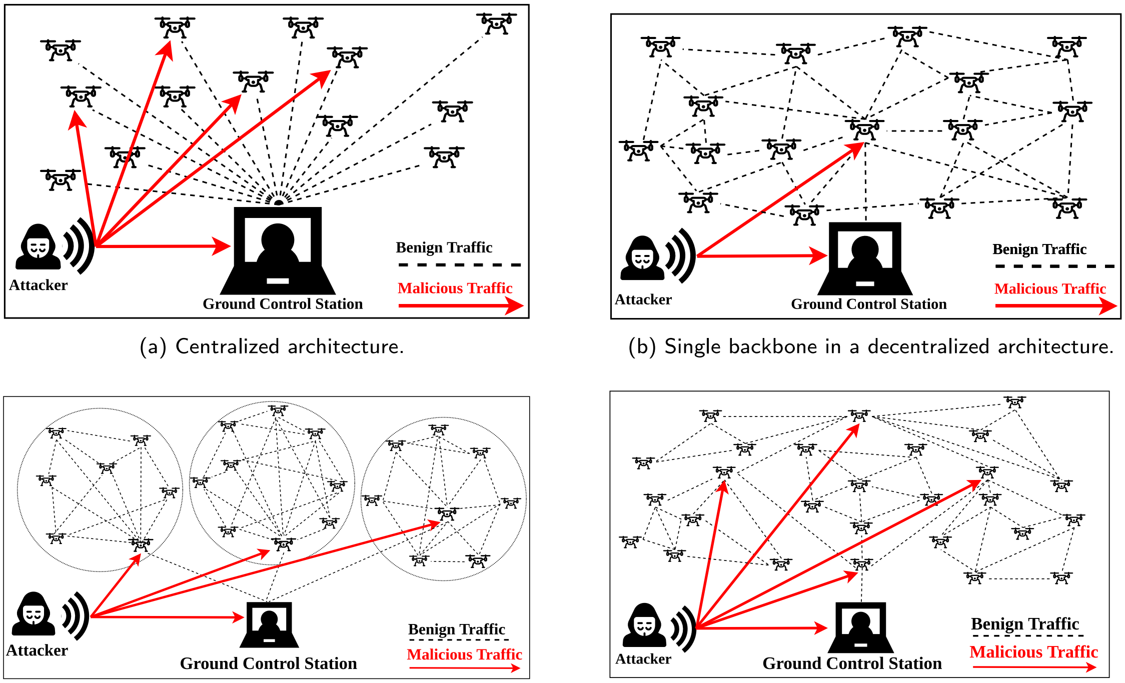
Network Layer Vulnerabilities and Threats. The UAV network operates in an ad hoc fashion, commonly called FANETs. These networks have a dynamic topology, and they present critical threats. A prior work presented general security threats of drone-assisted public safety networks [116]. It shows that the increase in UAV network's complexity results in more vulnerabilities to attacks. These attacks target mainly sensor inputs and communication modules. UAV communication threats such as intercepting or blocking the communication link between the Flight Controller and the GCS might cause a potential DoS attack. Furthermore, given FANETs' unique characteristics, including the latency and computational power to route data, there is a need to build cryptographic algorithms for FANETs that take these characteristics into consideration [26]. An attacker can disrupt the UAV network by sending malicious traffic directly through the GCS or indirectly through the UAVs. Whether in a centralized or decentralized architecture, adversaries constantly threaten the GCS. In both architectures, the GCS represents a single point of failure, and the security of the whole UAV network depends on the security of the GCS. However, even though the security mechanisms are implemented for the GCS, the attacker can still interrupt the flight mission by compromising the flying UAVs. It should be emphasized that in some scenarios, the flight mission can still be considered successful even if one or multiple UAVs are compromised. In this case, depending on the civilian application, the operator requires a minimum number of legitimate (uncompromised) UAVs to accomplish the mission.

In a centralized architecture, as illustrated in Fig. 5(a), the adversary needs to target and send malicious traffic to a specific number of UAVs, such that the minimum number of legitimate UAVs required for the flight mission to succeed cannot be satisfied. Consequently, the adversary causes the flight mission to fail by disrupting the entire UAV network.

Alternatively, for a decentralized UAV network architecture, the adversary needs only to compromise a particular UAV or UAVs to cause the flight mission to fail. In fact, for a single backbone UAV network, as depicted in Fig. 5(b), the adversary needs to send malicious traffic only to the backbone UAV since it serves as a gateway between the other UAVs and the GCS. When the attacker compromises the single backbone UAV, the group of UAVs or the whole network is disrupted. Therefore, the single backbone UAV constitutes the weakest link in the UAV network. For a single backbone UAV architecture, the UAV network's security depends on the security of the GCS, the single backbone UAV, and their communication link. However, if the UAVs are similar in terms of shape, size, and color, it is challenging for the adversary to determine the backbone UAV. In multiple backbone UAVs architectures, the GCS and the backbone UAVs of each swarm are particularly critical for the success of the flight mission. However, the flight mission could be completed even if a backbone UAV is compromised. From Fig. 5(c), we notice that the adversary needs to compromise four backbone UAVs or the GCS to disrupt the entire UAV network. Moving forward to more advanced UAV network architectures in mixed UAVs, Fig. 5(d) shows that securing the network of backbone UAVs is as crucial as securing the whole network. It is worth mentioning that the threats increase at the same level as the network complexity and the number of UAVs increase. In Table 6, we summarize the different attack points described for each UAV network architecture that, if compromised by the adversary, the flight mission will fail.

UAV routing protocols are vulnerable due to the inherent characteristics of UAV networks, such as dynamic topology, limited resources, and lack of encryption in their wireless links [20]. In this context, the adversary leverages these constraints to perform different routing attacks in the network layer. The adversary can disclose critical information in UAV networks that do not implement security mechanisms. With eavesdropping techniques, the adversary can leak routing information, topology information, and UAV positions [20]. Furthermore, without authentication and integrity considerations, UAV routing protocols are prone to additional attacks such as DoS attacks or route-cache poisoning attack [117], where the adversary inserts incorrect routing information into the caches of legitimate UAVs.

Transport Layer Vulnerabilities and Threats. UAV communication protocols suffer from vulnerabilities leading to various attacks if not properly secured. Despite their communication features, they must ensure basic security requirements such as confidentiality, integrity, availability, and authenticity. Recent studies show that MAVLink protocol, one of the most well-known UAV communication protocols, is vulnerable to



(a) Centralized architecture.

(b) Single backbone in a decentralized architecture.

(c) Swarm of UAVs in a decentralized architecture.

(d) Mixed UAVs in a decentralized architecture.

Fig. 5. Threats for UAV communication networks in different architectures.

Table 6
Attack points of different UAV network architectures.

Network architecture	Attack points
Centralized Architecture	– The Ground Control Station. – Specific number of UAVs.
Single Backbone UAV	– The Ground Control Station. – The backbone UAV. – The GCS-2-UAV communication link.
Swarm of UAVs	– The Ground Control Station. – The backbone UAVs of each swarm. – The GCS-2-UAV communication link of backbone UAVs. – The network of backbone UAVs.
Mixed UAVs	– The Ground Control Station. – The backbone UAVs. – The network of backbone UAVs. – The GCS-2-UAV communication link of backbone UAV.

ICMP flooding and packet injection attacks [59]. In addition, another transport layer protocol, the UranusLink, checks only the integrity of the message. Consequently, the adversary gathers the exchanged packets and discloses its content [61].

4.4.2. *Communication-based attacks*

In what follows, we present the common attacks exploiting UAV communications on the physical & MAC layer, the network layer, and the transport layer.

Attacks on the Physical & MAC Layer. Given the significant difference between aerial networks and traditional wireless networks, there is a need to choose the most suitable wireless technology for UAVs [1]. In this context, we categorize for each wireless communication technology in the physical & MAC layer, its unique features, and specific security issues. Although it is possible to find surveys on the security of each wireless communication technology on its own, we briefly list the major characteristics and security issues of wireless communication technologies in UAV systems in Table 7.

Attacks on the Network Layer. The attacks on the network layer of UAV communications include eavesdropping, DoS, man-in-the-middle, forgery, replay, and other attacks on the FANETs.

(a) Eavesdropping attacks. An attacker can perform an eavesdropping attack through the UAV-2-GCS communication link by gathering data such as live video feeds, sensor readings, and GPS data sent by the UAVs to the GCS. Since most UAVs avoid encrypting the wireless communication for the sake of improving communication performance [66], the attacker can eavesdrop on exchanged information, including telemetry feeds and GCS commands. Therefore, the adversary can violate confidentiality of the communication and the data by gathering sensitive information such as sensor readings and GPS data.

(b) DoS attacks. An adversary can compromise a UAV system by launching a DoS attack. In this case, the attacker can flood the flying UAV's network card with random traffic by sending multiple requests, causing an overload of its resources and disrupting its availability. Performing such attacks on UAVs can result in a substantial increase in the network latency and a decrease in the quality of video streaming applications for the user [131]. Another way to perform a DoS attack is by sending large packets to the GCS within a specific range to disable the control signal. Once the signal is disabled, the drone goes into a lost link-state, which results in a malfunctioning of the data link. Consequently, the operator can no longer send or receive data signals to the Flight Controller, which results in disrupting the communication link and losing control of the UAV. In [132], the authors simulated a Distributed DoS (DDoS) attack on UAVs using botnets. The DDoS attack was simulated by flooding the network traffic using User Datagram Protocol (UDP) packets. This type of simulation demonstrates the possibility of performing real-world DDoS attacks on UAVs. Besides, performing de-authentication attacks can also disable the operator from controlling the UAV. The de-authentication attack is a DoS attack that *sends* de-authentication packets to the UAVs to disrupt the UAV-2-GCS communication. As a result, the adversary blocks the UAV-2-GCS communication, and eventually, the UAVs are disconnected from the network. An example of such attacks is demonstrated by Skyjack [108].

(c) Man-in-the-Middle attacks. In this one of the most well-known attack [133], the adversary controls the UAV-2-GCS wireless channel

Table 7
Security issues of the wireless communication technologies used in physical & MAC layer of UAV communications.

Communication Technology	Category	Frequency	Range	Security issues
Wi-Fi	WLAN	2.4–5 GHz	20–120 m	– Commercial Wi-Fi-based UAVs are vulnerable to basic attacks, such as Wi-Fi de-authentication attack [48]. – Unencrypted Wi-Fi networks allow the adversary to perform spoofing or jamming attacks [118]. – Popular attacks against the IEEE 802.11 standard exist in the literature (e.g., flooding attacks, Key Retrieving Attacks, ARP injection attacks) [119].
Bluetooth	WPAN	2.4 GHz	10–200 m	– The sequence extraction of Frequency Hopping Spread Spectrum (FHSS)-type controllers using a Software Defined Radio (SDR) enables the likelihood of performing Bluetooth sniffing [120]. – A family of different vulnerabilities of Bluetooth communication known as BrakTooth can be applied in UAVs scenarios [121].
Zigbee	WPAN	2.4 GHz	10–100 m	– Threat analysis of autonomous UAVs shows that multiple vulnerabilities allow the adversary to locate the Zigbee transmitter, perform DoS and replay attacks [122]. – KillerBee is an example of an open-source exploitation framework designed to perform reconnaissance and exploit Zigbee vulnerabilities [123].
Long Range (LoRa)	LPWAN	868 MHz 915 MHz	05–15 km	– The LoRa Alliance does not consider security implementations and lacks security controls on the network servers [124]. – Limited security features, which does not fully support the end-to-end security and perfect forward secrecy [125]. – Prone to various security attacks: jamming attacks, replay attacks, and wormhole attacks [126].
Sigfox	LPWAN	868 MHz 902 MHz	03–30 km	– Lack of data confidentiality and authentication [126]. – Sigfox does not support encryption [127].
Narrowband-Internet of Things (NB-IoT)	LPWAN	200 KHz	10–35 km	– Several layerwise passive and active attacks exist: Malicious code injection, Man-in-the-Middle attack, and jamming attack [126,128].
Worldwide Interoperability for Microwave Access (WiMAX)	WMAN	2.3–5.8 GHz	01–48 km	– Considering UAVs as a collection of mobile nodes communicating within a WiMAX network, when compromised, they create a byzantine failure and disrupt the whole network [129]. – oS attacks can target different resources: storage and processing resources (e.g., memory, storage, CPU), energy resources (e.g., battery), and bandwidth [130].
Cellular Technology (GPRS, EDGE, UMTS/WCDMA, UMTS/HSPA, LTE, LTE Advanced - 4G, 5G)	WWAN	Sub-6 GHz	World wide	– Prone to jamming, spoofing, eavesdropping, hijacking, and DoS attacks [25].

and alters the benign packets with malicious content [134]. Thus, the adversary can act as a bridge between the UAV and the GCS, and compromise the bidirectional UAV-2-GCS communication. A video replay attack is an example of a Man-in-the-Middle attack, where the adversary fools the operator by transmitting malicious live feed data. VideoJak [135] is an example of such attacks.

