Article:
Tsao, Kai-Yun, Girdler, Thomas and VASILAKIS, VASILEIOS (2022) A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. Ad Hoc Networks. 102894. ISSN: 1570-8713

https://doi.org/10.1016/j.adhoc.2022.102894

Ad Hoc Networks 133 (2022) 102894

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Survey paper

A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks

Kai-Yun Tsao, Thomas Girdler, Vassilios G. Vassilakis *

Department of Computer Science, University of York, York, United Kingdom

ARTICLE INFO

Keywords:
Unmanned aerial vehicle (UAV)
Flying ad-hoc network (FANET)
Cyber security and privacy

ABSTRACT

Unmanned aerial vehicles (UAVs) are a rapidly evolving technology, and being highly mobile, UAV systems are able to cooperate with each other to accomplish a wide range of different tasks. UAVs can be used in commercial applications, such as goods delivery, as well as in military surveillance. They can also operate in civil domains like search-and-rescue missions, that require multiple UAVs to collect location data as well as transmit video streams. However, the malicious use of UAVs began to emerge in recent years. The frequency of such attacks has been significantly increasing and their impact can have devastating effects. Hence, the relevant industries and standardisation bodies are exploring possibilities for securing UAV systems and networks.

Our survey focuses on UAV security and privacy issues whilst establishing flying ad-hoc networks (FANETs) as well as on threats to the Internet of drones (IoD) infrastructure used to provide control and access over the Internet between UAVs and users. The goal of this survey is to categorise the versatile aspects of the UAV threat landscape and develop a classification approach based on different types of connections and nodes in FANETs and IoD. In particular, we categorise security and privacy threats on connections between UAVs, ground control stations, and personal pilot devices. All the most relevant threats and their corresponding defence mechanisms are classified using characteristics of the first four layers of the OSI model. We then analyse the conventional and novel UAV routing protocols, indicating their advantages and disadvantages from the cyber security perspective. To provide a deeper insight, the reviewed defence mechanisms have undergone a thorough examination of their security requirements and objectives such as availability, authentication, authorisation, confidentiality, integrity, privacy, and non-repudiation. Finally, we discuss the open research challenges, the limitations of current UAV standards, and provide possible future directions for research.

1. Introduction

An unmanned aerial vehicle (UAV), also known as a drone, is an aircraft which can operate without a human pilot inside it [1]. In the U.S. alone over 800,000 UAVs had been registered by the Federal Aviation Administration (FAA) at the end of August 2021 [2]. Sixty percent of them were for recreational purposes and the rest for commercial operations. Applications for UAVs include search and rescue (SAR) missions, remote monitoring (weather, traffic, or human surveillance), network relays, construction, and goods delivery [3,4]. UAV communication requirements are often based on their application; for example SAR is a time-critical activity where video must be sent back to the ground control station (GCS) in real time.

The U.K.'s aviation industry standards, safety, security, and risk management are directed by the Civil Aviation Authority (CAA) [5]. To decide where a UAV can be flown, CAA categorises them into five types based on their weight and capabilities. The *Drone Market Report 2020* [6] estimates that between 2020 to 2025, software improvements will result in the global UAV market increasing from £15.8bn to over £30.2bn. In terms of the U.K.'s gross domestic product (GDP), a PwC report [7] predicts that by 2023 UAVs will contribute £42bn, with net cost savings of £16bn and more than 628,000 jobs created. Worldwide, it is predicted that actual UAV sales will reach one million by the end of 2021 [6]. Philly [8] reports that in 2020, 15% of Americans will have flown a drone. UAVs can be used for civil, commercial, or military purposes.

There are several factors driving the expansion in UAV sales. Firstly, in changeable environments, their autonomous and sensing technologies enable advanced navigation as well as data collection techniques. Furthermore, UAVs can extend their operational coverage by using multi-node networks. For example, the flying ad-hoc network (FANET) [9] technology allows heterogeneous and homogeneous UAVs to communicate with one another. Whilst UAV's have limited computational

* Corresponding author.
E-mail address: vv573@york.ac.uk (V.G. Vassilakis).

https://doi.org/10.1016/j.adhoc.2022.102894
Received 30 December 2021; Received in revised form 1 May 2022; Accepted 5 May 2022
Available online 23 May 2022

Table 1
Survey organisation.

Section	Content
Section 2	Basic UAV components, FANET architectures and their operation are outlined.
Section 3	Existing surveys related to FANET security and privacy, with their limitations discussed. We highlight our surveys' novel contributions.
Section 4	A comprehensive taxonomy of FANET security and privacy threats based on threat vectors is provided.
Section 5	Security and privacy threats based on four OSI layers are outlined.
Section 6	FANET security solutions and standards are classified then compared.
Section 7	FANET research challenges and problems are documented.
Section 8	We conclude our work and discuss future research directions.

resources, technological advances are constantly improving the security and privacy of high-mobility UAV networks, such as FANETs. Existing surveys about UAV security, privacy, and communication architectures concentrate on the vulnerabilities found in system components, payload, mobility models, safety and physical privacy [1,9–16]. We have identified that little coverage was given to FANET security and privacy threats and solutions. Our work intends to address these shortcomings by focusing on: (i) security and privacy threats related to different nodes which constitute an unmanned aerial system (UAS), such as UAVs and GCS; (ii) security threats in FANETs, related to the first four layers of the OSI model, and (iii) security solutions available to address the threats to UAV communications and FANETs.

Our survey makes these novel contributions:

- *Security threats based on FANET threat vectors are analysed, classified, and compared in detail.* In particular, these threat vectors consist of six connection types and six node types. We then classify and compare 13 security threats based on security requirements and network types. The considered threats and solutions are over FANETs, Internet of drones (IoD), 5G mobile networks, radio wave (RW), wireless local area network (WLAN), wireless sensor network (WSN) as well as other ad-hoc network types.
- *We provide a comprehensive taxonomy of security threats and solutions based upon the four OSI layers related to FANETs and UAV communications.* We identify and compare 12 security threats, along with their 31 corresponding security solutions. We also review threats and solutions related to routing protocols in FANETs. We consider 7 particular routing protocol types and compare 22 related security solutions.
- *We identify and compare appropriate security solutions that have been proposed to mitigate FANET and IoD security threats.* We classify 23 specific security threats based on 7 security requirements, then compare the 40 proposed security solutions. Finally, we compare six existing standards and identify their limitations.

Table 1 provides the organisation of this survey.

2. Unmanned aerial systems and flying ad-hoc networks

In this section, we introduce the unmanned aerial system (UAS) components, identify communication architecture types and provide examples of how UAVs cooperate in FANETs. We also compare FANETs to other types of ad-hoc networks, and document their distinguishing characteristics.

The Internet of drones (IoD) [17] can be described as a network architecture that provides navigation services to drones within controlled air spaces. The IoD consists of node-to-node and end-to-end services and applications. Examples of services that can be provided by IoD include industrial or infrastructure inspections, fleet monitoring, search and rescue operations, and goods delivery systems [18]. FANET zones can be used within the IoD to create a multi-drone network, which is connected autonomously and provides coordination for every drone. When compared to a single-drone network, this establishes greater scalability, adaptability, and allows for drone self-organisation [19].

2.1. Components of an unmanned aerial system

According to the E.U. Commission Delegated Regulation 2019/945 [20], a UAS contains two main elements: an unmanned aircraft and a remote control device. As illustrated in Fig. 1, academic literature [15,21–23], normally depicts a UAS as containing UAVs, application equipment, data links, and ground devices [9,24]. We now outline each of these components.

A UAV normally contains the following components: (i) A single board computer with CPU and memory, (ii) sensor units such as global positioning system (GPS) receivers, accelerometers, infrared camera, gyroscope, magnetic orientation, and electro-optical sensors [15], (iii) battery, (iv) remote-control (RC) receiver and transmitter that transfers data between UAVs and GCS [21], (v) telemetry device that transmits signals to indicate the UAV flight status [25], (vi) flight controller that manages the core phases: take-off, ascent, cruise, descent, and landing [26], and (vii) inertial measurement unit (IMU) which is a sensor with accelerometer, gyroscope, and magnetometer that aids FANET operation and manages UAV altitude [27]. To achieve autonomous navigation, most scenarios employ the GPS, flight controller and inertial system [23]. Having UAV time and sensor data provided by the GPS is very advantageous to the flight controller, as it can define the UAV's exact position and control flight plans and paths in real time [15]. Depending on the usage scenario, the payload carries different equipment; as an example, this could be for thermal monitoring, video surveillance, or deploying chemical agents. This equipment can be installed on UAVs to collect useful data. For instance, a gas sensor could detect air pollution [21], whereas a video camera could send live streams whilst monitoring a wildfire.

A GCS can include ground devices such as personal computers, mobile phones, or tablets that remotely pilot a UAV using RC transmitters and telemetry [21,23]. GCS and UAV communicate via a data link in a real-time wireless transmission. Data links can be categorised into the following three types: (i) Line-of-Sight (LoS), where control signals are transmitted via radio waves [15], (ii) Visual Line of Sight (VLoS), where the remote pilot should be able to see the UAV clearly [28], and (iii) Beyond Line-of-Sight (BLoS), when the UAV cannot be seen via LoS; signals are then received from satellites or relay UAVs [12].

2.2. UAV communication architectures categorisation

Communication is a critical issue when deploying fast moving multi-UAV systems. Depending on data flow, UAV communications architectures are either centralised or decentralised. This categorisation is shown in Fig. 2 and explained below.

2.2.1. Centralised architectures

UAVs communicate with a central controller, meaning there is a single point of failure. Fig. 3 presents three types of centralised communication architectures [9]. In UAV-GCS, to obtain data, every UAV must directly connect to the GCS. This type of link is not advisable in changeable environments, such as stormy weather conditions. In UAV-satellite, communication is done via a satellite, which is suitable for when the distance between GCS and UAV is big. In UAV-cellular, communication is performed via appropriate cellular technology; it uses base stations to implement routing technology that facilitates communication between nodes.

