Internet of Drones Security: Taxonomies, Open Issues, and Future Directions

Abdelouahid Derhab[a,*], Omar Cheikhrouhou[b], Azza Allouch[c], Anis Koubaa[d,e], Basit Qureshi[d,e], Mohamed Amine Ferrag[f], Leandros Maglaras[g,h] and Farrukh Aslam Khan[a]

[a] *Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia*
[b] *Higher Institute of Computer Science of Mahdia, University of Monastir, Tunisia*
[c] *Faculty of Mathematical, Physical and Natural Sciences of Tunis, University of El Manar, Tunisia*
[d] *Robotics and Internet of Things Lab, Prince Sultan University, Saudi Arabia*
[e] *College of Computer Information Science, Prince Sultan University, Saudi Arabia*
[f] *Artificial Intelligence & Digital Science Research Center, Technology Innovation Institute, United Arab Emirates*
[g] *School of Computing at Edinburgh Napier University, UK*
[h] *Security Engineering Lab, Computer Science Department, Prince Sultan University, Saudi Arabia*

ARTICLE INFO

Keywords:
Internet of drones
UAV
Security
Taxonomy
Risk assessment
Countermeasure

ABSTRACT

Unmanned Aerial Vehicles (UAVs), also known as drones, have recently become one of the most important technological breakthroughs. They have opened the horizon for a vast array of applications and paved the way for a diversity of innovative solutions. Integrating drones with the Internet has led to the emergence of a new paradigm named the Internet of Drones (IoD). Several works dealt with the security of the IoD, and various surveys have been published on this topic over the past few years. The existing surveys either have limited scope or offer partial coverage of cybersecurity countermeasures. To address these gaps, in this paper, we provide a comprehensive survey related to the cyber and physical security of IoD. Differently from many surveys that only provide a classification of attacks/threats, we also propose three taxonomies that are related to (1) the assets of drones, (2) attacks, and (3) countermeasures. The first taxonomy is a two-level classification of the assets in the IoD. The first level considers the coarse-grained assets, which refer to the IoD's tangible elements, and the second level considers the fine-grained assets, which refer to the elements composing the coarse-grained assets. Based on the asset classification, we propose a taxonomy of attacks targeting the coarse and fine-grained assets, which allows a finer level of granularity to identify threats, and thus ensure better security. Also, we evaluate the risk of cyber and physical attacks by introducing a novel concept, named *Chain of Impact*, which connects four types of impacts, namely, *Direct*, *Mission*, *Drone*, and *Environment*. We propose a taxonomy of technical and non-technical countermeasures according to two implementation phases: *Pre-incident*, and *Post-incident (or recovery)*. The pre-incident countermeasures are further classified as: preventive and detective. In addition, we present the countermeasures along with their performance and limitations. Finally, open research challenges are identified and ranked according to the level of attention they should receive from the research community. Also, future research directions and suggestions are presented for the security of the IoD.

1. Introduction

The Internet of Drones (IoD) has recently emerged as a new paradigm where a set of flying vehicles/devices communicate among themselves with a Ground Control Station (GCS) using the Internet to perform a variety of tasks in different domains, such as disaster management, smart agriculture, environmental monitoring, surveillance, military, smart city management, healthcare, and more recently controlling the COVID-19 pandemic [28, 161]. For instance, some companies like Amazon adopted drones in their delivery systems, which helps them in ensuring fast delivery of parcels and lightweight freights and increasing the delivery rates. The IoD can also be used in rescue operations by delivering medical supplies and goods to people in remote and isolated areas. In precision agriculture, farmers can make real-time decisions based on data collected from drones. IoD has helped decrease the spread of COVID-19 infection by quickly delivering protective equipment and transporting the blood tests to laboratories. In general, the IoD offers reduced costs, time-efficiency, and high coverage surveillance and monitoring operations. Figure 1 presents different application domains of IoD.

According to the Federal Aviation Administration (FAA), [261], more than 900,000 drones were registered in the USA in August 2021. This number is continuously increasing due to the variety of benefits the IoD brings. As the IoD is utilized in different application domains, it has been targeted by attackers to cause harm to cyberspace, drones, people, and properties. The drones could be the target of an attack, or a means to perpetrate attacks and crimes. Therefore, the research community has paid increasing attention to IoD security, how to manage it securely, and address the cyber and physical attacks targeting them.

The deployment of IoD encompasses several challenges, particularly concerning the safety of operations. Several issues must be considered when deploying networked drones over the Internet. For example, a loss of connectivity may

*Corresponding author
abderhab@ksu.edu.sa (A. Derhab)
ORCID(s): 0000-0002-6498-1528 (A. Derhab)

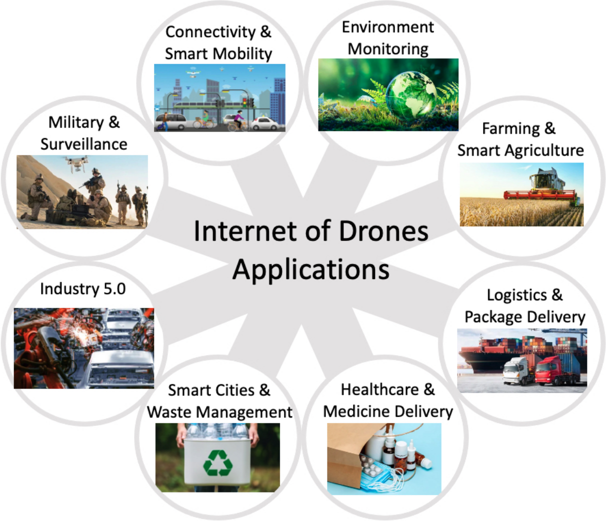
Internet of Drones Applications
Connectivity & Smart Mobility
Environment Monitoring
Farming & Smart Agriculture
Logistics & Package Delivery
Healthcare & Medicine Delivery
Smart Cities & Waste Management
Industry 5.0
Military & Surveillance

Figure 1: Application domains of IoD

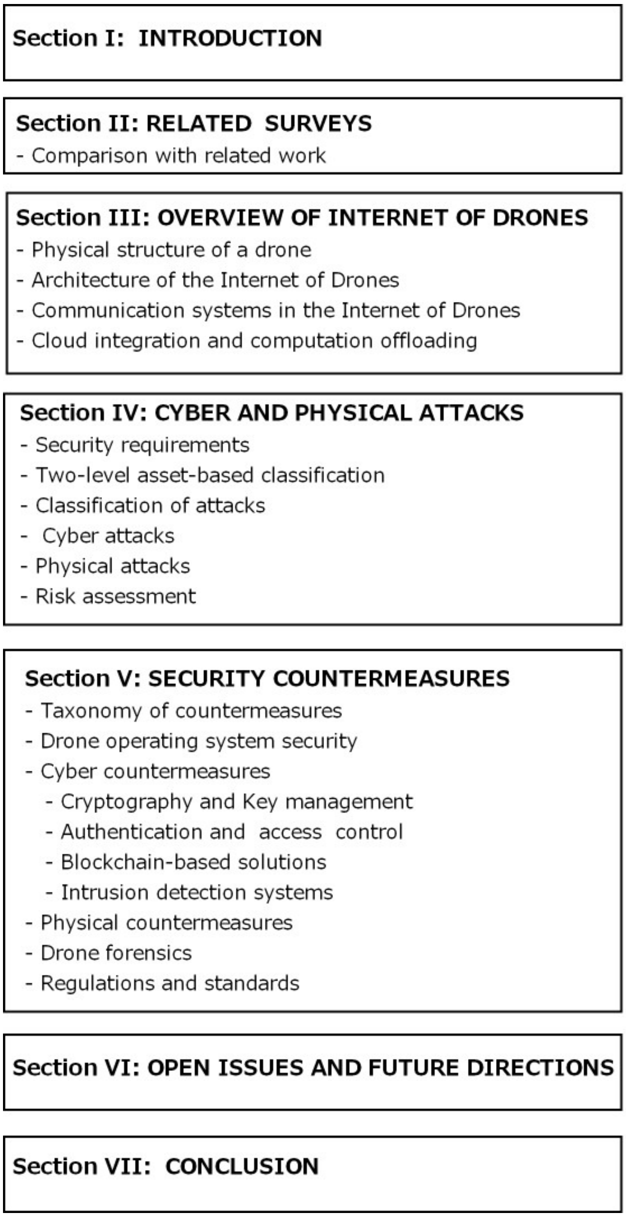
Section I: INTRODUCTION
Section II: RELATED SURVEYS
- Comparison with related work
Section III: OVERVIEW OF INTERNET OF DRONES
- Physical structure of a drone
- Architecture of the Internet of Drones
- Communication systems in the Internet of Drones
- Cloud integration and computation offloading
Section IV: CYBER AND PHYSICAL ATTACKS
- Security requirements
- Two-level asset-based classification
- Classification of attacks
- Cyber attacks
- Physical attacks
- Risk assessment
Section V: SECURITY COUNTERMEASURES
- Taxonomy of countermeasures
- Drone operating system security
- Cyber countermeasures
- Cryptography and Key management
- Authentication and access control
- Blockchain-based solutions
- Intrusion detection systems
- Physical countermeasures
- Drone forensics
- Regulations and standards
Section VI: OPEN ISSUES AND FUTURE DIRECTIONS
Section VII: CONCLUSION

Figure 2: Structure of the survey

lead to fatalities. Furthermore, the drones' communication and networking system is heavily exposed to cyber security attacks and threats, which may result in disasters if not adequately addressed. In this survey, we address the above challenges and discuss their countermeasures. Furthermore, we present a comprehensive overview of the IoD, starting from the drone system itself, and going through the different architectural models, applications, requirements, communication systems, and cloud integration.

In the literature, there are some surveys [307, 21, 110, 62, 64, 173, 141, 318, 325, 14, 193] that cover different aspects of IoD security. However, most of the surveys are short or restricted to a single security sub-topic. Others do not cover countermeasures or physical security. These gaps have motivated us to propose a more comprehensive survey on IoD security. Differently, this survey covers the cyber and physical security of the IoD, assesses the risks, and proposes three fine-grained taxonomies that are related to (1) components of drones (i.e., assets), (2) attacks, and (3) countermeasures. It assesses the cyber and physical risks of the IoD. It also provides a more comprehensive review by covering novel security topics such as operating system security. In particular, the main contributions of our survey are the following:

1. We present existing IoD-related surveys that cover several areas, including communication, cyber-physical systems (CPS), path planning, optimization, flight control, and security. Moreover, we compare the previous IoD security surveys and outline the key novelties of our survey.

2. We propose a *two-level classification* of the components in the IoD. The first level considers the coarse-grained assets, which refer to the IoD's tangible elements, and the second level considers the fine-grained assets, which refer to the elements composing the coarse-grained assets. This classification allows a finer level of granularity to identify threats; hence, better security can be ensured.

3. Based on the asset classification, we propose an attack taxonomy that considers the cyber and physical attacks targeting the coarse-grained and fine-grained assets.

4. We evaluate the risk of cyber and physical attacks, by introducing a novel concept, named *Chain of impact* that connects four types of impacts, i.e, *Direct*, *Mission*, *Drone*, and *Environment*.

5. We propose a taxonomy of countermeasures according to two implementation phases: *Pre-incident*, and *Post-incident* (or recovery). The pre-incident countermeasures are further classified as *preventive* and

detective. We provide better coverage of countermeasures by describing them and analyzing their strengths and limitations. We also cover novel topics, such as operating system security.

6. We identify ranked research challenges and recommend future research directions.

The survey structure is shown in Figure 2. The rest of the survey paper is organized as follows: In Section 2, we present non-security and security-focused related surveys on IoD and identify the main differences with our survey. Section 3 provides an overview of IoD. Section 4 presents the two-level asset-based and attack-based taxonomies and the cyber and physical risks that could affect the different components of the IoD. In Section 5, we provide a taxonomy of countermeasures and describe the different techniques. Section 6 identifies open issues and recommends some suggestions and future research directions. Finally, Section 7 concludes this survey.

2. Related surveys

In the literature, several surveys have covered various areas of IoD. Table 1 presents the different IoD surveys, and their corresponding focused research areas. Many surveys focused on communication and networking [102, 92, 130, 258, 339, 34, 111, 206], and flight control [332, 150, 280, 168, 169, 345]. Some surveys paid attention to cyber-physical aspects [272, 310], channel modelling and identification [142, 327, 159], path planning, mobility, and trajectory mining [101, 346, 324, 219, 103], traffic monitoring [133], vision, and target identification [131, 178, 66], optimization [227, 52, 47], and collaboration [60, 19, 312]. The rest of the surveys [204, 220, 273, 41, 160] were not limited to a specific area, but they either covered different areas or provided a general overview of the IoD.

We can also find some surveys in the literature that cover different aspects of IoD security. As shown in Table 2, we classify the IoD security surveys concerning the following criteria:

- *Taxonomy:* It indicates whether the Survey provided a taxonomy that organizes and classifies the state-of-the-art into different categories. In general, a taxonomy could help the research community better understand a research topic, identify issues at a high level of granularity, and guide future research efforts.
- *Cyber security:* It indicates whether the Survey considered the cyber security aspect of IoD.
- *Physical security:* It indicates whether the Survey considered the physical security aspect of IoD.
- *Risk assessment:* It indicates whether the Survey provides an assessment of risks against IoD. This assessment helps identify the risks that require more attention from academia and the industry community.
- *Countermeasure:* It indicates whether the Survey presented countermeasures to protect the IoD.
- *Open issues & future directions:* It indicates whether the Survey discussed open issues and provided recommendations for future research.
- *Observation:* It states any observations related to the Survey.

Vattapparamban et al. [307] presented aspects related to cybersecurity, privacy, and safety regulations of drones for smart city applications. Altawy et al. [21] described the cyber and physical threats to civilian drones. They also identified the corresponding security field for each threat that should be adopted, as well as research challenges and future research directions. He et al. [110] presented a short overview of threats and countermeasures related to IoD. Choudhary et al. [62] proposed a taxonomy to classify attacks with respect to the compromised security property, including confidentiality, integrity, availability, privacy, and trust. In [64], a short survey on intrusion detection systems (IDSs) in Unmanned Aerial Vehicle (UAV) environments is presented. The authors proposed a taxonomy to classify the state-of-the-art IDSs according to different criteria: (a) information-gathering sources (i.e., sensors, communication links, GCS, UAV), (b) deployment strategies (i.e., ground-coordinated and autonomous), (c) detection methods (i.e., specification, signature, and anomaly-based), (d) detection states (i.e., on-site and off-site), (e) IDS acknowledgment (i.e., instant and periodic acknowledgment), and (f) intrusion types (i.e., malware, message forgery, routing attacks, etc.). The authors also provided research challenges and future research directions for IDS in the UAV environment. Lin et al. [173] presented security solutions against some attacks, such as privacy leakage (i.e., identity and location), forward and backward security, insider attacks, and untrusted cloud service providers. Kharchenko et al. [141] analyzed and assessed the network vulnerability of IoD using the Intrusion Modes and Effects Criticality Analysis (IMECA) technique. Each vulnerability is assessed according to the occurrence probability and severity. In [318], authentication protocols for IoD are presented and compared with ensured security properties, communication cost, and computational cost. Open research challenges in the field of IoD authentication are identified. Yaacoub et al. [325] presented the threats that target drone systems and the threats that could arise from using drones to commit crimes and damage the physical environment. They also gave their countermeasures and proposed recommendations to improve drone security. Alladi et al. [14] surveyed many blockchain applications in UAV networks. Although security is not the main topic of this Survey, the authors presented the different scenarios where blockchain can be used to secure UAV networks. Mehta et al. [193] focused on security issues in UAVs with a 5G communication network. They classified the security issues with respect to compromised security property, including authentication, privacy, integrity, and availability.

Table 1
Non-security surveys on Internet of drones

Research topic	Reference	Outline
Communication and networking	Sharma et al. (2020) [275]	Survey of communication and network technologies for UAVs.
	Gupta et al. (2015) [102]	Survey of issues in UAV communication and networks.
	Fotouhi et al. (2019) [92]	Survey of cellular-specific issues and solutions for integration of UAVs into cellular networks
	Jiang et al. (2018) [130]	Survey on routing protocols in UAVs.
	Saleem et al. (2015) [258]	Discussion of issues and challenges related to the integration of UAVs and cognitive radio technology.
	Zeng et al. (2016) [339]	Overview of UAV-aided wireless communications
	Bekmezci et al. (2013) [34]	Review on FANETs and related issues in a layered approach.
	Hentati et Fourati (2020) [111]	Comprehensive survey of UAVs communication networks
	Mozaffari et al. (2019) [206]	a Comprehensive tutorial on the applications of UAVs in wireless communications.
Cyber-physical systems	Shakeri et al. (2019) [272]	Identify design challenges of multi-UAV systems for CPS applications and solutions to address them.
	Wang et al. (2019) [310]	Survey on the UAV networks from a CPS perspective
General or Multi-topic	Motlagh et al. (2016) [204]	Focus on delivering UAV-based IoT services from the sky and provide their corresponding architecture. Survey of the different networks that can be formed by UAVs
	Nayyar et al. (2020) [220]	Overview of technologies and applications related to the Internet of Drone Things.
	Shakhatreh et al. (2019) [273]	Present UAV civil applications and their challenges
	Boccadoro et al. (2020) [41]	Review of IoD aspects related to physical, datalink, network, application, and cross layers
	Ayamga et al. (2021) [28]	SWOT analysis of agricultural, medical, and military drones
	Zaidi et al. (2021) [338]	Comprehensive survey on the Internet of Flying Things (IoFT)
	Liu et al. (2020) [177]	Comprehensive survey on opportunities and challenges of UAV-enabled Internet of Everything (IoE)
	Kumar et al. (2022) [160]	Review of Internet of Quantum Drones
Channel modeling and identification	Khuwaja et al. (2018) [142]	Survey of the measurement methods for UAV channel modeling and Discussion of various channel characterization efforts.
	Yan et al. (2019) [327]	Review of channel modeling for UAV communications
	Kulkarni et al. (2021) [159]	Review of channel characteristic identification using machine learning
Path planning, mobility, and trajectory mining	Goerzen et al. (2010) [101]	Overview of motion planning algorithms from the perspective of UAV guidance
	Zhao et al. (2018) [346]	Overview of UAV path planning studies based on Computational intelligence methods
	Xie et al. (2013) [324]	Comprehensive survey of the mobility models of airborne networks
	Navarro et al. (2013) [219]	Survey of collective movement of mobile robots
	Hamdi et al. (2022) [103]	Survey on spatiotemporal trajectory data mining
Traffic monitoring	Kanistras et al. (2013) [133]	Survey of UAVs for traffic monitoring and management
Vision and target identification	Kanellakis et al. (2017) [131]	Review of vision-based applications for UAVs focusing on current developments and trends
	Lu et al. (2018) [178]	Review of the vision-based methods for UAV navigation
	Coluccia et al. (2020) [66]	Review on detection and classification of multirotor drones
Optimization	Otto et al. (2018) [227]	Survey of optimization approaches for civil applications of UAVs
	Cheikhrouhou et al. (2021) [52]	Comprehensive Survey on the Multiple Traveling Salesman Problem for ground and flying robots
	Chaari et al. (2022) [47]	Computation offloading for ground robots and drones
Collaboration	Chmaj et al. (2015) [60]	Survey of applications of distributed processing systems for UAV swarms.
	Alsamhi et al. (2019) [19]	Survey of collaborative drones to improve the smartness of smart cities
	Wang et al. (2017) [312]	Description of distributed gateway-selection algorithms and cloud-based stability-control mechanisms
Flight control	Ebeid et al. (2017) [77]	Survey of hardware and software open-source flight controller platforms
	Yang et al. (2016) [332]	Survey of autopilots for multi-rotor UAVs.
	Kortunov et al. (2016) [150]	Functionality analysis of autopilots provided by different manufacturers
	Shraim et al. (2018) [280]	Survey on different aspects of Quadrotors
	Li et al. (2015) [168]	Survey of flight control algorithms
	Li et al. (2012) [169]	Survey of Control Algorithms for Quadrotor Unmanned Helicopter
	Zhang et al. (2013) [345]	Survey on applications of multiple unmanned vehicles with an emphasis on strategies on path following, coordination, and control algorithms

They also presented blockchain-based security solutions in UAVs and proposed future research directions toward integrating blockchain with 5G-enabled UAV networks. Yahuza et al. [326] classified the attacks against drone systems into two major categories: attacks that lead to localization errors of drones and attacks targeting security and privacy requirements. The attacks of the second category are further

Table 2
Security-focused surveys on Internet of drones

Reference	Taxonomy	Cyber security	Physical security	Risk assessment	Countermeasures	Open issues & Future directions	Observation
Vattapparamban et al. (2016) [307]	No	Partial	Partial	No	Partial	No	Short survey
Altawy et al. (2017) [21]	No	Yes	Yes	No	Yes	Yes	Short description and limited coverage of countermeasures
He et al. (2017) [110]	No	Partial	No	No	Partial	Yes	Short survey
Choudhary et al. (2018) [62]	Attacks	Yes	No	Partial	No	Yes	No coverage of countermeasures
Choudhary et al. (2018) [64]	IDS	Yes	No	No	Yes	Yes	Scope of the survey is restricted to IDS
Lin et al. (2018) [173]	No	Partial	No	No	Partial	Yes	Short survey
Kharchenko et al. (2018) [141]	No	Yes	No	No	No	No	Short survey
Wazid et al. (2018) [318]	Authentication	Yes	No	No	Yes	Yes	Scope of the survey is restricted to Authentication
Yaacoub et al. (2020) [325]	Threats	Yes	Yes	No	Yes	Yes	Limited coverage of countermeasures
Alladi et al. (2020) [14]	No	Yes	No	No	Blockchain based solutions	Yes	Security is partly covered in the survey
Mehta et al. (2020) [193]	Security issues	Yes	No	No	Blockchain based security solutions in UAV	Yes	Scope of the survey is restricted to blockchain-based solutions in UAV and 5G-enabled UAV networks
Yahuza et al. (2021) [326]	Attacks	Yes	No	No	Yes	Yes	Physical security is not covered in the survey
Our survey	Assets Attacks Countermeasures	Yes	Yes	Yes	Technical and non-technical countermeasures covering the cybersecurity layers (preventive, detective, and corrective)	Yes	Novel taxonomies. Risk assessment is provided. More coverage of countermeasures. Operating system security is covered. Ranked open issues are provided

classified into subcategories with respect to integrity, availability, confidentiality, authenticity, and privacy. The authors also presented mitigation countermeasures for each attack subcategory.

2.1. Comparison with related surveys

Most of the IoD security surveys are short [307, 110, 173, 141], or restricted to one security sub-topic such as IDS [62], authentication [318], and blockchain [14, 193], and some surveys do not present countermeasures [62, 141]. Our Survey differs from the earlier-mentioned works in the following points:

- **Novel taxonomies:** Differently from many surveys that only provide a classification of attacks/threats, our survey proposes three taxonomies that are related to (1) components of drones (i.e., assets), (2) attacks, and (3) countermeasures. The proposed taxonomies allow a finer level of granularity for asset identification, which permits broader identification of possible attacks, and determines where to implement the countermeasures at the fine-grained level. It also determines when to implement the countermeasures.
- **Risk assessment:** There are no surveys that provide risk assessment related to IoD, except for [62], which presents a partial assessment by only considering the impact of threats. This assessment is based on a new concept called chain of impact. It aims to help researchers from academia and industrial communities identify the risks that require more attention and stronger countermeasures.
- **More coverage of countermeasures:** We provide a more comprehensive survey than the related surveys regarding countermeasures. Only two surveys consider physical security [21, 325]. The same surveys [21, 325] only give a summary description of the

countermeasure solutions. On the other hand, our survey presents the technical and non-technical countermeasures covering the three cybersecurity layers, i.e., preventive, detective, and recovery. It also discusses the solutions and presents their limitations.

- **Operating system security**: Our survey is the first one that discusses the security aspects of drones' operating systems.

- **Ranked open issues**: This survey is the first one that provides a ranking, which prioritizes the open issues in the IoD that require attention from the research community. It defines three priority and ranking levels, i.e., high, medium, and low.

3. Overview of Internet of drones

3.1. Physical structure of a drone

An unmanned aerial system is composed of a rigid body called a frame, and multiple motors are attached to this frame to generate the required thrust to lift the system in the air. There are different types of drones, depending on the number of motors attached to them, as shown in Figure 3.

- **Tricopter:** It has three motors, where two motors are brushless, and one is a servo motor. The brushless motors are typically used in small UAVs, and they are called so because they have no brushes in their commutator. They have higher efficiency as compared to brushed motors. The servo motor is a device that has an internal encoder, which allows converting any motion into a digital signal. The role of the servo motor in the Tricopter is to control the orientation (i.e., yaw) of the UAV. They present the advantage of being low-cost but are less reliable and robust than the other types.

- **Quadcopter:** It is the most common type of drone and has four brushless motors attached to each of its four wings and deviated by 90 degrees from each other. There are two possible configurations: (*i*) Quad-X, where the front direction of the UAV is in the middle of the two front motors, and (*ii*) Quad-Plus, where the forward direction of the UAV is looking at the first motor of the quadcopter, as illustrated in Figure 3. The motors rotate either in a clockwise direction (CW) or a counter-clockwise direction (CCW). For the Quad-X, the top-left and right-bottom motors must rotate in CCW, and the top-right and left-bottom motors must rotate in CW. Quad-X configuration is preferred for First Person View (FPV) applications because it provides a better camera view.

- **Hexacopter:** It has six motors attached to its frame. The angle between two consecutive wings is 60 degrees. This model has the advantage of providing 50% more thrust than a quadcopter model, thanks to its other two motors, but at the expense of higher energy dissipation from the two extra motors. This allows to carry heavier payloads and ensures a more reliable flight due to the redundancy but results in a 35% reduction of the flight time using the same battery as a quadcopter model. It also has two possible configurations: Hex-X and Hex-Plus.

- **Octocopter**: The Ocotocoper model has eight motors attached to its frame. The angle between two consecutive wings is 45 degrees. It is used for heavy payloads, such as carrying water tanks in smart agriculture or firefighting scenarios. This model is highly reliable as it can tolerate the power of any two non-consecutive motors without losing the ability to fly. It is also suitable for aerial photography. The Ocotocoper model is substantially more expensive than all other frame models due to the cost of extra motors and higher-capacity batteries. It also consumes much more energy due to the extra motors and the heavier weight. Similar to Quadcopters and Hexacopter, Octocopter can also be configured as Oct-X and Oct-Plus.

3.2. Architecture of the Internet of drones

This section presents the concept and architecture of IoD and its main components. The objective is to provide the reader with the general technical background to understand the different actors in an IoD ecosystem. In [99], the authors presented a generic abstract architecture that can be implemented by any IoD system while they focused on the concept of the layered networked control architecture. In this section, we present the architecture of the IoD ecosystem using a multi-layer system approach, where each layer identifies an actor in the system. The proposed architecture is also generic and instantiated on any specific IoD platform.

The general architecture of the IoD is presented in Figure 4. We decompose an abstract IoD system architecture into the following five major layers:

- **The Drone Layer:** This layer refers to the flying aerial unmanned systems, which are equipped with: (*i*) sensors to collect data from the environment, and (*ii*) actuators/containers to carry the payload between different locations. The drone's sensors depend on the type of data to collect. RGB camera sensors are used for collecting images, and videos in applications such as inspection, surveillance, AI-based computer vision [36], photogrammetry, and aerial surveys. Multispectral cameras are used in agriculture use cases to improve the efficiency of large farming operations, including plant health assessment, disease detection, and plant counting. Thermal cameras are used in search and rescue operations and structural health monitoring. Weather sensors can be used to collect atmospheric data. In the IoD context, each drone must be identifiable, i.e., it has a unique ID. It is essential to track every drone in the ecosystem and send it to control commands through the network. Furthermore,

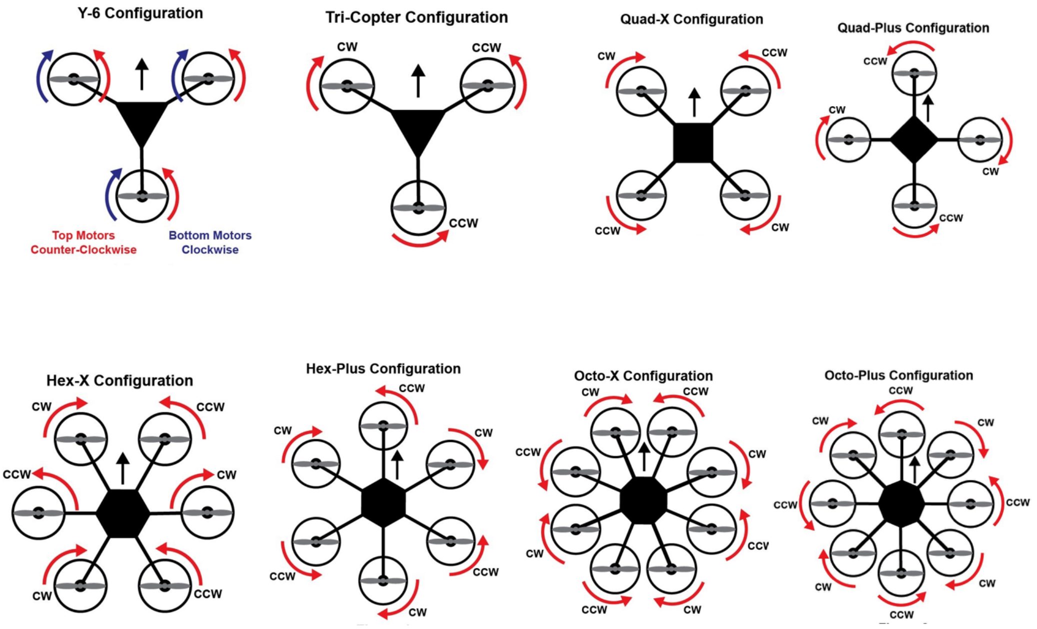

Figure 3: Multicopter models

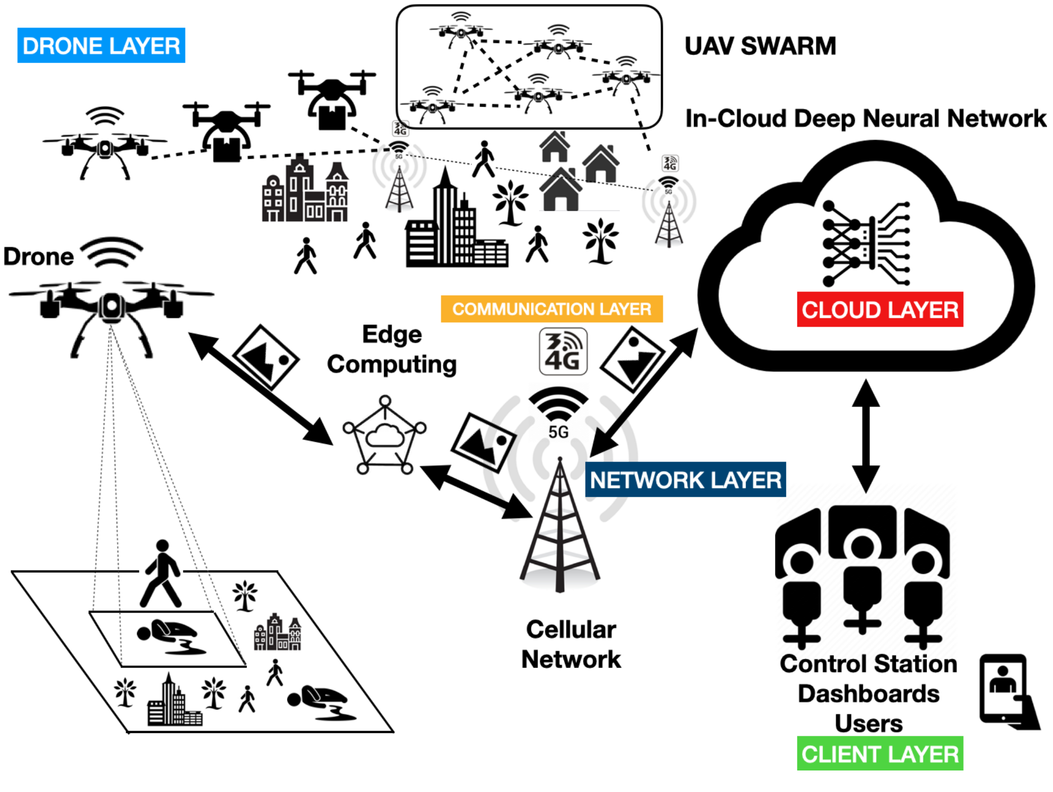

Figure 4: Internet-of-Drones Architecture

a unique ID is crucial from a security perspective in case of crashes or any hazards caused by the drone's operation. Drones must also be securely connected to the Internet to allow their secure tracking and monitoring in real time.