(d) Forgery attacks. The adversary can compromise UAVs communication integrity by transmitting a forged request to unauthenticated UAVs [116]. In this attack, the adversary generates the malicious request by impersonating a legitimate request and disrupts the UAV-2-GCS communication.

(e) Replay attacks. In UAV networks, the adversary can perform an eavesdropping attack to intercept several requests, then replay valid data to the UAVs. In this case, the UAVs might receive repeated data, and if no replay protection is implemented, the UAVs cannot distinguish legitimate requests from malicious ones [116].

(f) Attacks on FANETs routing. Different passive and active attacks can occur in Mobile Ad hoc Networks (MANETs) routing protocols which consist of injecting malicious nodes, controlling the network traffic, or disrupting the routing functionality [20]. Most existing attacks targeting routing protocols on MANETs are transferable to routing protocols on FANETs since FANETs are a subcategory of MANETs. To illustrate these attacks, we classify them into three categories based on their routing functionality [136]: *(i) the route discovery attacks:* they target the traffic control and include the blackhole [137], sleep deprivation [138], sybil [139], and wormhole [140] attacks. *(ii) The route maintenance attacks:* they aim to corrupt the routing control packets. Examples of such attacks are flooding [141] and Byzantine [142] attacks. *(iii) The data forwarding attacks:* they include the type of attacks that impact the payload traffic, such as real-time video traffic [143].

Attacks on the Transport Layer. Attacks on the transport layer of UAV communication can be grouped based on the UAV transport layer protocols.

(a) UranusLink Protocol Attacks. To the best of our knowledge, there is no existing attack against the UranusLink protocol. According to the design and implementation of UranusLink for real-world applications [60], UranusLink provides only integrity protection via the checksum field in the messages. However, an adversary with the ability to capture the exchanged packets can benefit from this vulnerability and disclose mission-related information [61].

(b) MAVLink Protocol Attacks. Authors in [58] classify MAVLink attacks into four classes depending on how data is compromised: interception, modification, interruption, and fabrication attacks. Since the MAVLink protocol does not provide authentication and encryption, the adversary can capture communication traffic through eavesdropping and thus collect exchanged data between the GCS and the UAVs. Moreover, he can perform system ID spoofing attacks. The authors in [144] presented a realistic scenario of compromising different UAVs operating under MAVLink protocol. The considered specimen attack scenario demonstrates an attacker's ability to perform a stealthy attack by capturing a flight mission's system-ID and spoofing MAVLink packets.

4.4.3. Countermeasures for communication-based attacks

Different security approaches have been proposed in the literature to ensure confidentiality, authentication, availability, and data integrity in UAV communications. In what follows, we present existing countermeasures against UAV communication-based attacks at the physical & MAC layer, network layer, and transport layer.

Countermeasures for the Physical & MAC Layer Attacks. Securing the physical properties of the communication channel (e.g., transmission medium, physical topology) is one of the mitigations against the physical & MAC layer attacks of UAVs. Given the wide use of UAVs across different wireless communication technologies, it is important to consider that securing wireless communications at the physical & MAC layer is challenging due to the characteristics of each communication technology (e.g., category, frequency, range). In addition, encryption algorithms such as AES can be employed at the physical & MAC layer communications. Moreover, artificial noise techniques that transmit generated noise to illegitimate users can also be used [145]. In addition to these, one of the best practices for secure communication in this layer is to keep the device firmware and related software up to date using the released security patches. We note that, the attacks and the countermeasures for the wireless communication technologies outlined in Table 7 are vast and it is possible to find a survey on the attacks and mitigations for each communication technology in the list. For this reason, we do not provide details with the countermeasures against the attacks on these well-known and widely used communication technologies in this survey.

Countermeasures for the Network Layer Attacks. To mitigate eavesdropping attacks on UAV networks, the operator can adopt authenticated encryption [146]. It protects the UAV-2-GCS communications by ensuring the confidentiality and authenticity of the exchanged data. In [147], the authors proposed an anti-eavesdropping power control algorithm in UAV communication systems. Power control algorithms present an efficient approach for building a UAV network topology that ensures the Quality of Service (QoS), and they are also used to prevent eavesdropping attacks. In the presence of an eavesdropper, the algorithm proposed by Zhang et al. [147] demonstrates that by optimizing the trajectory and transmitting power control between the UAV and the GCS, we maximize the secrecy rate (the difference between the rate of the UAV-2-GCS communication channel and the maximum rate of the eavesdropper [148]). Moreover, adopting a continuous authentication against eavesdropping attacks can identify a pilot's unique profile during the flight mission [36]. Another solution aims to use fingerprinting techniques to authenticate UAVs [149]. This approach achieves mutual authentication based on Physically Unclonable Functions (PUFs). The computation performance on a Raspberry Pi 3B shows communication and storage costs of 1600 bits and 352 bits, respectively. To prevent Man-In-The-Middle attacks, the authors in [150] developed a machine learning-based authentication mechanism for autonomous UAVs. The proposed model learns through times-series telemetry traces during the flight mission, and the simulation results on ArduPilot [42] show a precision rate of 93.4% for the K-Nearest Neighbour classifier over the Support Vector Machine (SVM) and the Logistic Regression (LR) classifiers.

The use of cryptographic primitives such as public-key cryptography guarantees the integrity and confidentiality of UAV communications. In [151], the authors proposed a secure communication scheme for UAV networks using hierarchical identity-based broadcast encryption (HIBBE) technique. The proposed approach guarantees message confidentiality and authentication through identity-based signcryption. Their performance analysis results show that the proposed scheme is resistant to DoS attacks. Another work presented a secure communication protocol based on an efficient certificateless Signcryption Tag KeyEncapsulation mechanism (eCLSC-TKEM) [152]. Furthermore, the protocol is energy-efficient and meets security and efficiency requirements for UAV communications. To secure commercial WiFi-based UAVs, the authors in [48] presented a comprehensive multi-layer security framework. Their proposed framework is efficient against basic attacks such as ARP cache poisoning attacks and DoS attacks.

For the Internet of Drones environments, Srinivas et al. [153] suggested a new temporal Credential-Based Anonymous Lightweight Authentication Scheme for UAVs, where a legitimate user can access real-time data of UAVs using his credentials. The proposed approach has a computation cost of 26.7 ms and a communication cost of 1536 bits. In [154], the authors presented a lightweight FPGA hardware solution to secure UAV-2-GCS communication of commercial Wi-Fi-based UAVs. It contains a cryptographic engine responsible for encrypting the communication control data. Thus, ensuring confidentiality and authentication. However, enabling cryptography-based approaches will require additional computation in both GCS and UAVs and increase energy consumption. Hence, these solutions may reduce the performance of the UAV-2-GCS communication.

IDSs aim to detect malicious intrusion activities such as DoS attacks. They can be deployed on the flying UAV or in the GCS. We distinguish three intrusion detection approaches [62]: *(i) Rule-based intrusion detection*, where specific rules for UAVs are applied in which rules follow the expected behavior of the UAV system [155], *(ii) Signature-based intrusion detection*, which relies on attack signatures [156], and *(iii) Anomaly-based detection* that detects known and unknown attacks based on learning or filtering mechanisms. However, these three approaches mentioned above cannot fully detect UAV intrusions. For example, the signature-based detection approach is weak against attacks that frequently change their patterns, which result in changing their signature. Additionally, the anomaly-based approach may suffer from false positives and false negatives. A recent work uses a hybrid detection approach that combines two or more approaches to accurately detect unknown attacks [157]. Other intrusion detection solutions rely on packet analysis techniques to ensure data integrity and network availability in UAVs [9].

In the literature, different security solutions have been proposed to secure MANET routing protocols from malicious actors [20,55]. These approaches can also be used in FANETs and include cryptographic schemes such as message authentication, digital signatures, and hashing. Hence, enabling the confidentiality and integrity of the UAV network. We distinguish the use of *secure-based routing protocols* for FANETs to guarantee the routing process and reliability in the presence of malicious nodes. This category includes the use of security mechanisms in the routing protocols [55]. Examples of secure-based routing protocols for UAVs networks are: SUANET (Secure UAV Ad hoc NETwork) [158], PASER (Position-Aware, Secure, and Efficient mesh Routing) [159], SUAP (Secure UAV Ad hoc routing Protocol) [136], AODV-SEC (Ad hoc On-demand Distance Vector-Secure) [160], and SRPU (Secure Routing Protocol for UAVs) [161]. Each of these protocols uses a specific strategy to satisfy the security and privacy of the routing path. For instance, the SUANET protocol uses a key management strategy between UAVs to enable confidentiality and authentication services [158]. In contrast, PASER protocol utilizes cryptographic functions to secure the routing packets in the UAV network [159]. SUAP routing protocol prevents the flooding attack [136]. AODV-SEC routing protocol ensures a secure route discovery process [160]. However, the implementation of *secure-based routing protocols* in realistic scenarios is challenging due to their complexity and spatial distribution.

Countermeasures for the Transport Layer Attacks. To prevent the adversary from disclosing sensitive information in the transport layer, it is important to implement security mechanisms enabling the confidentiality and integrity of the exchanged data (e.g., cryptographic protocols, secure key exchange). Singh et al. [163] proposed a blockchain-based security framework to secure the transfer of information among UAVs. In this approach, the UAVs can either perform transactions in the blockchain or add validated transactions onto the blockchain. The authors evaluated the proposed architecture with 100 drones to validate its suitability under different conditions. The results show that the overall computation time for the transaction phase reaches 19 ms, while the communication cost for the entire blockchain is 1983 bits. To mitigate MAVLink attacks, one approach proposes an architecture

Table 8
Summary of UAV Network and Transport Layer security issues, existing countermeasures and their limitations.

Layer	Attacks/threats	Countermeasures	Limitations
Network Layer	Eavesdropping attacks [66]	– The use of anti-eavesdropping power control algorithm in UAV communications [147]. – Adopting authenticated encryption [146].	– Cryptography-based approaches require additional computation and might increase energy consumption.
Network Layer	DoS attacks [131,132]	-Building IDS solutions [155,156].	-Impact on the performance of the GCS-2-UAV communication. -The signature-based IDS fails against attacks that change their patterns. -The anomaly-based IDS can suffer from false positives and false negatives.
Network Layer	Man-in-the-Middle attacks [134]	– Encrypting the communication control data [154]. – Implementing fingerprinting techniques to authenticate UAVs [149].	– Latency issues for time-critical UAVs applications.
Network Layer	Forgery attacks [116]	– Enabling a multi-layer security framework [48].	– The complexity of the network increases in multi-UAVs scenarios.
Network Layer	Replay attacks [116]	– Establishing a secure communication scheme (e.g., identity-based encryption) [151]. – The use of authentication mechanisms [37,66].	– Repeated requests can flood the network and cause a possible DoS.
Network Layer	Blackhole [137], Flooding [141], Sybil [139], Wormhole [140], Sleep deprivation [138], Byzantine [142], and Forwarding [143] attacks	– The use of secure-based routing protocols [55].	– High computation overheads and delay. – The security features are supported only by few routing protocols.
Transport Layer	Attacks on communication protocols [58,61]	– Building a high-level architecture for resiliency and trustworthiness capable of repairing the flight mission despite the attack [144]. – Embedding security services into hardware modules. – The use of classical security approaches such as encryption techniques and IDS approaches. – Exploiting the features of emerging technologies such as blockchain [162].	– The introduction of trade-offs between performance and security.

that consists of repairing and completing the mid-flight mission despite the cyber attack [144]. Other approaches also exist to secure the MAVLink communication protocol. In [58], the researchers divided existing MAVLink security solutions into hardware and software-based solutions. Hardware-based solutions rely on embedding security services into hardware modules, while software-based solutions include classical security approaches like encryption techniques and IDSs. Other solutions that aim to secure MAVLink communication protocol might benefit from the features of emerging technologies such as blockchain and Software-Defined Networking (SDN) [38].

Table 8 summarizes the UAV network and transport layer communication security issues, their existing countermeasures, and limitations. The communication-based attacks on UAVs at different layers enable the adversary to disrupt the communication link and jeopardize the flight mission. Specific countermeasures have been developed in the literature to guarantee the exchanged data's confidentiality, integrity, and availability. These countermeasures consist of building IDS solutions, adopting authenticated encryption to prevent eavesdropping attacks, enabling a multi-layer security framework, and using secure-based routing protocols. However, it is worth noting that the countermeasures mentioned above for UAV's communication-based attacks have some limitations and shortcomings. For example, building IDS solutions to prevent DoS attacks impact the performance of the UAV-2-GCS communication. Besides, latency issues occur when encrypting the communication control data. Moreover, the use of secure-based routing protocols significantly increases the computation overheads and introduces delays.