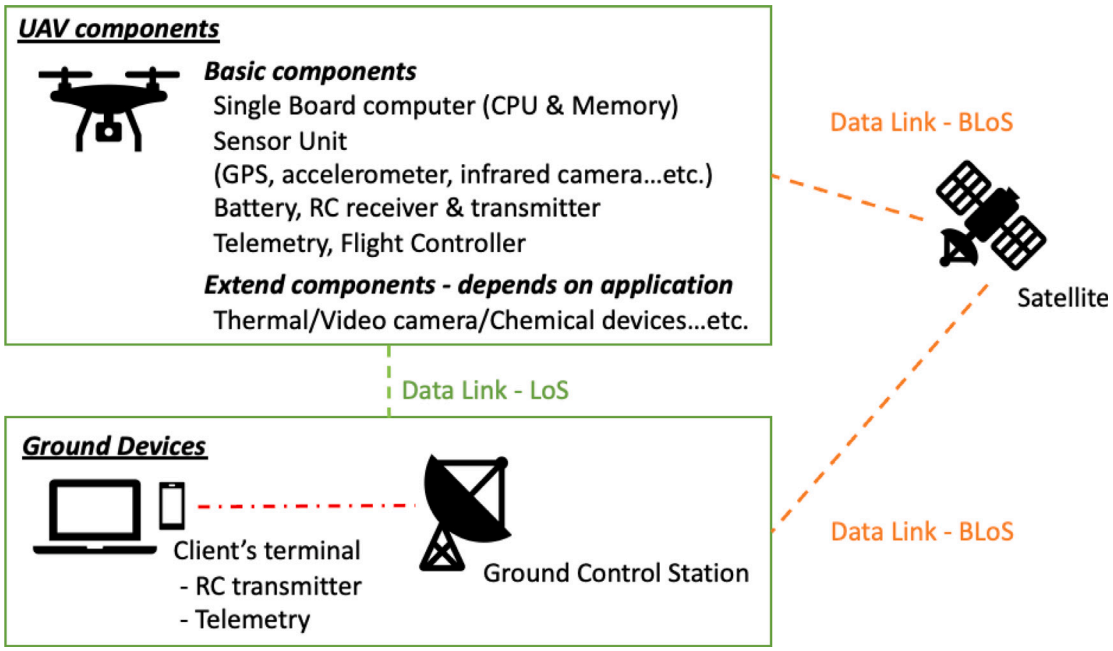


Fig. 1. Typical components of a UAS.

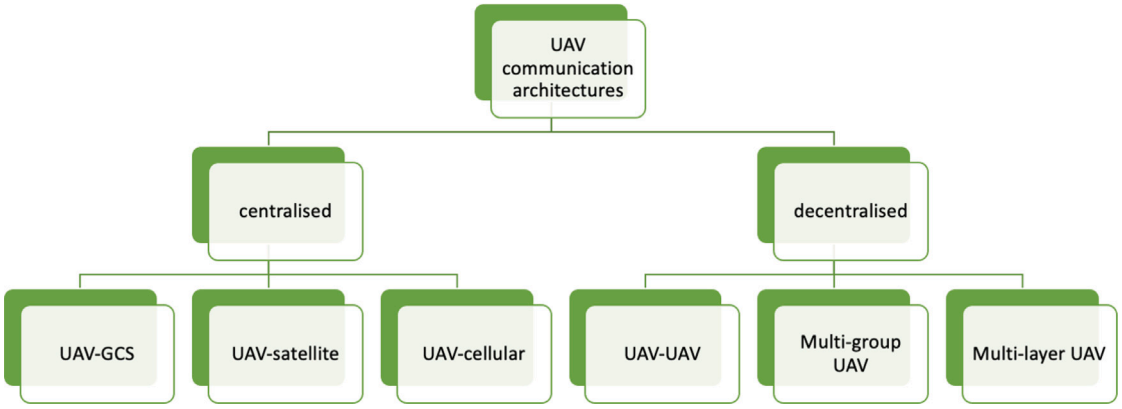


Fig. 2. UAV communication architectures.

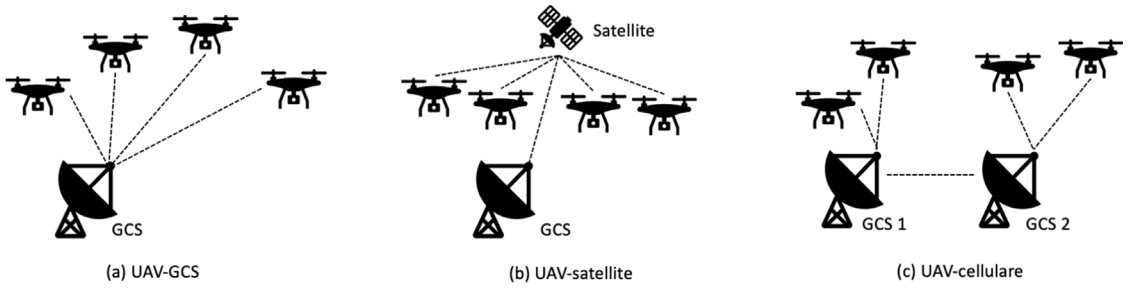


Fig. 3. Centralised UAV Communication Architectures.

2.2.2. Decentralised architectures

In a decentralised architecture, UAVs communicate directly or indirectly with the GCS. Backbone UAVs act as gateways between the GCS and other UAVs in the network by relaying data [29]. Ad-hoc networks use wireless devices or nodes to dynamically communicate with each other without needing an access point or GCS [30]. Generally speaking, FANET communication between UAVs is achieved without a central controller. Heterogeneous and homogeneous UAVs construct a flexible network environment where UAVs cooperate with each other to expand network coverage, with the network structure not affected by UAVs joining or leaving [31]. Fig. 4 shows a FANET with extended coverage while deploying three UAVs.

Fig. 5 shows different types of decentralised communication architectures [14,30]. These types are as follows. (a) *UAV Ad-Hoc Network*: the backbone UAV uses high power to access the GCS over long ranges, it then acts as a gateway and communicates using low power over short ranges to UAVs. This process effectively extends UAV network coverage and is suitable for small UAVs carrying lightweight transceivers. This

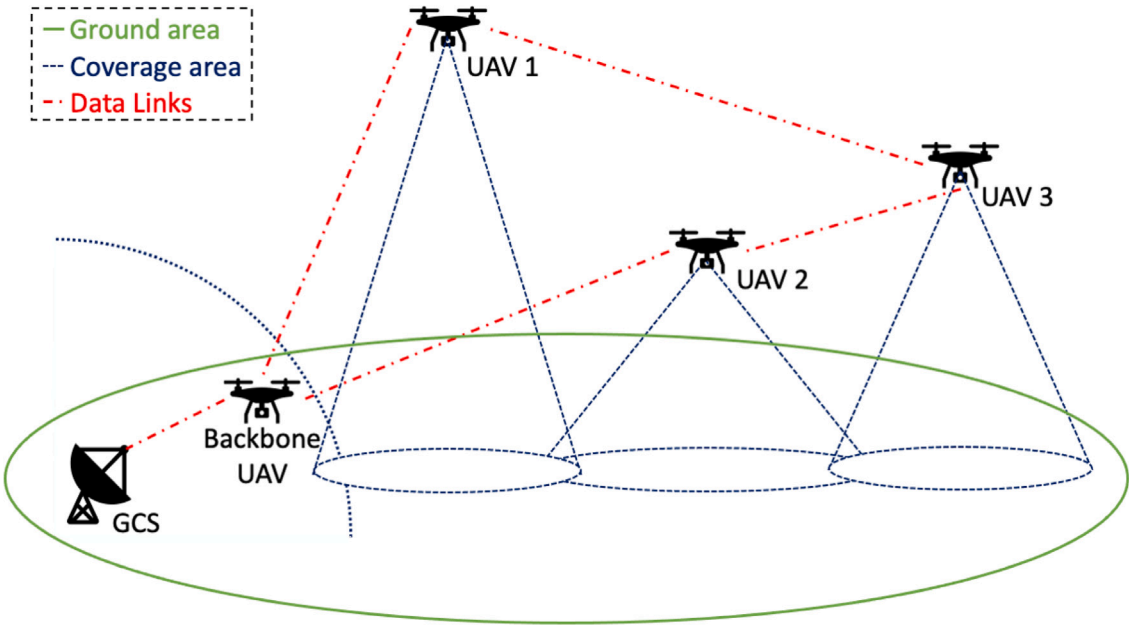


Fig. 4. Extend coverage area by using FANET.

architecture is appropriate for surveillance and monitoring applications while using homogeneous UAVs. (b) *Multi-group UAV Ad-Hoc Network*: UAVs form groups and each group works as a FANET, with a backbone UAV which communicates with the GCS though inter-group links. The intra-group communication does not involve the GCS which makes it appropriate for numerous heterogeneous UAVs working together. However, the GCS constitutes a potential single point of failure. (c) *Multi-layer UAV Ad-Hoc Network*: the lower layer is used for intra-group communication, whereas the upper layer is for backbone UAVs to communicate with other UAVs or GCS. The data exchange between groups does not rely on GCS, which reduces the throughput and computational loading of GCS. Compared to the previous architecture, this one prevents a single point of failure. Also, it is easy to expand the operational coverage, with UAVs communicating via multiple links. Given that in FANETs, UAVs cooperate with each other for tracking, path planning and hop efficiency, this infrastructure is easy-to-scale, has high mobility, and provides wide communication ranges. The infrastructure can also deal with hardware limitations in changeable environments [9].

2.3. FANET operation

In this subsection, we present FANET initialisation methods, its normal operation, as well as how UAVs join and leave the network. We illustrate the protocols, methods, and topologies that are employed when FANETs are formed. Fig. 6 presents an example of a FANET with a multi-group network architecture. Backbone UAVs communicate with other UAVs and the GCS using inter-group links.

2.3.1. Initialisation

It is assumed that all of the UAVs and GCS are legitimate before taking off. Each homogeneous UAV is configured with a function containing its ID and key pairs allowing cooperation with other UAVs. One UAV is selected as the backbone, the others register as group members. A control signal is sent from the GCS to the backbone UAV, which then acts as a gateway to communicate with other UAVs.

2.3.2. Normal operation

During the normal FANET operation, UAVs cooperate with each other to extend their mission coverage and exchange information as well as prevent collisions. Mission information is published by the backbone UAV, then transferred from one UAV to the next. In order to prevent a single point of failure, a backup backbone UAV is selected. This method of operation provides greater efficiency and resilience than multiple UAVs operating on their own [1].

2.3.3. Join and leave

An authorisation request is sent to the backbone UAV when a new UAV arrives in the FANET. After the backbone UAV authorises the new UAV with its ID and key pairs, communication commences using encrypted channels [32]. A collection of UAVs is known as a swarm; UAVs can leave the swarm due to environmental changes or link outages. If a UAV leaves the swarm due to low battery levels, other UAVs notify the backbone UAV, allowing the backbone to properly de-authenticate it from the network [32]. UAVs joining or leaving FANET create changes in its overall topology. When this occurs, the changes are publicly broadcast amongst all UAVs in the swarm. The process is known as 'self-organisation'; each UAV discovers its own neighbours and exchanges this information with other UAVs. Self-organisation allows connections between UAVs to be re-built and paths re-organised [16]. The service recovery management process can repair network disruption caused by radio signal interference and local failures. The energy management process controls battery consumption and load balances data forwarding. Medium access control (MAC) minimises errors caused by network collisions; these occur when two or more nodes exchange data at the same time.