- **The Communication Layer:** It refers to the communication protocols used to connect drones with the other actors and components of the system. Typical broadband communication systems are used, such as satellite communication, telecommunication networks (3G/4G/5G) [156], long-range WiFi [42], WiMAX [69], and IEEE 802.15.4 [153]. In the case of mission-critical or military applications, the communication layer may use private and proprietary protocols to avoid possible threats, such as jamming and interference. The communication protocols must also be secure, in particular encryption, to avoid unauthorized access to the data. The communication layer must provide reliable and secure services to the drone layer considering the criticality of the drone's operations. The required communication bandwidth depends on the application type. For high throughput applications, such as real-time drone video streaming and vision-based applications, the communication layer must provide high bandwidth channels to ensure streaming quality [154]. Bandwidth requirements are less stringent for IoT-like applications collecting low-rate data streams.

- **The Network Layer:** A network of drones can be organized in different topologies and architectures depending on the application's requirements. We can categorize the network layer into two main categories: (*i*) *centralized architecture*: a server or a ground station acts as a central node and coordinates the communication between the drones and users. This architecture is typically used in cloud-based UAV systems, where the cloud orchestrates and manages the UAV missions [156], and (*ii*) *distributed architecture*: there is no central entity that manages the communication between UAVs, but the communication is fully distributed and ad hoc. A UAV Swarm is a team of drones that communicate in an ad hoc manner to perform the desired mission [44]. In a typical scenario, one drone leader is chosen to coordinate the tasks of the drones without any intervention from external users, centralized ground stations, or servers. The distributed architecture is challenging because it requires the complete coordination of the drones in the swarm. However, this is hard to achieve because it involves broadcasting messages between the drones, resulting in flooding problems. Furthermore, the distributed architecture will require advanced ad hoc routing protocols, which is hard to accomplish due to the highly dynamic nature of drones' motion in swarms. Security is a concern for centralized and distributed networking architectures because messages must travel via multiple hops. Routing protocols must embed security mechanisms to avoid any data compromise.

- **The Cloud Layer:** The cloud layer is used for providing computation and storage services to drones and users. As UAVs are typically used to collect visual data, image frames are streamed to the cloud, which processes them using deep learning algorithms (i.e., convolutional neural networks) that are computation-intensive and storage-greedy and cannot be executed on typical drones. These algorithms might perform object detection and image segmentation and execute generative models, which are pretty demanding in terms of resources. The cloud also permanently stores the UAV flight mission data for possible scene reconstruction and analysis. The cloud can specify the business logic and constraints governed by the authority and applied by drone operators to coordinate drone missions, including flight schedules, mission planning, geofencing, and law enforcement. The cloud also regulates the traffic through the Unmanned Traffic Management (UTM) system, which manages drone operations and traffic among stakeholders (Client Layer). On the other hand, cloud storage and processing often represent a major concern regarding data privacy. Privacy-preserving approaches such as homomorphic encryption [12] were used with deep learning for aerial image processing to avoid disclosing private data on the cloud. Besides, the cloud should provide security features, including authentication, data integrity, confidentiality, and non-repudiation for all actors in the IoD ecosystem, including users, operators, and drones.

- **The Client Layer:** This layer refers to the end-users who use and manage the system through the Internet. It relies on software Application Program Interfaces (APIs) using Web services to interact with the cloud. The users monitor the UAVs through dashboards and remotely send commands to control them. Users can also perform video surveillance as UAVs stream their collected video frames through the cloud. The client application may provide several services and business rules for drones' missions (implemented in the cloud back-end), such as traffic management, geofencing, and path planning. There are different types of end-users (depending on the application and usage of IoD), which are referred to as stakeholders at the client layer. Let us consider a classic use case of a drone delivery mission, where a user requests a delivery mission of a package from a drone service provider. This scenario implies three types of users, including:

  - Operators: they represent drone service providers that operate drone missions, such as drone delivery missions, surveillance, and inspection.
  - Basic Users: these users interact with the cloud to request drone delivery services from the operators.
  - Authority: it represents the regulatory board that specifies the policies and by-laws of drone operations in the airspace. This may include civil aviation and defense authorities, as examples. The authority is responsible for validating the mission before the operator is allowed to execute the delivery mission.

Other types of applications may imply other types of users.

3.3. Communication paradigms in the Internet of drones

There have been several research works dealing with communication paradigms for IoD. Nowadays, the use of UAVs is widespread in civil/military applications. The complexity of communication systems in IoD varies; it can be as simple as a single UAV communicating with a ground station to carry out the objectives for a mission [236, 79, 284, 58], and as complex as Swarms of UAV systems cooperatively carrying out various aspects of joint missions [302, 331, 311, 203, 217, 27, 211, 146]. As UAVs are generally resource-constrained devices, they must consider various factors when addressing IoD communications, including energy efficiency, latency, and security. Here we present works addressing the IoD communication systems at two different levels: (i) Mobile Edge-Cloud Drone Communications and (ii) Decentralized Flying Ad-Hoc Networks.

i) Mobile Edge-Cloud Drone Communications: Mobile Edge Computing (MEC) provides cloud computing capabilities and services at the edge of the network. A UAV flying within the radio range of the MEC device can communicate with the device and provide access to a user over the cloud. This concept is extended to the Internet of Drones, where multiple drones connect to MEC device(s), effectively creating a mobile ad-hoc network within the line of sight. The IoD ensures highly efficient network operation and service delivery quality and, as a result, improves the user experience.

A cyber-physical system (CPS) based system was proposed by Narang et al. in [217]. The researchers presented the system architecture of the CPS-UAV integrated solution that is deployed as part of a large-scale disaster response system. The authors focus on network topology optimization and address communication issues within the mobile edge infrastructure and the multi-drone network. Authors in [203] presented a UAV-based Internet of Things platform used in the context of a crowd surveillance application. The proposed architecture of this system allows UAVs to capture real-time video and offload this video stream to a MEC device. Leveraging the underlying LTE/5G communication infrastructure, the video stream is transmitted to the cloud, where the image recognition system processes the data. The authors in this work demonstrate the working of the multiple-UAV cluster implementation. Wang et al., in their work in [311], demonstrated a bandwidth-efficient video analytics system using UAVs. The proposed system architecture minimizes the communication latency overhead by utilizing MEC. The MEC device captures the video stream from the drones in proximity, compressing the video data stream, and resulting in an optimized payload. The communication between the MEC device and the cloud utilizes an opportunistic approach to reduce latency and bandwidth usage. In [308], authors presented the Internet of Flying Things (IoFT) and discussed the opportunities and challenges for airborne MEC devices. A prototype for a Drone-as-a-Service (DaaS) is developed leveraging the fly-in and fly-out infrastructure for servers, where the flying UAV serves as an airborne mobile edge device. With this prototype implementation, it remains to be seen how the secure communication and load balancing between multiple MEC devices within the network would affect the system's performance.

The air-to-ground mobile edge network for UAVs is presented in [58]. Cheng et al., in this work, proposed the optimization of a multi-dimensional channel-based approach to drone management. The authors study the effects of the network topological changes on message transfer, scheduling, and device control. Tian et al. in [302] utilized a predictive authentication approach for IoD using a MEC device for secure communication. The drones use a lightweight online/offline signature to authenticate with the MEC device. The MEC manages and controls the authentication parameters within the MEC-drone network and serves as a secure communication device within the IoD. Furthermore, a predictive authentication approach was utilized to further reduce the cost of authentication within the UAV-MEC communication.

ii) Decentralized Flying Ad-Hoc Networks: Another communication aspect in IoD communication is UAV-UAV communication. The communications between flying drones can essentially be mapped to a Flying Ad-hoc Network (FANET) [212]. Similar to the vehicular network problem studied in the context of Vehicular Ad-hoc Networks (VANETs), drone-to-drone communications can be realized. Each device/node within a FANET can store the information or relay it to the next device in a multi-hop configuration. Furthermore, a drone can also work as a data mule to carry the information to another part of the network or even to a different network. Using the Delay Tolerant Network (DTN), this information can be relayed to other devices such as drones, MEC, or even a GCS. Due to the delay-tolerant capability, missions can be completed opportunistically in different time frames.

Flying ad-hoc network architecture is presented in [34]. Bekmezci et al. presented the potential advantages and disadvantages of ad-hoc communication between flying drones by classifying them into UAV-UAV, ground-UAV, and satellite-UAV communication challenges. They developed a protocol based on the work presented in [35]. This communication protocol focused on reducing the communication overhead by periodically broadcasting the link state updates.

Similar to Bekmezci et al.'s approach to utilizing MANET protocols for IoD communications, many recent works have addressed IoD communication issues, taking the lead from works in the context of MANETs and VANETs. Due to high mobility within FANETs, the network topology frequently changes, necessitating periodic route discovery. A route-switching algorithm was presented in Yanmaz et al. [216]. This algorithm tracks all possible routes from a source to all destinations within a FANET, similar to the AODV routing protocol [214] for MANETs. Furthermore, due to high mobility and ever-changing network topology and avoiding the risk of broken routes, the proposed protocol switches

Table 3
Research works in Computational Offloading to the Cloud in IoD

Research Work	Offloading mechanism	Latency	Energy	Storage	Security	Focus of work
Wang et al. (2020) [314]	UAV-MEC	Yes	Yes	No	No	Agent-based architecture for offloading from a UAV to MEC
Wu et al. (2019) [322]	UAV-MEC	No	Yes	No	No	Algorithms for efficient placement of tasks based on energy requirements
Sedjelmaci et al. (2019) [265]	UAV-MEC	Yes	Yes	No	Yes	A trust-based approach to detect, predict the DoS attacks on UAV-MEC communication channels
Mukherjee et al. (2020) [213]	UAV-UAV	Yes	No	No	No	Distributed tasks offloading within a swarm of UAVs
Koubaa et al. (2019) [156]	UAV-Cloud	Yes	No	Yes	No	Computation task offloading to the cloud using web-services on ROS
Koubaa et al. (2018) [155]	UAV-Cloud	Yes	No	Yes	No	Real-time object tracking using a cloud-based IoD

to risk-free routes when possible to avoid route failure. This mechanism is based on the earlier TSODR routing protocol [89] for MANETs. The Zone Routing Protocol (ZRP) [301] addresses FANET communications. A crowd of drones serving as relay nodes within the network is considered a zone. The communication within the zone is proactive, whereas a reactive protocol is used for intra-zone communication. In [174], researchers presented the GPMOR protocol, which predicts the movement of UAVs utilizing a Gaussian-Markov mobility model. This protocol considers the position of a UAV to determine the next hop in FANETs. It also addressed the communication delay due to network congestion by reducing the communication overhead. This protocol is also based on an earlier MANET protocol; namely, TORA [233].

The publisher-subscriber model for routing was used for MANET routing in [301]. Authors in [146] develop a communication protocol for FANETs using a data-centric approach based on this model. A UAV carries data and transports it to a destination utilizing the load-carry-deliver approach popular in DTN networks. Performance evaluation results from this protocol showed increased throughput; however, increasing the coverage area yields negative results in terms of overall performance. In [211], authors couple intrinsic properties of DTN routing with FANETs outlining the load-carry-deliver routing mechanism. Another work [27] similarly takes benefit of DTN routing protocols for MEC-UAV communication.

3.4. Cloud integration and computation offloading

In this section, we describe recent advances in cloud-based IoD systems with a focus on offloading computation from drones to the edge of the cloud [190]. UAVs have been used as aerial Base Stations (BSs). Compared to ground base stations, the aerial base stations provide better maneuverability, can be deployed on-demand, and can relocate to positions suitable to different environments. Drones generally have limited onboard resources for processing information, and limited storage [47]. Off-the-shelf UAV devices are usually resource-constrained regarding three aspects, i.e., size, weight, and power [154]. These UAVs are typically battery-powered and can carry a limited payload. A small UAV is usually limited in terms of battery capacity available onboard and a maximum flight time of around 25-50 minutes [274]. Applications or platforms requiring heavy computation may further drain the already limited power [154]. An IoD system may offload some energy-taxing computation-intensive tasks to a resource-rich drone or even to a Mobile Edge device within the cloud.

In the context of IoD, several criteria can define offloading computation to the cloud ranging from fast processing of large information on-the-go to storage of information for a long period [47]. Here, we describe recent works focusing on *(i)* latency issues, *(ii)* energy and load balancing, *(iii)* data management and storage, and *(iv)* safety, security, and privacy. Table 3 presents a summary of works describing task offloading in IoD. Here, we briefly describe the related works:

Wu et al. [322] proposed a three-layer architecture to address the efficient task offloading between a UAV and Mobile Edge Computing (MEC). They presented two algorithms: *i)* UAV position optimization, and *ii)* a task prediction algorithm. The proposed algorithms consider energy efficiency in task offloading for the UAV-MEC network considering various parameters, including UAV hovering parameters and accurate payload size for offloading tasks. Simulations validate the proposed algorithms, and the results show that the proposed algorithms reduce energy consumption. The authors also proposed using better optimization techniques to further improve the task placement on UAV-MEC systems.

Wang et al. [314] proposed an agent-based task offloading for a UAV-aided mobile edge cloud system. The proposed system architecture considers latency and energy aspects of scheduling tasks to be offloaded to a mobile edge or cloud. The agent is designed to select an offloading strategy based on various parameters, including payload size, available resources on user devices, UAV's available resources, and the MEC. An extensive simulation study is carried out to assess the impact of the task delay and energy consumption for offloading. The results show that an efficient task placement strategy is essential to improve the performance of task offloading to the cloud compared to scenarios with the absence of the agent.

Sedjelmaci et al. [265] presented an efficient cyber defense framework for UAV-edge computing networks. The authors addressed the security vulnerabilities on task offloading to a MEC, including a Denial-of-Service attack to put the UAV and the MEC out of service. They presented a Stackelberg game-based security framework where they model (i) the attack behavior of latency to offload tasks and (ii) the energy consumption in the UAV. A MEC-based agent detects and predicts malicious behaviors based on various parameters. The framework is validated using simulation studies, and the results show that as the number of attackers increases, the prediction rate for malicious nodes also increases. However, a large portion of energy consumption is attributed to detecting and preventing malicious behaviors.

Mukherjee et al. [213] proposed an intra-UAV swarm processing offloading scheme to address latency in processing-intensive tasks. They proposed a weighted-offloading technique that uses a Nash bargaining game between the probabilities of nodes processing the data or offloading to nodes by a queuing theory-based analysis of the network traffic in the UAV swarm. This work builds various datasets based on real-life hardware metrics calculated from a swarm of four UAVs in the context of rural farming. The authors extended this work by further carrying out an extensive simulation study with a large number of UAVs following various network topologies. The results show that the proposed scheme is highly scalable and performs faster than the star network topology.

Koubaa et al. [156] presented a service-oriented cloud-based drone management system. The Dronemap project discussed in this work addresses the control, monitoring, and communication of drones over the Internet. Dronemap utilizes the ROSLink protocol [152] for seamless inter-drone communication over the Internet. The system incorporates the cloud offloading mechanism in Dronemap to offload heavy computations [154] from the drone to the cloud. This is materialized by the use of Web services (SOAP and REST), where the user can schedule drone missions to accomplish the task at hand. In this work, the authors demonstrated a proof-of-concept implementation of the system in various scenarios showing that it is scalable and can be seamlessly deployed anywhere. In another work by the same authors [155], DroneTrack is presented. This system develops real-time Internet-enabled object tracking using a UAV. The DroneTrack leverages the Dronemap planner [156], which is a cloud-based system that can be deployed to control and manage UAVs over the Internet. The authors conducted an experimental study with three scenarios. The experimental study demonstrates the effectiveness of the proposed system.

4. Cyber and physical attacks

In this section, we present the security requirements of the IoD. Then, we provide a novel classification of assets in IoD systems. This classification is later used to propose a taxonomy for attacks and countermeasures. The proposed classification adopts the risk assessment approach, which organizations have widely adopted to identify all possible risks to assets, evaluate them, determine their impact, and make decisions on them to prioritize the implementation of security countermeasures. Specifically, we apply this approach by identifying the IoD's possible components (or assets), i.e., where exactly the different attacks could compromise the IoD. This will also help us know which vulnerability is exploited, the magnitude of the risk, and its impact, and later identify its corresponding countermeasures. Additionally, it will guide the academia and industry community to prioritize research efforts and focus more on attacks with high risks.

4.1. Security requirements

An IoD is a cyber-physical system that needs to ensure security regarding information and control. In our context, security could be defined as the ability of the IoD to correctly perform the intended operations without unauthorized access, alteration, disclosure of information, or loss of assets. It is required that IoD meets different security requirements, including authentication, confidentiality, availability, non-repudiation, integrity, and privacy.

- **Authentication:** It ensures that only authorized users (e.g., operators and end-users) and authorized devices (i.e., drone and GCS) are granted access to IoD resources. If authentication is not ensured, a malicious entity can impersonate a drone, get confidential information, and inject malicious commands and data.

- **Confidentiality**: It ensures that information is not disclosed to unauthorized users. In IoD, we can find different types of information: *(i)* data and commands that are exchanged among the different components of IoD, such as *(ii)* data that are captured by the drones (e.g., sensed values, captured images), *(iii)* data that are transferred over the network, and *(iv)* data that are exchanged among the subsets of the components such as system states that are sent on the communication channels among the sensors, controllers, actuators, and the transmission system.

- **Availability:** It ensures that all components of the IoD should perform the required operations correctly (i.e., monitoring, computation, control, actuation, transmission, and storage) and should be available when it is requested.

- **Integrity:** We consider two integrity properties: *data integrity* and *system integrity*. Data integrity ensures that no malicious or accidental modification or deletion of data, such as telemetry data and commands, is performed. Failure to satisfy data integrity could also lead to the compromise of availability, e.g., a flight control system that receives wrong GPS information, which negatively affects the mission planning of the drone. On the other hand, system integrity ensures that the deployed software and firmware are trusted and free from malicious codes.

- **Non-repudiation:** This requirement pertains to legal issues. As drones are involved in different types of applications, tracking user activities is necessary to determine liability in case of an accident or an incident caused by drones. In the case of communication, non-repudiation ensures the prevention of a sender from denying the generation of messages or a drone from denying sending images or messages. Also, piloting drones carelessly can result in physical damage and loss. Non-repudiation aims to ensure that the drone and the drone operators cannot deny their activities.
- **Privacy:** The drone mission can reveal user-specific information, such as visited locations and captured data. Therefore, drone missions must be protected against traffic analysis or data capturing to preserve user data privacy. Moreover, if drone-collected data is processed and outsourced (such as in a cloud system), adequate cryptographic techniques (such as homomorphic encryption) need to be set up to preserve user privacy [173].

The compromise of any security requirement could consequently compromise the safety requirement. By safety, we mean that drones can fly without causing human and physical damage. Integrating IoD with civil airspace makes it essential to ensure that drones can safely operate within the commonly shared aviation system and environment. A drone must avoid colliding with other drones, properties, and people.

4.2. Two-level asset-based classification

An asset is a concept primarily used in risk assessment methodology, which refers to any tangible or intangible objects that have value to the organization. Asset identification represents the first step in risk assessment. It helps identify the threats that could harm the assets and consequently identifies the countermeasures that can be put in place to mitigate these threats.

In the IoD context, an asset means any element of the IoD required to operate the IoD and its applications. Therefore it needs to be protected against cyber and physical threats. For better protection of the IoD, we adopt a fine-grain asset identification approach, which allows broader identification of possible threats, and hence better security can be achieved. To this end, we propose a two-level asset-based classification. In the first level, we find *coarse-grained assets*, which refer to the tangible elements of the IoD and the wireless communication media that interconnect these elements. In the second level, some coarse-grained assets can be divided into multiple *fine-grained assets*.

More precisely, in the IoD context, we propose the two-level asset-based classification, which considers the following coarse-grained and fine-grained assets, as shown in Table 4.

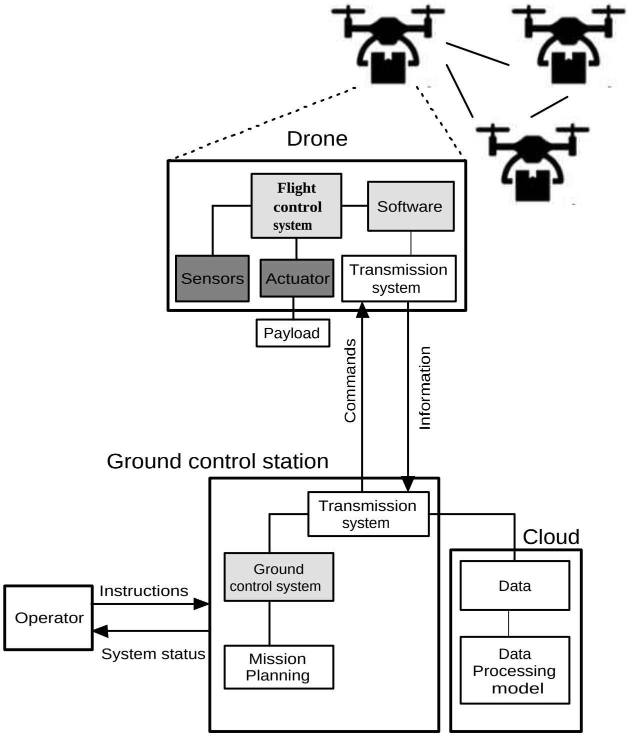

Figure 5: IoD assets

- ***Drone***: It consists of the following fine-grained assets:
  - *Flight control system*: It is the CPU that allows the pilot to fly the drone using steering commands and signals provided by the embedded sensors. It also provides the actuators updated information to adjust their speed and trajectory.
  - *Transmission system*: It represents the communication interface that allows the drone to communicate with the ground control system and other drones.
  - *Sensors*: The drone includes different sensors to sense its physical environment, like an accelerometer, gyroscope, magnetic orientation sensor, barometer, and camera. The data from sensors are used to compute the driving force of the motor, the movement direction, and the altitude for the drone to fly.
  - *GPS receiver*: It is a device that calculates the drone's geographical position based on signals received from satellites' navigation systems.
  - *actuator*: It is a device that helps the drone to make the right movement decision. This is done by converting energy into mechanical actions. The drone's motor is one of the best examples of an electromechanical actuator.
  - *software*: It is the component that connects the user to the drone's hardware. The generic software architecture of a drone consists of (a) system software, which includes firmware, device

driver, and operating system, and (b) application software that runs different functions such as: taking pictures, vision processing, video streaming, navigation, and mission execution.

- ***Ground control station***: It is a land-based control station that consists of the following fine-grained assets:
  - *Ground control system*: It is a software system that allows human operators to remotely control the drone during its operations.
  - *Transmission system*: It is used to exchange data and commands between the drone and the ground control system.
  - *Mission planning system*: It provides the flying trajectory for a single or group of drones to perform their missions.
- ***Cloud***: It is used to store, process, and analyze data collected by the drones and comprises the following fine-grained assets:
  - *Stored data*: It represents data obtained during drones' missions.
  - *Data processing model*: It is used to analyze the stored data to get insights from the drones' missions.
- ***Wireless communication medium***: It is used by communicating entities to transmit messages in the form of electromagnetic signals. Two types of messages are transmitted:
  - Information transmitted from drones to the ground control station or exchanged among the drones.
  - Commands that are transmitted from the human operator to the drones.
- ***People***: We identify two types of people:
  - Operators: They perform activities related to the drone's mission, like piloting the drone through some commands.
  - Pre-operators: They represent people who contribute to developing the required software to operate the IoD.
- ***Payload***: It represents the object that is carried by the drone.

The coarse-grained and fine-grained assets can also be classified according to Level-1 type and Level-2 type, respectively, as presented in Table 4. More specifically, the coarse-grained assets can be classified with respect to Level-1 type as follows:

- *Physical systems (PHS):* They represent all tangible elements with computation and communication capabilities, such as drones, ground control stations, and cloud systems.

Table 4
Two-level asset categorization

Coarse-grained asset	Level-1 type	Fine-grained asset	Level-2 type
Drone	PHS	Software	CY
		Flight control system	CY
		Transmission system	CY
		Sensors	CP
		GPS receiver	CP
		Actuator	CP
Ground control station	PHS	Ground control system	CY
		Transmission system	CY
		Mission planning	CY
Cloud	PHS	Data processing model	CY
		Stored Data	CY
Wireless communication medium	WCM	Transmitted information	CY
		Transmitted commands	CY
People	HM	Operators	HM
		Pre-operators	HM
Payload	PHO	Payload	PHO

- *Physical objects (PHO):* They represent all elements that have neither computation nor communication capabilities, such as carried payload.
- *Wireless communication channels (WCM):* They represent the different Wireless communication technologies, such as Wi-Fi, and 4G, which are used to exchange information among the physical systems of the IoD.
- *Human (HM):* They represent all persons who have a role in developing, implementing, deploying, and operating the IoD.

In addition, the fine-grained assets can be classified with respect to Level-2 type as follows:

- *Cyber fine-grained assets (CY)* : They refer to the fine-grained assets that belong to the cyber world, such as transmitted and stored data and all the components that perform either computation, control, or communication operations.
- *Cyber-physical fine-grained assets (CP) :* They refer to the fine-grained assets that connect the cyber world with the physical world, such as sensors and actuators.

In our classification, as *People* and *Payload* cannot be divided into smaller entities, we consider them as both coarse-grained and fine-grained assets. Thus, Level-1 and Level-2 of the different types of People are *Human*. Similarly, Level-1 and Level-2 of Payload is *Physical object*.

4.3. Classification of attacks

In the literature, the attacks against IoD are classified according to different criteria. Kim et al. [143] identified three types of attacks: hardware attacks against the UAV autopilot components, wireless attacks performed through a wireless communication medium, and sensor attacks spoofing that injects false data through the sensors of UAV. In [220], the attacks are classified with respect to the target layer, i.e., physical, data link, network, transport, perception layer, and application layers. In [156], the target layer criterion is also used to classify the attacks. Specifically, the attacks can be launched against three layers, i.e., the proxy layer, the cloud layer, and the drone layer. In [325], the threats are classified as threats that target drones and threats that use drones. On the other hand, many works [62, 193, 326] categorized the IoD attacks based on the compromised security properties such as attacks on confidentiality, integrity, availability, privacy, trust, and other properties. However, an attacker could compromise more than one security property.