5. Privacy issues of UAVs

The development of UAV technologies has raised a broad range of privacy issues for civilians that put them at high risk. In this section, we first divide the privacy issues into two categories: issues linked to individuals and issues associated with the regulations of UAVs. The categorization we apply and follow in this section is given in Fig. 6. Afterward, we present the privacy attacks against UAVs and their corresponding defense mechanisms.

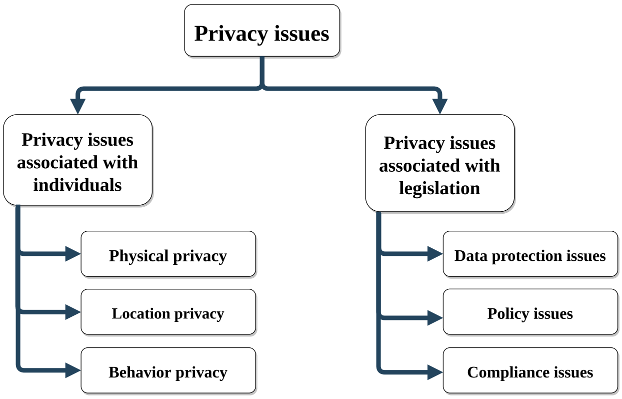


Fig. 6. Privacy issues of Unmanned Aerial Vehicles.

5.1. Privacy issues

The privacy issues of UAVs can be grouped into two categories: the issues associated with individuals, and the issues associated with legislation. The privacy issues linked to individuals deal with personal information obtained through a flying drone, while the privacy issues related to the legislation handle the regulations and procedures to guarantee the privacy for citizens, which is a fundamental human right.

5.1.1. Privacy issues associated with individuals

The integration of UAVs in the national airspace has triggered serious concerns for citizens regarding their privacy in their daily life.

A recent study presented the privacy concerns posed by the use of UAVs in airborne photography, and proposed strategies on how to preserve the privacy of citizens in various UAVs applications [164]. In [12], the authors divided the privacy leakage into three classes: physical privacy, location privacy, and behavior privacy.

In *physical privacy*, the attacker captures images and videos of people inside their houses for malicious purposes [165]. *Spying* activity on people through UAVs is one of the significant physical privacy issues. Hence, the need to establish regulations governing the use of UAVs in civilian airspace. UAVs can also be equipped with directional microphones to eavesdrop on private conversations.

Location privacy targets people's physical locations and their movements without their knowledge of being under surveillance [166]. Third parties could use it for business purposes (e.g., targeted advertising by location). Nowadays, the use of UAVs is switched from aerial surveillance to tracking individuals [167]. Indeed, one of the most challenging issues is to tell whether a flying drone is used for aerial surveillance or for tracking people [24]. Detecting such privacy invasion attacks is still an open research problem.

In *behavior privacy*, the attacker monitors the people's lifestyle and interests in public space [168]. Surveillance of individuals through systematic monitoring of their behaviors constitutes a major threat to behavioral privacy and may negatively impact people's psychological level [168].

5.1.2. Privacy issues associated with legislation

The large-scale deployment of UAVs into the civilian airspace created the need to establish legislation and proper privacy protection procedures that cope with the existing national and international law. In this context, efforts have been made by the European Commission to preserve citizen's privacy while ensuring the benefits of UAV applications [169,170]. However, the regulation governing the use of UAVs in civilian airspace might suffer from *several* issues that cannot guarantee citizen's privacy. These issues can be classified into three categories: data protection issues, policy issues, and compliance issues.

- Data protection issues: Even under authorization from legal entities, the flying UAVs can potentially obtain personal data (e.g., live images, audio recordings) without making nearby individuals aware of such actions. This would result in fear of citizens being under surveillance, thus violating civil liberties.
- Policy issues: The adoption of a set of policy measures for UAV operators (e.g., maximum flight altitude, RemoteID broadcast [45], restricted airspace, navigation during the night) can support personal data protection and transparency among the citizens. Nevertheless, it is challenging to monitor UAV operators in a real-time that are not following the required policies, which can trigger accountability issues.
- Compliance issues: Several aviation agencies (e.g., FAA — Federal Aviation Administration, EASA — European Aviation Safety Agency) release procedures and regulatory actions that UAV operators and manufacturers must comply to ensure a high level of safety. However, operators may not comply with the regulations, and mechanisms are needed to verify that they operate UAVs in compliance with the regulations. In addition, it is unlikely for manufacturers to produce UAVs that are compliant with all aviation agencies. This could be explained due to the lack of a unified standard for UAVs in terms of hardware, architectural design, and communication protocols.

5.2. Privacy attacks and defense mechanisms for UAVs

Compromising data privacy refers to compromising data secrecy that should not be revealed to third parties. In this context, privacy attacks against UAVs aim to disclose such data. On the other hand, information and resources that an adversary maliciously harvests from UAVs may not necessarily be personal [171]. In particular, UAVs can *spy* on organizations through video streaming, such as industrial espionage, and the attacker can disclose the private information of government agencies and corporations to unauthorized parties. For example, in a farming business that uses a swarm of UAVs to optimize its operations and improve the crop production, an adversary can spy on this organization by using the same UAV model. In this case, we cannot distinguish between the friendly UAV and the malicious one. It is known as the identification problem and exploited to perform malicious activities such as terrorism and smuggling [24]. Other types of privacy attacks involve leaking sensitive information monitored by the UAVs to unauthorized third parties, such as video footage, photos, and physical measurements. In addition, other types of sensitive data related to the flying UAVs, including the real-time GPS location, speed, height, and battery status, have to be preserved only for the operator. Preserving data privacy of the flying UAVs is a fundamental requirement for the safety of the flight mission [22]. In unencrypted communications, the adversary can perform a *traffic analysis attack* by listening to the traffic and extracting sensitive flight mission information. This type of passive attack compromises the confidentiality and privacy of the UAV. Even in encrypted communications, forensics techniques, including data extraction and analysis, can recover digital data [172]. Another type of privacy attack targeting UAVs occurs when the adversary has an *unauthorized access* to the critical components of the UAV system, such as the sensors and the storage (e.g., hijacking attack, injecting hardware trojans). In this case, the adversary discloses flight data to the public and jeopardizes the flight mission.

From a legislative point of view, it is important to implement appropriate safeguards such as forcing transparency on the users (i.e., the users should know who is responsible for the UAV and their purposes when flying nearby). Additionally, a data protection impact assessment should be carried out to evaluate the legitimacy of data processed by the UAVs and appropriate privacy-preservation mechanisms should be enforced (e.g., the use of blurring faces and respect for flight altitude in some areas).

Several studies have suggested privacy-preserving mechanisms to prevent leaking secret information to unauthorized parties. These mechanisms include encryption techniques and the design of tamper-proof hardware so that even in scenarios where the drones are hijacked, they cannot reveal sensitive information. In [173], the authors suggested an approach to detect privacy invasion attacks based on UAV's flight behavior. However, it fails to identify a UAV's purpose (whether it is legitimate or malicious). The researchers in [174] presented a privacy-preserving authentication scheme for UAV control systems. The proposed architecture has a mutual authentication to secure communication between entities and integrates cryptography mechanisms such as Elliptic Curve Cryptography (ECC), digital signature, and hash functions. Moreover, the suggested privacy protection protocol guarantees location privacy and proves its applicability in sensitive control areas. Similarly, a privacy-preserving authentication approach for UAVs was proposed in [175]. It is a predictive authentication framework considering identity, location, and flying routes as sensitive information. Other solutions can overcome privacy issues, such as implementing access policies and lightweight cryptography approaches. Some manufacturers include a list of no-fly GPS coordinates covering sensitive areas in the firmware of their product. Moreover, regular users can register their home location in the NoFlyZone Database [18].

6. Pitfalls and future research directions

As it appears and develops, the UAV technology brings certain advantages and benefits to our society. However, it can also create new potential threats and tools for malicious attacks on civilian users. Although the existing countermeasures aim to protect the operators from malicious activities, several open issues need to be addressed by the research community. In this section, we first present the lessons learned. Then, we identify open issues and discuss future research directions, which we believe will provide useful guidance for future UAV security research and practice.

6.1. Lessons learned and pitfalls

The rise of UAV technology created a plethora of cyber attacks, such as intercepting unencrypted data links from UAVs or spoofing the UAV network. Protecting the flight mission requires a comprehensive defense-in-depth approach.

UAV Manufacturer Issues. Our findings in this survey demonstrate that UAVs lack protection from various attacks at different levels. A possible reason for this shortcoming could be explained by manufacturers' interests in increasing the performance of their commercial products over security. Another reason is the additional cost needed from manufacturers to implement security mechanisms. UAV manufacturers should consider the security and privacy aspects while developing their products in all the supply chain phases.

Sensor-level Issues. At the Sensor-level, the diversity and complexity of onboard sensors (e.g., chemical, physical, mechanical) make them targeted components for adversaries. Moreover, existing countermeasures against spoofing, sniffing or jamming onboard sensors are limited due to the unique characteristics of UAVs. Although the existing security research covers sensor-based threats and attacks [64], in the context of UAVs, we need to consider additional parameters such as the authenticity of sensor readings, the energy and computation costs when securing sensed data against malicious actors.

Hardware-level Issues. At the Hardware-level, despite the type and characteristics of different commercial UAVs such as the firmware and hardware type, UAV hardware could be targeted in the manufacturing process, or before or during the flight mission. These scenarios are possible due to the vulnerabilities that can occur in UAV firmware and also due to the lack of encryption in custom chipsets. Given the popularity and diversity of existing UAVs, it is important to build a unified hardware security strategy that protects UAVs from hardware-based attacks.

Software-level Issues. At the Software-level, the adversaries can leverage the zero-day and existing software vulnerabilities in the flight stack as well as the GCS software to compromise the flight mission. The prevalence of software-based attacks demonstrates the need to develop robust defense solutions for UAV software security. However, existing UAV manufacturers avoid integrating software security implementations in their products for performance reasons. Therefore, the adversaries can take advantage of this gap to build malicious software (e.g., Maldrone [107], Snoopy [109], SkyJack [108]).

Communication-level Issues. At the Communication-level, designing a Multi-UAV network has to consider potential security issues according to the chosen network topology. Many UAV protocols are not properly secured and pose serious threats. Given that communication is a crucial part of the UAV system, we argue that standardized UAV protocols enabling reliable and secure communication have to be developed. Most of the existing communication protocols in UAVs are unencrypted or have limited cryptographic capabilities, thus enabling adversaries to compromise the communication channels. Moreover, existing security measures to protect civilian UAVs from malicious users are limited to single UAV systems [23]. Therefore, there is a need to develop countermeasures for multiple UAV scenarios.

Security-Performance Tradeoff. At any level of the UAV, when implementing security solutions, we need to assess the performance of the UAV system. In particular, the communication costs, the computation costs, the storage overheads, and the energy consumption. It is worth mentioning that implementing security mechanisms on the UAV system might negatively affect its performance given the computationally expensive operations [18]. In particular, the adoption of cryptographic primitives (e.g., signature operations, key generations, hash functions) may introduce additional communication and computation costs, which eventually affect the functionality of the UAV system. To that end, it is important to evaluate the performance of cryptographic operations over various UAV microcontroller units [176]. However, adding an extra security layer for each level without considering the abovementioned parameters might significantly decrease the performance of the flight mission. It should also be noted to consider the energy consumption and storage overheads, which can be crucial for resource-constrained UAVs such as micro aerial vehicles. For instance, the microcontroller unit of the Crazyflie drone has an ARM Cortex M-4 processor that runs at 168MHz, with 192 Kilobytes SRAM and 1 Megabyte flash memory [43]. In this case, adopting standard symmetric encryption such as AES requires a computation time of $32.96\,\mu s$. However, using a lightweight symmetric encryption scheme such as CHACHA-20 [177] will reduce the computational cost to $8.59\,\mu s$ [178]. Toward this point, we can derive possible tradeoffs between the performance and security considerations of UAVs.