2.4. FANET characteristics

In this subsection, we introduce the unique FANET characteristics as well as designs, outlining how they can be affected by security and privacy issues. FANET is a subset of mobile ad-hoc network (MANET) and vehicular ad-hoc network (VANET), sharing similar characteristics with them. MANET is a dynamic network structure which is formed with static or mobile nodes [33], VANET is a subset of MANET where the nodes are the moving vehicles. Due to the fact that UAVs typically fly in high altitudes with speeds of over 100mph [34], some of the

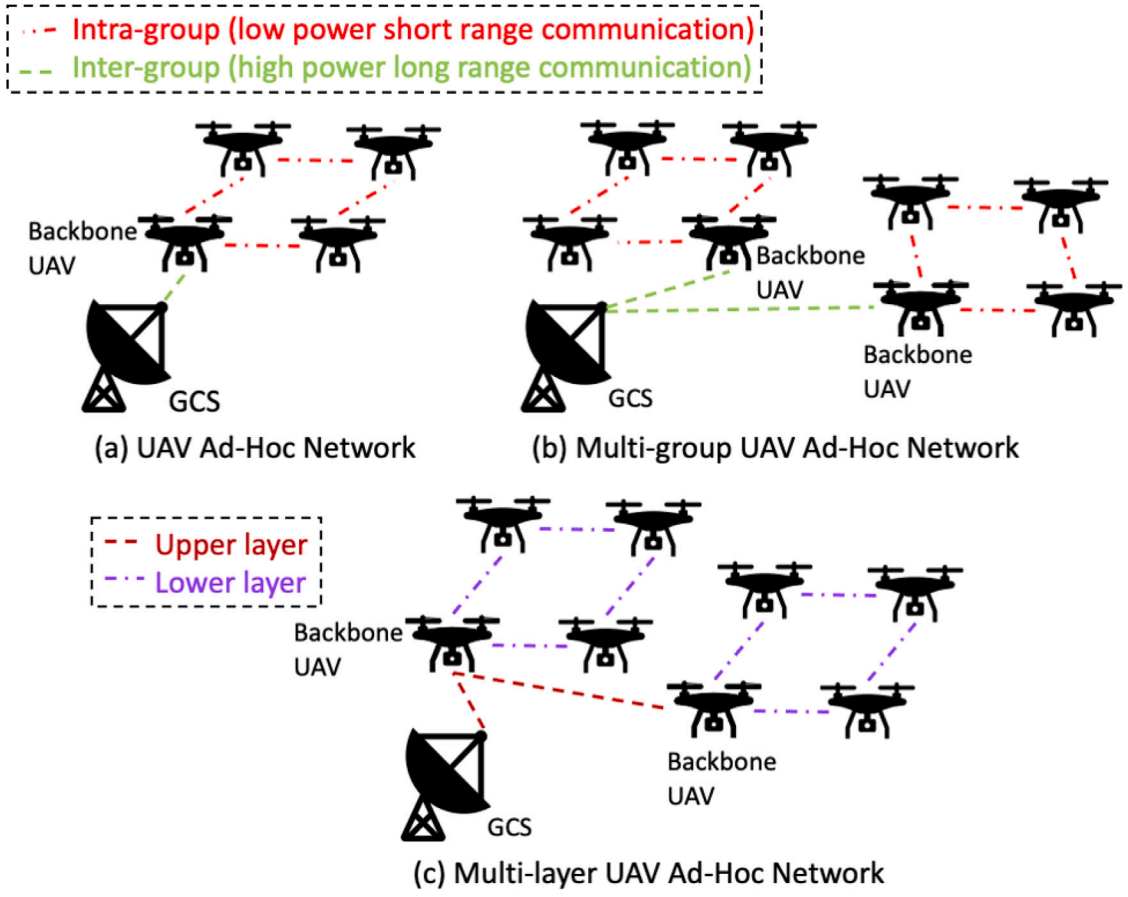


Fig. 5. Decentralised UAV communication architectures.

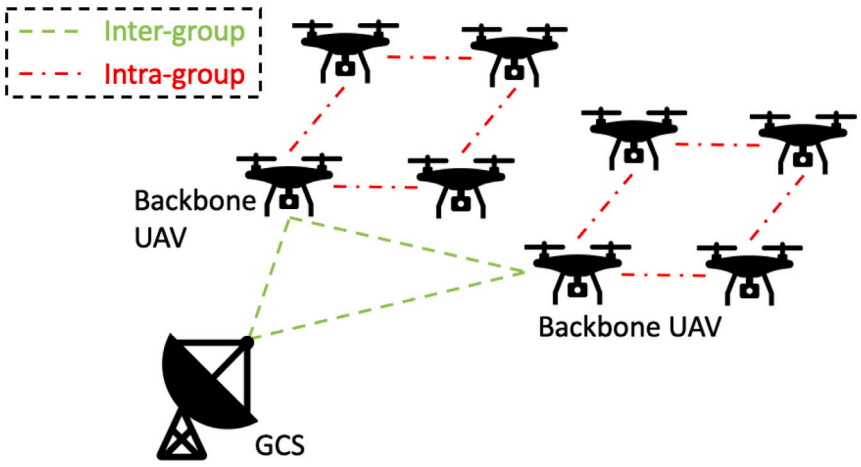


Fig. 6. Inter-group and intra-group communication in FANET.

FANET characteristics are different from those of MANETs and VANETs. For instance, in a typical MANET, the devices do not move around and are contained within a fixed area, hence node mobility is low. However, with FANET, UAVs fly missions based within large aerial areas and, therefore, the node mobility is relatively high. We now introduce FANET characteristics.

2.4.1. Node mobility

Depending on their application and model, UAVs might frequently change their location. Research indicates that UAV speeds can range between 30mph to 179mph [35]; hence FANET has a higher mobility level than MANET and VANET. This characteristic can lead to communication protocol design challenges.

2.4.2. Node density

Cooperating UAVs operate in a specific aerial area, which is usually greater than MANET and VANET; therefore they have the lowest node density [9]. This level of density can lead to communication range design challenges.

Table 2
UAV application scenarios and mobility models.

Scenario	Mobility Models	Explanation
Search and Rescue	RWP [36]	Randomly search target area.
	BSA [37], GM [38], ST [39]	Search specific area.
		Circle an area then chose a specific scan pattern.
	SRC [40], PPRZM [41]	Search for intended target within one specific area.
	DPR [42], SDPC [43]	
Construction	PPRZM	Follow a predefined path to lift elements.
	MP [44]	Operate within time and speed plans.
	DPR	Use the pattern to repeat similar work.
Delivery	PPRZM	UAV flies on predefined path to deliver goods.
	MP	UAV follows the flight time and path plan.
	DPR	Pheromone mapping to enhance network topology.
Network Relay and Coverage	Static [11]	Deploy fixed location UAVs for network communication.
	MG [45]	UAVs act as routers for vehicles to communicate with each other.
Urban Traffic Monitoring	Static	Monitor traffic using a fixed UAV.
	MG	Inspect streets.
	SRC	Monitor incidents before emergency services attendance.
Reconnaissance and Patrol	Static	Continuously monitor first line.
	SRC	Observe the target.
	BSA, GM	Use an unpredictable path in short time intervals to avoid adversaries gaining information.
	DPR, CLMN [46]	Maps of critical areas that might need to be avoided or included.
Environment Sensor	Static	Immobile UAVs act as sensors.

2.4.3. Mobility models

In regards to the mobility models, MANETs use nodes which are ground based, VANETs employ vehicles that move on the highway, whereas FANETs involve UAVs that fly in aerial areas and, in many cases, without significant space limitations. Each of these network types uses different path planning methods. In MANETs, node direction and speed are chosen randomly, but due to highway restrictions in VANETs, path plans are predefined. FANETs have applications that can use predefined plans if required [1]. Table 2 describes six UAV application scenarios with their associated mobility models [9,11]. These mobility models are explained below.

- Static: UAVs do not move to other places and stay in a fixed location [11]. UAVs can be used to monitor urban traffic, inspect streets, or provide a network relay as part of an Internet communication structure.
- Randomised: UAVs operate independently from each other; their direction and speed are chosen randomly over a period of time. The relevant methods are: random walk (RW) [47], random waypoint (RWP) [36], random direction (RD) [48], and Manhattan grid (MG) [45]. These mobility models can be used to achieve search and rescue goals in a randomly selected target area.
- Time and space dependent: These models provide steady changes during the flight. Boundless simulation area (BSA) [37] and Gauss–Markov (GM) [38] define direction and speed based on previous as well as current data calculations. The smooth turn (ST) [39] mobility model makes UAVs circle the sky until they select an appropriate turning point. As the time and space is consistent, UAVs are used for street inspections as well as search and rescue missions.
- Path planning: UAVs follow predefined patterns while flying in the sky. When their mission ends, a new pattern is randomly chosen. Semi-random circular (SRC) [40] makes UAVs circle around specific areas, using a curved movement. Directional patterns can be chosen using the paparazzi mobility model (PPRZM) [41], and their speed is defined randomly. In mission plan (MP) [44], the flight time and speed are predefined on each UAV, when the mission finishes before the flight time, the UAV flies back to the starting point. UAVs can circle a specific area, can help with search and rescue missions or are used for deliveries on a predefined path.
- Group based: There are restrictions on UAVs in certain aerial areas. In reference point group mobility (RPGM) [11], UAVs move randomly around a defined reference point using the RWP model. In Column (CLMN) [46], UAVs also move around the reference point, but then fly on a given line towards a certain direction. In nomadic community (NC), UAVs fly around a given point randomly. In Pursue (PRS) [46], the UAV goes behind a predefined target instead of flying randomly. UAVs can map a critical area with set targets, which is useful for patrol and reconnaissance.
- Topology control based: To fulfil certain topology requirements, UAVs need to communicate in real time. In distributed pheromone repel (DPR) [42], a pheromone map is held by each UAV, which it then follows. On other similar models, UAVs mark each area on the map then broadcast to others [49]. To extend connection coverage, self-deploy point coverage (SDPC) [43] creates UAV groups that construct a common communication architecture. UAVs scan then search a predefined, specific area to assist with search and rescue missions. UAVs can also be configured to repeatedly scan the same area.

2.4.4. Frequent topology changes

Due to link outages, FANET topologies are often difficult to compare to those in VANETs and MANETs. These outages are often caused by the fast movement of UAVs and unpredictable environmental conditions such as thunder or lightning [1,9].

2.4.5. Network lifetime and power consumption

In MANETs, network lifetime depends on the device and its computationally energy efficient protocols. In FANETs, the network communication is controlled by the UAV energy source, not the device itself; hence, there are typically no power resource problems [1].

2.4.6. Radio propagation models

MANETs and VANETs use ground-based operations; therefore, buildings could affect their radio signals, as opposed to FANETs which use sky-based radio propagation. Using LoS between GCS and UAV means that FANET radio signals are not subject to interference [9].