Differently from the attack classifications mentioned above, we use the two-level asset-based classification, which is proposed in Section 4.2 to introduce a novel classification of attacks in IoD. This classification considers the *Targeted Coarse-grained Asset*, and the *Targeted Fine-grained Asset* in addition to other criteria. More precisely, we classify the attacks with respect to different criteria, as presented in Figure 6. The main classification criterion is *Nature of Attack*, and accordingly, two classes are identified. The first class covers the cyber attacks, which are presented in Section 4.4. The second class covers the physical attacks, which are presented in Section 4.5. The other classification criteria, i.e., *Target*, *Compromised Security Requirements*, and *Impact*, of cyber and physical attacks, are presented in Table 5 and Table 6 respectively. In more detail, the attacks are classified according to the following criteria:

- ***Nature of attack***: The attack can be classified as cyber or physical.
  - Cyberattack occurs when there is cyber manipulation of the system without physical access.
  - By physical attack, we mean that an adversary gains physical access to an asset to damage it.
- ***Target***: It specifies the asset that is targeted by the attacks. We identify two types of targets:
  - *Targeted coarse-grained asset*: It indicates the coarse-grained asset that is targeted by the attack.
  - *Targeted fine-grained asset*: It indicates the fine-grained asset targeted by the attack.
- ***Compromised security requirements***: It specifies which attack compromises security requirements. The attack can take two types of behavior: passive and active. Passive attacks mainly compromise the confidentiality requirements, whereas active attacks compromise the rest of the security requirements.
- ***impact***: The attacks can inflict different types of negative impacts and undesirable consequences, and one impact can lead to another one. To this end, we introduce a novel concept, named *Chain of impact*, which connects four types of impacts: *direct impact*, *mission impact*, *drone impact*, and *environmental impact*, as shown in Figure 7.
  - *Direct impact*: It compromises the following impacts that can lead to a situation where the IoD fails to accomplish its mission:
    - ∗ *Data compromise*: It includes data disclosure, data loss, and data manipulation.
    - ∗ *Disruption of cyber and cyber-physical operations*: The execution of some operations in IoD, such as computation, communication, control, sensing, and actuation, could be disrupted through false data or vulnerable functions. This could result in mission failure due to compromised trajectory, hijacking of drones, drone crashing, and drone collision.
    - ∗ *loss of communication and GPS signals*: The mission of the IoD could be disturbed due to the absence of communication or the GPS signals.
  - *Mission impact*: It represents the negative effects of the attack on the mission of the IoD. It is characterized by the Disruption of cyber and cyber-physical operations of IoD, such as computation, communication, control, and sensing, which could lead to drone hijacking. Some false information (flight commands and GPS signals) could also result in drone hijacking. Once the drone is hijacked, it could be later captured by the adversary or damaged due to a crash or collision with other objects. The mission could fail due to compromised trajectory, hijacking of drones, drone crashing, and drone collision.
  - *Drone impact*: It represents the attack's negative effect on the drone's physical availability. The drone could be lost when captured by an adversary or damaged when it crashes or collides with other drones or objects.
  - *Environmental impact*: It represents the harmful effects of compromised IoD on the environment. It occurs when one or more processes and physical assets are compromised, which can damage the environment. It includes human loss and physical damage to properties when drones collide with stationary and moving objects.

An attack can cause a chain of impacts, as shown in Figure 7. The figure depicts a Finite State Machine (FSM), where the states represent the different impacts, and each arrowed line represents transitions

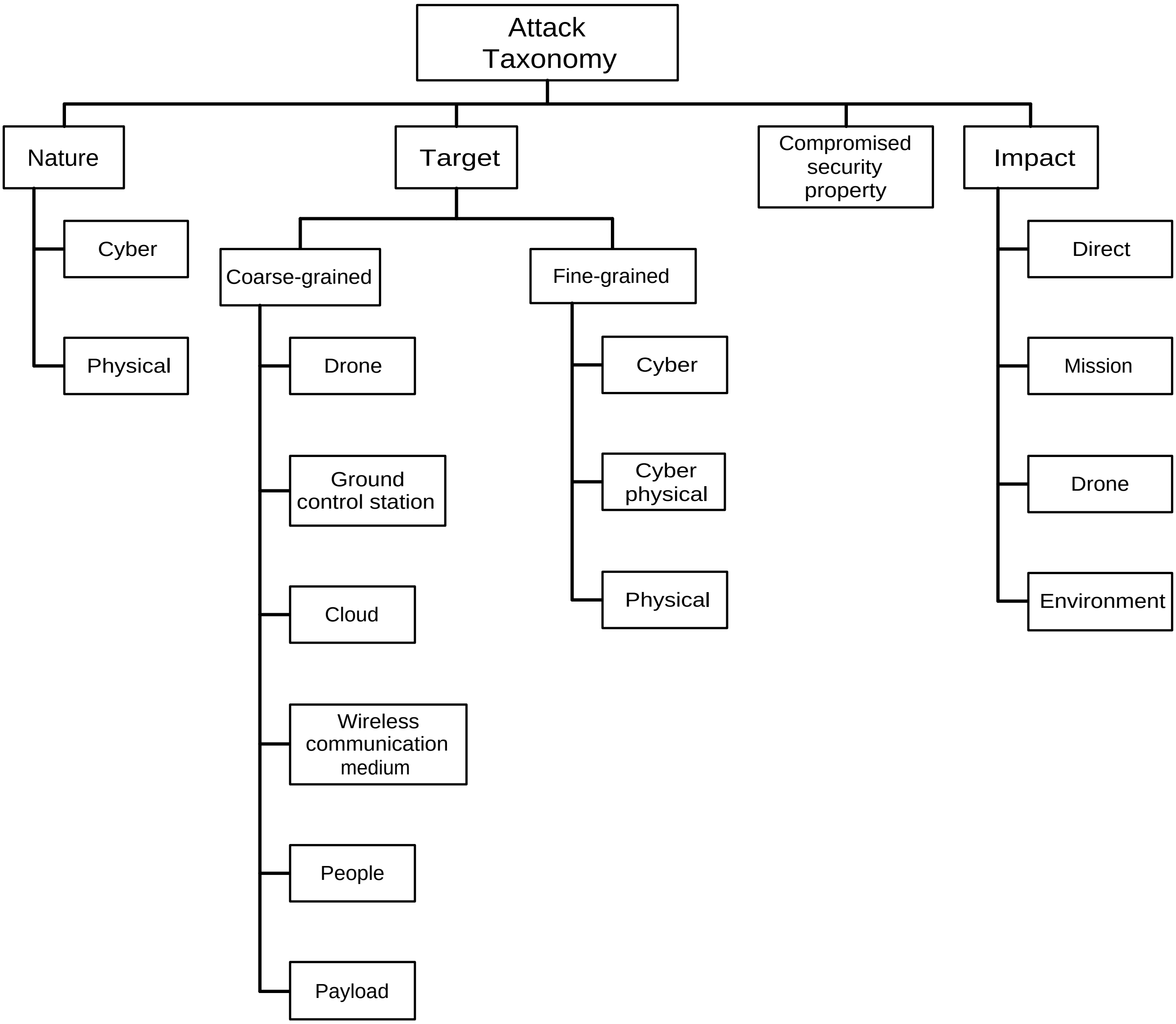

Figure 6: IoD Attack taxonomy

from one impact to another. The states of the FSM are Data Compromise (DC), Unauthenticated Access (UA), Communication Loss (CL), GPS Loss (GL), Trajectory Manipulation (TM), Operation Disruption (OD), Drone Hijacking (DH), Drone Capture (DT), Drone Damage (DD), Payload Loss (PL), and Environmental Impact (EI). The different chains of impact can be expressed, as shown in Table 5 and Table 6, as regular expressions over an alphabet

$$\Sigma = \{DC, UA, CL, GL, TM, OD, DH, DT, DD, PL, EI\}$$

We use two basic operations in regular expressions to express the chain of impact: (1) choice among alternatives, which is indicated by the character "|", and (2) concatenation, which is indicated by juxtaposition (without character).

4.4. Cyber attacks

4.4.1. Attacks targeting drones

- **Attacks targeting flight control system**
  - Manipulation of captured footage: This attack targets low-altitude UAVs, which rely on the video captured by their cameras for navigation and collision avoidance. An attacker with a high level of knowledge of the flight control system can replace the genuine footage with a fabricated one.
  - Manipulation of flight controller: If the attacker can manipulate the parameters of the flight controller by injecting false information or through malicious software, it is possible to disrupt the drone's operations.
- **Attacks targeting transmission system**

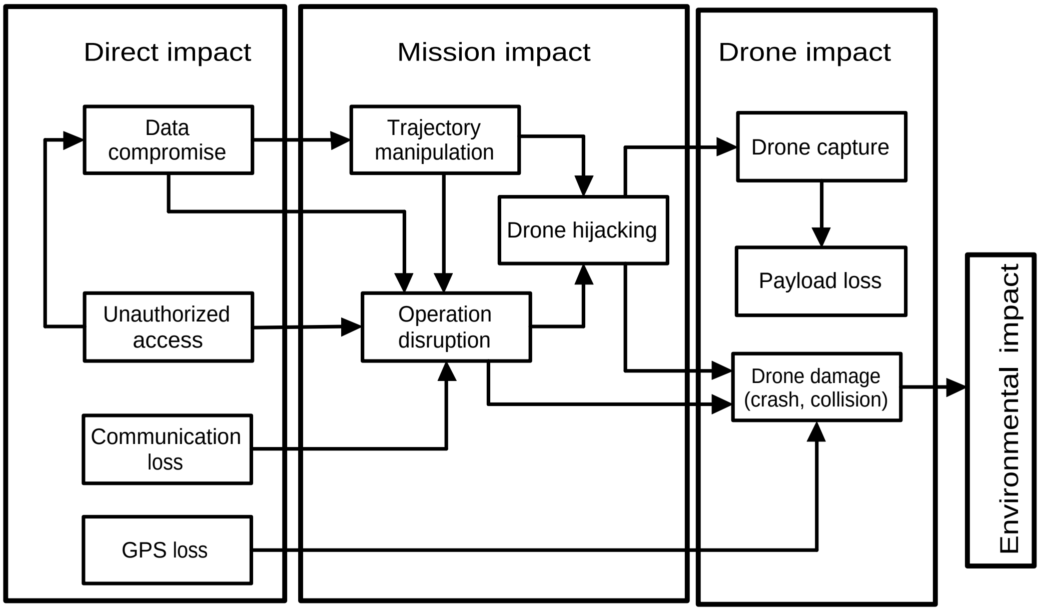

Figure 7: Chain of impact

- Flooding attack: In this attack, the intruder floods the drone with random commands, which prevents its transmission system from processing legitimate commands. This denial of service attack might discharge the drone's battery. Moreover, the attacker can prevent communication and consume the bandwidth by continuously sending random commands or control signals [188].

- **Attacks targeting sensors**
  - False sensor data injection: By injecting false sensor data, an attacker can disrupt the operation of the drone [3]. Examples of sensors that can be manipulated are infrared, radar, and electro-optical sensors. This attack targets the drone sensors asset and needs a high knowledge of the drone parameters to succeed.

- **Attacks targeting GPS receiver**: As GPS signals are unencrypted and unauthenticated, they could be targeted by GPS spoofing and GPS jamming attacks.
  - GPS spoofing: An attacker could send fake GPS signals to make the GPS receiver compute the wrong geographic coordinates. In this way, the attacker could hijack the drone and take control of its flight trajectory.
  - GPS jamming: It is possible to jam the GPS signals and prevent them from reaching the drone, which leads to the drone crashing.

4.4.2. Attacks targeting ground control station

- Manipulation of flight control commands: If the attacker can access the ground control system, it is possible to send malicious flight control commands to the drone, which could disturb its mission and could lead to a drone crash.

- Compromising the mission planning system: The role of the mission planning system is to assign and schedule flight missions of the drone or a fleet of drones. If the logic of the mission planning system is compromised through malware, the mission of the UAV system will fail.

4.4.3. Attacks targeting wireless medium

- Unauthorized disclosure of communication: As drones communicate through the wireless medium, interception of the exchanged message is an easy task, especially for attackers equipped with adequate materials. These intercepted messages, i.e., telemetry feeds and GCS commands, can be analyzed; hence, critical and confidential data might be revealed. An eavesdropping attack is difficult to detect as the attacker does not alter the exchanged message. However, deploying a strong encryption mechanism can mitigate this kind of passive attack.

- Signal spoofing: As signals are unencrypted and unauthenticated, the transmission systems cannot confirm their authenticity, and hence spoofed signals from the drones to GCS or vice versa could negatively disrupt the drone operations.

- Signal jamming: Signals are easily jammed, and the attacker interferes with communication between drones or between a drone and the ground control station, which could disable the communication and therefore put the system out of service. It could also disrupt

Table 5
Cyber attacks

Coarse-grained asset	Fine-grained asset	Attack	Vulnerability	Security objectives	Impact
Drone	Flight control system	Captured footage manipulation	Knowledge of system parameters that allows access to flight controller	Integrity	$(DC\ OD\ DH)\mid DC$
		Manipulation of flight controller parameters	Parameters are based on input that could be malicious	Integrity, Availability	$(DC\ OD\ DH\ DT)\mid(DD\ EI)$
	Transmission system	Flooding attack	It is easy to flood the channels with commands issued from unauthorized access	Availability	$CL\ OD\ DD\ EI$
	Sensors	False sensor data injection	directed energy that controls the electromagnetic spectrum	Integrity	$DC\ OD\ DD\ EI$
	GPS receiver	GPS spoofing	GPS signals are unauthenticated and unencrypted	Authentication, Integrity	$TM\ DH(DC\mid(DD\ EI))$
		GPS jamming	It is easy to jam GPS signals	Availability	$GL\ DD\ EI$
Ground control station	Ground control system	Manipulation of flight control commands	Flawed access control	System integrity, Availability	$OD((DH\ DT)\mid(DD\ EI))$
	Mission planning system	Compromising the logic of the mission planning system	Flawed system design	System integrity, Availability	$TM\ OD\ DD\ EI$
Wireless medium	Transmitted signal	Unauthorized Disclosure of Communication	Unencrypted communication	Confidentiality	DC
		Signal spoofing	Signals are unauthenticated and unencrypted	Authentication, Integrity	$DC\ OD\ ((DH\ DT)\mid(DD\ EI))$
		Signal jamming	It is easy to jam signals	Availability	$CL\ OD\ DD\ EI$
Cloud	Database	False data injection	Exploiting database vulnerabilities	Integrity	DC
	Data processing model	Adversarial learning	Knowing values that trick the model	System integrity	$OD\ ((DH\ DT)\mid(DD\ EI))$
People	Operator	Identity theft	Flawed access control/ social engineering	Authentication	$UA\ OD\ ((DH\ DT)/(DD\ EI))$
Drone, GCS	Transmission system	Man-in-the-middle attack	Flawed authentication	Authentication	$UA\ OD\ ((DH\ DT)/(DD\ EI))$
Drone, GCS, people	Ground control system, Software, people	Identity spoofing	Flawed authentication	Authentication	$UA\ OD\ ((DH\ DT)/(DD\ EI))$
Drone, GCS, people	Flight control system, Software, ground control system, Pre-operator	Malicious software	Flawed system design, malicious developer	Integrity	$DC\ OD$

drone operations as important command messages could not reach the drone, leading to crashes or collisions.

4.4.4. *Attacks targeting people*

Social engineering attacks such as phishing and spear phishing aim to lure drone operators into clicking on malicious links and downloading malicious attachments, compromising their devices. A Watering hole attack is also a social engineering technique where the attacker infects

Table 6
Physical attacks

Coarse-grained asset	Attack	Vulnerability	Security objectives	Impact
Drone	Weather condition threats	vulnerable to bad weather conditions	Availability	$(TM\|OD\|GL)DD\ EI$
	Civic challenges	Presence of static and dynamic obstacles	Availability	$DD\ EI$
	Battery depletion	Resource-constrained battery	Availability	$DD\ EI$
	Node tampering	Lack of physical security	Availability, Confidentiality	$DC\ OD$
	Physical capture	Lack of physical security	Availability, Confidentiality	$DC\|(DC\ OD)\|OD$
	Malicious drone injection	Lack of physical security	Confidentiality, Authentication, Integrity	$UA\ DC\ OD$
	Malicious code injection	Lack of physical security	Integrity, Availability	$UA\ OD$
	Malicious code modification	Lack of physical security	Integrity, Availability	$UA\ OD$
	Theft and vandalism	Flying within a visual distance	Availability	DD
	Interceptor drone	Flying within a visual distance	Availability	DD
	Physical social engineering	Non-compliance with security policy	Availability, Confidentiality, Integrity	$DC\ OD$
Ground control station	Node tampering	Lack of physical security	Availability, Confidentiality	$DC\ OD$
	Malicious code modification	Lack of physical security	Integrity, Availability	$UA\ OD$
	Malicious code injection	Lack of physical security	Integrity, Availability	$UA\ OD$
	Physical damage	Lack of physical security	Availability	DD
	Physical social engineering	Non-compliance with security policy	Availability, Confidentiality	$DC\ OD$
	Physical capture	Lack of physical security	Availability, Confidentiality	$DC\|(DC\ OD)\|OD$
People	Harming operator	Lack of physical security	Availability	OD
Payload	Theft, interceptor drone	Flying with a visual distance	Availability	$DT\ PL$

existing websites that users visit. This way, the users could download malware or be redirected to other websites to access the operator's device or network.

4.4.5. Attacks targeting the cloud

For IoD, the cloud system comprises two components: (1) a database of information sent by the drones and (2) the processing model to analyze the drones' data. The database could be compromised in the cloud due to many attacks [282]. Also, adversarial learning could target the processing model by injecting specific malicious input to mislead the model into making wrong decisions.

4.4.6. Attacks targeting many assets

- Identity spoofing: an attacker can spoof the identity of a legitimate user to get access to the IoD system. Moreover, an attacker can deploy a malicious drone with a spoofed identity to interact with other drones or the GCS. The lack of an efficient authentication mechanism allows an attacker to claim a legitimate identity and, therefore, access drones' carried data or request malicious action.

- Man-in-the-Middle attack: In this attack, a malicious deployed drone (or malicious GCS) tricks the communicating parties by making all exchanged messages pass through it. In this attack, generally launched between a drone and the GCS, the malicious entity first intercepts the message sent by the GCS (respectively sent by the drone) and then sends a modified version to the drone (respectively sent by the GCS). The communicating parties believe that they communicate directly with each other; however, the reality is that each one is communicating with a malicious entity. MIM can have several impacts ranging from eavesdropping the communication to taking control of the drone.

- Malicious Software: Malware such as Trojans, backdoors, and keyloggers can target the different assets of IoD systems, such as drones and GCSs, and result in disastrous impacts. There is an already available malware that targets the IoD, known as Maldrone [21]. Maldrone first opens a backdoored connection with its botmaster, thus enabling the reception of commands and taking control of the drone. The developer could initially implement the malicious software into the drone or access the drone through a malicious update of the firmware, operating system, and other installed applications. The drone vendors releasing software updates could be infected by attackers, so that the drone software is also infected.

- Denial of service attack: It aims to disturb the drone or network operation or to exhaust drones' resources through the following:
  - Jamming attack: the attacker interferes with communication between drones or between a drone and the ground control station. A jamming attack stops the drone and ground controller communication, putting the system out of service.
  - Denial of Service (DoS): Drones are characterized by limited resources. An attacker can exploit this characteristic to launch a DoS attack through excessive utilization of resources. DoS attacks can also be achieved by sending successive unnecessary requests to the drone, making it unable to respond to legitimate user requests.
  - Commands flooding: In this kind of DoS attack, the intruder floods the victim drone with random commands, consuming the victim's computation power and possibly discharging its battery. Moreover, the attacker can prevent communication and consume the bandwidth by continuously sending random commands or control signals [188].

4.5. Physical attacks

Besides the cyber attacks investigated above, IoD is also vulnerable to many physical attacks/threats. These types of attacks target the hardware components. For example, an attacker gains physical access to the IoD environment to destroy IoD devices and obtain sensitive information, leading to IoD devices malfunctioning or preventing the accomplishment of their missions. Their presence supposes an additional risk that should be considered. This section presents possible physical attacks targeting the IoD environment's physical assets (IoD devices).

- Weather condition threats: Drones are vulnerable to bad weather conditions since they may lead to deviations in their trajectories. Strong winds put the drone out of balance, and rain can damage the circuits. Harsh weather conditions, such as icing, freezing rain, thunderstorms, and clouds, can impact the drone's stability, operation, and travel distance and eventually cause accidents due to its lightweight design and battery dependence. Furthermore, weather conditions, turbulence, and ice storms can significantly affect cyber performance, resulting in GPS failure or a lost link state.
- Civic challenges: Dynamic obstacles or the presence of civic constituents pose a challenge to UAVs and may ultimately cause damage to the drone if they are hit. Civic components such as trees, buildings, street lights, electric cables, and poles are essential examples of such challenges as they may interfere with the drone path.
- Battery depletion: In the IoD environment, resources are limited; thus, an attacker can exploit excessive resource utilization. To do so, the attacker enables excessive services, which increase the resource depletion rate (battery) and thereby reduce the performance of the IoD in the target missions. This could lead to mission failure, drone crashes, and damage to its components.
- Node tampering: The attacker physically accesses the drone and tampers with its data and its software to get full control over the IoD environment and get sensitive and confidential information.
- Physical capture attack: Drones are not physically protected in the IoD environment. Therefore, drones are prone to physical capture attacks. An attacker having physical access to the drone can damage the drone's components, hence affecting the drone's operation. Another scenario is that the attacker can use the extracted data stored in the captured drones to disrupt communication between other nodes in the IoD environment. In this case, the drone will send false alerts to interrupt the correct functioning of the IoD. In such situations, an attacker may capture the IoD devices and switch off the services assigned to the entire IoD or alter the configuration settings, resulting in multiple mission failures and collisions.
- Malicious node injection: The attacker physically adds a fake node between legitimate nodes in the IoD network. Hence, the attacker grants access to sensitive information and controls data exchanged between IoD nodes.
- Physical damage: The attacker physically damages IoD components, thereby causing the unavailability of services.
- Malicious code injection: This attack focuses on physically introducing a malicious code into the IoD nodes, allowing the attacker to gain access to the IoD environment.
- Malicious code modification: With malicious code modification, the attacker can gain unauthorized access to the IoD network. The difference between this

attack and the malicious code injection attack is that the attacker does not inject new malicious codes into the physical component; instead, it modifies the current algorithms. The adversary exploits this attack to access the drone's control unit to alter its configuration, thereby interrupting its correct functioning. This attack can be cascaded to a UAV swarm.

- Theft and vandalism: As the drones fly within a visual distance, it makes them a prime target for theft and vandalism, which can be achieved using different methods ranging from an anti-drone rifle, and hostile drones, to a simple dart gun. The attacker uses these tools to destroy the drone and perform illegal activities such as stealing the package/cargo handled by the drone.
- Interceptor drone: Another approach to disable and crash drones is adopting another drone ("Interceptor Drone") equipped with interception tools. The interceptor drone attaches a net gun to it to stop the propellers from turning and causing the drone to crash, thereby causing harm to people and destroying facilities and the drone itself. Other drones are equipped with laser guns that emit a high-energy laser beam that causes a drone to burn in the air, fall to the ground, and possibly cause harm to third parties.
- Physical social engineering: The drone and the ground station are vulnerable to malicious hardware attacks. Whenever the attacker is granted access to the UAV flight control system and ground control unit, he can install additional components that give him control over the IoD and get sensitive data. Such an attack is conducted during the maintenance of the drone. On the other hand, hardware trojans, like backdoors, are inserted in the UAV's computation chips to compromise security mechanisms and lead to catastrophic consequences.

4.6. Risk assessment

Table 8 and Table 9 present the risk assessment of the different cyber and physical attacks respectively, which can target the IoD . The risk [248] is expressed as a function of the likelihood of the attack and the corresponding impact.

$$Risk = Likelihood \times Impact$$

To estimate the likelihood of the attack, we need to determine the extent to which the threat agent can exploit the vulnerability successfully. We assign two values to likelihood:

- High: The threat actor requires minor or no knowledge about the target system, limited expertise, and limited resources to exploit the vulnerability.
- Low: The threat actor requires detailed knowledge about the target system, a high level of expertise, and significant resources to exploit the vulnerability.

We assign the following values to impact:

- Low: In case of direct and mission impact.
- Moderate: In case of drone impact.
- High: In case of environmental impact.

Based on the likelihood and impact values, we assign fives values to the risk, i.e., insignificant, low, medium, high, and extreme, as shown in Table 7.

Table 7
Risk matrix

Likelihood/Impact	Low	Moderate	High
Low	Insignificant	Low	Medium
High	Medium	High	Extreme

In Table 8, we can notice that the risks, which are related to Flooding attacks, GPS spoofing, and GPS jamming, are extreme, as it is easy for the adversaries to access and compromise their corresponding assets, i.e., Transmission system and GPS receiver, and these attacks can damage the environment. This indicates that the above-mentioned attacks require greater attention and stronger countermeasures than other attacks. We can also notice that the risk related to a False data injection attack is insignificant since access to the cloud database is difficult and requires expertise and effort. Only stored data are compromised if the attack occurs, and the impact does not move to the drone or the environment. The rest of the risks are either low or medium.

In Table 9, weather conditions' threats, and civic challenges are considered extreme risks. For instance, weather conditions threats can easily affect the flying trajectory of the drone, damage its circuit, and damage the environment. Civic challenges can also cause damage to the drone and the environment. The risk related to interceptor drones and payload theft is high, especially when the drone flies within the visual distance of the adversary or the range of interception tools. The likelihood of these attacks is low because they require knowledge, expertise, and resources that are only within reach of expert people. As for drone security, physical access to the drone and tampering with its data and software is difficult and requires knowledge and expertise; thus, the likelihood of the attack is low. In case of a successful physical access attack, the impact can be either direct or mission, and therefore the risk is assigned an insignificant value. The risk could increase if another attack is launched to exploit the compromised data and software. As the ground control station is a secure facility, the likelihood of launching successful attacks is low. The risk is insignificant in the case of malicious node injection, malicious code modification, and physical and social engineering. In case of node tampering and physical capture, the mission of drones, which are associated with the ground control station, is affected, and hence the risk increases to low.

Table 8
Risk assessment of cyber attacks

Coarse-grained asset	Fine-grained asset	Attack	Likelihood	Impact	Risk
Drone	Flight control system	Captured footage manipulation	Low	High	Medium
		Manipulation of flight controller parameters	Low	High	Medium
	Transmission system	Flooding attack	High	High	Extreme
	Sensors	False sensor data injection	Low	High	Medium
	GPS receiver	GPS spoofing	High	High	Extreme
		GPS jamming	High	High	Extreme
Ground control station	Ground control system	Manipulation of flight control commands	Low	High	Medium
	Mission planning system	Compromising the logic of the mission planning system	Low	High	Medium
Wireless medium	Transmitted signal	Unauthorized Disclosure of Communication	High	Low	Medium
		Signal spoofing	High	Low	Medium
		Signal jamming	High	Low	Medium
Cloud	Database	False data injection	Low	Low	Insignificant
	Data processing model	Adversarial learning	Low	High	Medium
People	Operator	Identity theft	Low	High	Medium
Drone, GCS	Transmission system	Man-in-the-middle attack	Low	High	Medium
Drone, GCS, People	Ground control system, Software, people	Identity spoofing	Low	High	Medium
Drone, GCS, People	Flight control system, Software, ground control system, Pre-operator	Malicious software	Low	Moderate	Low

Table 9
Risk assessment of physical attacks

Coarse-grained asset	Attack	Likelihood	Impact	Risk
Drone	Weather conditions threats	[Low, High]	High	[Medium, Extreme]
	Civic challenges	[Low, High]	High	[Medium, Extreme]
	Battery depletion	Low	High	Medium
	Node tampering	Low	Moderate	Low
	Physical capture	Low	Moderate	Low
	Malicious drone injection	Low	Low	Insignificant
	Malicious code injection	Low	Low	Insignificant
	Malicious code modification	Low	Low	Insignificant
	Physical damage	Low	Moderate	Low
	Interceptor Drone	High	Moderate	High
	Physical social engineering	Low	Low	Insignificant
	Theft and vandalism	Low	High	Medium
Ground control station	Node tampering	Low	Moderate	Low
	Malicious node injection	Low	Low	Insignificant
	Malicious code modification	Low	Low	Insignificant
	Physical social engineering	Low	Low	Insignificant
	Physical damage	Low	Moderate	Low
	Physical capture	Low	Moderate	Low
People	Physical attack against operator	Low	High	Medium
Payload	Theft	High	Moderate	High

5. IoD Security Countermeasures

In this section, we discuss the security features provided by the drone operating system. We also present the cyber and physical countermeasures proposed in the literature for IoD and propose a taxonomy that classifies them.

5.1. Taxonomy of countermeasures

We classify the countermeasures, as shown in Figure 8, as follows:

- *Drone operating system security countermeasures*: They represent countermeasures that provide security to the drone operating system and test its security properties. The description of these countermeasures is presented in Section 5.2.

- *Technical countermeasures*: A countermeasure is considered technical if it involves technologies such as cryptography tools and IDSs, and they can be classified as: cyber and physical countermeasures.

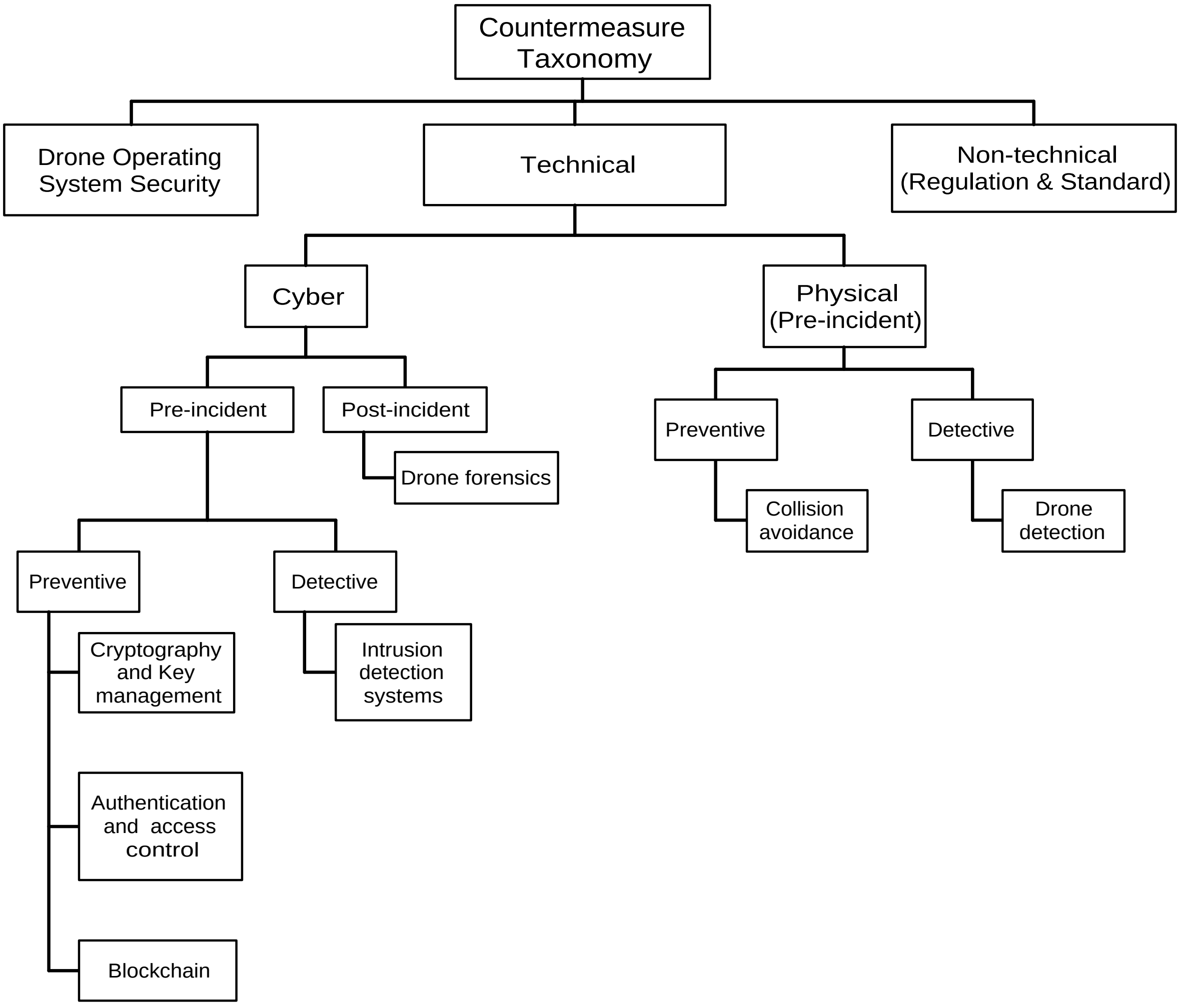

Figure 8: IoD countermeasure taxonomy

- *Cyber countermeasures*: We categorize them as: pre-incident and post-incident.
  - *Pre-incident countermeasures*: They represent the countermeasures implemented and deployed before the occurrence of security incidents and can be classified as: preventive and detective.
    - *Preventive*: They correspond to the actions required to prevent the attack from occurring. We can find three types of countermeasures:
      1. Cryptography and key management: These countermeasures are described in Section 5.3.1, and summarized in Table 10.
      2. Authentication and access control: These are described in Section 5.3.2, and summarized in Tables 11, 12, and 13.
      3. Blockchain-based solutions: These countermeasures are described in Section 5.3.3.
    - *Detective*: These countermeasures correspond to the IDSs, which are designed to detect the occurrence of attacks. The IDSs are described in Section 5.3.4, and summarized in Table 14.
  - *Post-incident (Recovery) countermeasures*: They correspond to the actions required to recover data from drones, and investigate incidents using forensics methods, which are described in Section 5.3.5, and summarized in Table 15.
- *Physical countermeasures*: They correspond to the actions required to deal with the physical attacks, and they are further classified as:
  - Preventive: They represent the collision avoidance methods, which are described in section 5.4.1

  - ∗ Detective: They represent the drone detection methods described in section 5.4.2.