Privacy Concerns. Besides security considerations, UAVs can also violate personal privacy, from spying on people's lifestyles to gathering sensitive data about organizations. The deployment of UAVs in the civilian airspace without specific regulations poses serious privacy concerns for individuals. Moreover, sensitive information collected by UAVs and transmitted to the GCS has to be protected from unauthorized parties. Therefore, privacy leakage has to be considered during the design of UAV systems. Two significant scientific gaps allow privacy invasion attacks: *The purpose detection problem* and *the identification problem* [24]. The *purpose detection problem* distinguishes between a legitimate and a malicious nearby UAV that violates an individual's privacy. Existing approaches to solving the purpose detection problem are minimal since they cannot detect spying actions on a specific Point of Interest (POI) [173,179,180]. A recent study demonstrated, using a cryptanalysis approach, that applying a periodical physical stimulus (LED flicker) on the spying UAV cameras causes a watermark on the encrypted UAV-2-GCS communication traffic [181]. The detection of such a watermark determines the legitimate or illegitimate purpose of the drone. However, this approach is limited to the Wi-Fi First-Person-View (FPV) transmission in the UAV-2-GCS communication channel. In the *identification problem*, given a multi-UAVs scenario, it is likely impossible to identify a foe UAV among legitimate ones. Although Identification Friend or Foe (IFF) methods [182] exist, they fail to distinguish a foe UAV that is nearby to a legitimate one with the same altitude and location (less than 4.9 m [183]). Therefore, the malicious entities leverage the existing scientific gaps to violate individuals' privacy. It should also be noted that the large-scale deployment of UAVs in the civilian airspace raises several challenges at a legislative level. These challenges include the establishment of regulations, procedures, and policies that coexist with the national and international laws, and which guarantee personal data protection.

6.2. Future research directions

In this subsection, we present promising security and privacy research directions of UAVs that could be investigated in future works.

UAV Forensics. When security incidents occur during a flight mission, forensics analysts are required to analyze the compromised UAVs. However, it is likely impossible to gather evidence from the drones that do not implement logging capabilities [18]. More specifically, important data such as flight trajectories and onboard-flight data are stored in the Flight Controller's volatile Random Access Memory (RAM), thus making the recovery process a challenging task. Therefore, building models is highly required to provide deep drone forensic analysis [184]. However, even with strong forensics models, the existing anti-forensics techniques could potentially thwart the digital investigation process [185]. A possible mitigation strategy considers adopting a forensic-by-design approach, which integrates the forensics requirements into the design of the UAV system [186]. Forensic investigation of UAVs is an unexplored topic of research in UAV security. Existing digital forensics models lack proper unification and standardization to enclose a wider window of commercial UAVs. This is a major issue in UAV forensics, where an adversary could potentially compromise specific UAVs whose forensic models have not been covered yet.

UAV Intrusion Detection Systems. Detecting intrusions against UAVs during a flight mission requires real-time network traffic analysis. To that end, implementing an IDS for UAVs enables the detection of different classes of intrusions such as signal modification, malware, routing attacks, and message forgery attacks [155]. In addition, the development of anomaly detection frameworks to monitor malicious behaviors plays an important role in detecting attack patterns [187]. Besides, the adoption of honeypots and honeynets along with the IDS can help to protect the flight mission from malicious entities [188]. In [189], the authors proposed HoneyDrone, a portable honeypot specifically designed to protect UAVs from malicious activities. It is lightweight and can be implemented on low-cost devices such as Raspberry Pi. Furthermore, HoneyDrone can handle real-world attacks such as Telnet attack and MAVLink attacks. Since UAV networks constitute a complex cyber–physical system that incorporates multiple components [10], the intrusion detection approaches should consider different information gathering sources to increase the performance. However, more information sources can also increase the communication cost and result in high computation overhead. Developing such solutions is challenging due to the existing security and performance tradeoffs. Therefore, there is a need to implement lightweight IDSs to monitor UAV communications and detect attacks. In this respect, some solutions utilize the behavioral profiling of the flight to detect abnormal behavior and malicious intrusions [190]. However, such approaches cannot detect cyber attacks that compromise UAVs while ensuring that the flight pattern is consistent.

Secure UAV Communications. The outcomes of our study at the UAV Communication-level demonstrate the need to develop proper UAV communication protocols and thus provide reliable and secure communication between different components of the UAV system. However, securing UAV communication channels while achieving maximum network throughput is still challenging for the research community. Given the lack of standardization for UAV-2-UAV and UAV-2-GCS communication protocols, it is important to consider potential attacks based on reverse engineering since these protocols are developed independently by the manufacturers (e.g., DJI Mavic, Crazyflie). Additionally, authentication of UAVs can secure the communication link and prevent impersonation and replay attacks [191]. Developing access policies for UAVs, such as authorization and authentication schemes, is still a challenging research topic [12]. Indeed, any unauthenticated UAV should not be part of the flight mission or gather exchanged data from other UAVs in the network. On the other hand, in multi-UAV scenarios, the use of specific networking models for UAVs such as FANETs [51] enables multi-UAV operations. However, FANETs are vulnerable to different attacks [26], and establishing secure communication in Multi-UAV networks remains an open research topic. Although several FANETs routing protocols were proposed in the literature [54], they cannot fully meet the security and privacy requirements, and further research in this category is needed [20].

Realistic Implementations. Practical development and deployment of UAVs require an emphasis on the tradeoffs between security and performance. From a security point of view, we have to consider the security and privacy requirements of the UAV system. Moreover, we need to consider the energy, computation costs, and storage overheads from a performance perspective. For example, implementing authentication mechanisms or developing lightweight cryptographic protocols for energy-constrained UAVs incorporates the use of cryptographic primitives. However, such implementations might consume too much energy and increase the computational cost. Therefore, finding a strategic solution and balancing both sides is considered as a major open research topic. Existing security countermeasures operate under specific hardware or software settings. Therefore, when proposing real-world implementations, we must consider the possible deployment challenges among different UAV systems. A possible solution consists of unifying a deployment interface for various types of UAV systems. Also, it should be emphasized that simulating cyber attack scenarios of UAVs in advance could demonstrate the resilience of existing security measures against cyber attacks before their deployments. Besides, existing simulation environments for UAV security analysis are limited [192], and this topic deserves further research efforts.

Privacy Preservation. The integration of UAVs in the national airspace has raised privacy preservation issues. These implications lead to the leakage of sensitive data collected by UAVs. The collected data might be uploaded to third party organizations such as cloud servers for storage or processing purposes. In this context, there is a need to protect the privacy of outsourced data. Different privacy-preserving approaches have been proposed in the literature. Examples of mitigating privacy invasion attacks include using privacy-enhancing technologies to preserve consumers' data and guarantee privacy protection with third party organizations. Namely, the secure computation or differential privacy mechanisms support the privacy of individual users and permit data coordination between UAVs while guaranteeing privacy. Other examples include homomorphic encryption to perform computational operations over encrypted data [193] and the Zero Knowledge Proof (ZPF) to validate data without disclosing it.

Secure Data Aggregation. The extensive use of UAVs in different application domains increased the amount of collected and shared data. The collected data is usually aggregated to use the resources efficiently. However, the data aggregation process needs to be protected against malicious actors. The deployment of aggregation schemes should consider encryption techniques to provide confidentiality, thus enabling a secure transfer of information between the GCS and UAVs. In addition, providing efficient and secure data aggregation approaches for UAVs will reduce energy and communication costs while ensuring confidentiality. However, developing such schemes remains an ongoing challenge.

Emerging Technologies. Recently, there has been an extensive use of emerging technologies to secure UAVs: Artificial Intelligence, blockchain technology, SDN, and fog computing [34,38]. These technologies are applied in various civilian applications. The distributed architecture of blockchain technology adds an extra layer of security at the communication level [194]. Besides, it becomes challenging for the adversary to tamper with UAVs communication that considers cryptographic mechanisms in the blockchain (e.g., smart contracts, cryptographic hash functions to store data as a chain of blocks, the consensus mechanisms). However, the major applications of blockchain for UAV communication security suffer from real-time deployment for highly mobile UAVs [195]. Moreover, the real-world implementation of blockchain technology to secure UAV networks is still an ongoing research topic. The evolution of Artificial Intelligence technology such as ML algorithms has demonstrated tremendous benefits for security-oriented applications, such as protecting UAV networks from attacks and privacy leakage. Different ML-based security frameworks have been proposed in the literature to address various security issues, including malicious drone detection and DoS attacks [196]. Recently, federated learning techniques are reported to show better results compared to traditional ML algorithms. For example, the use of drone authentication models based on drone's Radio Frequency features in IoT networks [197]. Nonetheless, there is a lack of existing UAV datasets to train ML models (e.g., network traffic datasets, malware datasets [198] [199]). Furthermore, some ML models can fail to detect cyber attacks on UAVs [38]. The use of SDN-based UAV networks enables the security of UAV communications. This technology offers dynamic flow control and a programmable network for different security functions. Hence, protecting the UAV network from potential cyber attacks. A major drawback of using such a technology is the high end-to-end delay for non-delay tolerant UAV applications. Moreover, the link between the data plane and the control plane could be subject to attacks. In addition to these, the integration of UAVs in smart cities implies processing and storing a large amount of data. To that end, the use of fog computing technology can help to process and store data. Moreover, fog computing supports secure communication between the UAVs and the fog layer that is scalable and has low latency. However, the current fog architecture is not tailored for the UAV model, and adopting such an architecture might increase the data processing time, especially for multi-UAV networks. The next generations of UAVs will incorporate diverse emerging technologies [200]. Therefore, there is a need from academia and industry for further research regarding the use of emerging technologies to secure UAVs in civilian applications [201].

7. Conclusion

In this paper, we presented an exhaustive survey on security and privacy issues of Unmanned Aerial Vehicles. We thoroughly dissected UAV security issues at four levels: the *Sensor-level*, the *Hardware-level*, the *Software-level*, and the *Communication-level*. Furthermore, we discussed the privacy issues of UAVs, threats, and possible solutions. Next, we presented the lessons learned with the security and privacy aspects of UAVs, and also provided possible future research directions. With the increased number of commercial UAVs in civilian airspace, security and privacy issues have become a highly urgent matter of national security. Therefore, industry, academia, and law enforcement need to collaborate and develop new security frameworks, standards, and regulations. Nowadays, existing drone manufacturers are deploying the next generation of commercial UAVs in the market, and security and privacy considerations are way behind. Our survey provides a valuable reference for the research community to learn more about building and designing secure UAV architectures.

CRediT authorship contribution statement

Yassine Mekdad: Investigation, Writing – original draft. **Ahmet Aris:** Conceptualization, Methodology, Review and editing. **Leonardo Babun:** Conceptualization, Methodology, Review and editing. **Abdeslam El Fergougui:** Supervision, Project administration. **Mauro Conti:** Supervision, Project administration. **Riccardo Lazzeretti:** Supervision, Review and editing. **A. Selcuk Uluagac:** Supervision, Funding acquisition, Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

This work is partially supported by the US National Science Foundation (Awards: NSF-CAREER-CNS-1453647, NSF-1663051, NSF-1718-116), partially supported by La Sapienza University of Rome within the Bando Ricerca 2020, Protocol n. RM120172B4CC529E, and partially supported by the EU - NGEU, Protocol n. PE00000014. The views are those of the authors only. All authors approved the version of the manuscript to be published.

References

[1] S. Hayat, E. Yanmaz, R. Muzaffar, Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint, IEEE Commun. Surv. Tutor. 18 (4) (2016) 2624–2661, http://dx.doi.org/10.1109/COMST.2016.2560343.

[2] L. Gupta, R. Jain, G. Vaszkun, Survey of important issues in UAV communication networks, IEEE Commun. Surv. Tutor. 18 (2) (2016) 1123–1152, http://dx.doi.org/10.1109/COMST.2015.2495297.

[3] N. Hossein Motlagh, T. Taleb, O. Arouk, Low-altitude unmanned aerial vehicles-based Internet of Things services: Comprehensive survey and future perspectives, IEEE Internet Things J. 3 (6) (2016) 899–922, http://dx.doi.org/10.1109/JIOT.2016.2612119.

[4] R. Kellermann, T. Biehle, L. Fischer, Drones for parcel and passenger transportation: A literature review, Transp. Res. Interdiscip. Perspect. 4 (2020) http://dx.doi.org/10.1016/J.TRIP.2019.100088.

[5] Commercial drone market size, 2021, URL https://www.grandviewresearch.com/industry-analysis/global-commercial-drones-market, (Online; Accessed 2 April 2022).

[6] F. Aviation Administration, FAA National Forecast FY 2019–2039 Full Forecast Document and Tables, Tech. Rep., 2019.

[7] Z. Liu, Z. Li, B. Liu, X. Fu, I. Raptis, K. Ren, Rise of mini-drones, in: Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing, 2015, pp. 7–12, http://dx.doi.org/10.1145/2757302.2757303.

[8] Map of world wide drone incidents - Dedrone, 2021, URL https://www.dedrone.com/resources/incidents/all. (Online; Accessed 2 April 2022).

[9] H. Sedjelmaci, S.M. Senouci, M.A. Messous, How to detect cyber-attacks in unmanned aerial vehicles network? in: 2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings, 2016, http://dx.doi.org/10.1109/GLOCOM.2016.7841878.