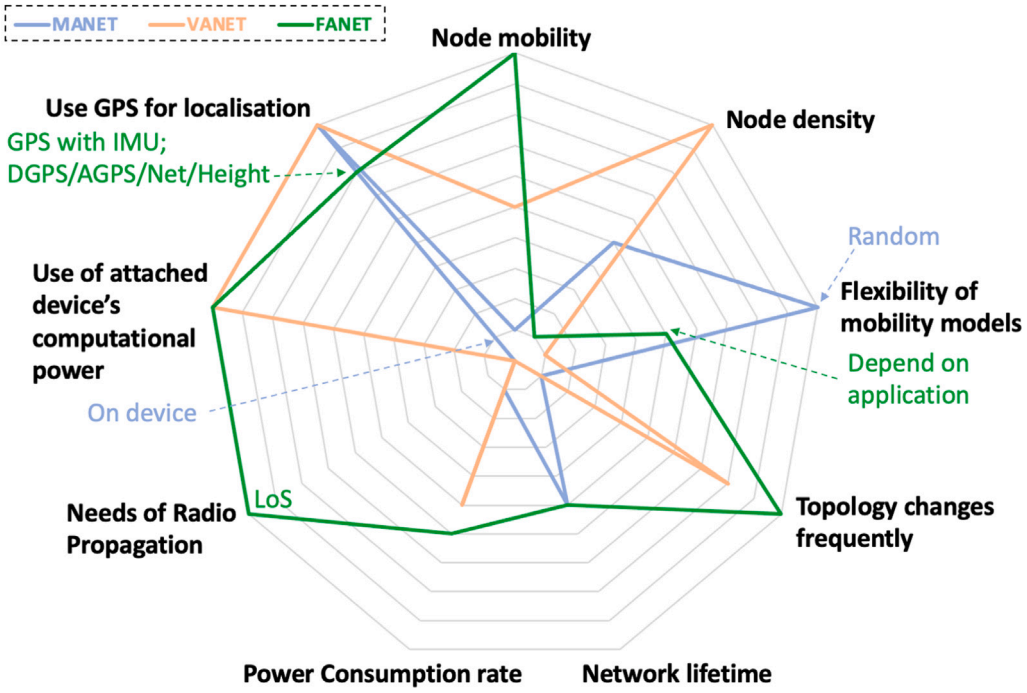


Fig. 7. Comparison of MANET, VANET, and FANET characteristics.

2.4.7. Computational power

Individual MANET devices such as personal digital assistants (PDAs), smart phones, and laptops have limited computational power. VANETs and FANETs employ customised devices for each application. UAVs can only carry devices of a limited weight and size, which restricts the available FANET computational power [1].

2.4.8. Localisation

An accurate geo-location plays a vital role in preventing collisions and gives better coverage to cooperating UAVs. The geo-location needs to be updated in real-time or short time periods. With MANETs, GPS governs the mobile node location. Whenever GPS is not accessible, a beacon node is deployed. To improve VANET safety, a navigation-grade GPS, assisted GPS (AGPS), and differential GPS (DGPS) can be implemented to help avoid vehicle collisions. In FANETs, as UAVs move quickly, data should be updated in real time. Hence, each UAV has its own GPS device and IMU, so that the geo-location data can be shared among UAVs [1].

Based on the above discussion, FANET design must incorporate the following characteristics: high node mobility, low node density, frequent topology changes, power consumption based on different UAV types, long network lifetimes, LoS radio propagation, and the use of GPS with IMU. Computational power depends on devices attached to the UAV and localisation which is achieved by GPS with IMU. UAV usage and coverage can be optimised by carefully managing these characteristics. Fig. 7 compares MANET, VANET, and FANET characteristics [1,11,13]. We outline them below: (i) the *node mobility* is low in MANETs, medium in VANETs, and high in FANETs; (ii) the *node density* is high in VANETs, medium in MANETs, and low in FANETs; (iii) while VANETs need a predefined *mobility model*, MANETs use it randomly, and FANETs choose it based on their application; (iv) the *topology change frequency* is slightly lower in VANETs than in FANETs, whereas it is low in MANETs; (v) *network lifetime* in MANETs is based on the device power consumption, unknown in VANETs, and based on UAV types in FANETs; (vi) FANETs require LoS for *radio propagation*, whereas MANETs and VANETs do not; (vii) MANETs and VANETs rely on GPS for *localisation*, whereas FANETs use GPS with IMU; (viii) for *computational power*, MANETs rely on its own device, VANETs and FANETs attach other devices to support it.

3. Related work

In this section, we review 10 existing surveys related to FANETs. These surveys are compared based on security and non-security features, as well as the coverage of security requirements and threats. Our comparison results demonstrate that the coverage of the security requirements and threats in the existing surveys is not sufficient. These results are presented in Tables 3, 4, 5, 6, 7, and 9, and are discussed below. Tables 3 to 7 use the following key: ✓ means the term is discussed in detail or clearly defined; **o** shows the term is mentioned without detailed discussion; and ✗ indicates that the term is not mentioned in context.

3.1. FANET features and security requirements

Most of the surveys reviewed UAS communication protocols, mobility models, as well as FANET security and privacy features. Table 3 compares the non-security features of the reviewed surveys. These features are: FANET characteristics, trajectory optimisation, UAV relay, hardware constraints, charging, mobility models, and communication protocols. Table 4 classifies FANET connections, nodes, communication protocols and their related security as well as privacy threats. Solutions to these threats based on network communication over FANET are also presented. Table 5 presents communication protocols security and privacy threats. Some surveys provided solutions in addition to threats.

Bekmezci et al. [1] provided a series of issues related to FANET communication protocols. The authors identified availability issues such as collision avoidance, data transmission quality, and flow control, but did not provide any solutions to these issues. Other surveys [9,10,12,13,15,16] outlined communication security threats and solutions in detail, but privacy threats and anonymisation of identities were not given much coverage. We note that Cabuk et al. [15] mainly discussed UAV manipulation using SkyNet [51] to collect data from personal mobile devices or computers. Work by Khan et al. [50], categorises attacks on communications between UAV and GCS based on security requirements and attacks. The authors summarise that although there are common FANET communication protocols, security within these

Table 3
Non-security features in existing surveys.

Reference	[1]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[50]	This survey
FANET charac.	✓	o	✓	✗	✗	✗	✗	✗	✓	✗	✓
Traj. optim.	✗	✓	✗	✗	o	✓	✗	✗	o	✗	✓
UAV relay	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓
Hardware constr.	✓	✓	✓	✗	✗	✓	✗	✓	✓	✗	✓
Charging	✗	✗	✗	✗	✗	✓	✗	✗	o	✗	✓
Mobility models	o	✓	✗	✓	✗	✗	✗	✗	o	✗	✓
Comm. protocols	✓	✓	✓	✗	✓	✓	✓	o	✓	✗	✓

Table 4
Security features in existing surveys. T: Threats, S: Solutions.

Ref.		[1]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[50]	This survey
Comm. protocols	T	o	✓	✓	✗	✓	✓	o	✓	✓	✓	✓
	S	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓
Privacy	T	✗	o	o	✗	✓	✗	✗	✓	✗	✓	✓
	S	✗	✗	✗	✗	✓	✗	✗	✓	✗	✓	✓

Table 5
Comparison of security and privacy threats (T) and solutions (S).

Ref.		[1]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[50]	This
Comm. protocols	T	o	✓	✓	✗	✓	✓	o	✓	✓	✗	✓
	S	✗	✓	✓	✗	✓	✓	✗	✓	✓	✗	✓
Privacy	T	✗	o	o	✗	✓	✗	✗	✓	✗	✓	✓
	S	✗	✗	✗	✗	✓	✗	✗	✓	✗	✓	✓

Table 6
The coverage of security requirements in existing surveys.

Ref.	[1]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[50]	This
Confiden.	o	✓	✓	✗	✓	✗	✗	✓	✗	✓	✓
Integrity	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✓
Availability	o	✓	✓	✗	✓	o	✓	✓	✓	✓	✓
Authentica.	o	✓	✓	✗	✓	✗	o	✓	✗	✓	✓
Authorizat.	✗	o	✓	✗	✓	✗	✗	✓	✗	✗	✓
Non-Repud.	✗	o	✓	✗	✓	✗	✗	✓	✗	✗	✓

protocols is an important issue. Finally, [12] investigates data relating to people's houses, locations and behaviours that can be discovered by airborne UAVs. After reviewing [12,15], privacy threats were identified when attackers connect to Internet of things (IoT) devices using UAVs. Methods to defend against these threats include adding UAVs to restricted zones in a *NoFlyZone* database [52] and using UAV tracking.

Fig. 8 shows the Microsoft STRIDE Threat Model [53], with threats on the left-hand side and security requirements on the right-hand side. Based on Fig. 8, Table 6 indicates whether or not the security requirements are covered in each survey. In [11], the authors focused on UAV application scenarios and mobility models. Other surveys [9,10,12,14–16] discussed the availability related to FANET. Some works [9,10,12,14,15] provided identity verification methods concerning the authentication security requirement; at the same time [9,10,12,15] addressed the confidentiality, integrity, and authorisation requirements whilst deploying cooperating UAVs. Fig. 9 depicts the percentage of the security requirements included in the surveys in Table 6. Symbols ✓, **o**, and ✗ are converted into weights 1, 0.5, and 0, respectively. Availability is the most discussed requirement with 25%. This is followed by authentication at 18%, confidentiality at 16%, and then integrity at 15%. Finally, authorisation and non-repudiation are at 13% each. Note that the information outlined in Table 6 and Fig. 9 only provides a brief overview of UAV security requirements. These security requirements and threats are further expanded on in Sections 4 and 5.

Table 7
Security threats in FANETs.

Ref.	[1]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[50]	This
Active interfering	o	o	✗	✗	✓	o	✗	✓	✓	✗	✓
Backdoor malware	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Black hole	✗	✗	✓	✗	o	✗	✗	✗	✓	✗	✓
Collisions	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Data tempering	✗	o	✗	✗	o	✗	✗	✓	✗	✗	✓
De-authentication	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
DoS	o	o	o	✗	✓	✗	✗	✗	✗	o	✓
Eavesdropping	✗	o	✓	✗	✓	✗	✗	✗	✗	o	✓
Flooding Attack	✗	✗	✗	✗	✗	✗	✗	✗	✗	o	✓
GPS Spoofing	✗	✗	✗	✗	✓	✗	✗	✓	✗	o	✓
Grayhole	✗	✗	✓	✗	o	✗	✗	✗	✗	✗	✓
Impersonation	✗	o	✓	✗	✗	✗	✗	✓	✗	o	✓
Insider	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Jamming	o	✗	o	✗	✓	✓	✗	✓	✗	o	✓
LLQ & HL	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
MITM	✗	✗	✗	✗	✓	✗	✗	✓	✗	o	✓
Modification	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗	✓
Replay	✗	o	✗	✗	✓	✗	✗	✗	✗	o	✓
Rushing	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓
Selfishness	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓
SPOF	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Sybil	✗	✗	✗	✗	o	✗	✗	✗	✗	✗	✓
SYN Flood	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Wormhole	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓

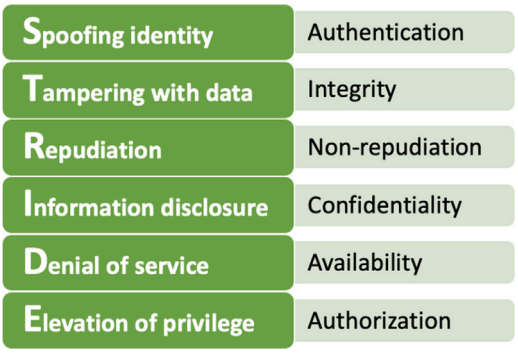


Fig. 8. The Microsoft STRIDE Threat Model.