- *Non-technical countermeasures*: These countermeasures include the regulations and standards to ensure IoD security, which are described in Section 5.5. One of these regulations' primary objectives is to allow drones' free movement within their specified territories.

5.2. Drone operating system security

The drone operating system represents an interface between the drone hardware and the application software/user. The operating system manages the drone hardware and other external devices, e.g., it controls the flight controller and takes input from the other instruments. It also embodies instructions for executing the application software. Unmanned aerial systems require secure, reliable, and compact software platforms. A real-time operating system (RTOS) is specially developed for resource-constrained and security-sensitive environments [181]. RTOS is used in systems requiring a response within very specific time limits. The system's reliability depends not only on the correctness of results but also on how fast the response is provided by the system [337]. Rani et al. [243] implemented and tested a hacking procedure on a commercial UAV known as Parrot AR.Drone by performing a cyber attack to take complete control over the UAV and expose the security vulnerabilities in commercial UAVs. The communication system's weaknesses were exploited to access the device, where the Robot Operating System (ROS) tools were used to control it by altering the flight path. It was demonstrated that a hacker could cause irrecoverable damage to the UAV and take over the UAV by compromising the communication links between the UAV and the operator. The hacker joystick was used in the experiments to control the Parrot AR.Drone, and various new commands were executed when the user was disconnected from the system. The authors also concluded that no system is completely secure because of the inherent shortcomings in the operating system that can lead to potential vulnerabilities. Pike et al. [238] focused on software integrity attacks related to modifying the control flow of a program. Code injection and return-to-libc attacks are examples of conventional methods for launching attacks against software integrity. Attacks related to control flow are pretty common, and various protection methods have been introduced to tackle such attacks, for example, canaries [93] and address-space layout randomization [271]. However, researchers have developed various ways to bypass these protections using methods such as return-oriented programming. Another technique, known as control-flow integrity (CFI) [2], is considered hard to exploit. It uses run-time checks to ensure that a program follows its static control-flow graph. The research community has recommended this technique as a potential candidate for protecting program integrity. Hence, the authors in [238] proposed a CFI-aware real-time operating system, called TrackOS, to provide CFI protections for critical embedded software in real-time embedded systems. In TrackOS, there is built-in support to perform CFI checks over various tasks, and these tasks do not need any specific run-time modifications or instrumentation to be examined. TrackOS overcame the delay and jitter issues associated with CFI program instrumentation. Instead of instrumenting a program, a separate monitor task performs the CFI checks on various untrusted tasks. The monitor task is a privileged task scheduled by the TrackOS, and it has access to the memory of other tasks. Dey et al. [74] studied security vulnerabilities related to Parrot Bebop 2 and DJI Phantom 4 Pro drones that use BusyBox, which is a Unix-based operating system. They also presented some defense mechanisms against the identified security vulnerabilities. They concluded that the Phantom 4 Pro is a highly secure and robust commercially available drone; however, it still requires further improvements and extensive security analysis. On the contrary, Parrot Bebop 2 drone lacked security measures; hence it is unsafe for personal or commercial usage. Lee et al. [166] proposed a security framework that operates in ROS for an unmanned aerial system (UAS) and explained the vulnerabilities. The framework focuses on security issues related to flight missions and the overhead caused by using additional security elements. The performance of the proposed framework is evaluated in both native and non-native ROS environments. The ROS uses a publisher-subscriber model for communication between different components that constitute the robot. Two nodes that exchange node information via the master node communicate messages using the publishing and subscribing functions as required. The security analysis shows that ROS lacks the essential security elements, and malicious nodes can also be connected in addition to the normal nodes. Moreover, breaking into the network is simple, and false injection and masquerade attacks are also possible. The false data can be transferred to the subscriber if the attack publisher establishes communication (through the master node) with the subscriber about the topic. In case of a successful attack, the attacker can destroy the system if the flight controller cannot control the altitude and exact position in the underlying environment.

5.3. Cyber countermeasures

5.3.1. Cryptography and Key management

Table 10
Summary of cryptography and key management solutions for the Internet of drones

Scheme	Year	Network model	Security mechanism	Security analysis	Advantage (+)	Performance analysis
Alrayes et al. [17]	2022	Drones	ECC-based El-Gamal encryption	N/A	+ Simulation analysis	Improved MES and PSNR
Ozmen et al. [230]	2019	Drones, recipients (i.e., Zone Service Providers, control stations, or servers), and trusted key generation center	Self-certified cryptography	Random oracle model and implementation on two drone processors (i.e., 8-bit AVR and 32-bit ARM)	+ Secure against Existentially Unforgeability under Chosen Message Attack + Secure against indistinguishability under chosen message attack	Offers up to 48 times less energy consumption compared to standard techniques.
Haque et al. [106]	2017	Base station and drones	Identity-based encryption Selective encryption technique Data hiding mechanism	Informal security analysis	+ Forward and backward secrecy + Resilience against node capture attack	Less memory and less communication
Wang et al. [309]	2017	LTE-based UAV control network (UAV, GCS, GRS, LTE)	Handover key management scheme	Informal security analysis	+ One-hop forward and backward key separation + Key separation under compromise of the first and the last GRS	More handover options
Sahingoz [254]	2013	Wireless Sensor Network and UAVs	Mobile Certification Authority (MCA)	N/A	+ Implementation on Sun SPOT motes	Improve scalability of key distribution
Chen et al. [57]	2018	Users, drones, GCS, cloud, and communication channel	Secure light-weight network coding pseudonym scheme	Formal analysis	+ Implementation on Android ARM-based 1 GHz processor	Achieves the highest unconditional security level compared secure Hash-based pseudonym scheme Reduce more than 90% of processing time as well as 10% of energy consumption
Demeri et al. [72]	2020	Wireless sensor nodes, Unmanned Aerial Systems, and communication channel	Combined public and secret key secure data delivery system	N/A	+ Implementation on F450 ARF quadcopter drone	Successful demonstration of the system in a flight test

Table 11
Summary of authentication and access control solutions for the Internet of Drones (Part 1)

elated to Parrot Bebop 2**Scheme**	**Year**	**Network model**	**Authentication model**	**Security analysis**	**Advantage (+)**	**Limitation (-)**	**Performance analysis**
Pu et al. [240]	2022	There are two communication entities: 1) drones and 2) zone service provider	Drone and Drone	Formal security verification using AVISPA tool	+ Establish a secure session key between drone and drone	- Location privacy	Medium communication cost
Bera et al. [38]	2021	The network model consists of three parts: drones, ground station server, and trusted commanding room	Mutual authentication	Formal security verification under AVISPA tool, random oracle model, informal security analysis	+ Secure against replay and man-in-the-middle attacks	- Trusted entity is required	Low computation cost for drone and GSS
Ko et al. [147]	2021	The network model consists of four parts: drones, users, ground station server, and certificate authority	Mutual authentication	BAN Logic, Scyther tool	+ Achieves perfect forward secrecy, perfect backward secrecy, and non-repudiation	- Certificate Authority is required	Implemented on a real UAV and Linux-based ground control station
Jan et al. [128]	2021	The network model consists of five parts: drone's service provider, ground station, drones, user, and certificate authority	Mutual authentication	Random Oracle Model, Verification tool ProVerif2	+ Resistant against stolen verifier attack, privileged insider attack, denial of service, replay attack, spoofing attack	- Certificate Authority is required	Low storage and computation cost
Zhang et al. [341]	2021	The network model consists of three parts: drones, users, and ground control server	User authentication and mutual authentication	Real-Or-Random (ROR) model, informal security analysis	+ Achieves User anonymity, and untraceability, perfect forward security, biometric template privacy	- Vulnerable to spoofing attack	Efficiency is slightly lower than symmetric cryptographic algorithms
Tanveer et al. [300]	2021	The network model consists of three parts: users, ground station, and drones	User and mutual authentication	Random oracle model, verification using Scyther tool, informal security analysis	Secure against replay, Man-in-the-middle attack, Stolen Smart Device/Card, password Guessing	- Known session key	Low storage, computational, and communication overhead
Khalid et al. [139]	2021	The network model consists of three parts: user, drones, and ground control server	User authentication	Informal security analysis	+ Resistant against replay, impersonation, known session key	- No formal security analysis is provided	Low computation costs
Hussain et al. [120]	2021	The network model consists of three parts: user, drone, and ground control server	Mutual authentication	Random oracle model	+ Ensure Anonymity and Untraceability + Secure against user/GCS/drone impersonation, Offline Password Guessing, Password Change	- Vulnerable to session key disclosure attacks	Medium communication and computation cost
Chaudhry et al. [51]	2021	The network model consists of two parts: drone, and ground station	Inter-drone and drone to ground station authentication	Real-or-Random (ROR) model	+ Resistant against replay, drone capture, drone impersonation, MIM, temporary secrets leakage	- Insecure against private key leakage of control server	Medium computation cost
Nikoog Hadam et al. [223]	2021	The network model consists of three parts: users, drones, and control server	Mutual authentication	Random oracle model, validation under Scyther tool	+ Achieves Anonymity, perfect forward secrecy	- Trusted entity is required - Vulnerable to spoofing attack	Low computation and communication overhead
Jan et al. [127]	2021	The network model consists of three parts: users, GCC, and drone	Information authentication	ProVerif2 and Real-Or-Random (ROR) model	+ Resistant against drone capture, man-in-the-middle, stolen verifier, replay, user impersonation, server impersonation, privileged insider attacks	- Known session key attack	Low storage and computation costs

Table 12
Summary of authentication and access control solutions for the Internet of Drones (Part 2)

Scheme	Year	Network model	Authentication model	Security analysis	Advantage (+)	Limitation (-)	Performance analysis
Alladi et al. [13]	2020	The network model consists of three parts: ground station, leader drones, and surveillance/mini drones	Mutual authentication	Security verification using Mao and Boyd logic	+ Achieves physical and session key security	- Vulnerable to spoofing attack	Medium communication cost
Cho et al. [61]	2020	The network model contains four parts: drones, ground station, certificate authority, and operator	Mutual Authentication	Formal security analysis using ProVerif tool	+ Provides revocability and pseudonymity + Resilient to known session key attack	- Location privacy is not considered	High communication cost
Ali et al. [11]	2020	The network model contains four parts: remote drone, drone user, ground station server, control room	Mutual Authentication	Random oracle model	+ Anonymity and untraceability of user + Protection against replay attack	- Identity privacy is not considered	Low communication cost
Ever [80]	2020	Hierarchical wireless sensor network architecture	Mutual authentication	Informal security analysis	+ Resilient to sensor node capture attack + Resilient to spoofing attack	- Location privacy is not considered	Medium energy saving
Chen et al. [53]	2020	The network model contains four parts: ground control station, player (mobile device), manufacturer (UAV), and trusted authority center	Mutual Authentication	Formal security verification under BAN logic	+ Provides the integrity and confidentiality + Availability and prevention of DoS attack	- known session key attack	Medium energy-saving
Mandal et al. [187]	2020	A large number of IoT smart devices are installed with cloud servers and trust authority	Mutual Authentication	Formal security verification under AVISPA tool	+ Secure against the online password guessing attack and gateway node impersonation attack + Anonymity and untraceability preservation	- Vulnerable to spoofing attack	Low communication cost
Zhang et al. [344]	2020	The network model contains three parts: drones, mobile users, and control server	Mutual Authentication	Random oracle model	+ Provides anonymity with untraceability + Resilient to drone capture attack	- Non-repudiation is not considered	Low communication cost
Hong et al. [113]	2020	Unmanned aerial vehicle cluster networks	Aggregate authentication	Random oracle model	+ Coalition attack resistance + Secure under computational Diffie-Hellman assumption	- known session key attack	Can reduce the communication and storage cost
Srinivas et al. [289]	2019	The network model contains four parts: remote drone, drone user, ground station server, control room	Mutual Authentication	Formal security verification under AVISPA tool	+ Secure against the denial-of-service attacks + Freely password/biometric change	- Vulnerable to spoofing attack	Medium energy-saving
Tian et al. [303]	2019	The network is composed of three major entities: UAVs, mobile edge computing devices, and a trusted authority	Predictive authentication	Cryptographic assumptions	+ Detects replay attacks + Security on repudiation threat	- Desynchronization attacks and known-key attacks are not considered	Medium communication cost
Cao et al. [45]	2019	The network model considers two types of devices, namely, 1) smart device and 2) dumb device	Mutual authentication	Implementation using Raspberry Pi 3	+ Resistant against four attacks, including man-in-the-middle attack, message replay attack, impersonation attack, and eavesdrop attack	- The mobile edge computing devices are not considered	Medium communication cost

Table 13
Summary of authentication and access control solutions for the Internet of Drones (Part 3)

Scheme	Year	Network model	Authentication model	Security analysis	Advantage (+)	Limitation (-)	Performance analysis
Choudhary et al. [63]	2019	The system model consists of the following three communication links: Drone to Drone links, Drone to Device links, and Virtual links.	User authentication	Simulation-based evaluations	+ Prevention of coagulation attacks + Detecting changes to the UAV-waypoints	- Location privacy	Medium communication cost
Chen and Wang [57]	2018	A cellular wireless network consisting of a set of drones connected to a cellular network, ground users, and ground base stations	User authentication	Cryptographic assumptions	+ Guarantee the unlinkability of locations + Data ownership privacy	- Known session key attack	High communication cost
Wazid et al. [317]	2018	The network model consists of various drones deployed in the different zones which can send data to the server	Authentication with key agreement	Formal security verification using AVISPA tool	+ Resist against privileged-insider and offline password guessing attack	- The mobile edge computing devices are not considered	High communication cost
Cheon et al. [59]	2018	Remotely-controlled drones	User authenticity	Random oracle model	+ Can detect four attack scenarios, including, tapping signal, network attack, controller attack, and attack on encrypted data	- Non-repudiation is not considered	High communication cost
Sun et al. [296]	2017	A ground control center with four types of nodes, including relay node, common senor node, cluster head node, and Sink node.	Watermark authentication	Security requirements	+ Robust against five attacks, namely, data transmission delay, packets forging, data tampering, data replay, and selective forwarding	- The Brute-force attack is not considered	Medium energy saving
Yoon et al. [333]	2017	The network model comprises three parts, including middleware, ground station, and UAVs.	Mutual authentication	Implementation using Raspberry Pi 3	+ Resist against the DoS attack	- Vulnerable to replay attack	High communication cost
Shoufan [279]	2017	The network model contains a typical flight setup with three parts, including, a UAV, UAV operator, and a radio-control transmitter	Continuous authentication	Machine learning-based evaluation	+ Detect malicious commands stemming + Identify authorized operators	- Privacy-preserving is not considered - Vulnerable to data replay attack	Low communication cost
Won et al. [321]	2017	Drone-based smart city applications	Data authentication	Game theory	+ Ensures the confidentiality of messages + Provides non-repudiation and authenticated key agreement	- Known session key attack	Low communication cost
Haque and Chowdhury [106]	2017	Hierarchical UAV network architecture	Data authentication	N/A	+ Provides network flexibility + Create trust and negotiate keys	- Vulnerable to spoofing attack	Medium communication cost
Wang et al. [309]	2017	LTE-based UAV control network	Authentication with key agreement	Cryptographic assumptions	+ Maintains a secure communication key of a ground relay station in service	- Identity privacy is not considered	High communication cost

As explained in Section 4.4 and Section 5.2, the communication links in IoD are unencrypted and could be compromised. To deal with this issue, it is important to deploy cryptography-based mechanisms that ensure secure communication among the entities of IoD. IoD's cryptography and key management solutions are summarized in Table 10. Ozmen et al. [230] proposed IoD-Crypt, a lightweight self-certified cryptographic system that aims to meet the requirements of resource-constrained IoD. IoD-Crypt is shown to ensure authentication and confidentiality of communication. It also reduces the certification overhead, i.e., it incurs up to 13 and 48 times less energy consumption than public-key primitives on two common drone processors, namely 8-bit AVR and 32-bit ARM, respectively. Haque et al. [106] proposed an Identity-Based Encryption (IBE) that offers better overhead efficiency as it does not need to use certificates as in public-key systems. It also employs a selective encryption algorithm that only encrypts some parts of the messages, which incurs less overhead. In addition, data hiding is also used to improve the confidentiality of messages. Wang et al. [309] proposed a handover key management scheme for the LTE-based UAV control network. To perform initial authentication, they employed the authentication and key agreement procedure and root key agreement between a UAV and Ground Relay Station (GRS). When a UAV moves from a GRS to a neighboring GRS, a new Access Stratum (AS) key is established between the UAV and the new GRS and is separated from the old AS. Security analysis has shown that the scheme does not reveal the AS key, as it ensures (a) one-hop forward and backward key separation and (b) key separation under the compromise of the first and the last GRS. Sahingoz [254] proposed a key management system for WSNs that leverages a UAV to distribute asymmetric keys to sensor nodes. Neighboring sensor nodes authenticate each other through their respective public keys. After that, they use the public keys to agree on the pairwise session key for the rest of the communication. Chen et al. [57] focused on decoupling the IoD cloud data that are stored in the cloud from the owner's pseudonyms. To this end, they proposed a two-tier coding method to mix the user identity with watchword/seed and then generate two keys: one key for certification and another one for anonymization. Compared to the secure hash-based pseudonym scheme, the network coding method can provide unlinkable pseudonyms to unconditional security level for Real-time Object Tracking Application (ROTA) [155]. It can also reduce more than 90% of processing time and 10% of energy consumption. Demeri et al. [72] designed and implemented Secure Aerial Data Delivery with Lightweight Encryption (SADDLE) on Fo450ARF quad-copter drone. SADDLE is a combined public and secret key secure data delivery system to generate bi-nodal secret session keys. To this end, some encryption primitives are used, such as Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol and Advanced Encryption Standard (AES-128). Alrayes et al. [17] applied Artificial Gorilla Troops Optimizer (AGTO) algorithm with an ECC-Based ElGamal encryption technique to generate an optimal key. The latter is used by drone-based emergency monitoring systems to encrypt the transmitted images. Simulation analysis showed that the peak signal-to-noise ratio (PSNR) and the mean square error (MSE) were improved under all images compared to other optimization algorithms.

5.3.2. *Authentication and access control*

As shown in Section 4.4, the signals are unauthenticated, and it is impossible to confirm their authenticity, which allows the injection of spoofed signals. To deal with this issue, it is important to deploy authentication mechanisms that ensure the authenticity of only legitimate entities in IoD. The authentication and access control solutions for the IoD are summarized in Table 11, Table 12 and Table 13. Sun et al. [296] proposed a data authentication scheme based on the message authentication code (MAC) for UAV communication. The scheme uses two phases: (1) data authentication and (2) cluster watermark authentication. The data authentication phase is used at the cluster head node to filter out the fake packets, while the cluster watermark authentication phase is used at the sink node to verify the authenticity and integrity of the data. The security analysis shows that Sun et al.'s scheme [296] is robust against five attacks, namely data transmission delay, packet forging, data tampering, data replay, and selective forwarding. To solve the problem of deauthenticating the drone in a hijacked environment, Yoon et al. [333] proposed an authentication system for UAV communication. The network model comprises three elements: middleware, ground station, and UAVs. The basic idea of the system is to use encrypted channels between these parts. Shoufan [279] designed a continuous authentication for UAV communication and considers a network model that contains three elements: a UAV, a UAV operator, and a radio-control transmitter. The scheme authenticates the behavior of the UAV operator, defined by the sequence of flight commands sent from the operator to the UAVs. Based on the assumption that each operator has a unique behavioral pattern, it is possible to identify authorized operators aiming at hijacking the UAVs.

Cho et al. [61] proposed a secure authentication framework named SENTINEL for the IoD infrastructure. SENTINEL framework creates a flight profile code for a UAV with a flight schedule. It records the flight profile code and its flight schedule in a centralized database accessible by the ground terminals. blueTo authenticate the communication between drone and drone, Pu et al. [240] proposed a mutual authentication and key agreement scheme, named PMAPD2D, which is used to establish a secure session key between drone and drone.

Srinivas et al. [289] proposed TCALAS, which is a temporal credential-based anonymous lightweight user authentication scheme for IoD. TCALAS uses three authentication factors: password, mobile device, and biometrics. Ali et al. [11] revealed that Srinivas et al.'s scheme [289] cannot withstand stolen verifier attacks. Hence, they proposed an improved IoD scheme, iTCALAS, based on the temporal credentials and lightweight symmetric key primitives. In order to provide data confidentiality and mutual authentication for mobile sinks used in the IoD applications, Ever [80] introduced a secure authentication framework, which is based on elliptic-curve cryptosystems. Chen et al. [53] proposed a traceable and privacy-preserving authentication, which combines hash function, digital signature, and elliptic curve cryptography for UAV applications. Mandal et al. [187] presented a user access control scheme based on certificateless-signcryption, named CSUAC-IoT. The scheme uses the following three authentication factors: a mobile device, personal biometrics, and user's password.

To provide the authentication with privacy preservation for IoD, Tian et al. [303] proposed an authentication scheme using mobile edge computing. More precisely, Tian et al.'s scheme [303] considers three significant elements, i.e., UAVs, mobile edge computing devices, and a trusted authority. Based on the online/offline signature, one-time random nonces, and timestamps, Tian et al.'s scheme can detect replay attacks and provide security on repudiation threats. Besides, to authenticate the IoT devices in air-ground collaborative surveillance operations, Cao et al. [45] proposed a lightweight authentication scheme, which is based on covert channels in the physical layer. The network model considers two types of devices, namely, 1) smart devices and 2) dumb devices. To resist against four attacks, including man-in-the-middle attack, message replay attack, impersonation attack, and eavesdrop attack, Cao et al.'s scheme [45] combines the benefits of two concepts: covert channels and physical layer fingerprints. Zhang et al. [344] proposed a lightweight authentication and key agreement scheme based on the bitwise XOR operations and only secure one-way hash function. Wang et al. [309] provided an LTE-based architecture to enhance the coordination of UAV control. Then, they presented a scheme of transfer key control for the LTE-based UAV control network. The security analyses show that the proposed scheme ensures the security of a communication key of a ground relay station in service, although the neighboring GRSes are affected.

To support user revocation, non-repudiation, and authenticated key agreement for the IoD, Won et al. [321] proposed a certificateless signcryption tag key encapsulation mechanism named eCLSC-TKEM, which is based on a certificateless data aggregation protocol. Wazid et al. [317] proposed a lightweight user authentication system where a user in the IoD environment requires access to the data directly from a UAV. The proposed system can resist node/sensing device/drone impersonation attacks. Alladi et al. [13] proposed a two-stage lightweight mutual authentication scheme for SDN-backed multi-UAV networks, which can provide independent aliasing, perfect forward secrecy, and perfect backward secrecy. Hong et al. [113] proposed a data aggregate authentication scheme, named IBE-AggAuth, for unmanned aerial vehicle cluster networks. The IBE-AggAuth scheme uses ID-based encryption and the elliptic curve computational Diffie-Hellman method to reduce computation and communication costs and provide data security. To enable real-time performance for autonomous safety flight, Cheon et al. [59] do not keep the secret keys for encryption on the drone. Instead, they proposed a linearly homomorphic authenticated encryption scheme named LinHAE. This scheme is secure against eavesdropping and forgery attacks.

Bera et al. [38] proposed ACPBS-IoT, an access control protocol for battlefield surveillance in drone-assisted IoT. ACPBS-IoT ensures mutual authentication between a drone and a GCS and sharing a session key. Security analysis shows that ACPBSIoT can resist different attacks, including impersonation, privileged-insider, replay attack, Man-in-the-middle attack, and Ephemeral Secret Leakage (ESL) attacks. Ko et al. [147] proposed a security protocol for military applications, consisting of two components: the first establishes authentication among the UAVs, and the second ensures authentication between a UAV and the GCS. Formal security analysis shows that the protocol can ensure mutual authentication, non-repudiation, perfect forward secrecy, and perfect backward secrecy. It can also resist man-in-the-middle and DoS attacks. Jan et al. [128] proposed an authentication protocol for IoD based on a hash message authentication (HMACSHA1). The protocol incurs less overhead with respect to computation and storage and is also formally analyzed and shown to be resistant against known attacks such as stolen verifier attacks, privileged insider, denial of service, replay, and spoofing attacks.

Zhang et al. [341] proposed three-factor authentication and key agreement protocol for IoD. The protocol employs an elliptic curve function named FourQ and a pre-calculation technique called Boyko-Peinado-Venkatesan (BPV). The security analysis shows that the protocol ensures essential security properties such as perfect forward secrecy. Experimental tests on Raspberry Pi B+ demonstrate that FourQ is five times faster than the conventional elliptic curve. Tanveer et al. [300] proposed RAMP-IoD, Robust Authenticated Key Management Protocol for IoD. RAMP-IoD is based on two lightweight cryptographic primitives: Authenticated Encryption with Associative Data (AEAD) and elliptic curve. RAMP-IoD is secure against different attacks, including replay, man-in-the-middle, stolen smart device/-card, and password-guessing attacks. It also incurs low computation, communication, and storage overheads. Khalid et al. [139] proposed a two-factor authentication scheme for drones based on an asymmetric cryptographic method. The authors showed that the proposed scheme offers less computation cost than RAMP-IoD [300] and is resistant to many attacks, such as replay, impersonation, and available session keys.

Hussain et al. [120] proposed an authentication scheme between a pair of users and drones based on symmetric encryption and elliptic curve cryptography. Based on formal security analysis, the scheme provides anonymity and untraceability and is secure against different attacks, including user/GCS/drone impersonation, offline password guessing, and password change. In [323], it was shown that Hussain et al.'s scheme is vulnerable to drone capture, privileged insider, and session key disclosure attacks. Chaudhry et al. [51] designed GCACS-IoD, a certificate-based access control scheme that provides two types of authentication: inter-drone and drone to the ground station. The scheme can resist replay, drone capture, drone impersonation, man-in-the-middle, and temporary secret leakage attacks. In [70], it was proved that GCACS-IoD is insecure against private key leakage of the control server. Nikooghadam et al. [223] proposed an authentication scheme for drone-assisted smart city surveillance. The scheme is based on elliptic curve cryptography, which considers three elements: users, drones, and control servers. It provides anonymity and perfect forward secrecy while incurring low computation and communication overhead. Jan et al. [127] proposed a scheme focusing on information authentication instead of identity authentication. They assumed that initially, the users, the drones, and the ground control station mutually authenticate each other. The scheme is resistant to drone capture, man-in-the-middle, stolen verifier, replay, user impersonation, server impersonation, and privileged insider attacks. It also incurs less storage and computation overheads.

5.3.3. Blockchain-based solutions

Blockchain technology can be effectively applied in almost all domains, especially for the IoD [82, 84, 87, 14]. To address the security vulnerabilities in the IoD, the blockchain technology [193] is a feasible solution with enormous potential. Sharma et al. [276] proposed a neural-blockchain combination for edge-enabled UAV networks. The blockchain network is used for reliable communications using distributed ledgers, which can help flatten services on the IoD. To maintain the reliability requirements of the blockchain network, a hybrid neural model is proposed. The operating drones in the defined network are configured via the drone caching framework based on the blocks. Ferrag and Leandros [83] proposed an intrusion detection and blockchain-based delivery framework, named DeliveryCoin, for drone-delivered services. The hash functions and short signatures are employed by the blockchain for achieving privacy preservation, while the machine learning techniques are employed for intrusion detection. In addition, a UAV-aided forwarding mechanism, named pBFTF, is adopted for achieving consensus inside the blockchain-based delivery platform.