[10] R. Guo, B. Wang, J. Weng, Vulnerabilities and attacks of UAV cyber physical systems, in: ACM International Conference Proceeding Series, 2020, pp. 8–12, http://dx.doi.org/10.1145/3398329.3398331.

[11] M. Yahuza, M.Y.I. Idris, I.B. Ahmedy, A.W.A. Wahab, T. Nandy, N.M. Noor, A. Bala, Internet of Drones security and privacy issues: Taxonomy and open challenges, IEEE Access 9 (2021) 57243–57270, http://dx.doi.org/10.1109/ACCESS.2021.3072030.

[12] J.-P. Yaacoub, H. Noura, O. Salman, A. Chehab, Security analysis of drones systems: Attacks, limitations, and recommendations, Internet Things 11 (2020) http://dx.doi.org/10.1016/j.iot.2020.100218.

[13] L. Watkins, J. Ramos, G. Snow, J. Vallejo, W.H. Robinson, A.D. Rubin, J. Ciocco, F. Jedrzejewski, J. Liu, C. Li, Exploiting multi-vendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems, in: Proceedings of the 1st ACM MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy, 2018, pp. 1–6.

[14] Z. Li, C. Gao, Q. Yue, X. Fu, Toward drone privacy via regulating altitude and payload, in: 2019 International Conference on Computing, Networking and Communications, IEEE, 2019, pp. 562–566, http://dx.doi.org/10.1109/ICCNC.2019.8685611.

[15] Drones as the new "Flying IoT" | IEEE computer society, 2022, URL https://www.computer.org/publications/tech-news/research/flying-iot-toward-low-power-vision-sky. (Online; Accessed 2 April 2022).

[16] A.I. Newaz, A.K. Sikder, M.A. Rahman, A.S. Uluagac, A survey on security and privacy issues in modern healthcare systems: Attacks and defenses, ACM Trans. Comput. Healthc. 2 (3) (2021) 1–44.

[17] L.P. Rondon, L. Babun, A. Aris, K. Akkaya, A.S. Uluagac, Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective, 2021, URL http://arxiv.org/abs/2102.10695.

[18] R. Altawy, A.M. Youssef, Security, privacy, and safety aspects of civilian drones: A survey, ACM Trans. Cyber-Phys. Syst. 1 (2) (2017) 1–25, http://dx.doi.org/10.1145/3001836.

[19] C.L. Krishna, R.R. Murphy, A review on cybersecurity vulnerabilities for unmanned aerial vehicles, in: 2017 IEEE International Symposium on Safety, Security and Rescue Robotics, SSRR, IEEE, 2017, pp. 194–199.

[20] J.-A. Maxa, M.-S.B. Mahmoud, N. Larrieu, Survey on UAANET routing protocols and network security challenges, Ad Hoc Sensor Wirel. Netw. (2017).

[21] G. Choudhary, V. Sharma, T. Gupta, J. Kim, I. You, Internet of Drones (IoD): Threats, vulnerability, and security perspectives, in: The 3rd International Symposium on Mobile Internet Security, no. 37, 2018, pp. 1–13.

[22] C. Lin, D. He, N. Kumar, K.K.R. Choo, A. Vinel, X. Huang, Security and privacy for the Internet of Drones: Challenges and solutions, IEEE Commun. Mag. 56 (1) (2018) 64–69, http://dx.doi.org/10.1109/MCOM.2017.1700390.

[23] H. Shakhatreh, A.H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N.S. Othman, A. Khreishah, M. Guizani, Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges, IEEE Access 7 (2019) 48572–48634, http://dx.doi.org/10.1109/ACCESS.2019.2909530.

[24] B. Nassi, A. Shabtai, R. Masuoka, Y. Elovici, SoK - Security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps, 2019, pp. 1–17, arXiv, URL http://arxiv.org/abs/1903.05155.

[25] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L.G. Giordano, A. Garcia-Rodriguez, J. Yuan, Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges, IEEE Commun. Surv. Tutor. 21 (4) (2019) 3417–3442.

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

[27] P. Boccadoro, D. Striccoli, L.A. Grieco, An extensive survey on the Internet of Drones, Ad Hoc Netw. 122 (2021).

[28] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, J. Wei, Survey on unmanned aerial vehicle networks: A cyber physical system perspective, IEEE Commun. Surv. Tutor. 22 (2) (2020) 1027–1070, http://dx.doi.org/10.1109/COMST.2019.2962207.

[29] A.I. Hentati, L.C. Fourati, Comprehensive survey of UAVs communication networks, Comput. Stand. Interfaces 72 (2020).

[30] Y. Zhi, Z. Fu, X. Sun, J. Yu, Security and privacy issues of UAV: A survey, Mob. Netw. Appl. 25 (1) (2020) 95–101, http://dx.doi.org/10.1007/s11036-018-1193-x.

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

[32] F. Noor, M.A. Khan, A. Al-Zahrani, I. Ullah, K.A. Al-Dhlan, A review on communications perspective of flying AD-HOC networks: Key enabling wireless technologies, applications, challenges and open research topics, Drones 4 (4) (2020).

[33] D. Mishra, E. Natalizio, A survey on cellular-connected UAVs: Design challenges, enabling 5G/B5G innovations, and experimental advancements, Comput. Netw. 182 (2020).

[34] F. Syed, S.K. Gupta, S. Hamood Alsamhi, M. Rashid, X. Liu, A survey on recent optimal techniques for securing unmanned aerial vehicles applications, Trans. Emerg. Telecommun. Technol. 32 (7) (2021).

[35] M. Yahuza, M.Y.I. Idris, I.B. Ahmedy, A.W.A. Wahab, T. Nandy, N.M. Noor, A. Bala, Internet of Drones security and privacy issues: Taxonomy and open challenges, IEEE Access 9 (2021) 57243–57270, http://dx.doi.org/10.1109/ACCESS.2021.3072030.

[36] B. Nassi, R. Bitton, R. Masuoka, A. Shabtai, Y. Elovici, SoK: Security and privacy in the age of commercial drones, in: 2021 2021 IEEE Symposium on Security and Privacy, no. Section IV, SP, 2021, pp. 73–90.

[37] A. Shafique, A. Mehmood, M. Elhadef, Survey of security protocols and vulnerabilities in unmanned aerial vehicles, IEEE Access 9 (2021) 46927–46948, http://dx.doi.org/10.1109/ACCESS.2021.3066778.

[38] V. Hassija, V. Chamola, A. Agrawal, A. Goyal, N.C. Luong, D. Niyato, F.R. Yu, M. Guizani, Fast, reliable, and secure drone communication: A comprehensive survey, IEEE Commun. Surv. Tutor. (2021).

[39] Teach, learn, and make with raspberry Pi, 2022, URL https://www.raspberrypi.org/. (Online; Accessed 2 April 2022).

[40] BeagleBoard.org - community supported open hardware computers for making, 2022, URL https://beagleboard.org/. (Online; Accessed 2 April 2022).

[41] S. Chen, D. F. Laefer, E. Mangina, State of technology review of civilian UAVs, Recent Pat. Eng. 10 (3) (2016) 160–174.

[42] Copter Home — Copter documentation, 2022, URL https://ardupilot.org/copter/. (Online; Accessed 2 April 2022).

[43] B. Ab, Crazyflie 2.1, 2022, pp. 7–9, URL https://www.seeedstudio.com/crazyflie-V2-1-p-2894.html. (Online; Accessed 2 April 2022).

[44] KKMulticopter Flashtool [lazyzero.de], 2022, URL https://lazyzero.de/en/modellbau/kkmulticopterflashtool/start. (Online; Accessed 2 April 2022).

[45] UAS remote identification overview, 2022, URL https://www.faa.gov/uas/getting_started/remote_id/. (Online; Accessed 2 April 2022).

[46] L. Petricca, P. Ohlckers, C. Grinde, Micro- and nano-air vehicles: State of the art, Int. J. Aerosp. Eng. 2011 (2011) http://dx.doi.org/10.1155/2011/214549.

[47] T. Andre, K.A. Hummel, A.P. Schoellig, E. Yanmaz, M. Asadpour, C. Bettstetter, P. Grippa, H. Hellwagner, S. Sand, S. Zhang, Application-driven design of aerial communication networks, IEEE Commun. Mag. 52 (5) (2014) 129–137.

[48] M. Hooper, Y. Tian, R. Zhou, B. Cao, A.P. Lauf, L. Watkins, W.H. Robinson, W. Alexis, Securing commercial WiFi-based UAVs from common security attacks, in: Proceedings - IEEE Military Communications Conference MILCOM, 2016, pp. 1213–1218, http://dx.doi.org/10.1109/MILCOM.2016.7795496.

[49] K.P. Valavanis, G.J. Vachtsevanos, Handbook of Unmanned Aerial Vehicles, Springer Netherlands, 2015, pp. 1–3022, http://dx.doi.org/10.1007/978-90-481-9707-1.

[50] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, M. Debbah, A tutorial on UAVs for wireless networks: Applications, challenges, and open problems, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2334–2360.

[51] I. Bekmezci, O.K. Sahingoz, Ş. Temel, Flying ad-hoc networks (FANETs): A survey, Ad Hoc Netw. 11 (3) (2013) 1254–1270.

[52] J. Li, Y. Zhou, L. Lamont, Communication architectures and protocols for networking unmanned aerial vehicles, in: 2013 IEEE Globecom Workshops, GC Wkshps, IEEE, 2013, pp. 1415–1420.

[53] A. Chriki, H. Touati, H. Snoussi, F. Kamoun, UAV-GCS centralized data-oriented communication architecture for crowd surveillance applications, in: 2019 15th International Wireless Communications and Mobile Computing Conference, IWCMC 2019, 2019, pp. 2064–2069, http://dx.doi.org/10.1109/IWCMC.2019.8766641.

[54] M.Y. Arafat, S. Moh, Routing protocols for unmanned aerial vehicle networks: A survey, IEEE Access 7 (2019) 99694–99720, http://dx.doi.org/10.1109/ACCESS.2019.2930813.

[55] O.S. Oubbati, M. Atiquzzaman, P. Lorenz, M.H. Tareque, M.S. Hossain, Routing in flying ad hoc networks: Survey, constraints, and future challenge perspectives, IEEE Access 7 (2019) 81057–81105, http://dx.doi.org/10.1109/ACCESS.2019.2923840.

[56] D. Shumeye Lakew, U. Sa'Ad, N.N. Dao, W. Na, S. Cho, Routing in flying ad hoc networks: A comprehensive survey, IEEE Commun. Surv. Tutor. 22 (2) (2020) 1071–1120, http://dx.doi.org/10.1109/COMST.2020.2982452.

[57] M.Y. Arafat, S. Moh, A survey on cluster-based routing protocols for unmanned aerial vehicle networks, IEEE Access 7 (2018) 498–516.

[58] A. Koubaa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, M. Khalgui, Micro air vehicle link (MAVlink) in a nutshell: A survey, IEEE Access 7 (2019) 87658–87680, http://dx.doi.org/10.1109/ACCESS.2019.2924410.

[59] Y.-M. Kwon, J. Yu, B.-M. Cho, Y. Eun, K.-J. Park, Empirical analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles, IEEE Access 6 (2018) 43203–43212.

[60] V. Kriz, P. Gabrlik, UranusLink-communication protocol for UAV with small overhead and encryption ability, IFAC-PapersOnLine 28 (4) (2015) 474–479, http://dx.doi.org/10.1016/j.ifacol.2015.07.080.

[61] N.A. Khan, N.Z. Jhanjhi, S.N. Brohi, A. Nayyar, Emerging use of UAV's: Secure communication protocol issues and challenges, in: Drones in Smart-Cities, Elsevier, 2020.

[62] G. Choudhary, V. Sharma, I. You, K. Yim, I.R. Chen, J.H. Cho, Intrusion detection systems for networked unmanned aerial vehicles: A survey, in: 2018 14th International Wireless Communications and Mobile Computing Conference, IWCMC 2018, IEEE, 2018, pp. 560–565, http://dx.doi.org/10.1109/IWCMC.2018.8450305.

[63] A.S. Uluagac, V. Subramanian, R. Beyah, Sensory channel threats to cyber physical systems: A wake-up call, in: 2014 IEEE Conference on Communications and Network Security, Institute of Electrical and Electronics Engineers Inc., 2014, pp. 301–309, http://dx.doi.org/10.1109/CNS.2014.6997498.

[64] A.K. Sikder, G. Petracca, H. Aksu, T. Jaeger, A.S. Uluagac, A survey on sensor-based threats and attacks to smart devices and applications, IEEE Commun. Surv. Tutor. 23 (2) (2021) 1125–1159, http://dx.doi.org/10.1109/COMST.2021.3064507.