3.2. Security threats and solutions

Table 7 outlines how the security threats discussed in the existing surveys could be used to manipulate FANETs, whereas Fig. 10 illustrates the percentage of each security threat. As before, symbols ✓, **o**, and ✗ are converted into weights 1, 0.5, and 0, respectively. It can be seen from Fig. 10 that the main threat is active interfering which accounts for 13%. This is followed by jamming with 12% and modification with 9%. Blackhole, DoS, eavesdropping, and impersonation are at 7% each. Data tempering, GPS spoofing, and man-in-the-middle (MITM) are at 6% each. Grayhole and replay are at 4% each. Rushing, selfishness as well as wormhole are at 3% each. Sybil is the least discussed at 1%. We observe that none of the surveys discusses the following security threats: backdoor malware, collisions, de-authentication, insider, low link quality and high latency (LLQ & HL), single point of failure (SPOF), and SYN flood. They are compared and categorised in Sections 5 and 6.

Tables 9 and 10 summarise the security solutions given in each survey and also highlight which solutions are covered in our survey. Given that our work focuses on UAV and FANET security and privacy only, some solutions from [12,13,15] are not presented. In Tables 9 and 10, the security requirements are: confidentiality, integrity, availability, authentication, and privacy. Detection is also added to show whether or not appropriate detection methods exist. We also define the abbreviations that relate to the solution names in Table 8.

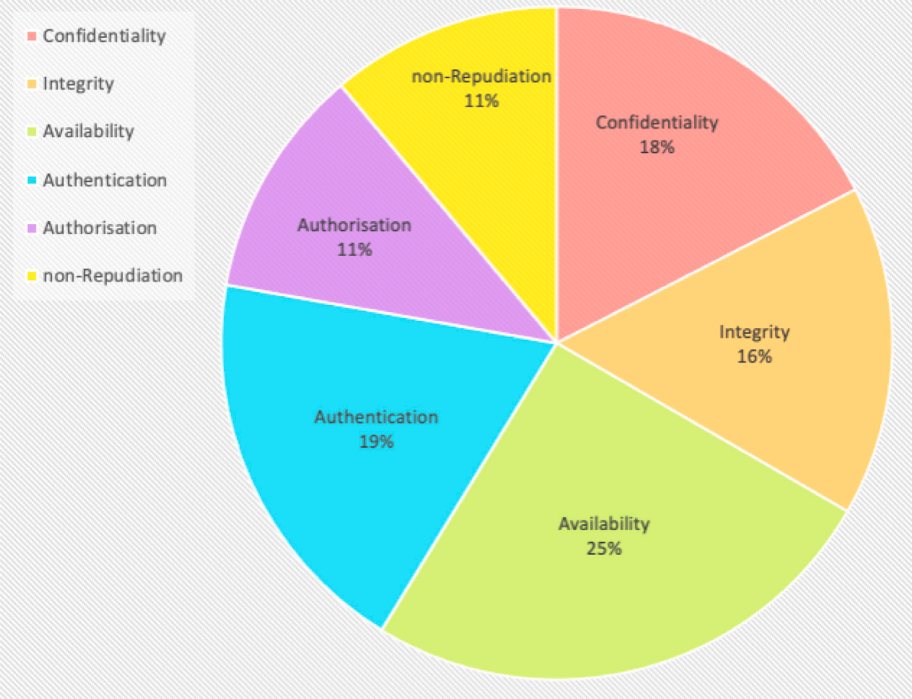


Fig. 9. Percentage of security requirements in existing surveys..

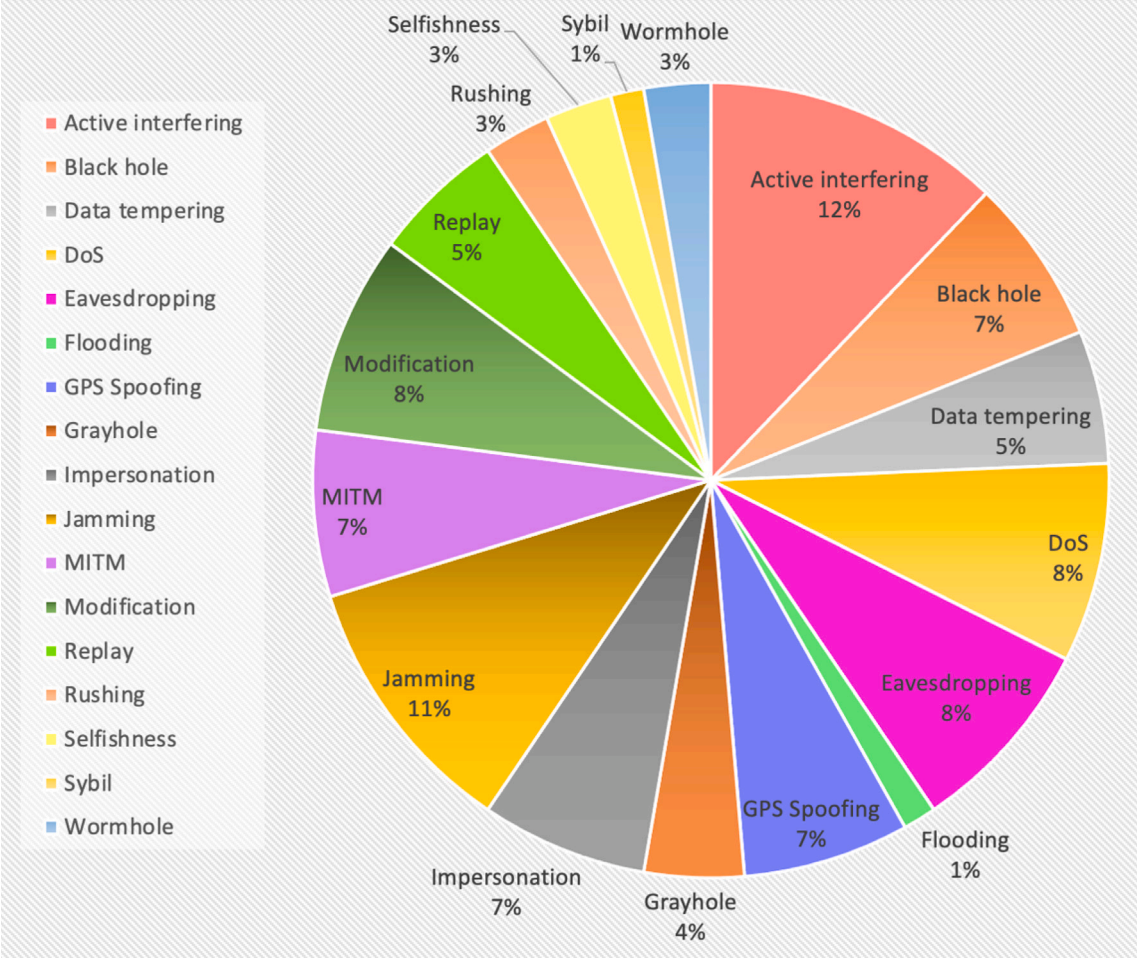


Fig. 10. Percentage of security threats in FANETs..

Table 8
Abbreviations of solutions.

HIBBE	Hierarchical Identity-Based Broadcast Encryption [54]
CBE	Certificate-Based Encryption [55]
eCLSC-TKEM	efficient Certificateless Signcryption Tag Key Encapsulation Mechanism [56]
SSM	Spread Spectrum Methods [10]
UFH	Uncoordinated Frequency Hopping [57]
U-DSSS	Uncoordinated DSSS ite47
USD-FH	Uncoordinated Seed Disclosure in Frequency Hopping [58]
SEAD	Secure Efficient Ad-hoc Distance [59]
LLSP	Link-Layer Security Protocol [60]
D & P schemes	D & P schemes [10]
HLWT-IDS	Hybrid lightweight IDS [12]
R-IDS	Rule-Based Intrusion Detection [61,62]
S-IDS	Signature-Based Intrusion Detection [63,64]
A-IDS	Anomaly-Based Detection [65]
QL	Q-Learning [66]
TPPA	Traceable and Privacy-Preserving Authentication [67]
FE	Functional Encryption [68]
QMR	Q-learning-based Multi-objective optimisation Routing protocol [69]
QFLR	Q-learning-based Fuzzy Logic for multi-objective Routing protocol [70]
FL	Federated Learning [71]
AN	Autonomous Navigation [72]
AS	Authenticity of the drone Signals [73]
LBA	Location-Based authentication [74]
DroneSig	Lightweight Digital Signal Protocol [75]
Lids	Lightweight Distributed detection Scheme [76]
CRP-PUF	Challenge-Response Pair of Physical Unclonable Function [77]
JarmRout	Jamming-Resilient Multipath Routing Protocol [78]
IHP	Improved Protocol based on Hussain et al's Design [79]
GCACS-IoD	Certificate-based Generic Access Control Scheme for Internet of Drones [80]
DNA-DAW	Distributed Network Architecture with Double-Authentication Watermark [81]
SAUVA	Secure Agent Unmanned Aerial Vehicle [82]

4. A taxonomy of security threats based on threat vectors

In this section, we present our taxonomy of FANET security threats based on threat vectors, as shown in Fig. 11. The set of threat vectors consists of six connection types and six node types. We then classify and compare 20 security threats based on security requirements and network types. By using the STRIDE Threat Model [53] in Fig. 11, we identified the threats in both connections and nodes, which are categorised in Table 11. We then consider their impact with relation to security and privacy in Tables 12, 13, and 14.

Fifteen of these threats are related to connections, whereas five threats are related to nodes. In addition, fifteen security solutions are presented to the threats; these solutions are discussed in detail later in Section 6. The existing solutions are over six network types: 5G mobile networks, FANETs, other types of Ad-Hoc Networks, RW, WLAN, and WSN.

4.1. Threat vectors

Below, we describe the threat vectors of Fig. 11.