Islam et al. [126] proposed a blockchain-enabled data acquisition scheme to provide security and data integrity through unmanned aerial vehicle swarm and blockchain technology. Specifically, the unmanned aerial vehicle swarm shares a shared key with the IoT devices to maintain communications before initiating data acquisition. The digital signature algorithm and hash bloom filter are employed in order to resist and avoid two types of man-in-the-middle attacks: manipulation and eavesdropping. Fernández-Caramés et al. [81] proposed a drone-based and blockchain-based system for Industry 4.0, where the drones are used to collect the inventory data, and the blockchain technology is used to enable the creation of smart contracts. Aggarwal et al. [7] designed a secure data dissemination scheme based on blockchain technology and game theory for the IoD. A forger node selection algorithm and Proof-of-Stake (PoS) algorithm are employed to verify and validate blocks. Throughout evaluation performance, the proposed scheme shows that it can provide identity anonymity, data integrity, accountability, authorization, and authentication, compared to four related schemes [173, 171, 135, 277].

Bera et al. [37] introduced an access control system based on blockchain technology, which can enable safe interaction between UAVs as well as between UAVs and the ground station server. The protected data collected by the ground station server are used to form transactions, and the latter is used to create blocks. The blocks are then added to the blockchain through the cloud servers connected to the ground station server via the ripple protocol consensus algorithm. Lei et al. [167] proposed an advanced and systematic approach based on blockchain technology that incorporates on-demand verification, forwarding strategy, and interest-key-content binding to detect poisonous content efficiently. In order to support decentralized interest-key-content binding storage and enable the detection of internal attackers, the authors developed an adaptive and scalable delegated consensus algorithm over named data networking for mission-critical unmanned aerial vehicle ad hoc networks.

Islam and Shin [124] proposed a secure outdoor health monitoring system based on blockchain technology and UAV consolidated with MEC. In the proposed system, Health Data (HD) are collected from sensors carried by the users, and this health data is forwarded to the next MEC server via a UAV. Before being transmitted to MEC, the health data is encrypted to protect against cyber attacks. García-Magariño et al. [97] designed an agent-based approach based on the blockchain technology and trust policies for ensuring the surveillance and security of UAV networks as well as to detect compromised UAVs. For disaster rescue, Su et al. [293] proposed a lightweight framework, named LVBS, for secure data sharing based on blockchain technology and unmanned aerial vehicles. The LVBS framework adopts a credit-based consensus algorithm to safely and immutably track node behavior and record data transactions with increased efficiency and security to achieve consensus. Islam et al. [123] proposed an intelligent surveillance architecture based on blockchain technology, in which a drone monitors and uses a two-phase authentication process to check vehicles at sea. The experimental results demonstrate that the proposed authentication scheme is significantly faster and uses less power than existing authentication schemes. Islam and Shin [125] proposed a blockchain-based data acquisition scheme, in which data are first encrypted and then transferred to the MEC server with the help of a UAV. Han et al. [105] used blockchain technology to detect global navigation satellite system signal attacks for UAV networks.

Mitra et al. [199] implemented a public blockchain-based testbed for drone-assisted wildlife monitoring. The drones collect data from IoT devices, which are attached to animals. The collected data of each flying zone is sent to its corresponding Ground Station Server (GSS). The latter creates blocks and validates them using the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. To this end, the GSS broadcasts the block to the P2P network of GSS nodes. Alsamhi [18] focused on the synergy between federated learning and blockchain in IoD. The drones collect data from the smart environment, run local models, and share the models with their neighbors and ground server to allow collaborative learning and improve model accuracy. The role of blockchain is to allow privacy-preserving data sharing in the IoD. Irshad et al. [122] proposed a BOD5-IOD, blockchain-oriented Data Delivery and Collection (DDC) system to ensure authentication between drones and their corresponding ground control servers. The DDC records all the transactions among the system nodes and generates their private blocks. In [23], the blockchain model was proposed to hide the identity of drones during message exchanges. Sing et al. [283] defined an architecture named blockchain of drones, where each drone creates blocks and communicates with other drones and the ground station. They proposed the Advanced Byzantine Fault Tolerance (ABFT) protocol as a consensus mechanism for blockchain. ABFT offers higher scalability than other Byzantine Fault Tolerance (BFT) systems like PBFT (Practical BFT), hBFT, and ReBFT. Nguyen et al. [221] proposed a blockchain-based architecture for conducting search and rescue missions using IoD. The architecture consists of small and big drones and edge servers to perform offloading operations. Allouch et al. [15] proposed UTM-Chain, a blockchain-based solution for unmanned traffic management. UTM-Chain provides secure sharing of data between UAVs and their ground control stations. In [71], blockchain and EdgeDrone concept [210] are integrated to ensure secure data delivery for forest fire surveillance applications. The authors in [195] proposed PROACT: a lightweight consensus protocol for IoD based on accumulated trust [196]. The blockchain is maintained and updated by the GCSs and the cloud servers. Certain GCSs are selected to become BC miners based on their trust ratings. Each GCS validates the transactions that it receives from drones before forwarding them to the set of trusted GCSs (TGCSs), which act as miners. The trusted GCSs assume the responsibility of mining new blocks, while all GCSs participate in the process of block validation. Each GCS accumulates trust points in order to become a TGCS. Each time a GCS validates a transaction correctly, it receives positive trust points and vice versa. When the GCS accumulates enough trust points over a sufficiently long period, it is selected by the TGCSs to become a BC miner. One of the TGCSs acts as the blockchain orderer that receives block requests from the TGCSs and orders the corresponding blocks in the blockchain, which allows multiple TGCSs to produce their blocks and add them to the blockchain in parallel. A TGCS collects the transactions from its drones, sends a request to the blockchain orderer, creates its block, and waits for its turn to add the block to the blockchain. When its turn arrives, the TGCS adds the previous block's hash to its block and broadcasts the latter to the TGCSs to add it to the blockchain.

5.3.4. Intrusion detection systems

As presented in Section 4.4, some attacks against IoD, such as DoS attacks, cannot be prevented. Hence, there is a need for an intrusion detection system (IDS), which is the second line of defense when the intruder has already entered the network and tampers with its performance. IDSs can generally be classified as rule-based or misuse detection, where the former lie on specific rules that define the presence of an intruder, and the latter learn the regular operation of the system and trigger an alarm once a deviation happens. Most of the traditional techniques mentioned in the literature suffer from either poor performance or high overhead [73]. Once an IDS is deployed in such a complex system, like the IoD, the produced alarms must be both highly accurate to improve the security system's performance and minimal in order not to affect the correct performance of control applications that run over the medium.

Recently, several works have investigated the efficiency of an IDS for detecting attacks in a UAV environment. The different IDS methods, which are proposed for securing UAVs, are presented in Table 14. Yu et al. [335] applied snort for DoS and GPS spoofing attack detection in a simulated environment comprising a GCS and a limited number of UAVs. Condomines et al. [67] conducted both simulated and emulated tests, using paparazziUAV [1], an open-source drone hardware and software project encompassing autopilot system to better represent realistic scenarios and test the efficiency of their proposed defense mechanism. They used network traffic datasets that include anomalies to construct digital signatures in three dimensions for DoS attacks and used those signatures to detect future attacks. Although the proposed method is designed to detect both constant and progressive flash crowds, it was tested under simplistic scenarios with one attack and a limited number of valid nodes.

Hoang et al. [112] presented an IDS that combines OCSVM and K-means clustering in a UAV-aided wireless system, an idea that was presented a couple of years ago for detecting anomalies in Industrial Control Systems (ICS) [183]. The proposed method is tested on a scenario consisting of three nodes: one of them is the attacker, and only a passive attack occurs (i.e., the eavesdropping attack). Arthur [26] presented a lightweight system that can be embedded in modern UAVs for providing accurate detection of GPS spoofing and DoS attack, as well as consuming little energy from the UAV. The IDS combines Self-Taught Learning (STL) with a multiclass SVM to detect the attacker. It is tested in a realistic environment that consists of twenty UAVs, four Ground Stations, and a Control Station, making the results valuable.

Table 14
Summary of IDSs for Internet of Drones

Scheme	Year	Network model	IDS model	Security analysis	Corase-grained/Fine-grained asset	Detected attacks	Limitations
Yu et al. [335]	2019	The network is composed of a GCS and UAVs	Rule-based (Snort)	Rule-based	Wireless communication channels/Transmitted information	GPS spoofing attack DoS Attack	Simplistic scenarios
Condomines et al. [67]	2019	The network is composed of a GCS and UAVs	Combination of a linear controller/observer and spectral analysis of the traffic	Traffic signature with WLM	Wireless communication channels/Transmitted information	Constant and progressive flash-crowds	Missing accuracy and precision metrics
Hoang et al. [112]	2019	The network is composed of three nodes	OC-SVM and K-means clustering	Unsupervised learning	Wireless communication channels/Transmitted information	Detects eavesdropping attacks	Selection of features
Arthur et al. [26]	2019	The network is composed of twenty UAVs, four Ground Stations and a Control Station	Self-Taught Learning (STL) with a multiclass SVM, return-to-home mode	Anomaly-based	Wireless communication channels/Transmitted information Drone/GPS receiver	GPS spoofing and Jamming attacks	Selection of features
Tan et al. [299]	2019	Several nodes	Deep belief network (DBN) and PSO	Unsupervised learning combined with supervised learning	Wireless communication channels/Transmitted information	Several attacks	Use of KDD'99 dataset Not tested on UAVs
Vanitha et al. [306]	2020	Several nodes	Deep feed-forward neural network	Flow-based monitoring	Wireless communication channels/Transmitted information	Several attacks	Use of a simulated dataset
Sedjelmaci et al. [266]	2017	The network is composed of ground stations and UAVs	Rule-based & SVM	SSI, JITTER	Wireless communication channels/Transmitted information	False information dissemination, GPS spoofing, jamming, black hole and gray hole attack	Delay tolerant routing
Fotohi et al. [90]	2020	The network is composed of UAVs	Probability based	Human Immune System	Wireless communication channels/Transmitted information	Blackhole, Wormhole, grayhole, False information dissemination	Delay and communication overhead, probabilistic models
Straub et al. [292]	2017	N/A	N/A	Blackboard Architecture model	N/A	N/A	No validation or evaluation
Zhang et al. [342]	2018	The network is composed of UAVs and a router	Probability-based	Bayesian Nash equilibrium game theory	Wireless communication channels/Transmitted information	DoS attacks	No comparison with other methods
Ramadan et al. [241]	2021	Drones and base station	LSTM-RNN	Network traffic	Wireless communication channels/Transmitted information	Several attacks	No comparison with other methods
Ouiazzane et al. [228]	2022	Drones	Decision Tree	Network traffic	Wireless communication channels	DoS	Only one attack scenario
Whelan et al. [320]	2022	Drones	PCA & One Class Classifiers	Network traffic	Wireless communication channels	Spoofing, Jamming	One UAV was used

To secure UAVs that carry out explorations in isolated areas and to collect and send critical information about the conditions of these areas, Sedjelmaci et al. [266] implemented and tested several IDSs that can deal with several different attacks, achieving good accuracy with low false positives. Fotohi [90] proposed a novel IDS that can secure UAVs against several attacks, but at the cost of high communication overhead among nodes, to identify secure routes. Also, the proposed IDS assumes that this secure route will not change in the next communication attempt, which is not so realistic in highly mobile environments like UAVs. Sun et al. [295] proposed an IDS based on the Bayesian Nash equilibrium theory. The proposed IDS performs well in terms of accuracy, detection rate, and overhead compared to other methods, but the validation was based on probabilistic models rather than realistic datasets. In another work [292], the authors presented a theoretical model of IDS based on a Blackboard architecture, but no validation or evaluation results are provided. Zhang et al. [342] presented an IDS based on Wavelet Leader Multifractal analysis for creating signatures of traffic and evaluated their method in a hybrid experimental system using real traces. The method performs well under DoS service attacks showing high similarity rates, but no comparison with other methods is presented.

Deep learning can achieve better performance as compared to traditional machine learning IDSs, especially when massive data analysis is required [336], and thus can be used to develop IDSs for modern complex systems where massive, high-dimensional, nonlinear data must be used for training, and testing [299]. Authors in [85] conducted a comparative study of several deep learning IDS techniques using novel datasets and tried to showcase the pros and cons of each method. As also stated in [86, 306, 10], no method can be considered as the 'winner' for all attacks' scenarios, and smart combinations of techniques could be used to detect most of the abnormal situations inside the system accurately. Ramadan et al. [241] proposed a distributed IDS that is deployed on drones and the base station. Each drone runs the LSTM-RNN model to detect the attacks on the drone itself. The base station also runs the LSTM-RNN model to confirm the detected attack and notify the other drones. The authors tested their model on different datasets such as KDDCup 99, NSL-KDD, UNSW-NB15, Kyoto, CICIDS2017, and TON_IoT. Recently, the authors in [228] proposed a model based on machine learning techniques and a multi-agent system that is capable of detecting DoS attacks against drones. The detection of DoS attacks is an important countermeasure that can be used to ensure the high availability of drone systems, especially those used in emergencies. The proposed method was tested using the CICIDS2017 dataset and was proven to be very accurate. In another recent work, [30], the authors applied machine learning-based classification techniques to detect several attacks against drones. The authors used the DJI Phantom 4 drone dataset acquired from VTO Labs in this work. This dataset comprises DAT files of flight logs obtained from various flights undertaken by a single drone. The evaluation of several methods showed the superiority of the random forest algorithm. Finally, the authors in [320] combined principal component analysis (PCA) and one-class classifiers to detect attacks to be able to train the IDS using only normal data. The proposed MAVIDS can be deployed on every UAV allowing for fast detection and potential mitigation of cyber attacks even during communication errors with the GCS.

5.3.5. *Drone forensics*

Drone forensics is an emerging field within digital forensics aiming to extract and analyze evidence from a UAV and its components to identify attackers and their malicious actions [8]. Drone forensics is essential as the drone flies above populated areas and can be manipulated by radical forces and perpetrators to launch illegal activities. Although forensics investigation is well established in traditional fields, there is a lack of a standard regarding the procedures of collecting and processing evidence for a security incident in the IoD field [189]. Due to the nature of the IoD environment, several challenges obstruct the standardization of forensics procedures. First, several drone platforms and architectures make it difficult to build a standard procedure that can be applied to these various architectures and platforms. Moreover, the presence of several components and devices in the drone expands the complexity of the investigation, as the forensics analysis will have to handle the supporting devices and find and correlate the evidence collected from these different devices. Furthermore, IoD systems are generally linked to the cloud to offload resource taxing tasks [47]. This property moves the processing and handling of data from the drone to the cloud, and therefore, extends the perimeter of the incident investigation. Moreover, cloud service providers rarely cooperate with investigators, and even if cloud providers are willing to cooperate, the data may be stored across different servers and countries. This requires the permissions granted to different entities and authorities [189]. In what follows, we present the main forensics methods proposed for drones. These methods are summarized in Table 15. Clark et al. [65] noted that the DJI Phantom III drone was used in several illegal activities such as dropping bombs, remote surveillance, and plane watching. This motivated the authors to develop a DRone Open source Parser called DROP, which can analyze proprietary encrypted DAT files extracted from the drone's internal storage. The extracted data can identify drone locations over time and the flying time. However, this work is limited to only DJI drones. Renduchintala et al. [245] proposed a more comprehensive forensic framework. The authors first divided drone forensics into two categories: digital forensics and hardware/physical vehicle forensics. Digital forensics includes analyzing network traffic exchanged by drones, system logs, sensor readings, file storage systems, and camera recordings. As for hardware forensics, it includes: identifying drone type, checking for customization, carrying loads, fingerprints, and location. The authors proposed a forensic model to examine the drone's physical components. They developed a Java-based application to analyze and visualize the flight logs

Table 15
Summary of forensics methods for drones

Reference	Year	Drone Platform	Description
Horsman [114]	2016	Parrot Bebop	Recover flight data using Android and iOS devices
Clark et al. [65]	2017	DJI Phantom III	Development of open source tool called DROP able to parse proprietary and encrypted DAT files extracted from the drone's internal storage.
Azhar et al. [29]	2018	DJI Phantom 3 Professional and Parrot AR Drone 2.0	Open source forensic tool
Roder et al. [247]	2018	DJI Phantom 3	Guideline for drone forensics
Renduchintala et al. [245]	2019	DJI Phantom 4 and the Yuneec Typhoon H	A forensic framework that includes physical and digital forensics able to analyze log parameters using a JavaFX application.
Iqbal et al. [121]	2019	Parrot Bebop 2 drone	Acquire flight data, extract drone-pruned media, and establish ownership
Salamh et al. [255]	2019	Yuneec typhoon H	Technical forensic process
Kao et al. [134]	2019	DJI Spark	Collect and analyze of artifacts from the recorded flight data
Yousef et al. [334]	2020	DJI Mavic 2 Pro, DJI Mavic Air, DJI Spark, and DJI Phantom 4	Data analysis
Stanković et al. [290]	2021	DJI Mini 2	Forensics investigation on data stored on mobile devices and SD cards
Kumar et al. [161]	2021	DJI Phantom 4 Pro, Yuneec Typhoon H, and Parrot Bebop 2	Analysis of GPS logs
Salamh et al. [257]	2021	Phantom 4 and Matrice 210	Testing available forensic software tools
Parghi et al. [231]	2022	Yuneec Typhoon drone	Analyze data from storage of flight paths
Husnjak et al. [119]	2022	DJI Mavic Air	Forensic investigation
Dhamija et al. [75]	2022	GCS of a Parrot Bebop drone	Testing different open-source tools

of the drones. However, this work is limited to only log files in CSV file format. Iqbal et al. [121] investigated a Parrot Bebop 2 drone to acquire flight data, extract drone-pruned media, and establish ownership. However, their work is limited to small-scale drones.

Barton and Azhar [32] and [29] used Kali Linux to provide open-source forensic tools to perform forensic analysis using two drones, namely DJI Phantom 3 and A.R Drone. To visualize the flight path, the open-source GeoPlayer tool was used. To this end, the authors analyzed and investigated the recorded flight logs on both the internal memory of the UAV and the controlling application.

Horsman [114] provided the results of a digital forensic investigation of a test Parrot Bebop UAV and was able to recover flight data using Android and iOS devices. Roder et al. [247] proposed a guideline for drone forensics using DJI Phantom 3 drone as a case study. Salamh et al. [256] discuss the static and live digital evidence challenges related to UAV and possible Anti-UAV forensic techniques. In [255], the authors presented a technical forensic process for analyzing digital evidence, which is extracted from the Yuneec Typhoon H drone. Kao et al. [134] collected and analyzed artifacts from the recorded flight data extracted from the DJI Spark drone and its associated devices, such as SD cards and mobile phones. Stanković et al. [290] conducted a forensics investigation of DJI Mini 2 and its associated data, which are stored on mobile devices and SD cards. Yousef et al. [334] extracted and analyzed data from four drones: DJI Mavic 2 Pro, DJI Mavic Air, DJI Spark, and DJI Phantom 4. The analysis results indicate that applying forensics on these drones is not easy due to their improved security. Hence, it is essential to develop novel forensic processes and tools. In [231], the authors analyzed the digital evidence like log files, pictures, and videos from the storage of the Yuneec Typhoon drone. Kumar et al. [161] focused on analyzing GPS logs from drones to identify the crime location and previous flight paths. To this end, they developed a tool designed for three drone models: DJI Phantom 4 Pro, Yuneec Typhoon H, and Parrot Bebop 2, which converts GPS data to an understandable format. Husnjak et al. [119] found a significant amount of data by applying a forensic investigation on DJI Mavic Air and its associated mobile app DJI GO 4. Salamh et al. [257] tested available forensic software tools on two drone models: Phantom 4 and Matrice 210. In [75], different open-source tools are applied to the GCS of a Parrot Bebop drone.

5.4. Physical countermeasures

Collision avoidance is one of the challenges faced by UAVs. In shared airspace, a UAV can collide with both stationary and moving obstacles and other aircraft, which would endanger its mission. On the other hand, when assigning a mission to UAVs with a planned path over multiple waypoints to a drone connected to the Internet, the UAV could encounter obstacles not considered in the planned trajectory. Indeed, several collision avoidance methods have been put forward for the collision problem.

In addition, the extensive use of drones has created safety threats, which have increased the number of drones that cause accidents and unforeseen incidents. These issues have highlighted the need for methods intended to track and detect drones used for malicious activities.

5.4.1. Collision avoidance methods

The collision avoidance methods fall into four categories, namely path planning approaches, geometric-based approaches, potential field approaches, and vision-based approaches.

(*1*) Path planning approach: It aims to find a short and collision-free flight trajectory towards the desired target where obstacles are static and pre-known. In general, path planning approaches are further divided into the following three categories of algorithms [346, 330, 286, 244]:

- *Graph-based algorithms:* Graph-based search algorithms have become popular in route planning. This method divides the search space into a grid and represents the grid by a set of cells. Among the most relevant methods, we can find Djikstra's algorithm [215, 192], A* [184], Lazy θ* [218] ,D*-Lite [115, 207, 96], and the Kinematic A* [6]. These algorithms are applied to the UAV path planning [192] because they provide fast search capabilities but do not produce smooth trajectories and are not suitable for large areas.

- *Randomly sampling search algorithms:* In this category, the environment is sampled into a set of nodes that randomly search for a free-collision path. Algorithms like Rapidly-exploring Random Tree (RRT) [329, 94, 328, 260], Dynamic Domain RRT (DDRRT) [328], RRT* [76, 319], Probabilistic Roadmap (PRM) [6], Rapidly exploring Random Belief Tree (RRBT) [5], and Visibility Graph [117] belong to randomly sampling search algorithms and have been used in the UAV domain. Random sampling search algorithms give the advantages of having a simple structure and dealing with a complex environment.

- *learning based algorithms:* They have become the most popular way to perform UAV path planning. The key idea in learning-based algorithms is to use a training process to guide the UAV in a given state. Learning-based methods give the advantage of solving complex and multi-objective problems. Some evolutionary methods have been adopted for the solution of UAV path planning. For instance, genetic algorithms have been used for single and multiple UAV path-planning [253, 235, 222, 200, 316, 288], which led to satisfactory results. The successful application of reinforcement learning for UAV path planning can be found in [343, 340, 237, 315, 49, 313].

  Other interesting approaches include the usage of neural networks in UAV path planning [158, 98, 172, 137].

(*2*) Geometric approach:

This approach aims to avoid conflicts, and collisions based on geometric characteristics analysis [232, 40]. There are two geometric collision avoidance techniques: collision cone and velocity obstacle. The collision-cone-based technique is suitable for detecting and avoiding collision between UAVs and obstacles. Both of them move in a dynamic environment [209, 270, 68, 46]. Velocity Obstacle techniques are successful at computing collision-free trajectories in a dynamic environment [88, 16, 163, 129].

(*3*) Potential field approach:

One successful approach used in collision avoidance is the Potential Field approach. Many researchers use it to solve the collision avoidance problem among UAVs and obstacles. This approach treats each UAV as a charged particle, and the repulsive forces between aircraft generate collision avoidance maneuvers. The potential field method has the advantage of simple implementation and low computational complexity and is a good solution for real-time implementation. Indeed, it was applied to UAV navigation [145, 56, 179, 246, 294, 208, 234, 55, 182, 4, 251, 176, 268]. However, it is not appropriate for a dynamic environment due to the existence of local minimum risks and poor performance.

(*4*) Vision-based approach:

Different Vision-based obstacle detection methods have been proposed to tackle the collision avoidance problem. Many researchers utilized images captured by cameras mounted on UAVs to solve the collision avoidance problem in the indoor environment [262]. Other works, such as in [186, 115, 48, 191, 242, 263], used a technique based on stereo cameras to predict the closeness of the obstacles to the UAV. This method requires a high computational cost, which is unsuitable for handling real-time situations. Due to the heavy computational capabilities, a simple vision-based collision avoidance approach was proposed in [95, 202, 9, 22, 252, 138, 148], which uses a monocular camera to generate a collision-free trajectory, where heavyweight computations are performed off-board.

5.4.2. Drone detection methods

The drone detection methods are divided into the following two categories: acoustic and optical.

(*1*) Acoustic Detection: Several works have proposed the use of acoustic sensors, as an efficient technology, to detect drones. Some studies compare acoustic signatures generated by drone's motors and rotating propellers with other collected sound signatures [24, 278, 109, 39, 198, 50, 267]. Other studies detect the sound of propellers and motors based on special microphones [108, 144]. The sound is analyzed, and acoustic features are extracted. However, weather conditions and noise affect the accuracy of detection. Moreover, the detection range is limited.

(*2*) Optical Detection:

It is worth mentioning that most of the literature has considered image data and video streams collected from cameras for drone detection. As an example, studies in [298, 175, 250] focus on detecting drones through image processing based on machine learning algorithms.

Other studies detect UAVs by detecting motion cues [116, 249], visual marks [259], shape descriptors [305] and flight pattern. In terms of advantages, camera-based detection enables long-range detection. However, detection performances are poor in bad weather conditions.

5.5. Regulations and standards

In order to protect both safety and privacy of the citizens, the EU and USA are putting into force regulations and laws. Besides safeguarding their citizens' lives, drones' free circulation within their territories is one of the primary targets of these regulations. In the EU, new drone rules came into force on the 1st of July, 2020. To be allowed to fly over the EU, both technical and operational requirements define minimum safety capabilities that a drone must have, like identification, certification, and remote pilot requirements. Moreover, operators of drones have to register in any of the Member States [201]. The Federal Aviation Administration (FAA) in the US has issued several restrictions on drone operations compared to the European environment. Pilots must obtain a Part 107 (certificate for commercial drone operations) certificate and register their UAVs to be allowed to fly over USA [197].

On top of the rules mentioned above, the UAV sector, especially in the EU, is affected by other regulations. These include the Recommendation on Cybersecurity of 5G Networks, General Data Protection Regulation (GDPR), the NIS Directive (involves the aviation sector), the Electronic Communications Code (involves electronics communications), and the Cyber Security Act (involves cyber security certification of devices and applications) that cover different aspects of security and privacy that are all directly or indirectly connected to a UAV. Especially regarding the cybersecurity Act, UAVs will need to be certified by a National Certification Authority in terms of cyber security, following the certification framework that the EU is building [33].

6. Open Issues and future directions

Although several solutions have been proposed to address the security and safety of IoD, several issues are still open and need the efforts of researchers and industry personnel.

6.1. Tracking and compliance for drone-to-everything services using blockchain technology

The tracking of components that go into drone-to-everything services is critical for ensuring safety and regulatory compliance. Blockchain technology can be used to store IoT data on shared blockchain ledgers, enabling all parties to identify the origin of components throughout the drone's life. The security and privacy of sharing this information should be carefully investigated. The key security issue is performing secure, easy, and cost-effective access authentication and authorization for drone-to-everything services. In addition, the drivers' mobility pattern is a crucial privacy issue that an attacker can learn and use for tracking the component that goes into drone-to-everything services. Thus, exploring efficient and privacy-preserving schemes based on blockchain technology is crucial to secure component tracking and compliance.

6.2. Novel Intrusion Detection Systems

Most IDS solutions in IoD focus on detecting intrusions related to wireless communications among UAVs and the ground station, but they do not cover other intrusions associated with the compromise of the ground control station, the drone, or intrusions that bypass the cloud system to manipulate stored data. Thus, future research should focus on designing novel IDSs that consider the following:

- *Extension of IDS research:* It is recommended that future research extend the IDSs to secure other components of IoD, such as drones, ground control systems, and cloud servers, and investigate their performance in detecting attacks. Another important aspect is the constant change of the network topology, similar to a vehicular network [151]. Methods that can cope with the highly dynamic situations must be developed [291] and tested in realistic scenarios, taking into consideration the interconnection with other systems as well.

- *IDS Dataset for IoD:* Most IDSs are tested on network simulators or evaluated using real experiments. They are not tested on drone datasets, except for Baig et al. [30] that used DJI Phantom 4 drone dataset. As presented in Section 5.3.4, the IDSs for IoD are tested under non-IoD network traffic datasets such as KDDCup99, NSL-KDD, UNSW-NB15, Kyoto, and CICIDS2017. Similar to IDSs in different fields [165, 269, 149, 140], the research community needs to create a Benchmark IDS dataset [281] for IoD, which consists of attacks and legitimate traffic and considers specific features of a UAV. This will help attract research attention in designing, evaluating, and comparing different IDS solutions for IoD.

- *Adversarial learning:* Adversarial machine learning is a technique that aims to deceive the learning model by manipulating the input data, which causes the model to misclassify the data. Adversarial attacks on IDSs in IoD must also be investigated, similar to the work presented in [25], where attackers manipulated the IDS itself to report false alarms, either negative or positive. As many IDSs are designed based on machine learning, future research should focus on fortifying the IDS by generating adversarial samples through Generative Adversarial Networks (GAN) and training the IDS model on them.

6.3. Security and safety co-engineering lifecycle management

Secure software development lifecycle (SSDL) is a framework that integrates security into the different phases of the software development lifecycle, i.e., requirements, design, implementation, verification, and release. Development of safety and security co-engineering lifecycle has already been addressed in cyber-physical systems and embedded systems [285, 264, 239, 304], which integrates safety and security development lifecycle in a coordinated way. Likewise, this integration could be considered as a research direction in the context of IoDs by focusing on three levels: risk analysis, countermeasures, and testing.

6.3.1. Interdependent security and safety risks

The interdependencies between cyber and safety risks examine how cyberattacks affect the physical world and compromise safety properties. Similarly, they examine how safety risks compromise cyber security objectives. In [157], several risk analysis approaches integrating security and safety risks have been proposed for cyber-physical systems. In the context of IoD, it is recommended to follow the same approach by jointly analyzing aspects related to security and safety. To this end, many formal methods can be leveraged, such as fault tree analysis and attack tree analysis, that consider both security and safety.

6.3.2. Interdependent security and safety countermeasures

Kriaa et al. [157] defined four types of security-safety interactions, i.e., conditional dependency (fulfillment of security requirements conditions safety and vice versa), mutual reinforcement (fulfillment of safety requirements contributes to security, or vice-versa), antagonism (safety and security requirements or measures lead to conflicting situations), and independency (there are no interactions between security and safety). Research efforts should consider conditional dependency and antagonism interactions. One example of security conditioning safety is that an IPS/IDS incorrectly classifies regular messages as malicious. Hence, it could affect the correct functionality of drones and compromise their safety.

6.3.3. Combined security and safety testing

Before deploying the different components of IoD, it is of paramount importance to test them to ensure that security and safety requirements are met. It has been shown in [157] that there are four types of interactions between security and safety. Similar to other domains [285], it would be recommended to develop testing and validation methodologies that combine security and safety properties in IoD.