[65] J. Aru Saputro, E. Egistian Hartadi, M. Syahral, Implementation of GPS attacks on DJI phantom 3 standard drone as a security vulnerability test, in: Proceeding - 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering, ICITAMEE 2020, Institute of Electrical and Electronics Engineers Inc., 2020, pp. 95–100, http://dx.doi.org/10.1109/ICITAMEE50454.2020.9398386.

[66] E. Deligne, ARDrone corruption, J. Comput. Virol. 8 (1) (2012) 15–27.

[67] K. Wesson, T. Humphreys, Hacking drones, Sci. Am. 309 (5) (2013) 54–59, http://dx.doi.org/10.1038/scientificamerican1113-54.

[68] A.J. Kerns, D.P. Shepard, J.A. Bhatti, T.E. Humphreys, Unmanned aircraft capture and control via GPS spoofing, J. Field Robotics 31 (4) (2014) 617–636, http://dx.doi.org/10.1002/rob.21513.

[69] S.-H. Seo, B.-H. Lee, S.-H. Im, G.-I. Jee, Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal, J. Position. Navigation Timing 4 (2) (2015) 57–65.

[70] G. Roth, Simulation of the Effects of Acoustic Noise on MEMS Gyroscopes (Thesis), 2009, URL https://etd.auburn.edu//handle/10415/1773.

[71] M.A. Fischler, R.C. Bolles, Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography, Commun. ACM 24 (6) (1981) 381–395, http://dx.doi.org/10.1145/358669.358692.

[72] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, W. Yi, Efficient drone hijacking detection using two-step GA-XGBoost, J. Syst. Archit. 103 (2020).

[73] M. Varshosaz, A. Afary, B. Mojaradi, M. Saadatseresht, E.G. Parmehr, Spoofing detection of civilian UAVs using visual odometry, ISPRS Int. J. Geo-Inf. 9 (1) (2019) http://dx.doi.org/10.3390/ijgi9010006.

[74] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, W. Yi, An efficient UAV hijacking detection method using onboard inertial measurement unit, ACM Trans. Embed. Comput. Syst. (TECS) 17 (6) (2018) 1–19.

[75] T. Abera, R. Bahmani, F. Brasser, A. Ibrahim, A.-R. Sadeghi, M. Schunter, DIAT: Data integrity attestation for resilient collaboration of autonomous systems, in: NDSS, 2019.

[76] A.D. Wu, E.N. Johnson, M. Kaess, F. Dellaert, G. Chowdhary, Autonomous flight in GPS-denied environments using monocular vision and inertial sensors, J. Aerosp. Inf. Syst. 10 (4) (2013) 172–186.

[77] A.D. Wu, E.N. Johnson, M. Kaess, F. Dellaert, G. Chowdhary, Autonomous flight in GPS-denied environments using monocular vision and inertial sensors, J. Aerosp. Inf. Syst. 10 (4) (2013) 172–186, http://dx.doi.org/10.2514/1.I010023.

[78] J. Whelan, T. Sangarapillai, O. Minawi, A. Almehmadi, K. El-Khatib, Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles, in: Q2SWinet 2020 - Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, 2020, pp. 23–28, http://dx.doi.org/10.1145/3416013.3426446.

[79] M.P. Arthur, Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS, in: CITS 2019 - Proceeding of the 2019 International Conference on Computer, Information and Telecommunication Systems, IEEE, 2019, http://dx.doi.org/10.1109/CITS.2019.8862148.

[80] H. Choi, W.-C. Lee, Y. Aafer, F. Fei, Z. Tu, X. Zhang, D. Xu, X. Deng, Detecting attacks against robotic vehicles: A control invariant approach, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 801–816.

[81] R. Quinonez, J. Giraldo, L. Salazar, E. Bauman, A. Cardenas, Z. Lin, SAVIOR: Securing autonomous vehicles with robust physical invariants, in: Proceedings of the 29th USENIX Security Symposium, 2020, pp. 895–912.

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

[83] D. Davidson, H. Wu, R. Jellinek, V. Singh, T. Ristenpart, Controlling UAVs with sensor input spoofing attacks, in: 10th USENIX Workshop on Offensive Technologies, WOOT 16, 2016.

[84] D. He, Y. Qiao, S. Chan, N. Guizani, Flight security and safety of drones in airborne fog computing systems, IEEE Commun. Mag. 56 (5) (2018) 66–71.

[85] J. Vosatka, Introduction to hardware Trojans, in: The Hardware Trojan War: Attacks, Myths, and Defenses, Springer International Publishing, 2017, pp. 15–51, http://dx.doi.org/10.1007/978-3-319-68511-3_2.

[86] M.A. Rahman, M.T. Rahman, M. Kisacikoglu, K. Akkaya, Intrusion detection systems-enabled power electronics for unmanned aerial vehicles, in: 2020 IEEE CyberPELS, 2020, pp. 1–5, http://dx.doi.org/10.1109/CyberPELS49534.2020.9311545.

[87] S. Gil Casals, P. Owezarski, G. Descargues, Generic and autonomous system for airborne networks cyber-threat detection, in: AIAA/IEEE Digital Avionics Systems Conference - Proceedings, 2013, http://dx.doi.org/10.1109/DASC.2013.6712578.

[88] J.N. Yasin, S.A.S. Mohamed, M.H. Haghbayan, J. Heikkonen, H. Tenhunen, J. Plosila, Unmanned aerial vehicles (UAVs): Collision avoidance systems and approaches, IEEE Access 8 (2020) 105139–105155, http://dx.doi.org/10.1109/ACCESS.2020.3000064.

[89] J. Hannah, R. Mills, R. Dill, Traffic collision avoidance system: Threat actor model and attack Taxonomy, in: Proceedings of the 22nd International Conference on New Trends in Civil Aviation 2020, NTCA 2020, IEEE, 2020, pp. 17–26, http://dx.doi.org/10.23919/NTCA50409.2020.9291180.

[90] M. Alwateer, S.W. Loke, A.M. Zuchowicz, Drone services: issues in drones for location-based services from human-drone interaction to information processing, J. Location Based Serv. 13 (2) (2019) 94–127, http://dx.doi.org/10.1080/17489725.2018.1564845.

[91] J. Lee, S. Ryu, H.J. Kim, Stable flight of a flapping-wing micro air vehicle under wind disturbance, IEEE Robot. Autom. Lett. 5 (4) (2020) http://dx.doi.org/10.1109/lra.2020.3009064.

[92] M. Fyrbiak, S. Strauß, C. Kison, S. Wallat, M. Elson, N. Rummel, C. Paar, Hardware reverse engineering: Overview and open challenges, in: 2017 IEEE 2nd International Verification and Security Workshop, IVSW, IEEE, 2017, pp. 88–94.

[93] K. Hodgkins, Anti-drone shoulder rifle lets police take control of UAVs with radio pulses. (2015), 2015, URL https://www.digitaltrends.com/cool-tech/battle-innovations-anti-drone-gun/. (Online; Accessed 2 April 2022).

[94] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, Y. Elovici, dr0wned-cyber-physical attack with additive manufacturing, in: 11th USENIX Workshop on Offensive Technologies, WOOT 17, 2017.

[95] V. Desnitsky, I. Kotenko, Simulation and assessment of battery depletion attacks on unmanned aerial vehicles for crisis management infrastructures, Simul. Model. Pract. Theory 107 (2021) http://dx.doi.org/10.1016/j.simpat.2020.102244.

[96] A.B. Lopez, K. Vatanparvar, A.P. Deb Nath, S. Yang, S. Bhunia, M.A. Al Faruque, A security perspective on battery systems of the Internet of Things, J. Hardw. Syst. Secur. 1 (2) (2017) 188–199.

[97] N. Rodday, Hacking a professional drone, Black Hat Asia (2016) URL https://www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf.

[98] C. Nigh, A. Orailoglu, AdaTrust: Combinational hardware Trojan detection through adaptive test pattern construction, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 29 (3) (2021) 544–557, http://dx.doi.org/10.1109/TVLSI.2021.3053553.

[99] J. McNeely, M. Hatfield, A. Hasan, N. Jahan, Detection of UAV hijacking and malfunctions via variations in flight data statistics, in: Proceedings - International Carnahan Conference on Security Technology, Institute of Electrical and Electronics Engineers Inc., 2016, http://dx.doi.org/10.1109/CCST.2016.7815713.

[100] Z. Williams, J.E. Lueg, S.A. Lemay, Supply chain security: An overview and research agenda, Int. J. Logist. Manag. 19 (2) (2008) 254–281, http://dx.doi.org/10.1108/09574090810895988.

[101] M. Podhradsky, C. Coopmans, N. Hoffer, Improving communication security of open source UAVs: Encrypting radio control link, in: 2017 International Conference on Unmanned Aircraft Systems, ICUAS 2017, Institute of Electrical and Electronics Engineers Inc., 2017, pp. 1153–1159, http://dx.doi.org/10.1109/ICUAS.2017.7991460.

[102] GitHub - GaloisInc/gec: embedded-friendly crypto a la SMACCM, 2022, URL https://github.com/GaloisInc/gec/. (Online; Accessed 2 April 2022).

[103] N. Garg, N. Roy, Enabling self-defense in small drones, in: Proceedings of the 21st International Workshop on Mobile Computing Systems and Applications, 2020, pp. 15–20.

[104] D. He, G. Yang, H. Li, S. Chan, Y. Cheng, N. Guizani, An effective countermeasure against UAV swarm attack, IEEE Netw. 35 (1) (2021) 380–385, http://dx.doi.org/10.1109/MNET.011.2000380.

[105] C. Pu, Y. Li, Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system, in: IEEE Workshop on Local and Metropolitan Area Networks, Vol. 2020-July, 2020, http://dx.doi.org/10.1109/LANMAN49260.2020.9153239.

[106] P. Paul, S. Moore, S. Tam, Tamper protection for security devices, in: Proceedings BLISS 2008 - 2008 ECSIS Symposium on Bio-Inspired, Learning, and Intelligent Systems for Security, 2008, pp. 92–96, http://dx.doi.org/10.1109/BLISS.2008.27.

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

[108] J. Crook, Infamous Hacker Creates Skyjack to Hunt, Hack, and Control Other Drones, Tech. Rep., TechCrunch, 2013.

[109] This drone can steal what's on your phone, 2022, URL https://money.cnn.com/2014/03/20/technology/security/drone-phone/index.html. (Online; Accessed 2 April 2022).

[110] H. Oz, A. Aris, A. Levi, A.S. Uluagac, A survey on ransomware: Evolution, taxonomy, and defense solutions, ACM Comput. Surv. (2022) http://dx.doi.org/10.1145/3514229.

[111] G. Canfora, M. Di Penta, L. Cerulo, Achievements and challenges in software reverse engineering, Commun. ACM 54 (4) (2011) 142–151.

[112] Amazon.com Inc., Revising the airspace model for the safe integration of small unmanned aircraft systems, 2015, pp. 2–5, NASA UTM 2015: The Next Era of Aviation, 1.

[113] A. Seshadri, A. Perrig, L. Van Doom, P. Khosla, SWATT: SoftWare-based attestation for embedded devices, in: Proceedings - IEEE Symposium on Security and Privacy, Vol. 2004, 2004, pp. 272–282, http://dx.doi.org/10.1109/SECPRI.2004.1301329.

[114] E. Dushku, M.M. Rabbani, M. Conti, L.V. Mancini, S. Ranise, SARA: Secure asynchronous remote attestation for IoT systems, IEEE Trans. Inf. Forensics Secur. 15 (2020) 3123–3136, http://dx.doi.org/10.1109/TIFS.2020.2983282.

[115] S. Gallagher, Parrot UAVs easily taken down or hijacked, researchers demonstrate, Ars Technica (2015).

[116] D. He, S. Chan, M. Guizani, Drone-assisted public safety networks: The security aspect, IEEE Commun. Mag. 55 (8) (2017) 218–223.

[117] B. Wu, J. Chen, J. Wu, M. Cardei, A survey of attacks and countermeasures in mobile ad hoc networks, Wirel. Netw. Secur. (2007) 103–135, http://dx.doi.org/10.1007/978-0-387-33112-6{_}5.

[118] J.-S. Pleban, R. Band, R. Creutzburg, Hacking and securing the AR.Drone 2.0 quadcopter: Investigations for improving the security of a toy, SPIE 9030 (2014) http://dx.doi.org/10.1117/12.2044868, URL https://ui.adsabs.harvard.edu/abs/2014SPIE.9030E..0LP/abstract.

[119] C. Kolias, G. Kambourakis, A. Stavrou, S. Gritzalis, Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset, IEEE Commun. Surv. Tutor. 18 (1) (2016) 184–208, http://dx.doi.org/10.1109/COMST.2015.2402161.