- **Connections**

1. C1: connection between client terminals and GCS; client terminals can be personal computers (PC) or mobile devices.
2. C2: connection between GCS and backbone UAV; possible communication methods include Internet, radio, or satellite communications.
3. C3: connection between backbone UAV and other UAVs in a FANET.
4. C4: connection among legitimate UAVs in a FANET.
5. C5: connection of a FANET with an unknown UAV who sends join requests.
6. C6: connection to a cloud service from the backbone UAV, other UAVs, or ground devices (GDs). GDs include client terminals and GCS. In cases where UAVs or GDs have limited resources, operational data is transferred to a cloud service for computation, then sent back to the UAV or GD for execution.

- **Nodes**

1. *A client terminal* can be a PC or a mobile phone; these transmit pilot control signals to a UAV.
2. *Authorised UAVs* that form the FANET.
3. *New UAVs* that send requests to join the FANET.
4. *GCS* is the node that exchanges data via a wireless link with the backbone UAV.
5. *Backbone UAV* acts as a gateway to transfer data between UAVs and a GCS. It uses a long-range signal to communicate with the GCS.
6. *Cloud Services* compute UAV operational data [17].

4.2. A taxonomy of security threats

Tables 12, 13, and 14 provide a taxonomy of security threats based on connections and nodes. In addition, they identify the relevant *Impact* on Confidentiality (C), Integrity (I), Availability (A), and Privacy (P). For each type of threat, appropriate solutions have been presented. The last column in the tables provides specific sections of this survey where the relevant information has been explained in detail.

Tables 12 and 13 present solutions related to the five network types: FANET (F), IoD, RW, 5G, WLAN, and WSN. In order to gauge the recency of the solution, its publication year is provided. We observe that the solutions consider different numbers of threats; for example [32] mitigates four security threats, whereas [17,88] only two.

The five network types are categorised according to the design of the solutions. For example, solutions for eavesdropping tend to focus on designs that are based on radio waves [87] and 5G [88]. Some jamming solutions are designed using WLAN [10,57,99,100]; solutions to prevent Sybil attacks are designed in WSN architecture. Other, non-specific designs utilise aerial networks with FANETs or the IoD.

Table 14 provides a taxonomy of security threats based on nodes. The solutions are given in a chronological order, with further details outlined in Section 4.4. It should be noted that Section 6 provides an explanation or workaround for solutions not listed here. Fig. 12 presents 12 security threats based on connections and nodes. These are explained in the subsections below. The security solutions, shown in the figure, are explained in Section 6.

4.3. Security threats on connections

We now evaluate the security threats on connections (C1 to C6) of Fig. 12.

C1: Communication between a client terminal and a GCS. A client terminal sends control signals to a GCS via wireless connections. This wireless connection could be eavesdropped, the client terminal could be maliciously controlled or infected with malware. We discuss these threats below:

Table 9
Coverage of security requirements and solutions in existing surveys (Part I).

Ref.	[9]	[10]	[12]	[13]	[15]	This Survey
Conf.	CBE [55] eCLSC-TKEM [56] HIBBE [54]	SEAD [59] SSM: UFH [57] U-DSSS [57] USD-FH [58] DSSS [57]	R-IDS [61,62] TPPA [67] QL [66] FE [68]	✗	AN [72]	CoMAD [32], DM [83], ETS [84], IBE-Lite [17], MDD [85,86], mmWave-ULA [87], PA [88], TBC [89], DroneSig [75], CRP-PUF [77], JarmRout [78], IHP [79], GCACS-IoD [80], DNA-DAW [81]
Int.	CBE [55] eCLSC-TKEM [56]	SEAD [59] SSM: UFH [57] U-DSSS [57] USD-FH [58] DSSS [57]	R-IDS [61,62] TPPA [67] QL [66] FE [68]	✗	AN [72]	DM [83], ETS [84], IBE-Lite [17], MDD [85,86], TBC [89], DroneSig [75], IHP [79], GCACS-IoD [80], DNA-DAW [81]
Aval.	HIBBE [54] CBE [55]	SEAD [59] SSM: UFH [57] U-DSSS [57] USD-FH [58] DSSS [57]	A-IDS [65] R-IDS [61,62] TPPA [67] QL [66]	FL [71] QFLR [70] QMR [69] RLSRP-PPMAC [90]	A-IDS [91]	AFRL [92], AMUAV [93], CADA [94], CF-MAC [95], CoMAC [32], CUSUM [96], DRI & CC [97], DSSS [10], FBTM [98], FHSS [99,100], FLBD [101], H-IDS [102], HID-RS [103], IBE-Lite [17], LODMAC [104], LTA-OLSR [105], MPR [106], QFLR [70], QMR [69], RLSRP-PPMAC [90], SAODV [107], TBC [89], TBP [108], UFH [57], ZSP [17], DroneSig [75], Lids [76], JarmRout [78], IHP [79], SAUAV [82], GCACS-IoD [80], DNA-DAW [81]

Table 10
Coverage of security requirements and solutions in existing surveys (Part II).

Ref.	[9]	[10]	[12]	[13]	[15]	This Survey
AuthN	CBE [55] eCLSC-TKEM [56] HIBBE [54]	LLSP [60] ARAN [109]	eCLSC-TKEM [56] TPPA [67]	✗	AS [73]	ARAN [109], CoMAD [32], LWT-SEA [17], PA [88], S-RSSI [110], IHP [79], GCACS-IoD [80], DNA-DAW [81]
Privacy	HIBBE [54] CBE [55]	✗	TPPA [67]	✗	✗	CoMAD [32], DM [83], MDD [85,86], mmWave-ULA [87], PA [88], TBC [89], CRP-PUF [77], JarmRout [78], IHP [79], GCACS-IoD [80], DNA-DAW [81]
Detect.	✗	D&P schemes [83,111,112]	R-IDS [61,62] S-IDS [63,64] A-IDS [65]	FL [71]	A-IDS [91] LBA [74]	DM [83], H-IDS [102], MDD [85,86], TBC [89], DNA-DAW [81]

- *Eavesdropping*. This is also called a *passive attack*. The attacker passively listens over the network to the message in order to obtain important information without tampering with the data [113]. This information could be an encryption key, sent during the authentication process [32], or sensitive UAV messages. Fig. 13 shows the basic model of an eavesdropping attack.
- *Insider threat*. An employee who steals or manipulates data to damage FANET is called an insider. This attack assumes that the employee has access rights to the UAV's location and identity data, which is used for navigation [17].
- *Replay attack*. Secure communications contain only messages that are encrypted. Instead of decrypting these messages, the attacker re-sends them to the GCS. The GCS is misled into believing that the attacker is the original sender, creating a potential data communication channel between the attacker and GCS [114]. Fig. 14 provides an illustration of a replay attack.

C2: Communication between a GCS and a backbone UAV. According to [12], standard wireless communication protocols are implemented between a GCS and a backbone UAV. This could be the IEEE 802.11 standard (using 2.4 GHz, 5 GHz) or Bluetooth. If authentication methods are not properly configured, these protocols could be subject to eavesdropping or man-in-the-middle (MITM) attacks. Below, we discuss three possible communication methods, their security threats and workarounds.

- *Internet (WiFi) - high frequency*. Connections are based on well-known and public standard wireless communications, such as Bluetooth or IEEE 802.11 2.4/5 GHz. These normally deploy single-factor authentication, which can be prone to eavesdropping or MITM attacks [12]. To secure the communication, appropriate security features should be implemented and the 3 GHz, 4 GHz, 5 GHz frequency bands or 4G+ (LTE) standard should be utilised.
- *Radio frequency (RF) - low frequency*. According to NASA [115], radio spectrum frequencies are between 1 kHz and 100 GHz. WiFi tends to use super high frequencies (SHF) from 3 to 30 GHz, whilst broadcast radio transmissions are mainly on the very high frequency band (VHF) which is from 30 to 300Mhz. In radio propagation, an interference mitigation technique is deployed whilst using an up-link to control the flight and a down-link to transfer telemetry and payload data [9]. In order to prevent radio jamming, interference between frequencies should be considered. This type of *jamming attack* is discussed in further detail below.
- *Satellite*. Satellites use GPS to synchronise data in real-time; this means that the UAV can be called back when it is out of LoS. Satellite communications are relatively secure, but expensive and require regular maintenance [12]. Satellites are not widely employed by commercial or civil UAVs, hence their security issues are not discussed in this survey in detail.

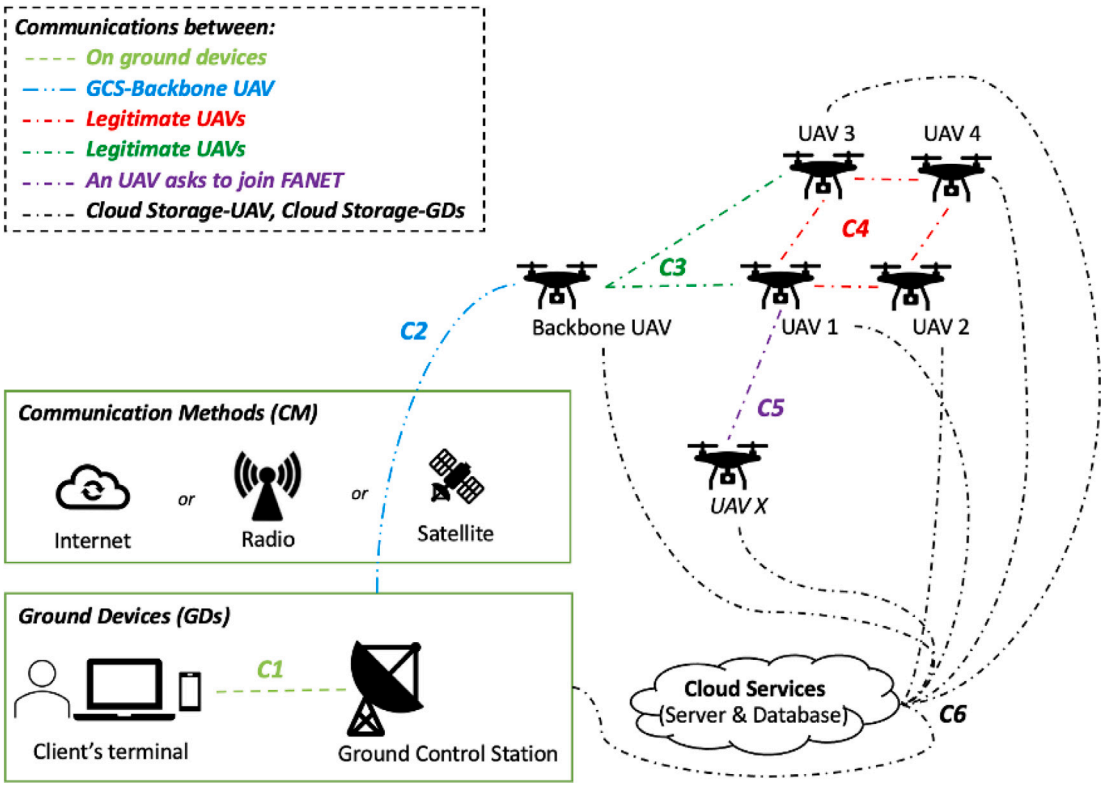


Fig. 11. Security threat vectors in FANETs.