6.4. Formal verification of IoD security

As discussed in this survey, the IoD represents a complex cyber-physical system that combines diverse multidisciplinary techniques. Therefore, governing the security issue of this system remains challenging. One research area that needs the focus of academic and industrial researchers is the formal validation of designed protocols and techniques, especially those related to security and safety. More precisely, proposed security and safety solutions must be formally proved secure to avoid disastrous consequences, primarily when IoD is used in civilian applications.

The modeling of security solutions must consider the complex aspects of the UAV as a standalone system and the network aspects when drones operate as a connected fleet. The actual adoption of IoD in civil applications has revealed that drones can operate well alone but fail to handle network-based attacks.

6.5. UAV integration with other networks

The IoD is integrated with different networks, such as 5G, IoT, Wi-Fi, and vehicular networks. This integration allows using drones as a supporting platform to improve communication performance and network coverage. On the other hand, the combined network will be exposed to emerging and complex attacks originating from IoD to harm other networks and vice-versa. These emerging attacks should be investigated using different methods, such as attack trees and attack graph analysis. This integration also requires rethinking the protocols to cope with the resource-constrained drones. We identify two types of protocols: the drones could switch to different networks during their missions, and hence they should ensure seamless, secure communication and continuous connectivity. The IoD could play the role of a relay between nodes in a network, e.g., vehicular networks. It is crucial to design an integration architecture that considers end-to-end communication and authentication protocols executed across heterogeneous networks.

6.6. Lightweight cryptographic operations

In IoD, messages are continuously exchanged between the drones and the GCS, which incurs high communication overhead. As drones operate on battery and can fly long distances, they require lightweight cryptographic protocols to secure IoD communication. To this end, some techniques could be investigated such as single-round function [224], or lightweight quantum cryptography [170, 162].

As IoD is characterized by highly dynamic topology, a dynamic cryptographic approach could also be investigated [194]. It has been recommended in [173] that drones should use homomorphic encryption to aggregate several ciphertexts into a single ciphertext without the need for decryption. More efforts could be made to further improve the efficiency of homomorphic encryption algorithms in IoD by getting inspiration from other works [107, 287, 104].

6.7. Malware detection and prevention

It has been shown that drones could be infected by malware [226]. However, there is no existing research on detecting drone malware. In [297], the malware classification model is proposed for ground control stations, but it was not tested on a drone malware dataset. Instead, it was tested on the Microsoft malware classification challenge dataset [225].

Malware detection is an old topic that has been well-investigated by academia and industry. The detection of malicious software depends on the operating system and requires specific detection features. For instance, to detect a WIN32 malicious application, the anti-malware solution [100] needs to use features like opcodes, bytecodes, Portable Executable (PE) metadata, and API calls. In the case of Android OS, anti-malware solutions [136] extract features like permissions, intents, and API calls to distinguish between benign and malicious mobile applications. The embedded applications in the drone run on specific operating systems such as RTOS [181]. Hence, to detect malicious drones, the anti-malware solution has to consider features specific to the drone OS, such as API calls and drone navigation state with respect to altitude, position, velocity, acceleration, and orientation [132]. Therefore, it is recommended that the research community investigate the topic of drone malware detection. In fact, there is still room for contributions by taking inspiration from other solutions in the literature. They can explore different approaches, such as malware detection using static and/or dynamic analysis of the code, signature-based detection, anomaly-based detection, supervised and unsupervised learning, etc.

Cybercriminals have widely used ransomware against desktop, mobile, IoT, and vehicle platforms [205, 54, 229, 118, 31]. The aim is to encrypt data or lock access to a system until the victim pays a ransom. We predict that a ransomware threat that targets drones could emerge in the short term, but by taking another form, i.e., the cybercriminal hijacks the drone and releases it when a ransom is paid. The research community could think about this issue in advance, inspired by earlier works, and come up with a malware detection system that monitors the behavior of the compromised application, and identifies the suspicious API calls in the early stages before the ransomware attack happens.

Building a public dataset for drone malware is also an option to boost this research direction, as done in other domains such as mobile malware [347, 185, 164] and IoT malware [180, 149].

6.8. Fleet of drones security

In a fleet of drones, the drones must cooperate to accomplish the group mission. If some drones are compromised or faulty, the mission will be affected. To deal with this issue, future research efforts should focus on there aspects: *trust management*, *federated learning*, and *privacy-preserving collaborative learning*

6.8.1. Trust management

To secure IoD security and ensure the fulfillment of its mission, it is important to detect compromised/faulty drones and isolate/repair them. This can be achieved by implementing a trust management mechanism that observes the behavior of drones and assigns trust or reputation values to them, which helps identify trustworthy and rogue nodes. Trust management in IoD is not well-investigated [91]. To this end, researchers could get inspiration from trust management solutions in other fields, such as IoT [20] and vehicular networks [78].

6.8.2. Federated learning

Federated learning is a technique that trains machine learning techniques across different devices holding local data without exchanging them. The devices exchange parameters, i.e., weights and biases in the case of deep learning, to build a global model shared by all nodes. For instance, each drone has a different mission experience and is targeted by other attacks. Thus, future research should investigate how to leverage federated learning and build a more robust collaborative IDS by combining the different local models.

6.8.3. Privacy-preserving collaborative learning

Fleets of drones have to adopt a collaborative model to accomplish their missions. This collaboration should ensure the privacy of sensitive data and learning models. In [43], three privacy concerns are identified, i.e., concerns related to sensitive input data during model training, during model prediction, and model sharing with other participants. If the learning process in IoD comprises private information, these concerns need to be addressed in the future work.

6.9. Policies and regulations

Governments should adopt some regulations to ensure the safety of people and properties:

- Firmer laws: Strict laws must be considered to give licenses and authorization to people who want to fly drones. Also, there should be punishments for the illegal use of drones or when drones fly over vital or forbidden areas.

- Implementation of in-depth controls: In-depth controls should be implemented to protect people and properties from the threats coming from drones, which could result in physical damage and human casualties. To this end, controls could be implemented through in-depth defense layers: deterrent, preventive, detective, and corrective, i.e., they occur when an issue is detected.

- Security governance in IoD: A security governance approach should be applied by the organizations that own or operate IoD to ensure their cyber and physical security. It involves people's roles and responsibilities, implementation of countermeasures, security and safety testing, and incidence response plans in case of a security breach or mission failure. Another aspect of security governance is to provide drone security training for drone operators so that they can understand the cyber and physical threats, how to deal with cyber and physical incidents, how to make the drone return home safely, and how to protect the critical infrastructure and assets of the organization against malicious drones.

6.10. Incident response and mission continuity

Incident response and business continuity plans are the key components of security strategies in organizations. The incident response aims to respond to and recover from incidents, whereas business continuity aims to limit the impact of incidents and ensure the timely resumption of essential operations. In the context of IoD, we can inspire security strategies to develop an incident response plan that indicates how to deal with all incidents that could occur in IoD. As the objective of IoD is to accomplish their missions, we can also think about mission continuity instead of business continuity to deal with how drones could ensure the timely

Table 16
Prioritized open issues in IoD

Open issue topic	Risk Value	Countermeasure Effectiveness	Priority Importance	Priority Ranking
Tracking and compliance for drone-to-everything services using blockchain technology	Insignificant	Preventive	3	Low
Novel Intrusion Detection Systems	Extreme	Detective	10	Medium
Security and safety co-engineering lifecycle management	Extreme	Preventive	15	High
Formal verification of IoD security	Extreme	Preventive	15	High
UAV integration with other networks	Extreme	Preventive	15	High
Lightweight cryptographic operations	Extreme	Preventive	15	High
Malware detection and prevention	Medium	Preventive	9	Medium
Fleet of drones security	Extreme	Detective	10	Medium
Policies and regulations	Extreme	Preventive	15	High
Incident response and mission continuity	Extreme	Recovery	5	Low

resumption of their operations and missions. To this end, it is vital to think about designing fault-tolerant and attack-tolerant solutions that ensure mission continuity.

6.11. Ranked open issues in IoD

In this section, we suggest ranking the above-mentioned topics related to open issues, as shown in Table 16, to identify which topics require greater attention from the research community. To this end, we propose a formal approach that considers two parameters:

- *Risk Value*: Each one of the above topics aims to address some attacks. We give priority to the topics that are associated with attacks of higher risk values. We use the risk values that are defined in Section 4.6, and range from *Insignificant* to *Extreme*, and are assigned the following values:

Qualitative value	Quantitative value
Insignificant	1
Low	2
Medium	3
High	4
Extreme	5

- *Countermeasure Effectiveness:* Research efforts should focus on proposing security countermeasures with higher effectiveness. The countermeasures are classified as: preventive, detective, and recovery.
  - The preventive countermeasures are the most effective, as they prevent the occurrence of the incident.
  - The detective countermeasures act when the incident occurs.
  - The recovery countermeasures act after an incident occurs.

  For each countermeasure type, we assign the following effectiveness values:

Countermeasure	Countermeasure Effectiveness
Preventive	3
Detective	2
Recovery	1

We define the *Priority Importance* using the following formula:

$$Risk\ Value \times Countermeasure\ Effectiveness$$

Based on the *Priority Importance* value, we define the *Priority Ranking* of the topic as follows:

$$\begin{matrix} Priority \\ Ranking \end{matrix} = \begin{cases} Low & \text{if } Priority\ Importance \in [1,5] \\ Medium & \text{if } Priority\ Importance \in [6,10] \\ High & \text{if } Priority\ Importance \in [11,15] \end{cases}$$

From Table 16, we can observe that most of the topics are associated with *Extreme* risks, which target the drone and its fine-grained assets, as shown in Table 8 and Table 9. The risk associated with *tracking and compliance for drone-to-everything services using blockchain technology* topic is insignificant, as it targets blockchain services, which are deployed in secure environments. In Table, 8, the risk of compromising the drone, specifically the flight control system, is *Medium*.

Our proposed ranking approach shows that:

- The following five topics require high attention:
  - Security and safety co-engineering lifecycle management.
  - Formal verification of IoD security.
  - UAV integration with other networks.
  - Lightweight cryptographic operations.
  - Policies and regulations.

- The following three topics require medium attention:
  - Novel intrusion detection systems.
  - Malware detection and prevention.
  - Fleet of drone security.
- The following two topics require low attention:
  - Tracking and compliance for drone-to-everything services using blockchain technology.
  - Incident response and mission continuity.

7. Conclusion

In this paper, we have provided a comprehensive survey related to the cyber and physical security of the Internet of Drones (IoD). Previous security-focused surveys on IoD had a limited scope and focused on classifying the various attacks and threats with partial coverage of cybersecurity countermeasures. We have attempted to address these gaps in this survey and presented various novelties that are not present in the existing literature. Specifically, we have proposed three taxonomies that are related to *(i)* assets of drones, *(ii)* attacks, and *(iii)* countermeasures. The proposed taxonomies allow finer-level of granularity for asset identification, which allows broader identification of possible attacks. Additionally, we have evaluated the IoD risks and identified their impacts using a novel concept, named *Chain of Impact*. We have also proposed a taxonomy of technical and non-technical countermeasures according to two implementation phases: *Pre-incident*, and *Post-incident*. In addition, we have presented the countermeasures along with their performance results and limitations. Finally, we have identified the open issues and suggested future research directions for IoD security. We have ranked the identified open issues according to the level of attention they should receive from the research community. Particularly, the interaction between security and safety, formal verification of IoD security, UAV integration with other networks, lightweight cryptographic operations, and policies and regulations should be given the highest priority.

Nomenclature

ABFT	Advanced Byzantine Fault Tolerance
AEAD	Authenticated Encryption with Associative Data
AGTO	Artificial Gorilla Troops Optimizer
AS	Access Stratum
BFT	Byzantine Fault Tolerance
BPV	Boyko-Peinado-Venkatesan
BS	Base Station
CFI	Control-Flow Integrity
CL	Communication Loss
CP	Cyber-Physical Fine-Grained Assets
CPS	Cyber-Physical System
CY	Cyber Fine-Grained Assets
DB	Deep Belief Network
DC	Data Compromise
DD	Drone Damage
DDC	Data Delivery and Collection
DDRRT	Dynamic Domain RRT
DH	Drone Hijacking
DoS	Denial of Service
DT	Drone Capture
DTN	Delay Tolerant Network
ECDH	Elliptic Curve Diffie-Hellman
EI	Environmental Impact
FAA	Federal Aviation Administration
FANET	Flying Ad-hoc Network
FSM	Finite State Machine
GAN	Generative Adversarial Network
GCS	Ground Control Station
TGCS	Trusted Ground Control Station
GDPR	General Data Protection Regulation
GRS	Ground Relay Station
GL	GPS Loss
HD	Health Data
ICS	Industrial Control System
IDS	Intrusion Detection System
IoFT	Internet of Flying Things
IoD	Internet of Drones
IoE	Internet of Everything
MAC	Message Authentication Code
MEC	Mobile Edge Computing
MCA	Mobile Certification Authority
MSE	Mean Square Error
PBFT	Practical Byzantine Fault Tolerance
PCA	Principal Component Analysis
PE	Portable Executable
PHS	Physical Systems
PHO	Physical Objects
PL	Payload Loss
POS	Proof-of-Stake
PRM	Probabilistic Roadmap
PSNR	Peak Signal-to-Noise Ratio
ROR	Real Or Random
ROS	Robot Operating System
ROTA	Real-time Object Tracking Application
RRT	Rapidly-exploring Random Tree
RTOS	Real-Time Operating System

SADDLE	Secure Aerial Data Delivery with Lightweight Encryption
SSDL	Secure Software Development Lifecycle
STL	Self-Taught Learning
TM	Trajectory Manipulation
OD	Operation Disruption
UA	Unauthenticated Access
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
VANET	Vehicular Ad-hoc Network
ZRP	Zone Routing Protocol

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.

References

[1] Paparazzi autopilot team. `https://github.com/paparazzi`. Accessed: May 13, 2021.

[2] M. Abadi, M. Budiu, U. Erlingsson, and J. Ligatti. Control-flow integrity principles, implementations, and applications. 13(1), 2009.

[3] A. Abbaspour, K. K. Yen, S. Noei, and A. Sargolzaei. Detection of fault data injection attack on uav using adaptive neural network. *Procedia computer science*, 95:193–200, 2016.

[4] H. V. Abeywickrama, B. A. Jayawickrama, Y. He, and E. Dutkiewicz. Potential field based inter-uav collision avoidance using virtual target relocation. In *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, pages 1–5. IEEE, 2018.

[5] M. W. Achtelik, S. Weiss, M. Chli, and R. Siegwart. Path planning for motion dependent state estimation on micro aerial vehicles. In *2013 IEEE international conference on robotics and automation*, pages 3926–3932. IEEE, 2013.

[6] R. K. Agarwal. *Recent advances in aircraft technology*. IntechOpen, 02 2012.

[7] S. Aggarwal, M. Shojafar, N. Kumar, and M. Conti. A new secure data dissemination model in internet of drones. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2019.

[8] A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, S. Razak, and F. M. Ghabban. Research challenges and opportunities in drone forensics models. *Electronics*, 10(13):1519, 2021.

[9] A. Al-Kaff, F. García, D. Martín, A. De La Escalera, and J. M. Armingol. Obstacle detection and avoidance system based on monocular camera and size expansion algorithm for uavs. *Sensors*, 17(5):1061, 2017.

[10] A. Aldweesh, A. Derhab, and A. Z. Emam. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 189:105124, 2020.

[11] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman. Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles. *IEEE Access*, 8:43711–43724, 2020.

[12] M. Alkhelaiwi, W. Boulila, J. Ahmad, A. Koubaa, and M. Driss. An efficient approach based on privacy-preserving deep learning for satellite image classification. *Remote Sensing*, 13(11), 2021.

[13] T. Alladi, V. Chamola, N. Kumar, et al. Parth: A two-stage lightweight mutual authentication protocol for uav surveillance networks. *Computer Communications*, 2020.

[14] T. Alladi, V. Chamola, N. Sahu, and M. Guizani. Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications*, page 100249, 2020.

[15] A. Allouch, O. Cheikhrouhou, A. Koubâa, K. Toumi, M. Khalgui, and T. Nguyen Gia. Utm-chain: Blockchain-based secure unmanned traffic management for internet of drones. *Sensors*, 21(9):3049, 2021.

[16] J. Alonso-Mora, T. Naegeli, R. Siegwart, and P. Beardsley. Collision avoidance for aerial vehicles in multi-agent scenarios. *Autonomous Robots*, 39(1):101–121, 2015.

[17] F. S. Alrayes, S. S. Alotaibi, K. A. Alissa, M. Maashi, A. Alhogail, N. Alotaibi, H. Mohsen, and A. Motwakel. Artificial intelligence-based secure communication and classification for drone-enabled emergency monitoring systems. *Drones*, 6(9):222, 2022.

[18] S. H. Alsamhi, F. A. Almalki, F. Afghah, A. Hawbani, A. V. Shvetsov, B. Lee, and H. Song. Drones' edge intelligence over smart environments in b5g: Blockchain and federated learning synergy. *IEEE Transactions on Green Communications and Networking*, 2021.

[19] S. H. Alsamhi, O. Ma, M. S. Ansari, and F. A. Almalki. Survey on collaborative smart drones and internet of things for improving smartness of smart cities. *IEEE Access*, 7:128125–128152, 2019.

[20] A. Altaf, H. Abbas, F. Iqbal, and A. Derhab. Trust models of internet of smart things: A survey, open issues, and future directions. *Journal of Network and Computer Applications*, 137:93–111, 2019.

[21] R. Altawy and A. M. Youssef. Security, privacy, and safety aspects of civilian drones: A survey. *ACM Transactions on Cyber-Physical Systems*, 1(2):7, 2017.

[22] H. Alvarez, L. M. Paz, J. Sturm, and D. Cremers. Collision avoidance for quadrotors with a monocular camera. In *Experimental Robotics*, pages 195–209. Springer, 2016.

[23] N. Andola, V. K. Yadav, S. Venkatesan, S. Verma, et al. Spychain: A lightweight blockchain for authentication and anonymous authorization in iod. *Wireless Personal Communications*, pages 1–20, 2021.

[24] M. Z. Anwar, Z. Kaleem, and A. Jamalipour. Machine learning inspired sound-based amateur drone detection for public safety applications. *IEEE Transactions on Vehicular Technology*, 68(3):2526–2534, 2019.

[25] G. Apruzzese, M. Colajanni, L. Ferretti, and M. Marchetti. Addressing adversarial attacks against security systems based on machine learning. In *2019 11th International Conference on Cyber Conflict (CyCon)*, volume 900, pages 1–18. IEEE, 2019.

[26] M. P. Arthur. Detecting signal spoofing and jamming attacks in uav networks using a lightweight ids. In *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pages 1–5. IEEE, 2019.

[27] G. S. S. Aujla, N. Kumar, S. Garg, K. Kaur, and R. Ranjan. Edcsus: Sustainable edge data centers as a service in sdn-enabled vehicular environment. *IEEE Transactions on Sustainable Computing*, pages 1–1, 2019.

[28] M. Ayamga, S. Akaba, and A. A. Nyaaba. Multifaceted applicability of drones: A review. *Technological Forecasting and Social Change*, 167:120677, 2021.

[29] M. Azhar, T. E. A. Barton, and T. Islam. Drone forensic analysis using open source tools. *Journal of Digital Forensics, Security and Law*, 13(1):6, 2018.

[30] Z. Baig, N. Syed, and N. Mohammad. Securing the smart city airspace: Drone cyber attack detection through machine learning. *Future Internet*, 14(7):205, 2022.

[31] P. Bajpai, R. Enbody, and B. H. Cheng. Ransomware targeting automobiles. In *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security*, pages 23–29, 2020.

[32] T. E. A. Barton and M. H. B. Azhar. Open source forensics for a multi-platform drone system. In *International Conference on Digital Forensics and Cyber Crime*, pages 83–96. Springer, 2017.

[33] E. Bassi. European drones regulation: Today's legal challenges. In *2019 International Conference on Unmanned Aircraft Systems (ICUAS)*, pages 443–450. IEEE, 2019.

[34] I. Bekmezci, O. Sahingoz, and Temel. Flying ad-hoc networks (fanets): a survey. *Ad Hoc Networks*, 11:1254–1270, 05 2013.

[35] B. Bellur and R. G. Ogier. A reliable, efficient topology broadcast protocol for dynamic networks. In *IEEE INFOCOM '99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No.99CH36320)*, volume 1, pages 178–186 vol.1, 1999.

[36] B. Benjdira, A. Koubaa, A. T. Azar, Z. Khan, A. Ammar, and W. Boulila. Tau: A framework for video-based traffic analytics leveraging artificial intelligence and unmanned aerial systems. *Engineering Applications of Artificial Intelligence*, 114:105095, 2022.

[37] B. Bera, D. Chattaraj, and A. K. Das. Designing secure blockchain-based access control scheme in iot-enabled internet of drones deployment. *Computer Communications*, 153:229–249, 2020.

[38] B. Bera, A. K. Das, S. Garg, M. J. Piran, and M. S. Hossain. Access control protocol for battlefield surveillance in drone-assisted iot environment. *IEEE Internet of Things Journal*, 2021.

[39] A. Bernardini, F. Mangiatordi, E. Pallotti, and L. Capodiferro. Drone detection by acoustic signature identification. *Electronic Imaging*, 2017(10):60–64, 2017.

[40] K. Bilimoria. A geometric optimization approach to aircraft conflict resolution. In *18th Applied aerodynamics conference*, page 4265, 2000.

[41] P. Boccadoro, D. Striccoli, and L. A. Grieco. An extensive survey on the internet of drones. *Ad Hoc Networks*, 122:102600, 2021.

[42] F. Boehm and A. Schulte. Air to ground sensor data distribution using ieee802.11n wi-fi network. In *2013 IEEE/AIAA 32nd Digital Avionics Systems Conference (DASC)*, pages 4B2–1–4B2–10, Oct 2013.

[43] A. Boulemtafes, A. Derhab, and Y. Challal. A review of privacy-preserving techniques for deep learning. *Neurocomputing*, 384:21–45, 2020.

[44] M. Campion, P. Ranganathan, and S. Faruque. A review and future directions of uav swarm communication architectures. In *2018 IEEE International Conference on Electro/Information Technology (EIT)*, pages 0903–0908, May 2018.

[45] X. H. Cao, X. Du, and E. P. Ratazzi. A light-weight authentication scheme for air force internet of things. *arXiv preprint arXiv:1902.03282*, 2019.

[46] C. Carbone, U. Ciniglio, F. Corraro, and S. Luongo. A novel 3d geometric algorithm for aircraft autonomous collision avoidance. In *Proceedings of the 45th IEEE Conference on Decision and Control*, pages 1580–1585. IEEE, 2006.

[47] R. Chaâri, O. Cheikhrouhou, A. Koubâa, H. Youssef, and T. N. Gia. Dynamic computation offloading for ground and flying robots: Taxonomy, state of art, and future directions. *Computer Science Review*, 45:100488, 2022.

[48] A. Chakraborty and B. Srinivasan. A novel stereo based obstacle avoidance system for unmanned aerial vehicles. *International Journal of Computer Applications*, 975:8887, 2015.

[49] U. Challita, W. Saad, and C. Bettstetter. Deep reinforcement learning for interference-aware path planning of cellular-connected uavs. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–7. IEEE, 2018.

[50] X. Chang, C. Yang, J. Wu, X. Shi, and Z. Shi. A surveillance system for drone localization and tracking using acoustic arrays. In *2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, pages 573–577. IEEE, 2018.

[51] S. A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A. K. Bashir, and Y. B. Zikria. Gcacs-iod: A certificate based generic access control scheme for internet of drones. *Computer Networks*, 191:107999, 2021.

[52] O. Cheikhrouhou and I. Khoufi. A comprehensive survey on the multiple traveling salesman problem: Applications, approaches and taxonomy. *Computer Science Review*, 40:100369, 2021.

[53] C.-L. Chen, Y.-Y. Deng, W. Weng, C.-H. Chen, Y.-J. Chiu, and C.-M. Wu. A traceable and privacy-preserving authentication for uav communication control system. *Electronics*, 9(1):62, 2020.

[54] J. Chen, C. Wang, Z. Zhao, K. Chen, R. Du, and G.-J. Ahn. Uncovering the face of android ransomware: Characterization and real-time detection. *IEEE Transactions on Information Forensics and Security*, 13(5):1286–1300, 2017.

[55] Y. Chen, J. Yu, X. Su, and G. Luo. Path planning for multi-uav formation. *Journal of Intelligent & Robotic Systems*, 77(1):229–246, 2015.

[56] Y.-b. Chen, G.-c. Luo, Y.-s. Mei, J.-q. Yu, and X.-l. Su. Uav path planning using artificial potential field method updated by optimal control theory. *International Journal of Systems Science*, 47(6):1407–1420, 2016.

[57] Y.-J. Chen and L.-C. Wang. Privacy protection for internet of drones: A network coding approach. *IEEE Internet of Things Journal*, 6(2):1719–1730, 2018.

[58] N. Cheng, W. Xu, W. Shi, Y. Zhou, N. Lu, H. Zhou, and X. Shen. Air-ground integrated mobile edge networks: Architecture, challenges, and opportunities. *IEEE Communications Magazine*, 56(8):26–32, 2018.

[59] J. H. Cheon, K. Han, S.-M. Hong, H. J. Kim, J. Kim, S. Kim, H. Seo, H. Shim, and Y. Song. Toward a secure drone system: Flying with real-time homomorphic authenticated encryption. *IEEE access*, 6:24325–24339, 2018.

[60] G. Chmaj and H. Selvaraj. Distributed processing applications for uav/drones: a survey. In *Progress in Systems Engineering*, volume 1089, pages 449–454. Springer, 08 2015.

[61] G. Cho, J. Cho, S. Hyun, and H. Kim. Sentinel: A secure and efficient authentication framework for unmanned aerial vehicles. *Applied Sciences*, 10(9):3149, 2020.

[62] G. Choudhary, V. Sharma, T. Gupta, J. Kim, and I. You. Internet of drones (iod): Threats, vulnerability, and security perspectives. *arXiv preprint arXiv:1808.00203*, 2018.

[63] G. Choudhary, V. Sharma, and I. You. Sustainable and secure trajectories for the military internet of drones (iod) through an efficient medium access control (mac) protocol. *Computers & Electrical Engineering*, 74:59–73, 2019.

[64] G. Choudhary, V. Sharma, I. You, K. Yim, R. Chen, and J.-H. Cho. Intrusion detection systems for networked unmanned aerial vehicles: a survey. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pages 560–565. IEEE, 2018.

[65] D. R. Clark, C. Meffert, I. Baggili, and F. Breitinger. Drop (drone open source parser) your drone: Forensic analysis of the dji phantom iii. *Digital Investigation*, 22:S3–S14, 2017.

[66] A. Coluccia, G. Parisi, and A. Fascista. Detection and classification of multirotor drones in radar sensor networks: A review. *Sensors*, 20(15):4172, 2020.

[67] J.-P. Condomines, R. Zhang, and N. Larrieu. Network intrusion detection system for uav ad-hoc communication: From methodology design to real test validation. *Ad Hoc Networks*, 90:101759, 2019.

[68] M. Coppola, K. N. McGuire, K. Y. Scheper, and G. C. de Croon. On-board communication-based relative localization for collision avoidance in micro air vehicle teams. *Autonomous robots*, 42(8):1787–1805, 2018.

[69] I. Dalmasso, I. Galletti, R. Giuliano, and F. Mazzenga. Wimax networks for emergency management based on uavs. In *2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL)*, pages 1–6, Oct 2012.

[70] A. K. Das, B. Bera, M. Wazid, S. S. Jamal, and Y. Park. igcacs-iod: An improved certificate-enabled generic access control scheme for internet of drones deployment. *IEEE Access*, 2021.

[71] S. Datta and D. Sinha. Besddffs: Blockchain and edgedrone based secured data delivery for forest fire surveillance. *Peer-to-Peer Networking and Applications*, 14(6):3688–3717, 2021.

[72] A. Demeri, W. Diehl, and A. Salman. Saddle: Secure aerial data delivery with lightweight encryption. In *Science and Information Conference*, pages 204–223. Springer, 2020.

[73] Z. Dewa and L. A. Maglaras. Data mining and intrusion detection systems. *International Journal of Advanced Computer Science and*

Applications, 7(1):62–71, 2016.

[74] V. Dey, V. Pudi, A. Chattopadhyay, and Y. Elovici. Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study. In *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*, pages 398–403, 2018.

[75] R. Dhamija, P. Parghi, and A. K. Agrawal. Bebop drone gcs forensics using open-source tools. In *Proceedings of the International Conference on Paradigms of Communication, Computing and Data Sciences*, pages 369–377. Springer, 2022.

[76] R. DuToit, M. Holt, M. Lyle, and S. Biaz. Uav collision avoidance using rrt* and los maximization technical report# csse12-03.

[77] E. Ebeid, M. Skriver, and J. Jin. A survey on open-source flight control platforms of unmanned aerial vehicle. In *2017 Euromicro Conference on Digital System Design (DSD)*, pages 396–402. IEEE, 2017.

[78] H. El-Sayed, H. A. Ignatious, P. Kulkarni, and S. Bouktif. Machine learning based trust management framework for vehicular networks. *Vehicular Communications*, 25:100256, 2020.

[79] Y. K. Ever]. A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. *Computer Communications*, 155:143 – 149, 2020.

[80] Y. K. Ever. A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. *Computer Communications*, 2020.

[81] T. M. Fernández-Caramés, O. Blanco-Novoa, M. Suárez-Albela, and P. Fraga-Lamas. A uav and blockchain-based system for industry 4.0 inventory and traceability applications. In *Multidisciplinary Digital Publishing Institute Proceedings*, volume 4, page 26, 2018.

[82] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal*, 6(2):2188–2204, 2018.

[83] M. A. Ferrag and L. Maglaras. Deliverycoin: An ids and blockchain-based delivery framework for drone-delivered services. *Computers*, 8(3):58, 2019.

[84] M. A. Ferrag, L. Maglaras, and H. Janicke. Blockchain and its role in the internet of things. In *Strategic Innovative Marketing and Tourism*, pages 1029–1038. Springer, 2019.

[85] M. A. Ferrag, L. Maglaras, H. Janicke, and R. Smith. Deep learning techniques for cyber security intrusion detection : A detailed analysis. BCS eWiC, 2019.