[120] H. Shin, K. Choi, Y. Park, J. Choi, Y. Kim, Security analysis of FHSS-type drone controller, in: International Workshop on Information Security Applications, Vol. 9503, Springer Verlag, 2015, pp. 240–253, http://dx.doi.org/10.1007/978-3-319-31875-2{_}20.

[121] M.E. Garbelini, S. Chattopadhyay, V. Bedi, S. Sun, E. Kurniawan, BRAKTOOTH: Causing havoc on bluetooth link manager, 2021.

[122] O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, P. Toivanen, Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned, in: 2014 14th International Conference on Hybrid Intelligent Systems, HIS 2014, 2003, pp. 199–206, http://dx.doi.org/10.1109/HIS.2014.7086198.

[123] J. Wright, KillerBee: Practical ZigBee exploitation framework or "wireless hacking and the kinetic world", in: 11th ToorCon Conference, San Diego, 2009.

[124] A. Gemalto, S. And, LoRaWAN ™ Security a White Paper Prepared for the LoRa ALLIANCE™ Full End-To-End encryption for IoT Application Providers, Tech. Rep., 2017.

[125] I. You, S. Kwon, G. Choudhary, V. Sharma, J.T. Seo, An enhanced LoRaWAN security protocol for privacy preservation in IoT with a case study on a smart factory-enabled parking system, Sensors 18 (6) (2018).

[126] S. Chacko, M.D. Job, Security mechanisms and vulnerabilities in LPWAN, IOP Conf. Ser.: Mater. Sci. Eng. 396 (1) (2018) http://dx.doi.org/10.1088/1757-899X/396/1/012027.

[127] N. Neji, T. Mostfa, Communication technology for unmanned aerial vehicles: A qualitative assessment and application to precision agriculture, in: 2019 International Conference on Unmanned Aircraft Systems, ICUAS, IEEE, 2019, pp. 848–855.

[128] V. Kumar, R.K. Jha, S. Jain, NB-IoT security: A survey, Wirel. Pers. Commun. 113 (4) (2020) 2661–2708, http://dx.doi.org/10.1007/s11277-020-07346-7.

[129] K. Saranya, M. Dorairangaswamy, A study on evaluation of DoS attacks in WiMAX networks, Int. Res. J. Eng. Technol. (2017).

[130] J.H.K. Han, M.Y. Alias, G.B. Min, Potential denial of service attacks in IEEE802.16e-2005 networks, in: 2009 9th International Symposium on Communications and Information Technology, ISCIT 2009, 2009, pp. 1207–1212, http://dx.doi.org/10.1109/ISCIT.2009.5341115.

[131] G. Vasconcelos, G. Carrijo, R. Miani, J. Souza, V. Guizilini, The impact of DoS attacks on the AR.Drone 2.0, in: Proceedings - 13th Latin American Robotics Symposium and 4th Brazilian Symposium on Robotics, LARS/SBR 2016, 2016, pp. 127–132, http://dx.doi.org/10.1109/LARS-SBR.2016.28.

[132] F.A.G. Muzzi, P.R.d.M. Cardoso, D.F. Pigatto, K.R.L.J.C. Branco, Using botnets to provide security for safety critical embedded systems - A case study focused on UAVs, J. Phys.: Conf. Ser. 633 (1) (2015) http://dx.doi.org/10.1088/1742-6596/633/1/012053.

[133] M. Conti, N. Dragoni, V. Lesyk, A survey of man in the middle attacks, IEEE Commun. Surv. Tutor. 18 (3) (2016) 2027–2051, http://dx.doi.org/10.1109/COMST.2016.2548426.

[134] N.M. Rodday, R.O. De Schmidt, A. Pras, Exploring security vulnerabilities of unmanned aerial vehicles, in: Proceedings of the NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, 2016, pp. 993–994, http://dx.doi.org/10.1109/NOMS.2016.7502939.

[135] VideoJak: hijacking IP video calls, 2011, URL http://videojak.sourceforge.net/. (Online; Accessed 2 April 2022).

[136] J.-a. Maxa, M.-s.B. Mahmoud, N. Larrieu, J.-a. Maxa, M.-s.B. Mahmoud, N. Larrieu, S. Routing, P. Design, Secure routing protocol design for UAV ad hoc networks, in: 2015 IEEE/AIAA 34th Digital Avionics Systems Conference, DASC, 2015, pp. 4A5–1.

[137] F.H. Tseng, L.D. Chou, H.C. Chao, A survey of black hole attacks in wireless mobile ad hoc networks, Human-Cent. Comput. Inf. Sci. 1 (1) (2011) 1–16, http://dx.doi.org/10.1186/2192-1962-1-4.

[138] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, R. Brooks, The sleep deprivation attack in sensor networks: Analysis and methods of defense, Int. J. Distrib. Sens. Netw. 2 (03) (2006) http://dx.doi.org/10.1080/15501320600642718.

[139] J.R. Douceur, The sybil attack, in: International Workshop on Peer-To-Peer Systems, Vol. 2429, Springer Verlag, 2002, pp. 251–260, http://dx.doi.org/10.1007/3-540-45748-8{_}24.

[140] Y.C. Hu, A. Perrig, Wormhole attacks in wireless networks, IEEE J. Sel. Areas Commun. 24 (2) (2006) 370–379, http://dx.doi.org/10.1109/JSAC.2005.861394.

[141] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, A survey of routing attacks in mobile ad hoc networks, IEEE Wirel. Commun. 14 (5) (2007) 85–91.

[142] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, H. Rubens, Mitigating Byzantine Attacks in Ad Hoc Wireless Networks, Tech. Rep. Version 1 March, 2004.

[143] Y.-C. Hu, A. Perrig, D.B. Johnson, Rushing attacks and defense in wireless ad hoc network routing protocols, in: Proceedings of the 2nd ACM Workshop on Wireless Security, 2003, pp. 30–40, http://dx.doi.org/10.1145/941311.941317.

[144] K. Highnam, K. Angstadt, K. Leach, W. Weimer, A. Paulos, P. Hurley, An uncrewed aerial vehicle attack scenario and trustworthy repair architecture, in: 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop, DSN-W, IEEE, 2016, pp. 222–225.

[145] J. Zhang, T.Q. Duong, R. Woods, A. Marshall, Securing wireless communications of the Internet of Things from the physical layer, an overview, Entropy 2017, Vol. 19 19 (8) (2017) 420, http://dx.doi.org/10.3390/E19080420.

[146] M. Bellare, C. Namprempre, Authenticated encryption: Relations among notions and analysis of the generic composition paradigm, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2000, pp. 531–545.

[147] G. Zhang, Q. Wu, M. Cui, R. Zhang, Securing UAV communications via trajectory optimization, in: GLOBECOM 2017-2017 IEEE Global Communications Conference, Vol. 2018-Janua, 2017, pp. 1–6, http://dx.doi.org/10.1109/GLOCOM.2017.8254971.

[148] J. Barros, M.R. Rodrigues, Secrecy capacity of wireless channels, in: IEEE International Symposium on Information Theory - Proceedings, 2006, pp. 356–360, http://dx.doi.org/10.1109/ISIT.2006.261613.

[149] T. Alladi, Naren, G. Bansal, V. Chamola, M. Guizani, SecAuthUAV: A novel authentication scheme for UAV-Ground station and UAV-UAV communication, IEEE Trans. Veh. Technol. 69 (12) (2020) 15068–15077, http://dx.doi.org/10.1109/TVT.2020.3033060.

[150] M. Karimibiuki, M. Aibin, Y. Lai, R. Khan, R. Norfield, A. Hunter, Drones' face off: Authentication by machine learning in autonomous IoT systems, in: 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, UEMCON, IEEE, 2019, pp. 0329–0333.

[151] S. He, Q. Wu, J. Liu, W. Hu, B. Qin, Y.N. Li, Secure communications in unmanned aerial vehicle network, in: International Conference on Information Security Practice and Experience, Vol. 10701 LNCS, Springer Verlag, 2017, pp. 601–620.

[152] J. Won, S.-H. Seo, E. Bertino, A secure communication protocol for drones and smart objects, in: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, 2015, pp. 249–260.

[153] J. Srinivas, A.K. Das, N. Kumar, J.J. Rodrigues, TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of Drones environment, IEEE Trans. Veh. Technol. 68 (7) (2019) 6903–6916.

[154] A. Shoufan, H. Alnoon, J. Baek, Secure communication in civil drones, Commun. Comput. Inf. Sci. 576 (2015) 177–195.

[155] G. Choudhary, V. Sharma, I. You, K. Yim, I.R. Chen, J.H. Cho, Intrusion detection systems for networked unmanned aerial vehicles: A survey, in: 2018 14th International Wireless Communications and Mobile Computing Conference, IWCMC 2018, 2018, pp. 560–565, http://dx.doi.org/10.1109/IWCMC.2018.8450305.

[156] T. Kacem, D. Wijesekera, P. Costa, A. Barreto, An ADS-B intrusion detection system, in: 2016 IEEE Trustcom/BigDataSE/ISPA, IEEE, 2016, pp. 544–551.

[157] J.P. Condomines, R. Zhang, N. Larrieu, Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation, Ad Hoc Netw. 90 (2019) http://dx.doi.org/10.1016/j.adhoc.2018.09.004.

[158] J.A. Maxa, M.S. Ben Mahmoud, N. Larrieu, Secure routing protocol design for UAV ad hoc networks, in: AIAA/IEEE Digital Avionics Systems Conference - Proceedings, 2015, http://dx.doi.org/10.1109/DASC.2015.7311581.

[159] M. Sbeiti, N. Goddemeier, D. Behnke, C. Wietfeld, PASER: Secure and efficient routing approach for airborne mesh networks, IEEE Trans. Wireless Commun. 15 (3) (2016) 1950–1964, http://dx.doi.org/10.1109/TWC.2015.2497257.

[160] A. Aggarwal, S. Gandhi, N. Chaubey, P. Shah, M. Sadhwani, AODVSEC: A novel approach to secure ad hoc on-demand distance vector (AODV) routing protocol from insider attacks in MANETs, 2012, arXiv preprint arXiv:1208.1959.

[161] J.A. Maxa, M.S. Ben Mahmoud, N. Larrieu, Joint model-driven design and real experiment-based validation for a secure UAV ad hoc network routing protocol, in: ICNS 2016: Securing an Integrated CNS System to Meet Future Challenges, AIAA/IEEE, 2016, pp. 1–2, http://dx.doi.org/10.1109/ICNSURV.2016.7486324.

[162] I. García-Magariño, R. Lacuesta, M. Rajarajan, J. Lloret, Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain, Ad Hoc Netw. 86 (2019) 72–82, http://dx.doi.org/10.1016/j.adhoc.2018.11.010.

[163] M. Singh, G.S. Aujla, R.S. Bali, A deep learning-based blockchain mechanism for secure internet of drones environment, IEEE Trans. Intell. Transp. Syst. 22 (7) (2020) 4404–4413.

[164] B. Jiang, J. Yang, H. Song, Protecting privacy from aerial photography: State of the art, opportunities, and challenges, in: IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2020, 2020, pp. 799–804, http://dx.doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162649.

[165] A.H. Michel, D. Gettinger, Drone Incidents: A Survey of Legal Cases, Bard College Center for Study of the Drone: Annandale-on-the-Hudson, NY, USA, 2017.

[166] R.L. Finn, D. Wright, M. Friedewald, Seven types of privacy, in: European Data Protection: Coming of Age, Springer Netherlands, 2013, pp. 3–32.

[167] G.S. McNeal, Drones and aerial surveillance: Considerations for legislators, in: The Robots are Coming: The Project on Civilian Robotics, Brookings Institution, 2014.

[168] R. Clarke, The regulation of civilian drones' impacts on behavioural privacy, Comput. Law Secur. Rev. 30 (3) (2014) 286–305, http://dx.doi.org/10.1016/j.clsr.2014.03.005.

[169] Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues Relating to the Utilisation of Drones, Working Paper June, 2015, URL https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf. (Online; Accessed 2 April 2022).

[170] G. Buttarelli, European data sup.: Opinion on drones, 2014, URL https://edps.europa.eu/sites/default/files/publication/14-11-26_opinion_rpas_en.pdf. (Online; Accessed 2 April 2022).

[171] S.M. Lui, L. Qiu, Individual privacy and organizational privacy in business analytics, in: Proceedings of the Annual Hawaii International Conference on System Sciences, 2007, http://dx.doi.org/10.1109/HICSS.2007.268.

[172] F.E. Salamh, U. Karabiyik, M.K. Rogers, E.T. Matson, A comparative UAV forensic analysis: Static and live digital evidence traceability challenges, Drones 5 (2) (2021) http://dx.doi.org/10.3390/DRONES5020042.