The security threats of eavesdropping, jamming, MITM, and replay that these connections could be subject to are now outlined.

- *Eavesdropping*. Similarly to the eavesdropping attack in C1, Fig. 15 shows an attacker listening to unencrypted messages over the communication channel; they then learn that a UAV is being sent, for example, to the University of York.
- *Jamming*. Can be created by intentional or unintentional causes. When a radio signal is interfered by other signals, legitimate communications are disrupted [92]. In some literature, jamming attacks are also called *active interfering* [9] or *interference,07*. According to [92], three jamming models can cause disruption: (i) constant jamming model is used to follow the regular radio signal; (ii) random jamming model swaps between sleeping and jamming mode; and (iii) in the reactive jammer (jamming attacker) model, a radio signal is transmitted whenever activity is heard on the communication channel [92]. Fig. 16 uses a red circle to illustrate the range of the jammer, where communication between the GCS and UAV is interrupted.
- *Man-in-the-middle (MITM)*. As opposed to eavesdropping, the attacker actively manipulates the message after listening to it [116]. Fig. 17 illustrates a situation where a GCS has communicated with the backbone UAV, the original connection is intercepted by a malicious UAV and discarded. The malicious UAV is then able to drop, modify, or send messages to the GCS.
- *Replay*. Similar to the replay attack in C1, Fig. 18 shows the attacker sniffing encrypted messages between a GCS and a UAV. The attacker then re-transmits these messages to the backbone UAV, disguising itself as a legitimate sender.

C3 and C4: Communications between a backbone UAV and other UAVs. Note that C3 and C4 are slightly different, although they have some similarity. Whereas C3 is the connection between a backbone UAV and other UAVs, C4 is the connection among the non-backbone UAVs that forward and share the information they receive from the backbone UAV. Due to their similarity, C3 and C4 are discussed together in Tables 11, 12, and 13.

Data sharing and privacy issues may exist in the communication that takes place between UAVs. A VANET pseudonym scheme (PUCA) to anonymise communications uses real identities [117]. However, in some FANET architectures, the UAVs need to broadcast their location to avoid collisions. In this case, PUCA might not be suitable for FANET. UAV-to-UAV communication is a type of peer-to-peer (P2P) communication, where communication standards are not currently defined [12]. Hence, it is easier to launch attacks over different P2P communication channels. For this purpose, eavesdropping, jamming, MITM, replay, and Sybil are now considered by adversaries.

- *Eavesdropping*. Attackers listen to unencrypted messages amongst the backbone UAV and UAVs in a similar manner to C1 and C2. Fig. 19 shows an attacker eavesdropping, they discover that at least one UAV is going, for example, to York Minster to take 5 photos.
- *Jamming*. A basic model for a jamming attack is illustrated in Fig. 20. The jammer's range is denoted by a red circle; communications between UAV 1, UAV 2, and the backbone are interfered with [92].
- *Man-in-the-middle (MITM)*. The original communication channels are interrupted and replaced by a malicious UAV [32,116]. The malicious UAV then has the ability to modify, drop or send fake messages. Fig. 21 shows the MITM attack between a backbone UAV and UAV 1, and between UAV 1 and UAV 2.
- *Replay*. A malicious UAV flies around a swarm of UAVs listening to any encrypted messages. Posing as a legitimate sender, the malicious UAV then re-sends these encrypted messages to another UAV [32]. This process is depicted in Fig. 22.
- *Sybil attack*. After a malicious UAV joins the FANET, it creates virtual identities (known as Sybil nodes) such as v1, v2 and v3, shown in Fig. 23. Legitimate UAVs are deceived into believing that these virtual identities have joined the network. If a

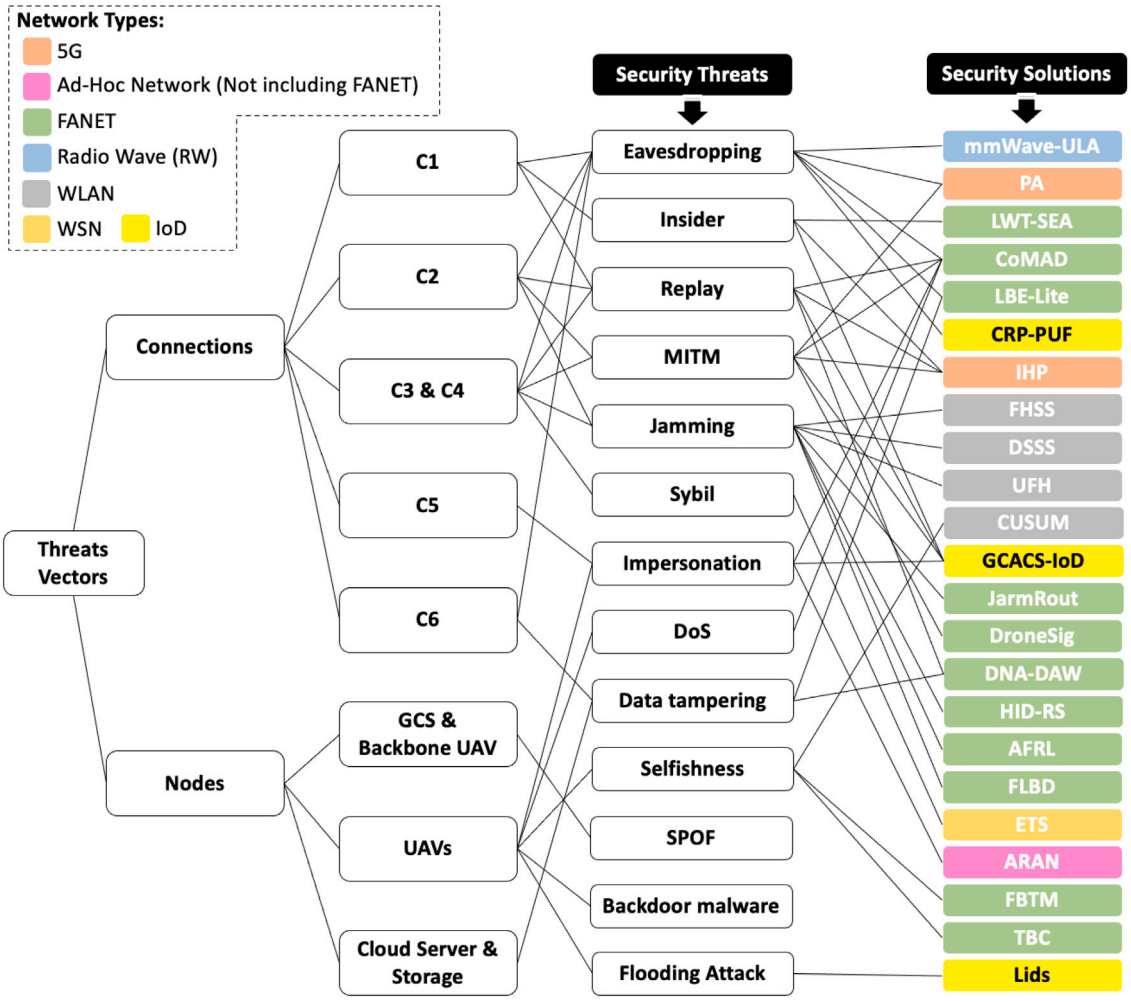


Fig. 12. Security threats on connections and nodes.

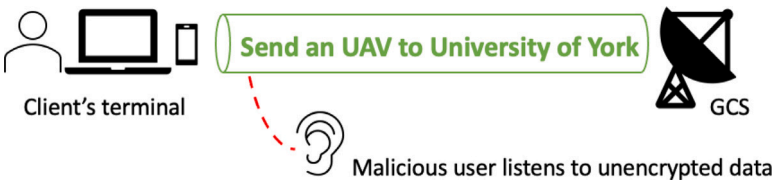


Fig. 13. Eavesdropping Attack.

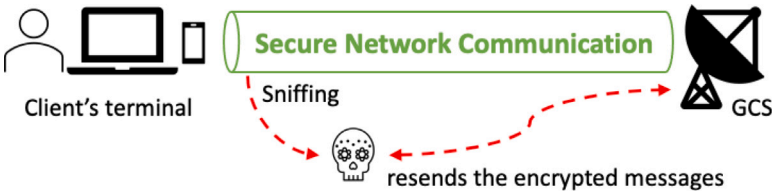


Fig. 14. Replay Attack.

sufficient amount of Sybil nodes are deployed, further attacks, like blackhole, rushing, or grayhole (discussed below) can take place [118].

C5: A new UAV requests to join the FANET. An important threat here is the *impersonation/identity spoofing*. A malicious UAV uses a spoofed identity [32] to attempt FANET re-entry. The malicious UAV claims that it was originally part of the FANET, rather than initiating the usual authentication process of sending a *request message* to the backbone UAV. Fig. 24 shows UAV X impersonating UAV 3 to deceive UAV 1 into believing that it is a part of FANET.

C6: Communications among a backbone UAV, non-backbone UAVs, and ground devices (GDs) to cloud services. Cloud Security Guidance from the National Cyber Security Centre (NCSC) [119] provides several recommendations during data transfer. These recommendations include

Fig. 15. Unencrypted Eavesdropping Attack.

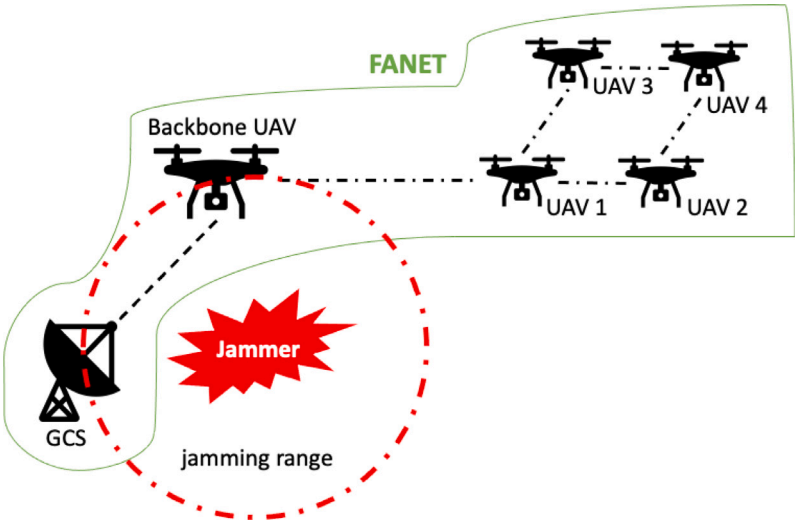


Fig. 16. GCS Jamming Attack.