[86] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50:102419, 2020.

[87] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras. Security and privacy for green iot-based agriculture: Review, blockchain solutions, and challenges. *IEEE Access*, 8:32031–32053, 2020.

[88] P. Fiorini and Z. Shiller. Motion planning in dynamic environments using velocity obstacles. *The International Journal of Robotics Research*, 17(7):760–772, 1998.

[89] J. H. Forsmann, R. E. Hiromoto, and J. Svoboda. A time-slotted on-demand routing protocol for mobile ad hoc unmanned vehicle systems. In G. R. Gerhart, D. W. Gage, and C. M. Shoemaker, editors, *Unmanned Systems Technology IX*, volume 6561, pages 530 – 540. International Society for Optics and Photonics, SPIE, 2007.

[90] R. Fotohi. Securing of unmanned aerial systems (uas) against security threats using human immune system. *Reliability Engineering & System Safety*, 193:106675, 2020.

[91] R. Fotohi, E. Nazemi, and F. S. Aliee. An agent-based self-protective method to secure communication between uavs in unmanned aerial vehicle networks. *Vehicular Communications*, 26:100267, 2020.

[92] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan. Survey on uav cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Communications Surveys & Tutorials*, 21(4):3417–3442, 2019.

[93] M. Frantzen and M. Shuey. Stackghost: Hardware facilitated stack protection. In *10th USENIX Security Symposium (USENIX Security 01)*, Washington, D.C., Aug. 2001.

[94] E. Frazzoli, M. A. Dahleh, and E. Feron. Real-time motion planning for agile autonomous vehicles. *Journal of guidance, control, and dynamics*, 25(1):116–129, 2002.

[95] C. Fu, M. A. Olivares-Mendez, R. Suarez-Fernandez, and P. Campoy. Monocular visual-inertial slam-based collision avoidance strategy for fail-safe uav using fuzzy logic controllers. *Journal of Intelligent & Robotic Systems*, 73(1-4):513–533, 2014.

[96] M. Garcia, A. Viguria, and A. Ollero. Dynamic graph-search algorithm for global path planning in presence of hazardous weather. *Journal of Intelligent & Robotic Systems*, 69(1-4):285–295, 2013.

[97] I. García-Magariño, R. Lacuesta, M. Rajarajan, and J. Lloret. Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. *Ad Hoc Networks*, 86:72–82, 2019.

[98] S. A. Gautam and N. Verma. Path planning for unmanned aerial vehicle based on genetic algorithm & artificial neural network in 3d. In *2014 International Conference on Data Mining and Intelligent Computing (ICDMIC)*, pages 1–5. IEEE, 2014.

[99] M. Gharibi, R. Boutaba, and S. L. Waslander. Internet-of-drones. *IEEE Access*, 4:1148–1162, 2016.

[100] D. Gibert, C. Mateu, and J. Planes. The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. *Journal of Network and Computer Applications*, 153:102526, 2020.

[101] C. Goerzen, Z. Kong, and B. Mettler. A survey of motion planning algorithms from the perspective of autonomous uav guidance. *Journal of Intelligent and Robotic Systems*, 57(1-4):65, 2010.

[102] L. Gupta, R. Jain, and G. Vaszkun. Survey of important issues in uav communication networks. *IEEE Communications Surveys Tutorials*, 18(2):1123–1152, 2016.

[103] A. Hamdi, K. Shaban, A. Erradi, A. Mohamed, S. K. Rumi, and F. D. Salim. Spatiotemporal data mining: a survey on challenges and open problems. *Artificial Intelligence Review*, 55(2):1441–1488, 2022.

[104] K. Han, M. Hhan, and J. H. Cheon. Improved homomorphic discrete fourier transforms and fhe bootstrapping. *IEEE Access*, 7:57361–57370, 2019.

[105] R. Han, L. Bai, J. Liu, and P. Chen. Blockchain-based gnss spoofing detection for multiple uav systems. *Journal of Communications and Information Networks*, 4(2):81–88, 2019.

[106] M. S. Haque and M. U. Chowdhury. A new cyber security framework towards secure data communication for unmanned aerial vehicle (uav). In *International Conference on Security and Privacy in Communication Systems*, pages 113–122. Springer, 2017.

[107] K. Hariss, H. Noura, and A. E. Samhat. Fully enhanced homomorphic encryption algorithm of more approach for real world applications. *Journal of Information Security and Applications*, 34:233–242, 2017.

[108] G. Haroush, C. Leung, A. Malhotra, P. Olexa, A. Wilson, and Y. Zhao. Detection of civil unmanned aerial vehicles by sound processing.

[109] L. Hauzenberger and E. Holmberg Ohlsson. Drone detection using audio analysis. 2015.

[110] D. He, S. Chan, and M. Guizani. Drone-assisted public safety networks: The security aspect. *IEEE Communications Magazine*, 55(8):218–223, 2017.

[111] A. I. Hentati and L. C. Fourati. Comprehensive survey of uavs communication networks. *Computer Standards Interfaces*, 72:103451, 2020.

[112] T. M. Hoang, N. M. Nguyen, and T. Q. Duong. Detection of eavesdropping attack in uav-aided wireless systems: Unsupervised learning with one-class svm and k-means clustering. *IEEE Wireless Communications Letters*, 2019.

[113] W. Hong, L. Jianhua, L. Chengzhe, and W. Zhe. A provably secure aggregate authentication scheme for unmanned aerial vehicle cluster networks. *Peer-to-Peer Networking and Applications*, 13(1):53–63,

2020.

[114] G. Horsman. Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digital Investigation*, 16:1–11, 2016.

[115] S. Hrabar. 3d path planning and stereo-based obstacle avoidance for rotorcraft uavs. In *2008 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pages 807–814. IEEE, 2008.

[116] S. Hu, G. H. Goldman, and C. C. Borel-Donohue. Detection of unmanned aerial vehicles using a visible camera system. *Applied optics*, 56(3):B214–B221, 2017.

[117] S. Huang and R. S. H. Teo. Computationally efficient visibility graph-based generation of 3d shortest collision-free path among polyhedral obstacles for unmanned aerial vehicles. In *2019 International Conference on Unmanned Aircraft Systems (ICUAS)*, pages 1218–1223. IEEE, 2019.

[118] M. Humayun, N. Jhanjhi, A. Alsayat, and V. Ponnusamy. Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, 22(1):105–117, 2021.

[119] S. Husnjak, I. Forenbacher, D. Peraković, and I. Cvitić. Uav forensics: Dji mavic air noninvasive data extraction and analysis. In *5th EAI International Conference on Management of Manufacturing Systems*, pages 115–127. Springer, 2022.

[120] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar. Amassing the security: An ecc-based authentication scheme for internet of drones. *IEEE Systems Journal*, 2021.

[121] F. Iqbal, B. Yankson, M. A. AlYammahi, N. AlMansoori, S. M. Qayed, B. Shah, and T. Baker. Drone forensics: examination and analysis. *International Journal of Electronic Security and Digital Forensics*, 11(3):245–264, 2019.

[122] A. Irshad, S. A. Chaudhry, A. Ghani, and M. Bilal. A secure blockchain-oriented data delivery and collection scheme for 5g-enabled iod environment. *Computer Networks*, page 108219, 2021.

[123] A. Islam, K. Sadia, M. Masuduzzaman, and S. Y. Shin. Bumar: A blockchain-empowered uav-assisted smart surveillance architecture for marine areas. In *Proceedings of the International Conference on Computing Advancements*, pages 1–5, 2020.

[124] A. Islam and S. Y. Shin. Bhmus: Blockchain based secure outdoor health monitoring scheme using uav in smart city. In *2019 7th International Conference on Information and Communication Technology (ICoICT)*, pages 1–6. IEEE, 2019.

[125] A. Islam and S. Y. Shin. Buav: A blockchain based secure uav-assisted data acquisition scheme in internet of things. *Journal of Communications and Networks*, 21(5):491–502, 2019.

[126] A. Islam and S. Y. Shin. Bus: A blockchain-enabled data acquisition scheme with the assistance of uav swarm in internet of things. *IEEE Access*, 7:103231–103249, 2019.

[127] S. U. Jan, I. A. Abbasi, and F. Algarni. A key agreement scheme for iod deployment civilian drone. *IEEE Access*, 9:149311–149321, 2021.

[128] S. U. Jan, F. Qayum, and H. U. Khan. Design and analysis of lightweight authentication protocol for securing iod. *IEEE Access*, 9:69287–69306, 2021.

[129] Y. I. Jenie, E.-J. v. Kampen, C. C. de Visser, J. Ellerbroek, and J. M. Hoekstra. Selective velocity obstacle method for deconflicting maneuvers applied to unmanned aerial vehicles. *Journal of Guidance, Control, and Dynamics*, 38(6):1140–1146, 2015.

[130] J. Jiang and G. Han. Routing protocols for unmanned aerial vehicles. *IEEE Communications Magazine*, 56(1):58–63, 2018.

[131] C. Kanellakis and G. Nikolakopoulos. Survey on computer vision for uavs: Current developments and trends. *Journal of Intelligent & Robotic Systems*, 87(1):141–168, 2017.

[132] V. Kangunde, R. S. Jamisola, and E. K. Theophilus. A review on drones controlled in real-time. *International journal of dynamics and control*, 9(4):1832–1846, 2021.

[133] K. Kanistras, G. Martins, M. J. Rutherford, and K. P. Valavanis. A survey of unmanned aerial vehicles (uavs) for traffic monitoring. In *2013 International Conference on Unmanned Aircraft Systems (ICUAS)*, pages 221–234. IEEE, 2013.

[134] D.-Y. Kao, M.-C. Chen, W.-Y. Wu, J.-S. Lin, C.-H. Chen, and F. Tsai. Drone forensic investigation: Dji spark drone as a case study. *Procedia Computer Science*, 159:1890–1899, 2019.

[135] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman. Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of uavs. In *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*, pages 84–89. IEEE, 2017.

[136] E. B. Karbab, M. Debbabi, A. Derhab, and D. Mouheb. *Android Malware Detection Using Machine Learning: Data-driven Fingerprinting and Threat Intelligence*. Springer, 2021.

[137] K. Kelchtermans and T. Tuytelaars. How hard is it to cross the room?–training (recurrent) neural networks to steer a uav. *arXiv preprint arXiv:1702.07600*, 2017.

[138] A. G. Kendall, N. N. Salvapantula, and K. A. Stol. On-board object tracking control of a quadcopter with monocular vision. In *2014 international conference on unmanned aircraft systems (ICUAS)*, pages 404–411. IEEE, 2014.

[139] H. Khalid, S. J. Hashim, S. M. S. Ahamed, F. Hashim, and M. A. Chaudhary. Secure real-time data access using two-factor authentication scheme for the internet of drones. In *2021 IEEE 19th Student Conference on Research and Development (SCOReD)*, pages 168–173. IEEE, 2021.

[140] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain. A novel two-stage deep learning model for efficient network intrusion detection. *IEEE Access*, 2019.

[141] V. Kharchenko and V. Torianyk. Cybersecurity of the internet of drones: Vulnerabilities analysis and imeca based assessment. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, pages 364–369. IEEE, 2018.

[142] A. A. Khuwaja, Y. Chen, N. Zhao, M.-S. Alouini, and P. Dobbins. A survey of channel modeling for uav communications. *IEEE Communications Surveys & Tutorials*, 20(4):2804–2821, 2018.

[143] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge. Cyber attack vulnerabilities analysis for unmanned aerial vehicles. In *Infotech@ Aerospace 2012*, page 2438. 2012.

[144] J. Kim, C. Park, J. Ahn, Y. Ko, J. Park, and J. C. Gallagher. Real-time uav sound detection and analysis system. In *2017 IEEE Sensors Applications Symposium (SAS)*, pages 1–5. IEEE, 2017.

[145] Y. Kitamura, T. Tanaka, F. Kishino, and M. Yachida. 3-d path planning in a dynamic environment using an octree and an artificial potential field. In *Proceedings 1995 IEEE/RSJ International Conference on Intelligent Robots and Systems. Human Robot Interaction and Cooperative Robots*, volume 2, pages 474–481. IEEE, 1995.

[146] J. Ko, A. Mahajan, and R. Sengupta. A network-centric uav organization for search and pursuit operations. In *Proceedings, IEEE Aerospace Conference*, volume 6, pages 6–6, 2002.

[147] Y. Ko, J. Kim, D. G. Duguma, P. V. Astillo, I. You, and G. Pau. Drone secure communication protocol for future sensitive applications in military zone. *Sensors*, 21(6):2057, 2021.

[148] L.-K. Kong, J. Sheng, and A. Teredesai. Basic micro-aerial vehicles (mavs) obstacles avoidance using monocular computer vision. In *2014 13th International Conference on Control Automation Robotics & Vision (ICARCV)*, pages 1051–1056. IEEE, 2014.

[149] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems*, 100:779–796, 2019.

[150] V. Kortunov, O. Mazurenko, A. Gorbenko, W. Mohammed, and A. Hussein. Review and comparative analysis of mini-and micro-uav autopilots. In *2015 IEEE international conference actual problems of unmanned aerial vehicles developments (APUAVD)*, pages 284–289. IEEE, 2015.

[151] D. Kosmanos, A. Pappas, F. J. Aparicio-Navarro, L. Maglaras, H. Janicke, E. Boiten, and A. Argyriou. Intrusion detection system for platooning connected autonomous vehicles. In *2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, pages

1–9. IEEE, 2019.

[152] A. Koubaa, M. Alajlan, and B. Qureshi. Roslink: Bridging ros with the internet-of-things for cloud robotics. 2017.

[153] A. Koubaa, M. Alves, and E. Tovar. Ieee 802.15.4: a federating communication protocol for time-sensitive wireless sensor networks. 2006.

[154] A. Koubaa, A. Ammar, M. Alahdab, A. Kanhouch, and A. T. Azar. Deepbrain: Experimental evaluation of cloud-based computation offloading and edge computing in the internet-of-drones for deep learning applications. *Sensors*, 20(18), 2020.

[155] A. Koubaa and B. Qureshi. Dronetrack: Cloud-based real-time object tracking using unmanned aerial vehicles over the internet. *IEEE Access*, 6:13810–13824, 2018.

[156] A. Koubâa, B. Qureshi, M.-F. Sriti, A. Allouch, Y. Javed, M. Alajlan, O. Cheikhrouhou, M. Khalgui, and E. Tovar. Dronemap planner: A service-oriented cloud-based management system for the internet-of-drones. *Ad Hoc Networks*, 86:46 – 62, 2019.

[157] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand. A survey of approaches combining safety and security for industrial control systems. *Reliability engineering & system safety*, 139:156–178, 2015.

[158] V. Kroumov, J. Yu, and K. Shibayama. 3d path planning for mobile robots using simulated annealing neural network. *International Journal of Innovative Computing, Information and Control*, 6(7):2885–2899, 2010.

[159] N. Kulkarni, S. Nalbalwar, and A. Nandgaonkar. Challenges in wireless communication channel characteristic identification using machine learning: A review. In *Proceedings of the 3rd International Conference on Communication Information Processing (ICCIP)*, 2021.

[160] A. Kumar, D. A. de Jesus Pacheco, K. Kaushik, and J. J. Rodrigues. Futuristic view of the internet of quantum drones: review, challenges and research agenda. *Vehicular Communications*, 36:100487, 2022.

[161] A. Kumar, K. Sharma, H. Singh, S. G. Naugriya, S. S. Gill, and R. Buyya. A drone-based networked system and methods for combating coronavirus disease (covid-19) pandemic. *Future Generation Computer Systems*, 115:1–19, 2021.

[162] S. Kumari, M. Singh, R. Singh, and H. Tewari. A post-quantum lattice based lightweight authentication and code-based hybrid encryption scheme for iot devices. *Computer Networks*, 217:109327, 2022.

[163] E. Lalish and K. A. Morgansen. Distributed reactive collision avoidance. *Autonomous Robots*, 32(3):207–226, 2012.

[164] A. H. Lashkari, A. F. A. Kadir, H. Gonzalez, K. F. Mbah, and A. A. Ghorbani. Towards a network-based framework for android malware detection and characterization. In *2017 15th Annual conference on privacy, security and trust (PST)*, pages 233–23309. IEEE, 2017.

[165] H. Lee, S. H. Jeong, and H. K. Kim. Otids: A novel intrusion detection system for in-vehicle network by using remote frame. In *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, pages 57–5709. IEEE, 2017.

[166] H. Lee, J. Yoon, M.-S. Jang, and K.-J. Park. A robot operating system framework for secure uav communications. *Sensors*, 21(4), 2021.

[167] K. Lei, Q. Zhang, J. Lou, B. Bai, and K. Xu. Securing icn-based uav ad hoc networks with blockchain. *IEEE Communications Magazine*, 57(6):26–32, 2019.

[168] L. Li, L. Sun, and J. Jin. Survey of advances in control algorithms of quadrotor unmanned aerial vehicle. In *2015 IEEE 16th International Conference on Communication Technology (ICCT)*, pages 107–111. IEEE, 2015.

[169] Y. Li and S. Song. A survey of control algorithms for quadrotor unmanned helicopter. In *2012 IEEE Fifth International Conference on Advanced Computational Intelligence (ICACI)*, pages 365–369. IEEE, 2012.

[170] Y. Li, P. Zhang, and R. Huang. Lightweight quantum encryption for secure transmission of power data in smart grid. *IEEE Access*, 7:36285–36293, 2019.

[171] X. Liang, J. Zhao, S. Shetty, and D. Li. Towards data assurance and resilience in iot using blockchain. In *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*, pages 261–266. IEEE, 2017.

[172] T. P. Lillicrap, J. J. Hunt, A. Pritzel, N. Heess, T. Erez, Y. Tassa, D. Silver, and D. Wierstra. Continuous control with deep reinforcement learning. *arXiv preprint arXiv:1509.02971*, 2015.

[173] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang. Security and privacy for the internet of drones: Challenges and solutions. *IEEE Communications Magazine*, 56(1):64–69, 2018.

[174] L. Lin, Q. Sun, J. Li, and F. Yang. A novel geographic position mobility oriented routing strategy for uavs. *Journal of Computational Information Systems*, 8(2):709–716, 2012.

[175] H. Liu, F. Qu, Y. Liu, W. Zhao, and Y. Chen. A drone detection with aircraft classification based on a camera array. In *IOP Conference Series: Materials Science and Engineering*, volume 322, page 052005, 2018.

[176] J. Y. Liu, Z. Q. Guo, and S. Y. Liu. The simulation of the uav collision avoidance based on the artificial potential field method. In *Advanced Materials Research*, volume 591, pages 1400–1404. Trans Tech Publ, 2012.

[177] Y. Liu, H.-N. Dai, Q. Wang, M. K. Shukla, and M. Imran. Unmanned aerial vehicle for internet of everything: Opportunities and challenges. *Computer communications*, 155:66–83, 2020.

[178] Y. Lu, Z. Xue, G.-S. Xia, and L. Zhang. A survey on vision-based uav navigation. *Geo-spatial information science*, 21(1):21–32, 2018.

[179] G.-c. Luo, J.-q. Yu, Y.-s. Mei, and S.-y. Zhang. Uav path planning in mixed-obstacle environment via artificial potential field method improved by additional control force. *Asian Journal of Control*, 17(5):1600–1610, 2015.

[180] T. Luo, Z. Xu, X. Jin, Y. Jia, and X. Ouyang. Iotcandyjar: Towards an intelligent-interaction honeypot for iot devices. *Black Hat*, pages 1–11, 2017.

[181] Lynx. Real time operating systems (rtos) and secure hypervisors for unmanned systems. `https://www.unmannedsystemstechnology.com/company/lynx-software-technologies/`. Accessed: 05-09-2021.

[182] T. T. Mac, C. Copot, A. Hernandez, and R. De Keyser. Improved potential field method for unknown obstacle avoidance using uav in indoor environment. In *2016 IEEE 14th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, pages 345–350. IEEE, 2016.

[183] L. A. Maglaras and J. Jiang. A novel intrusion detection method based on ocsvm and k-means recursive clustering. *ICST Trans. Security Safety*, 2(3):e5, 2015.

[184] P. Maini and P. Sujit. Path planning for a uav with kinematic constraints in the presence of polygonal obstacles. In *2016 international conference on unmanned aircraft systems (ICUAS)*, pages 62–67. IEEE, 2016.

[185] D. Maiorca, D. Ariu, I. Corona, M. Aresu, and G. Giacinto. Stealth attacks: An extended insight into the obfuscation effects on android malware. *Computers & Security*, 51:16–31, 2015.

[186] S. Majumder, R. Shankar, and M. S. Prasad. Obstacle size and proximity detection using stereo images for agile aerial robots. In *2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN)*, pages 437–442. IEEE, 2015.

[187] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K.-K. R. Choo, and Y. Park. Certificateless-signcryption-based three-factor user access control scheme for iot environment. *IEEE Internet of Things Journal*, 7(4):3184–3197, 2020.

[188] M. R. Manesh and N. Kaabouch. Cyber attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Computers & Security*, 2019.

[189] E. Mantas and C. Patsakis. Who watches the new watchmen? the challenges for drone digital forensics investigations. *Array*, page 100135, 2022.

[190] X. Masip-Bruin, E. Marín-Tordera, G. Tashakor, A. Jukan, and G. Ren. Foggy clouds and cloudy fogs: a real need for coordinated management of fog-to-cloud computing systems. *IEEE Wireless*

Communications, 23(5):120–128, October 2016.

[191] K. McGuire, G. De Croon, C. De Wagter, K. Tuyls, and H. Kappen. Efficient optical flow and stereo vision for velocity estimation and obstacle avoidance on an autonomous pocket drone. *IEEE Robotics and Automation Letters*, 2(2):1070–1076, 2017.

[192] F. L. L. Medeiros and J. D. S. Da Silva. A dijkstra algorithm for fixed-wing uav motion planning based on terrain elevation. In *Brazilian Symposium on Artificial Intelligence*, pages 213–222. Springer, 2010.

[193] P. Mehta, R. Gupta, and S. Tanwar. Blockchain envisioned uav networks: Challenges, solutions, and comparisons. *Computer Communications*, 2020.

[194] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab. An efficient ofdm-based encryption scheme using a dynamic key approach. *IEEE Internet of Things Journal*, 6(1):361–378, 2018.

[195] K. Mershad. Proact: Parallel multi-miner proof of accumulated trust protocol for internet of drones. *Vehicular Communications*, 36:100495, 2022.

[196] K. Mershad, O. Cheikhrouhou, and L. Ismail. Proof of accumulated trust: A new consensus protocol for the security of the iov. *Vehicular Communications*, 32:100392, 2021.

[197] J. Meryamka. The rise of drones: a study on the creation of experimental zones amid the regulatory disconnect. Master's thesis, University of Twente, 2018.

[198] V. Mirelli, S. Tenney, Y. Bengio, N. Chapados, and O. Delalleau. Statistical machine learning algorithms for target classification from acoustic signature. In *Proc. MSS Battlespace Acoust. Magn. Sensors*, pages 1–18, 2009.

[199] A. Mitra, B. Bera, and A. K. Das. Design and testbed experiments of public blockchain-based security framework for iot-enabled drone-assisted wildlife monitoring. In *IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1–6. IEEE, 2021.

[200] S. Mittal and K. Deb. Three-dimensional offline path planning for uavs using multiobjective evolutionary algorithms. In *2007 IEEE Congress on Evolutionary Computation*, pages 3195–3202. IEEE, 2007.

[201] M. Mlezivová. Unmanned aircraft as a subject of safety and security. *MAD-Magazine of Aviation Development*, 6(3):12–16, 2018.

[202] T. Mori and S. Scherer. First results in detecting and avoiding frontal obstacles from a monocular camera for micro unmanned aerial vehicles. In *2013 IEEE International Conference on Robotics and Automation*, pages 1750–1757. IEEE, 2013.

[203] N. H. Motlagh, M. Bagaa, and T. Taleb. Uav-based iot platform: A crowd surveillance use case. *IEEE Communications Magazine*, 55(2):128–134, 2017.

[204] N. H. Motlagh, T. Taleb, and O. Arouk. Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives. *IEEE Internet of Things Journal*, 3(6):899–922, 2016.

[205] R. Moussaileb, N. Cuppens, J.-L. Lanet, and H. L. Bouder. A survey on windows-based ransomware taxonomy and detection mechanisms. *ACM Computing Surveys (CSUR)*, 54(6):1–36, 2021.

[206] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah. A tutorial on uavs for wireless networks: Applications, challenges, and open problems. *IEEE communications surveys & tutorials*, 21(3):2334–2360, 2019.

[207] I. Mugarza and J. C. Mugarza. A coloured petri net-and d* lite-based traffic controller for automated guided vehicles. *Electronics*, 10(18):2235, 2021.

[208] A. Mujumdar and R. Padhi. Nonlinear geometric and differential geometric guidance of uavs for reactive collision avoidance. Technical report, INDIAN INST OF SCIENCE BANGALORE (INDIA), 2009.

[209] A. Mujumdar and R. Padhi. Reactive collision avoidance of using nonlinear geometric and differential geometric guidance. *Journal of guidance, control, and dynamics*, 34(1):303–311, 2011.

[210] A. Mukherjee, N. Dey, and D. De. Edgedrone: Qos aware mqtt middleware for mobile edge computing in opportunistic internet of drone things. *Computer Communications*, 152:93–108, 2020.

[211] A. Mukherjee, N. Dey, R. Kumar, B. K. Panigrahi, A. E. Hassanien, and J. M. R. Tavares. Delay tolerant network assisted flying adhoc network scenario: modeling and analytical perspective. *Wireless Networks*, 25(5):2675–2695, 2019.

[212] A. Mukherjee, V. Keshary, K. Pandya, N. Dey, and S. C. Satapathy. Flying ad hoc networks: A comprehensive survey. In S. C. Satapathy, J. M. R. Tavares, V. Bhateja, and J. R. Mohanty, editors, *Information and Decision Sciences*, pages 569–580, Singapore, 2018. Springer Singapore.

[213] A. Mukherjee, S. Misra, A. Sukrutha, and N. S. Raghuwanshi. Distributed aerial processing for iot-based edge uav swarms in smart farming. *Computer Networks*, 167:107038, 2020.

[214] S. Murthy and J. J. Garcia-Luna-Aceves. An efficient routing protocol for wireless networks. *Mobile Networks and applications*, 1(2):183–197, 1996.

[215] I. A. Musliman, A. A. Rahman, V. Coors, et al. Implementing 3d network analysis in 3d-gis. *International archives of ISPRS*, 37(part B), 2008.

[216] R. Muzaffar and E. Yanmaz. Trajectory-aware ad hoc routing protocol for micro aerial vehicle networks. In *IMAV 2014: International Micro Air Vehicle Conference and Competition 2014, Delft University of Technology, Delft, The Netherlands*, 2014.

[217] M. Narang, W. Liu, J. Gutierrez, and L. Chiaraviglio. A cyber physical buses-and-drones mobile edge infrastructure for large scale disaster emergency communications. In *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pages 53–60, 2017.

[218] A. Nash, S. Koenig, and C. Tovey. Lazy theta*: Any-angle path planning and path length analysis in 3d. In *Twenty-Fourth AAAI Conference on Artificial Intelligence*. Citeseer, 2010.

[219] I. Navarro and F. Matía. A survey of collective movement of mobile robots. *International Journal of Advanced Robotic Systems*, 10(1):73, 2013.

[220] A. Nayyar, B.-L. Nguyen, and N. G. Nguyen. *The Internet of Drone Things (IoDT): Future Envision of Smart Drones*, pages 563–580. 2020.

[221] T. Nguyen, R. Katila, and T. N. Gia. A novel internet-of-drones and blockchain-based system architecture for search and rescue. In *2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, pages 278–288. IEEE, 2021.

[222] I. K. Nikolos, E. S. Zografos, and A. N. Brintaki. Uav path planning using evolutionary algorithms. In *Innovations in intelligent machines-1*, pages 77–111. Springer, 2007.

[223] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam. A provably secure and lightweight authentication scheme for internet of drones for smart city surveillance. *Journal of Systems Architecture*, 115:101955, 2021.

[224] H. Noura, R. Melki, A. Chehab, M. M. Mansour, and S. Martin. Efficient and secure physical encryption scheme for low-power wireless m2m devices. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pages 1267–1272. IEEE, 2018.

[225] C. Osborne. Microsoft malware classification challenge. `https://www.kaggle.com/c/malware-classification`, 2015. Accessed: 2021-04-28.

[226] C. Osborne. Maldrone: Malware which hijacks your personal drone. `https://www.zdnet.com/article/maldrone-malware-which-hijacks-your-personal-drones/`, January 27, 2015. Accessed: 2021-04-28.

[227] A. Otto, N. Agatz, J. Campbell, B. Golden, and E. Pesch. Optimization approaches for civil applications of unmanned aerial vehicles (uavs) or aerial drones: A survey. *Networks*, 72(4):411–458, 2018.

[228] S. Ouiazzane, M. Addou, and F. Barramou. A multiagent and machine learning based denial of service intrusion detection system for drone networks. In *Geospatial Intelligence*, pages 51–65. Springer,

2022.

[229] H. Oz, A. Aris, A. Levi, and A. S. Uluagac. A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, 54(11s):1–37, 2022.

[230] M. O. Ozmen, R. Behnia, and A. A. Yavuz. Iod-crypt: A lightweight cryptographic framework for internet of drones. *arXiv preprint arXiv:1904.06829*, 2019.

[231] P. Parghi, R. Dhamija, and A. K. Agrawal. Innovative approach to onboard media forensic of a drone. In *IOT with Smart Systems*, pages 307–314. Springer, 2022.

[232] J.-W. Park, H.-D. Oh, and M.-J. Tahk. Uav collision avoidance based on geometric approach. In *2008 SICE Annual Conference*, pages 2122–2126. IEEE, 2008.

[233] V. Park and S. Corson. Temporally-ordered routing algorithm (tora). Technical report, IETF internet draft, 2001.

[234] T. Paul, T. R. Krogstad, and J. T. Gravdahl. Uav formation flight using 3d potential field. In *2008 16th Mediterranean Conference on Control and Automation*, pages 1240–1245. IEEE, 2008.