[173] S. Birnbach, R. Baker, I. Martinovic, Wi-Fly?: Detecting privacy invasion attacks by consumer drones, NDSS (2017) http://dx.doi.org/10.14722/ndss.2017.23335.

[174] C.-L. Chen, Y.-Y. Deng, W. Weng, C.-H. Chen, Y.-J. Chiu, C.-M. Wu, A traceable and privacy-preserving authentication for UAV communication control system, Electronics 9 (1) (2020).

[175] Y. Tian, J. Yuan, H. Song, Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones, J. Inf. Secur. Appl. 48 (2019).

[176] M.O. Ozmen, R. Behnia, A.A. Yavuz, IoD-crypt: A lightweight cryptographic framework for Internet of Drones, 2019, arXiv preprint arXiv:1904.06829.

[177] P. Singh, K. Deshpande, Performance evaluation of cryptographic ciphers on IoT devices, 2018, arXiv preprint arXiv:1812.02220.

[178] M.O. Ozmen, A.A. Yavuz, Dronecrypt-an efficient cryptographic framework for small aerial drones, in: MILCOM 2018-2018 IEEE Military Communications Conference, MILCOM, IEEE, 2018, pp. 1–6.

[179] A. Rozantsev, V. Lepetit, P. Fua, Flying objects detection from a single moving camera, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2015, pp. 4128–4136.

[180] E.E. Case, A.M. Zelnio, B.D. Rigling, Low-cost acoustic array for small UAV detection and tracking, in: IEEE National Aerospace and Electronics Conference, 2008, pp. 110–113.

[181] B. Nassi, R. Ben-Netanel, A. Shamir, Y. Elovici, Drones' cryptanalysis-smashing cryptography with a flicker, in: 2019 IEEE Symposium on Security and Privacy, SP, IEEE, 2019, pp. 1397–1414.

[182] Identification friend or foe - Wikipedia, 2022, URL https://en.wikipedia.org/wiki/Identification_friend_or_foe. (Online; Accessed 2 April 2022).

[183] GPS.gov: GPS accuracy, 2022, URL https://www.gps.gov/systems/gps/performance/accuracy/. (Online; Accessed 2 April 2022).

[184] A. Al-Dhaqm, R.A. Ikuesan, V.R. Kebande, S. Razak, F.M. Ghabban, Research challenges and opportunities in drone forensics models, Electronics (Switzerland) 10 (13) (2021) http://dx.doi.org/10.3390/electronics10131519.

[185] S. Atkinson, G. Carr, C. Shaw, S. Zargari, Drone forensics: The impact and challenges, in: Advanced Sciences and Technologies for Security Applications, Springer, 2021, pp. 65–124, http://dx.doi.org/10.1007/978-3-030-60425-7_4.

[186] N.H. Ab Rahman, W.B. Glisson, Y. Yang, K.K.R. Choo, Forensic-by-design framework for cyber-physical cloud systems, IEEE Cloud Comput. 3 (1) (2016) 50–59, http://dx.doi.org/10.1109/MCC.2016.5.

[187] J. Schumann, P. Moosbrugger, K.Y. Rozier, R2U2: Monitoring and diagnosis of security threats for unmanned aerial systems, in: Runtime Verification, Vol. 9333, Springer, Cham, 2015, pp. 233–249, http://dx.doi.org/10.1007/978-3-319-23820-3_15.

[188] J. Franco, A. Aris, B. Canberk, A.S. Uluagac, A survey of honeypots and honeynets for Internet of Things, industrial Internet of Things, and cyber-physical systems, IEEE Commun. Surv. Tutorials (2021) 1, http://dx.doi.org/10.1109/COMST.2021.3106669.

[189] J. Daubert, D. Boopalan, M. Mühlhäuser, E. Vasilomanolakis, Honeydrone: A medium-interaction unmanned aerial vehicle honeypot, in: NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2018, pp. 1–6.

[190] Z. Birnbaum, A. Dolgikh, V. Skormin, E. O'Brien, D. Muller, C. Stracquodaine, Unmanned aerial vehicle security using behavioral profiling, in: 2015 International Conference on Unmanned Aircraft Systems, ICUAS 2015, Institute of Electrical and Electronics Engineers Inc., 2015, pp. 1310–1319, http://dx.doi.org/10.1109/ICUAS.2015.7152425.

[191] M. Rodrigues, J. Amaro, F.S. Osório, B.K. RLJC, Authentication methods for UAV communication, in: 2019 IEEE Symposium on Computers and Communications, ISCC, IEEE, 2019, pp. 1210–1215.

[192] A.Y. Javaid, W. Sun, M. Alam, UAVSim: A simulation testbed for unmanned aerial vehicle network cyber security analysis, in: 2013 IEEE Globecom Workshops, GC Wkshps 2013, IEEE Computer Society, 2013, pp. 1432–1436, http://dx.doi.org/10.1109/GLOCOMW.2013.6825196.

[193] A. Acar, H. Aksu, A.S. Uluagac, M. Conti, A survey on homomorphic encryption schemes: Theory and implementation, ACM Comput. Surv. 51 (4) (2018) http://dx.doi.org/10.1145/3214303.

[194] E. Ghribi, T.T. Khoei, H.T. Gorji, P. Ranganathan, N. Kaabouch, A secure blockchain-based communication approach for UAV networks, in: IEEE International Conference on Electro Information Technology, Vol. 2020-July, IEEE Computer Society, 2020, pp. 411–415, http://dx.doi.org/10.1109/EIT48999.2020.9208314.

[195] A. Kumari, R. Gupta, S. Tanwar, N. Kumar, A taxonomy of blockchain-enabled softwarization for secure UAV network, Comput. Commun. 161 (2020) 304–323.

[196] E. Matson, B. Yang, A. Smith, E. Dietz, J. Gallagher, UAV detection system with multiple acoustic nodes using machine learning models, in: Proceedings - 3rd IEEE International Conference on Robotic Computing, IRC 2019, Institute of Electrical and Electronics Engineers Inc., 2019, pp. 493–498, http://dx.doi.org/10.1109/IRC.2019.00103.

[197] A. Yazdinejad, R.M. Parizi, A. Dehghantanha, H. Karimipour, Federated learning for drone authentication, Ad Hoc Netw. 120 (2021) http://dx.doi.org/10.1016/J.ADHOC.2021.102574.

[198] Y. Mekdad, G. Bernieri, M. Conti, A. El Fergougui, The rise of ICS malware: A comparative analysis, in: European Symposium on Research in Computer Security, Springer, 2021, pp. 496–511.

[199] Y. Mekdad, G. Bernieri, M. Conti, A.E. Fergougui, A threat model method for ics malware: the trisis case, in: Proceedings of the 18th ACM International Conference on Computing Frontiers, 2021, pp. 221–228.

[200] A. Nayyar, B.-L. Nguyen, N.G. Nguyen, The internet of drone things (IoDT): Future envision of smart drones, in: First International Conference on Sustainable Technologies for Computational Intelligence, Springer, 2020, pp. 563–580.

[201] E. Nowroozi, Y. Mekdad, M.H. Berenjestanaki, M. Conti, A.E. Fergougui, Demystifying the transferability of adversarial attacks in computer networks, IEEE Trans. Netw. Serv. Manag. (2022).

Yassine Mekdad received the Master's Degree in Cryptography and Information Security from Mohammed V University of Rabat, Morocco, in 2016. He has been awarded with a fellowship by Fondazione Ing. Aldo Gini and holds a guest researcher position with the SPRITZ research group at the University of Padua, Italy. He has also been awarded with a Fulbright fellowship. Currently, he works as a Research Scholar at the Cyber-Physical Systems Security Lab (CSL) at Florida International University, Miami, FL, USA. His research interest principally covers security problems in Cyber-physical systems (CPS). In particular, the security and privacy topics in the Internet of Things (IoT), Industrial Internet-of-Things (IIoT), and Cyber-physical systems (CPS). Furthermore, he works on the security of critical infrastructure networks (e.g., SCADA systems, smart-grid). He is also working on research problems at the intersection of the cybersecurity and networking fields with an emphasis on their practical and applied aspects. He is a member of the IEEE Cybersecurity Community and IEEE Young Professionals.

Ahmet Aris Visiting Research Assistant Professor in the Department of Electrical and Computer Engineering at Florida International University. He is conducting research in Cyber-Physical Systems Security Lab (CSL) at Florida International University under the supervision of Dr. A. Selcuk Uluagac. He earned both Ph.D. and MSc. in Computer Engineering from the Graduate School of Science, Engineering and Technology at Istanbul Technical University, Turkey. He also worked as a Research and Teaching Assistant at the Faculty of Computer and Informatics Engineering for 3.5 years and worked at Medianova CDN R&D Center for one year (August 2018 September 2019) as an R&D Analyst. In addition, he conducted research in the Networked Embedded Systems (NES) Group at Computer Systems Lab at the Swedish Institute of Computer Science (SICS) for three months as a visiting researcher in 2017. His research interests include but are not limited to IoT Security, Network Security, Web Security, Adversarial Machine Learning, and Malware.

Leonardo Babun CyberCorps Scholarship for Service Alumnus. He is also a member of the Cyber-Physical Systems Security Lab (CSL) in the Department of Electrical and Computer Engineering at Florida International University. He completed his Doctoral degree in Electrical and Computer Engineering in 2020, and a Master's degree in Computer Engineering in 2019, both from the Department of Electrical and Computer Engineering at Florida International University. He also completed a Master's degree in Electrical Engineering at Florida International University in 2015. His research interests are focused on Cyber-Physical Systems (CPS) and the Internet of Things (IoT) security and privacy.

Abdeslam El Fergougui received the Ph.D. degree in Computer Science from Mohammed V University in Rabat Morocco. He is currently a professor in the department of Computer science, Faculty of sciences Meknes, Moulay Ismail University. His current research interests include Network, Sensor Network, cryptography, security. Furthermore, he assured several advanced training workshops in its field of action. He also assured several training courses in several Moroccan and international universities. He has managed several national and international projects. He is an active member of AUF (University Agency of Francophonie) where he provides training at the international level. As a researcher, he is a member of the reading committee of several journals and conferences in his field.

Mauro Conti Full Professor at the University of Padua, Italy. He is also affiliated with TU Delft and University of Washington, Seattle. He obtained his Ph.D. from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a Post-Doc Researcher at Vrije Universiteit Amsterdam, The Netherlands In 2011 he joined as Assistant Professor at the University of Padua, where he became Associate Professor in 2015 and Full Professor in 2018. He has been Visiting Researcher at GMU, UCLA, UCI, TU Darmstadt, UF, and FIU. He has been awarded with a Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013). His research is also funded by companies, including Cisco, Intel, and Huawei. His main research interest is in the area of Security and Privacy. In this area, he published more than 350 papers in the topmost international peer-reviewed journals and conferences. He is Area Editor-in-Chief for IEEE Communications Surveys & Tutorials, and Associate Editor for several journals, including IEEE Communications Surveys & Tutorials, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, and IEEE Transactions on Network and Service Management. He was Program Chair for TRUST 2015, ICISS 2016, WiSec 2017, ACNS 2020, and General Chair for SecureComm 2012, SACMAT 2013, CANS 2021, and ACNS 2022. He is a Senior Member of the IEEE and ACM. He is a member of the Blockchain Expert Panel of the Italian Government. He is a Fellow of the Young Academy of Europe.

Riccardo Lazzeretti received the Computer Science Engineering degree (cum laude) and the Ph.D. degree from the University of Siena, Italy, in 2007 and 2012, respectively. From November 2009 to May 2010, he was with Philips Lab, Eindhoven, The Netherlands From 2012 to 2015, he continued his research with the University of Siena, and from 2016 to March 2017 with the University of Padua, Italy. Since 2017, he has been an Assistant Professor with the Department of Computer, Control, and Management Engineering, Sapienza University of Rome, Italy. His research activity mainly focuses on security and privacy. He is an elected member of IEEE Information Forensics and Security Technical Committee, and an Associate Editor of the Journal of Information Security and Applications (Elsevier).

A. Selcuk Uluagac leads the Cyber-Physical Systems Security Lab at Florida International University, focusing on security and privacy of Internet of Things and Cyber-Physical Systems. He has a Ph.D. and M.S. from Georgia Institute of Technology, and M.S. from Carnegie Mellon University. In 2015, he received the US National Science Foundation CAREER award and US Air Force Office of Sponsored Research's Summer Faculty Fellowship, and in 2016, Summer Faculty Fellowship from the University of Padova, Italy. Currently, He serves on the editorial boards of the IEEE Transactions on Mobile Computing, Elsevier Computer Networks, and the IEEE Communications and Surveys and Tutorials.