[235] Y. V. Pehlivanoglu. A new vibrational genetic algorithm enhanced with a voronoi diagram for path planning of autonomous uav. *Aerospace Science and Technology*, 16(1):47–55, 2012.

[236] A. A. Pereira, J. P. Espada, R. G. Crespo, and S. R. Aguilar. Platform for controlling and getting data from network connected drones in indoor environments. *Future Generation Computer Systems*, 92:656 – 662, 2019.

[237] H. X. Pham, H. M. La, D. Feil-Seifer, and L. V. Nguyen. Autonomous uav navigation using reinforcement learning. *arXiv preprint arXiv:1801.05086*, 2018.

[238] L. Pike, P. Hickey, T. Elliott, E. Mertens, and A. Tomb. Trackos: A security-aware real-time operating system. In Y. Falcone and C. Sánchez, editors, *Runtime Verification*, pages 302–317, Cham, 2016. Springer International Publishing.

[239] C. Ponsard, P. Massonet, and G. Dallons. Co-engineering security and safety requirements for cyber-physical systems. *ERCIM NEWS*, (106):45–46, 2016.

[240] C. Pu, A. Wall, K.-K. R. Choo, I. Ahmed, and S. Lim. A lightweight and privacy-preserving mutual authentication and key agreement protocol for internet of drones environment. *IEEE Internet of Things Journal*, 2022.

[241] R. A. Ramadan, A.-H. Emara, M. Al-Sarem, and M. Elhamahmy. Internet of drones intrusion detection using deep learning. *Electronics*, 10(21):2633, 2021.

[242] P. Ramon Soria, B. C. Arrue, and A. Ollero. Detection, location and grasping objects using a stereo sensor on uav in outdoor environments. *Sensors*, 17(1):103, 2017.

[243] C. Rani, H. Modares, R. Sriram, D. Mikulski, and F. L. Lewis. Security of unmanned aerial vehicle systems against cyber-physical attacks. *The Journal of Defense Modeling and Simulation*, 13(3):331–342, 2016.

[244] C. T. Recchiuto and A. Sgorbissa. Post-disaster assessment with unmanned aerial vehicles: A survey on practical implementations and research approaches. *Journal of Field Robotics*, 35(4):459–490, 2018.

[245] A. Renduchintala, F. Jahan, R. Khanna, and A. Y. Javaid. A comprehensive micro unmanned aerial vehicle (uav/drone) forensic framework. *Digital Investigation*, 30:52–72, 2019.

[246] H. Rezaee and F. Abdollahi. Adaptive artificial potential field approach for obstacle avoidance of unmanned aircrafts. In *2012 IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM)*, pages 1–6. IEEE, 2012.

[247] A. Roder, K.-K. R. Choo, and N.-A. Le-Khac. Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study. *arXiv preprint arXiv:1804.08649*, 2018.

[248] R. Ross. Guide for conducting risk assessments nist special publication 800-30 revision 1. *US Dept. Commerce, NIST, Gaithersburg, MD, USA, Tech. Rep*, 2012.

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

[250] A. Rozantsev, S. N. Sinha, D. Dey, and P. Fua. Flight dynamics-based recovery of a uav trajectory using ground cameras. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 6030–6039, 2017.

[251] J. Ruchti, R. Senkbeil, J. Carroll, J. Dickinson, J. Holt, and S. Biaz. Unmanned aerial system collision avoidance using artificial potential fields. *Journal of Aerospace Information Systems*, 11(3):140–144, 2014.

[252] S. Saha, A. Natraj, and S. Waharte. A real-time monocular vision-based frontal obstacle detection and avoidance for low cost uavs in gps denied environment. In *2014 IEEE International Conference on Aerospace Electronics and Remote Sensing Technology*, pages 189–195. IEEE, 2014.

[253] O. K. Sahingoz. Flyable path planning for a multi-uav system with genetic algorithms and bezier curves. In *2013 International Conference on Unmanned Aircraft Systems (ICUAS)*, pages 41–48. IEEE, 2013.

[254] O. K. Sahingoz. Multi-level dynamic key management for scalable wireless sensor networks with uav. In *Ubiquitous Information Technologies and Applications*, pages 11–19. Springer, 2013.

[255] F. E. Salamh, U. Karabiyik, and M. K. Rogers. Rpas forensic validation analysis towards a technical investigation process: A case study of yuneec typhoon h. *Sensors*, 19(15):3246, 2019.

[256] F. E. Salamh, U. Karabiyik, M. K. Rogers, and E. T. Matson. A comparative uav forensic analysis: Static and live digital evidence traceability challenges. *Drones*, 5(2):42, 2021.

[257] F. E. Salamh, M. M. Mirza, and U. Karabiyik. Uav forensic analysis and software tools assessment: Dji phantom 4 and matrice 210 as case studies. *Electronics*, 10(6):733, 2021.

[258] Y. Saleem, M. H. Rehmani, and S. Zeadally. Integration of cognitive radio technology with unmanned aerial vehicles: issues, opportunities, and future research challenges. *Journal of Network and Computer Applications*, 50:15–31, 2015.

[259] L. V. Santana, A. S. Brandao, M. Sarcinelli-Filho, and R. Carelli. A trajectory tracking and 3d positioning controller for the ar. drone quadrotor. In *2014 international conference on unmanned aircraft systems (ICUAS)*, pages 756–767. IEEE, 2014.

[260] A. Saravanakumar, A. Kaviyarasu, and R. Ashly Jasmine. Sampling based path planning algorithm for uav collision avoidance. *Sādhanā*, 46(3):1–8, 2021.

[261] M. Satell. Ultimate list of drone stats for 2021. `https://www.phillybyair.com/blog/drone-stats`. Accessed: January 15, 2021.

[262] J. B. Saunders. Obstacle avoidance, visual automatic target tracking, and task allocation for small unmanned air vehicles. 2009.

[263] K. Schmid, T. Tomic, F. Ruess, H. Hirschmüller, and M. Suppa. Stereo vision based indoor/outdoor navigation for flying robots. In *2013 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pages 3955–3962. IEEE, 2013.

[264] C. Schmittner, Z. Ma, and E. Schoitsch. Combined safety and security development lifecylce. In *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, pages 1408–1415. IEEE, 2015.

[265] H. Sedjelmaci, A. Boudguiga, I. B. Jemaa, and S. M. Senouci. An efficient cyber defense framework for uav-edge computing network. *Ad Hoc Networks*, 94:101970, 2019.

[266] H. Sedjelmaci, S. M. Senouci, and N. Ansari. A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(9):1594–1606, 2017.

[267] A. Sedunov, A. Sutin, N. Sedunov, H. Salloum, A. Yakubovskiy, and D. Masters. Passive acoustic system for tracking low-flying aircraft. *IET Radar, Sonar & Navigation*, 10(9):1561–1568, 2016.

[268] P. K. Selvam, G. Raja, V. Rajagopal, K. Dev, and S. Knorr. Collision-free path planning for uavs using efficient artificial potential field algorithm. In *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, pages 1–5. IEEE, 2021.

[269] E. Seo, H. M. Song, and H. K. Kim. Gids: Gan based intrusion detection system for in-vehicle network. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pages 1–6. IEEE, 2018.

[270] J. Seo, Y. Kim, S. Kim, and A. Tsourdos. Collision avoidance strategies for unmanned aerial vehicles in formation flight. *IEEE Transactions on aerospace and electronic systems*, 53(6):2718–2734, 2017.

[271] H. Shacham, M. Page, B. Pfaff, E.-J. Goh, N. Modadugu, and D. Boneh. On the effectiveness of address-space randomization. In B. Pfitzmann and P. Liu, editors, *Proceedings of CCS 2004*, pages 298–307. ACM Press, Oct. 2004.

[272] R. Shakeri, M. A. Al-Garadi, A. Badawy, A. Mohamed, T. Khattab, A. K. Al-Ali, K. A. Harras, and M. Guizani. Design challenges of multi-uav systems in cyber-physical applications: A comprehensive survey and future directions. *IEEE Communications Surveys & Tutorials*, 21(4):3340–3385, 2019.

[273] H. Shakhatreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani. Unmanned aerial vehicles (uavs): A survey on civil applications and key research challenges. *Ieee Access*, 7:48572–48634, 2019.

[274] S. Sharafeddine and R. Islambouli. On-demand deployment of multiple aerial base stations for traffic offloading and network recovery. *Computer Networks*, 156:52 – 61, 2019.

[275] A. Sharma, P. Vanjani, N. Paliwal, C. M. W. Basnayaka, D. N. K. Jayakody, H.-C. Wang, and P. Muthuchidambaranathan. Communication and networking technologies for uavs: A survey. *Journal of Network and Computer Applications*, page 102739, 2020.

[276] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K.-K. R. Choo. Neural-blockchain-based ultrareliable caching for edge-enabled uav networks. *IEEE Transactions on Industrial Informatics*, 15(10):5723–5736, 2019.

[277] V. Sharma, I. You, and G. Kul. Socializing drones for inter-service operability in ultra-dense wireless networks using blockchain. In *Proceedings of the 2017 international workshop on managing insider security threats*, pages 81–84, 2017.

[278] Z. Shi, X. Chang, C. Yang, Z. Wu, and J. Wu. An acoustic-based surveillance system for amateur drones detection and localization. *IEEE transactions on vehicular technology*, 69(3):2731–2739, 2020.

[279] A. Shoufan. Continuous authentication of uav flight command data using behaviometrics. In *2017 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, pages 1–6. IEEE, 2017.

[280] H. Shraim, A. Awada, and R. Youness. A survey on quadrotors: Configurations, modeling and identification, control, collision avoidance, fault diagnosis and tolerant control. *IEEE Aerospace and Electronic Systems Magazine*, 33(7):14–33, 2018.

[281] K. Siddique, Z. Akhtar, F. A. Khan, and Y. Kim. Kdd cup 99 data sets: a perspective on the role of data sets in network intrusion detection research. *Computer*, 52(2):41–51, 2019.

[282] A. Singh and K. Chatterjee. Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79:88–115, 2017.

[283] J. Singh and S. Venkatesan. Blockchain mechanism with byzantine fault tolerance consensus for internet of drones services. *Transactions on Emerging Telecommunications Technologies*, 32(4):e4235, 2021.

[284] K. Skiadopoulos, K. Giannakis, A. Tsipis, K. Oikonomou, and I. Stavrakakis. Impact of drone route geometry on information collection in wireless sensor networks. *Ad Hoc Networks*, page 102220, 2020.

[285] M. Sojka, M. Kreč, and Z. Hanzálek. Case study on combined validation of safety & security requirements. In *Proceedings of the 9th IEEE International Symposium on Industrial Embedded Systems (SIES 2014)*, pages 244–251. IEEE, 2014.

[286] B. Song, G. Qi, and L. Xu. A survey of three-dimensional flight path planning for unmanned aerial vehicle. In *2019 Chinese Control And Decision Conference (CCDC)*, pages 5010–5015. IEEE, 2019.

[287] W.-T. Song, B. Hu, and X.-F. Zhao. Privacy protection of iot based on fully homomorphic encryption. *Wireless Communications and Mobile Computing*, 2018, 2018.

[288] A. Sonmez, E. Kocyigit, and E. Kugu. Optimal path planning for uavs using genetic algorithm. In *2015 International Conference on Unmanned Aircraft Systems (ICUAS)*, pages 50–55. IEEE, 2015.

[289] J. Srinivas, A. K. Das, N. Kumar, and J. J. Rodrigues. Tcalas: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment. *IEEE Transactions on Vehicular Technology*, 68(7):6903–6916, 2019.

[290] M. Stanković, M. M. Mirza, and U. Karabiyik. Uav forensics: Dji mini 2 case study. *Drones*, 5(2):49, 2021.

[291] B. Stewart, L. Rosa, L. A. Maglaras, T. J. Cruz, M. A. Ferrag, P. Simões, and H. Janicke. A novel intrusion detection mechanism for scada systems which automatically adapts to network topology changes. *EAI Endorsed Trans. Indust. Netw. & Intellig. Syst.*, 4(10):e4, 2017.

[292] J. Straub. Development and testing of an intrusion detection system for unmanned aerial systems. In *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, pages 1–9. IEEE, 2017.

[293] Z. Su, Y. Wang, Q. Xu, and N. Zhang. Lvbs: Lightweight vehicular blockchain for secure data sharing in disaster rescue. *IEEE Transactions on Dependable and Secure Computing*, 2020.

[294] J. Sun, J. Tang, and S. Lao. Collision avoidance for cooperative uavs with optimized artificial potential field algorithm. *IEEE Access*, 5:18382–18390, 2017.

[295] J. Sun, W. Wang, Q. Da, L. Kou, G. Zhao, L. Zhang, and Q. Han. An intrusion detection based on bayesian game theory for uav network. In *11th EAI International Conference on Mobile Multimedia Communications*, page 56. European Alliance for Innovation (EAI), 2018.

[296] J. Sun, W. Wang, L. Kou, Y. Lin, L. Zhang, Q. Da, and L. Chen. A data authentication scheme for uav ad hoc network communication. *The Journal of Supercomputing*, pages 1–16, 2017.

[297] Y. Sung, S. Jang, Y.-S. Jeong, J. Hyuk, et al. Malware classification algorithm using advanced word2vec-based bi-lstm for ground control stations. *Computer Communications*, 153:342–348, 2020.

[298] B. Taha and A. Shoufan. Machine learning-based drone detection and classification: State-of-the-art in research. *IEEE Access*, 7:138669–138682, 2019.

[299] X. Tan, S. Su, Z. Zuo, X. Guo, and X. Sun. Intrusion detection of uavs based on the deep belief network optimized by pso. *Sensors*, 19(24):5529, 2019.

[300] M. Tanveer, N. Kumar, M. M. Hassan, et al. Ramp-iod: A robust authenticated key management protocol for the internet of drones. *IEEE Internet of Things Journal*, 2021.

[301] M. H. Tareque, M. S. Hossain, and M. Atiquzzaman. On the routing in flying ad hoc networks. In *2015 Federated Conference on Computer Science and Information Systems (FedCSIS)*, pages 1–9, 2015.

[302] Y. Tian, J. Yuan, and H. Song. Efficient privacy-preserving authentication framework for edge-assisted internet of drones. *Journal of Information Security and Applications*, 48:102354, 2019.

[303] Y. Tian, J. Yuan, and H. Song. Efficient privacy-preserving authentication framework for edge-assisted internet of drones. *Journal of Information Security and Applications*, 48:102354, 2019.

[304] Á. Török and Z. Pethő. Introducing safety and security co-engineering related research orientations in the field of automotive security. *Periodica Polytechnica Transportation Engineering*, 48(4):349–356, 2020.

[305] E. Unlu, E. Zenou, and N. Riviere. Using shape descriptors for uav detection. *Electronic Imaging*, 2018(9):128–1, 2018.

[306] N. Vanitha and P. Ganapathi. Traffic analysis of uav networks using enhanced deep feed forward neural networks (edffnn). In *Handbook of Research on Machine and Deep Learning Applications for Cyber Security*, pages 219–244. IGI Global, 2020.

[307] E. Vattapparamban, İ. Güvenç, A. İ. Yurekli, K. Akkaya, and S. Uluağaç. Drones for smart cities: Issues in cybersecurity, privacy, and

public safety. In *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 216–221. IEEE, 2016.

[308] L. S. W. The internet of flying-things: Opportunities and challenges with airborne fog computing and mobile cloud in the clouds. *arXiv preprint arXiv:1507.04492*.

[309] G. Wang, K. Lim, B.-S. Lee, and J. Y. Ahn. Handover key management in an lte-based unmanned aerial vehicle control network. In *2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pages 200–205. IEEE, 2017.

[310] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei. Survey on unmanned aerial vehicle networks: A cyber physical system perspective. *IEEE Communications Surveys & Tutorials*, 22(2):1027–1070, 2019.

[311] J. Wang, Z. Feng, Z. Chen, S. George, M. Bala, P. Pillai, S. Yang, and M. Satyanarayanan. Bandwidth-efficient live video analytics for drones via edge computing. In *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, pages 159–173, 2018.

[312] J. Wang, C. Jiang, Z. Han, Y. Ren, R. G. Maunder, and L. Hanzo. Taking drones to the next level: Cooperative distributed unmanned-aerial-vehicular networks for small and mini drones. *IEEE Vehicular Technology Magazine*, 12(3):73–82, 2017.

[313] L. Wang, K. Wang, C. Pan, and N. Aslam. Joint trajectory and passive beamforming design for intelligent reflecting surface-aided uav communications: A deep reinforcement learning approach. *IEEE Transactions on Mobile Computing*, 2022.

[314] R. Wang, Y. Cao, A. Noor, T. A. Alamoudi, and R. Nour. Agent-enabled task offloading in uav-aided mobile edge computing. *Computer Communications*, 149:324 – 331, 2020.

[315] T. Wang, R. Qin, Y. Chen, H. Snoussi, and C. Choi. A reinforcement learning approach for uav target searching and tracking. *Multimedia Tools and Applications*, 78(4):4347–4364, 2019.

[316] Y. Wang and W. Chen. Path planning and obstacle avoidance of unmanned aerial vehicle based on improved genetic algorithms. In *Proceedings of the 33rd Chinese Control Conference*, pages 8612–8616. IEEE, 2014.

[317] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues. Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment. *IEEE Internet of Things Journal*, 6(2):3572–3584, 2018.

[318] M. Wazid, A. K. Das, and J.-H. Lee. Authentication protocols for the internet of drones: taxonomy, analysis and future directions. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–10, 2018.

[319] D. J. Webb and J. Van Den Berg. Kinodynamic rrt*: Asymptotically optimal motion planning for robots with linear dynamics. In *2013 IEEE International Conference on Robotics and Automation*, pages 5054–5061. IEEE, 2013.

[320] J. Whelan, A. Almehmadi, and K. El-Khatib. Artificial intelligence for intrusion detection systems in unmanned aerial vehicles. *Computers and Electrical Engineering*, 99:107784, 2022.

[321] J. Won, S.-H. Seo, and E. Bertino. Certificateless cryptographic protocols for efficient drone-based smart city applications. *IEEE Access*, 5:3721–3749, 2017.

[322] G. Wu, Y. Miao, Y. Zhang, and A. Barnawi. Energy efficient for uav-enabled mobile edge computing networks: Intelligent task prediction and offloading. *Computer Communications*, 2019.

[323] T.-Y. Wu, X. Guo, Y.-C. Chen, S. Kumari, and C.-M. Chen. Amassing the security: An enhanced authentication protocol for drone communications over 5g networks. *Drones*, 6(1):10, 2022.

[324] J. Xie, Y. Wan, J. H. Kim, S. Fu, and K. Namuduri. A survey and analysis of mobility models for airborne networks. *IEEE Communications Surveys & Tutorials*, 16(3):1221–1238, 2013.

[325] J.-P. Yaacoub and O. Salman. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, page 100218, 2020.

[326] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor, and A. Bala. Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access*, 9:57243–57270, 2021.

[327] C. Yan, L. Fu, J. Zhang, and J. Wang. A comprehensive survey on uav communication channel modeling. *IEEE Access*, 7:107769–107792, 2019.

[328] K. Yang and S. Sukkarieh. 3d smooth path planning for a uav in cluttered natural environments. In *2008 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pages 794–800. IEEE, 2008.

[329] K. Yang and S. Sukkarieh. Real-time continuous curvature path planning of uavs in cluttered environments. In *2008 5th International Symposium on Mechatronics and Its Applications*, pages 1–6. IEEE, 2008.

[330] L. Yang, J. Qi, J. Xiao, and X. Yong. A literature review of uav 3d path planning. In *Proceeding of the 11th World Congress on Intelligent Control and Automation*, pages 2376–2381. IEEE, 2014.

[331] L. Yang, H. Zhang, M. Li, J. Guo, and H. Ji. Mobile edge computing empowered energy efficient task offloading in 5g. *IEEE Transactions on Vehicular Technology*, 67(7):6398–6409, 2018.

[332] Z. Yang, F. Lin, and B. M. Chen. Survey of autopilot for multi-rotor unmanned aerial vehicles. In *IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society*, pages 6122–6127. IEEE, 2016.

[333] K. Yoon, D. Park, Y. Yim, K. Kim, S. K. Yang, and M. Robinson. Security authentication system using encrypted channel on uav network. In *2017 First IEEE International Conference on Robotic Computing (IRC)*, pages 393–398. IEEE, 2017.

[334] M. Yousef, F. Iqbal, and M. Hussain. Drone forensics: A detailed analysis of emerging dji models. In *2020 11th International Conference on Information and Communication Systems (ICICS)*, pages 066–071. IEEE, 2020.

[335] J. Yu, B.-M. Cho, K.-J. Park, et al. Detecting uav attacks through network monitoring. Vertical Flight Society, 2019.

[336] K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A. K. Bashir, and F. A. Khan. Securing critical infrastructures: Deep-learning-based threat detection in iiot. *IEEE Communications Magazine*, 59(10):76–82, 2021.

[337] W. Yu. Real-time operating system security. `http://people.cs.ksu.edu/~danielwang/Investigation/RTOS_Security/RTOS_Security.pdf`. Accessed: 2021-05-9.

[338] S. Zaidi, M. Atiquzzaman, and C. T. Calafate. Internet of flying things (ioft): A survey. *Computer Communications*, 165:53–74, 2021.

[339] Y. Zeng, R. Zhang, and T. J. Lim. Wireless communications with unmanned aerial vehicles: Opportunities and challenges. *IEEE Communications Magazine*, 54(5):36–42, 2016.

[340] B. Zhang, Z. Mao, W. Liu, and J. Liu. Geometric reinforcement learning for path planning of uavs. *Journal of Intelligent & Robotic Systems*, 77(2):391–409, 2015.

[341] N. Zhang, Q. Jiang, L. Li, X. Ma, and J. Ma. An efficient three-factor remote user authentication protocol based on bpv-fourq for internet of drones. *Peer-to-Peer Networking and Applications*, pages 1–14, 2021.

[342] R. Zhang, J.-P. Condomines, N. Larrieu, and R. Chemali. Design of a novel network intrusion detection system for drone communications. In *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, pages 1–10. IEEE, 2018.

[343] T. Zhang, G. Kahn, S. Levine, and P. Abbeel. Learning deep control policies for autonomous aerial vehicles with mpc-guided policy search. In *2016 IEEE international conference on robotics and automation (ICRA)*, pages 528–535. IEEE, 2016.

[344] Y. Zhang, D. He, L. Li, and B. Chen. A lightweight authentication and key agreement scheme for internet of drones. *Computer Communications*, 2020.

[345] Y. Zhang and H. Mehrjerdi. A survey on multiple unmanned vehicles formation control and coordination: Normal and fault situations. In *2013 International conference on unmanned aircraft systems (ICUAS)*, pages 1087–1096. IEEE, 2013.

[346] Y. Zhao, Z. Zheng, and Y. Liu. Survey on computational-intelligence-based uav path planning. *Knowledge-Based Systems*, 158:54–64, 2018.

[347] Y. Zhou and X. Jiang. Dissecting android malware: Characterization and evolution. In *2012 IEEE symposium on security and privacy*, pages 95–109. IEEE, 2012.

Abdelouahid Derhab is an Associate Professor with the Center of Excellence in Information Assurance (COEIA), King Saud University, Saudi Arabia. He received the Engineer's, M.Sc., and Ph.D. degrees in computer science from the University of Sciences and Technology Houari Boummediene (USTHB), Algiers, in 2001, 2003, and 2007, respectively. He was a Computer Science Engineer and a full-time Researcher with the CERIST Research Center, Algeria, from 2002 to 2012. He was an Assistant Professor with King Saud University, from 2012 to 2018. He also served as a workshop chair, a technical committee chair, and a reviewer for many journals and international conferences. He is also a cyber-security policy analyst at Global Foundation for Cyber Studies and Research (GFCYBER). His research interests are malware analysis, network security, intrusion detection, mobile security, the Internet of Things, smart grid, blockchain, and cyber security policies.

Omar Cheikhrouhou is currently an Assistant Professor at Higher Institute of Computer Science of Mahdia, University of Monastir, Tunisia. He is also a researcher at CES Lab (Computer and Embedded System), University of Sfax, National School of Engineers, Tunisia. He has received his Ph.D. degrees in Computer Science from the National School of Engineers of Sfax in March 2012. His Ph.D. deals with security of Wireless Sensor Networks and more precisely in "Secure Group Communication in Wireless Sensor Networks". Currently, his research interests span over several areas related to Wireless Sensor Networks, CyberSecurity, Edge Computing, Blockchain, Multi-Robot System Coordination, Smart and Secure Health-care, etc. He was selected amongst the top 2% of the most cited research in 2021. Dr. Omar has several publications in high-quality international journals and conferences. He has received some awards, including the "Governor Prize" from the Governor of Sfax in 2005.

Azza Allouch received the master's degree from the National School of Electronics and Telecommunication, Sfax, in 2016. She is currently pursuing the Ph.D. degree with the School of Intelligent Systems Science and Engineering, Jinan University, China, in cooperation with the Faculty of Mathematical, Physical and Natural Sciences of Tunis (FST), University of El Manar, Tunisia. She is an Associate Member of the LISI Laboratory, National Institute of Applied Sciences and Technology, University of Carthage, Tunisia. She is also with the Robotics and Internet-of-Things Laboratory, Prince Sultan University, Saudi Arabia, and Gaitech Robotics, China. Her research interests include machine learning, Blockchain, and UAV.

Anis Koubaa is the Director of the Research and Initiatives Center and the leader and founder of the Robotics and Internet-of-Things Lab at Prince Sultan University. He is a Full Professor in Computer Science and has been working on several R&D projects on data science and unmanned systems, deep learning, robotics, and Internet-of-Things. He is a Senior Fellow of the Higher Education Academy of the UK. He presented several training programs on drones, data science, Python programming, deep learning, and several other technologies. He is known for his course series and books on Robot Operating System (ROS) and more than 10 other Books with Springer and Elsevier. Anis Koubaa received the Rector Best Teacher Award in 2016 at Prince Sultan University and the Best Research Award in 2012 at Al-Imam University. He is also nominated in the carrier-based top 2% scientists list made by Stanford University. The current research interests of Anis Koubaa deal with developing automated solutions for logistics using drones and robots for delivery systems. Anis is the author of the ROSLink protocol that enables robots and drones to talk the cloud systems and develop cloud robotics solutions. He also leads AI projects on real-time face surveillance, vehicle detection, and license plate recognition. He is also developing AI and automation solutions for smart cities and smart agriculture.

Basit Qureshi specializes in Cloud computing with a focus on performance issues in Energy-aware and Green-computing, integrating Cloud and Internet-of-Things applications in the context of Smart cities. He is with the College of Computer & Information Science at Prince Sultan University. He is an associate professor and the chair of the Department of Computer Science at Prince Sultan University. He received his Ph.D. degree in Computer Science from the University of Bradford in the year 2011. Prior to that, he received his Master of Science degree in Computer Science from Florida Atlantic University in 2002 and his Bachelor of Science degree in Computer Science from Ohio University, OH USA in 2000. He is a Fellow of the Higher Education Academy (UK). He is also a senior member of IEEE, a member of IEEE Computer Society, IEEE Communication Society, and the ACM.

Mohamed Amine Ferrag received the Bachelor's, Master's, Ph.D., and Habilitation degrees in computer science from Badji Mokhtar—Annaba University, Annaba, Algeria, in June, 2008, June, 2010, June, 2014, and April, 2019, respectively. From 2014 to 2022, he was an Associate Professor with the Department of Computer Science, Guelma University, Algeria. From 2019 to 2022, he was a Visiting Senior Researcher with the NAU-Lincoln Joint Research Center of Intelligent Engineering, Nanjing Agricultural University, China. Since 2022, he has been the Led Researcher with Artificial Intelligence & Digital Science Research Center, Technology Innovation Institute, Abu Dhabi, United Arab Emirates. His research interests include wireless network security, network coding security, applied cryptography, blockchain technology, AI for Cyber Security. He has published over 100 papers in international journals and conferences in the above areas. He has been conducting several research projects with international collaborations on these topics. He was a recipient of the 2021 IEEE TEM BEST PAPER AWARD. He is featured in Stanford University's list of the world's Top 2 % scientists for the years 2020,2021,2022. He is a Senior Member of the Institute of Electrical & Electronic Engineers (IEEE) and a member of the Association for Computing Machinery (ACM).

Leandros Maglaras is Full Professor of cybersecurity in the School of Computer Science and Informatics of De Montfort University. From September 2017 to November 2019, he was the Director of the National Cyber Security Authority of Greece. He obtained the B.Sc. (M.Sc. equivalent) in Electrical and Computer Engineering from the Aristotle University of Thessaloniki, Greece in 1998, M.Sc. in Industrial Production and Management from the University of Thessaly in 2004, and M.Sc. and Ph.D. degrees in Electrical & Computer Engineering from University of Thessaly, in 2008 and 2014 respectively. In 2018 he was awarded a Ph.D. in Intrusion Detection in SCADA systems from the University of Huddersfield He is featured in Stanford University list of the world Top 2% scientists. He is a Senior Member of the Institute of Electrical & Electronics Engineers (IEEE) and is an author of more than 170 papers in scientific magazines and conferences.

Farrukh Aslam Khan is a Professor of Cybersecurity at the Center of Excellence in Information Assurance, King Saud University, Saudi Arabia. He received the M.S. degree in computer system engineering from the GIK Institute of Engineering Sciences and Technology, Pakistan, and the Ph.D. degree in computer engineering from Jeju National University, South Korea, in 2003 and 2007, respectively. He also received professional trainings from the Massachusetts Institute of Technology, New York University, IBM, and other institutions. He has published more than 120 research articles in refereed international journals and conferences. He has supervised/co-supervised five Ph.D. students and 18 M.S. thesis students. His research interests include cybersecurity, wireless sensor networks and e-health, bio-inspired and evolutionary computation, and the Internet of Things. He is on the panel of reviewers of over 40 reputed international journals and numerous international conferences. He has co-organized several international conferences and workshops. He serves as an Associate Editor for prestigious international journals, including IEEE Access, PLOS One, Neurocomputing (Elsevier), Ad Hoc and Sensor Wireless Networks, KSII Transactions on Internet and Information Systems, Human-Centric Computing and Information Sciences (Springer), and Complex & Intelligent Systems (Springer). He is a Fellow of the British Computer Society (BCS) and a Senior Member of the IEEE.