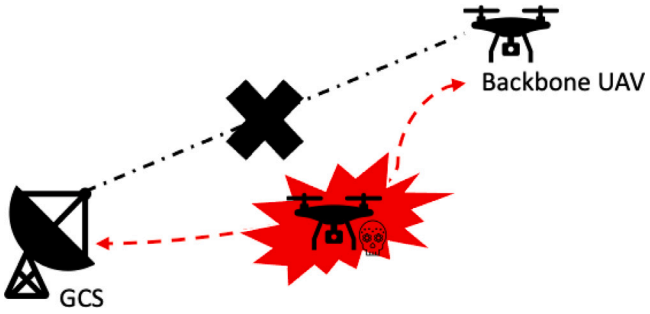


Fig. 17. GCS MITM Attack.

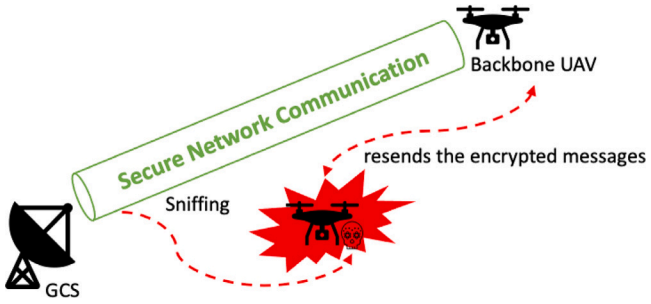


Fig. 18. Backbone UAV Replay Attack.

the rejection of unauthorised data injection and deploying encryption methods to prevent data from tampering as well as eavesdropping.

- *Data tampering*. Sensitive data might be tampered with during transmission. These data could be session keys, operational information or UAV sensor readings [17,32].
- *Eavesdropping*. Communications between cloud server, cloud database and UAVs or a GCS should be protected from eavesdropping.

In the sections above, we discussed the most important security threats in FANETs. C3 to C6 are concerned with high mobility and frequent topology changes [1,9]. C1 and C2 share the same characteristics; although C1 and C2 barely change location they can still be affected by the connected UAVs. Hence it is important to have real-time data updates without any delays. Time is crucial for both data transmission and in preventing replay attacks which can cause authentication process failures for legitimate UAVs.

4.4. Security threats on nodes

We now discuss the security threats on nodes, which are individual devices that exist in the UAS [22,23]. Fig. 11 depicts nodes that could be client terminals, GCS, or UAV. FANET operation can be affected by the node security, for example if a node fails to forward messages, another node could take over control of the mission.

Client terminal. It could be attacked in order to send malicious or fake commands which affect FANET operation. Each attack method

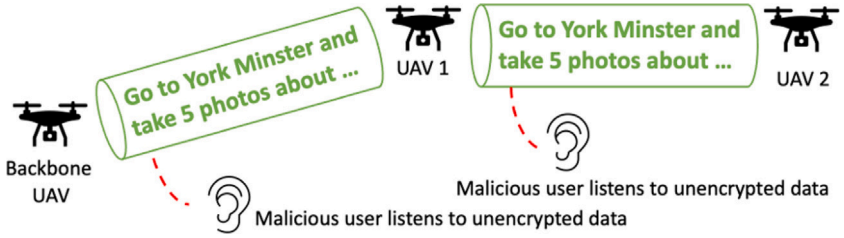


Fig. 19. UAV Eavesdropping Attack.

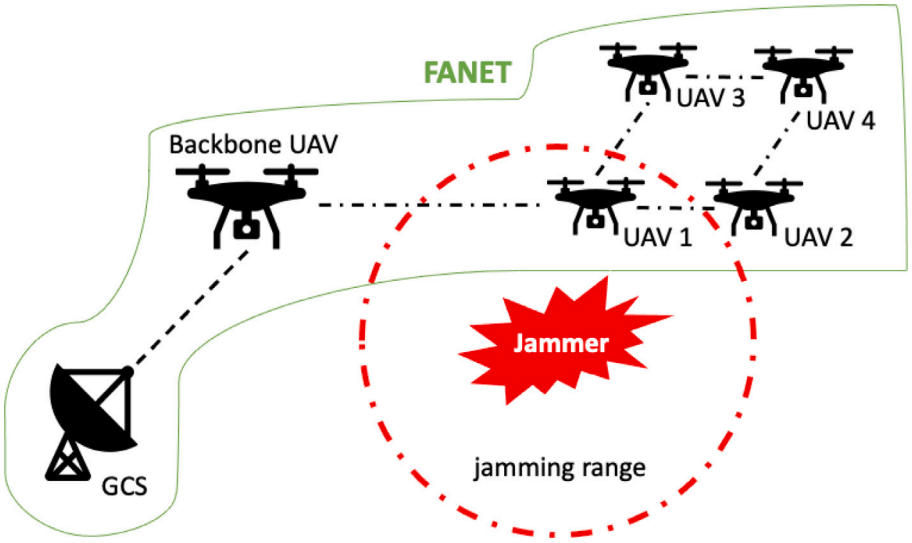


Fig. 20. UAV Jamming Attack.

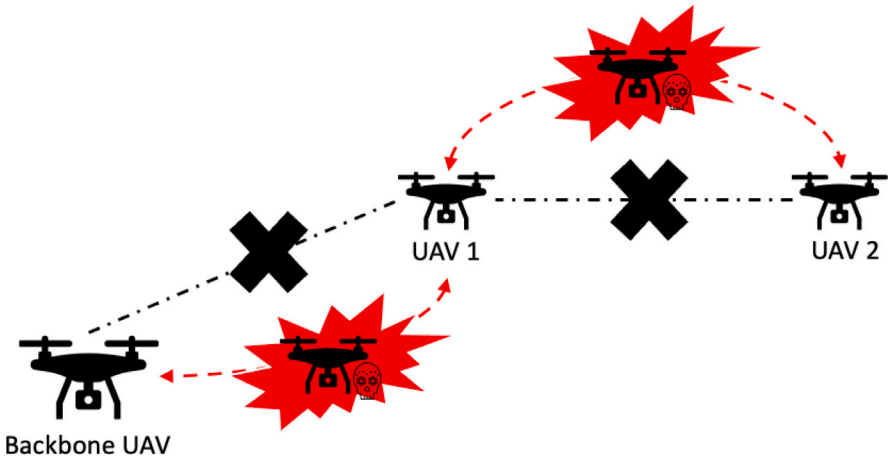


Fig. 21. UAV MITM Attack.

could be specific to the terminal hardware (e.g., personal computer, mobile phone) and its platform (e.g., Apple, Android).

GCS and backbone UAV — single point of failure (SPOF). Normally there is one GCS and one backbone UAV operational. In order to provide resilience, multiple GCSs, and backbone UAVs should be implemented that can automatically operate in case of failure [32].

UAVs. The following major threats have been identified:

- *Backdoor*. In 2015, The Hacker News [120] reported that the *Parrot AR drone* contained a backdoor that allowed the UAV radio signal to be hijacked. In the same year, a researcher Rahul Sasi [121] claimed that the first UAV backdoor malware *Maldrone* had been developed for the *Parrot AR drone*. Maldrone can be installed silently and uses a TCP connection to a bot controller to interact with UAV communications and proxy their data. Maldrone can disable the original UAV pilot then remotely take control, meaning the UAV is hijacked and waiting for orders from the attacker. Fig. 25 shows a Maldrone attack.
- *Denial of service (DoS) attack*. These attempt to make FANET services unavailable. The attacker overloads UAVs by flooding them with data, such as sending a massive amount of replay or fake authentication messages [15,32,122]. Attackers can make a UAV operate abnormally or manipulate controller commands to interrupt the UAV flight path. Fig. 26 illustrates a DoS attack on UAV 1. The attacker pretends it wants to join FANET by sending a large amount of fake authentication messages. The messages

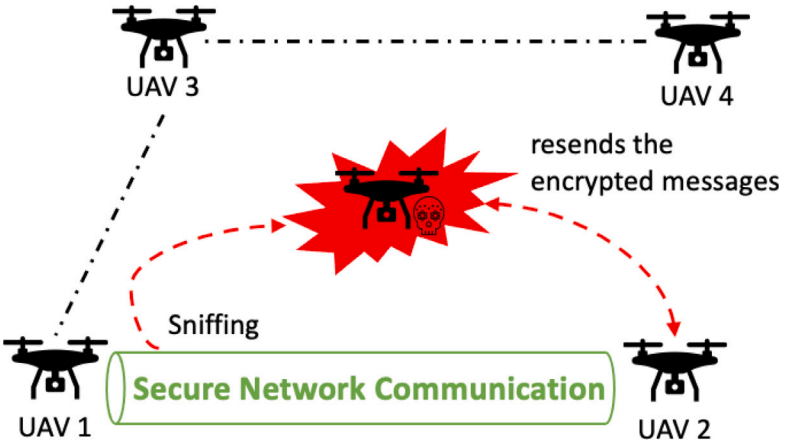


Fig. 22. UAV Replay Attack.

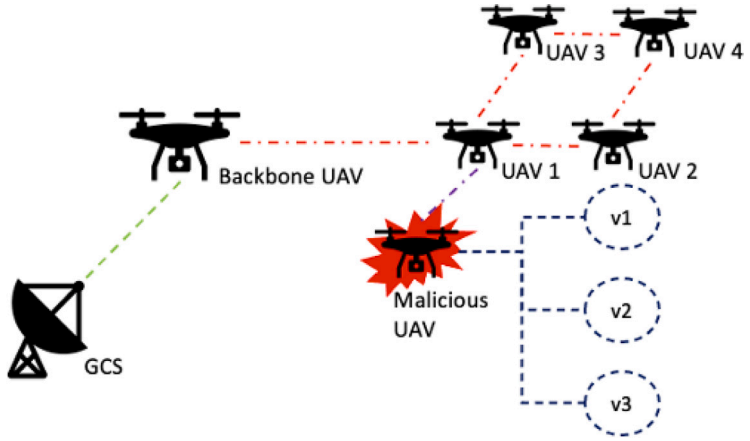


Fig. 23. An example of Sybil attack.

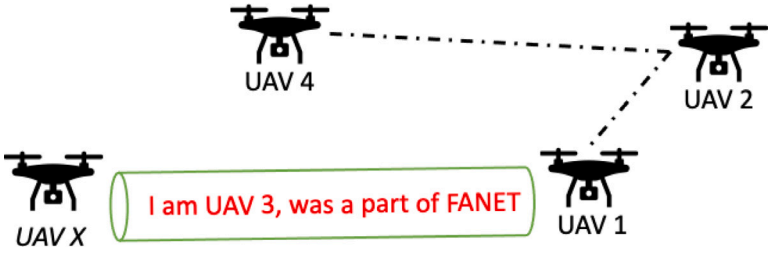


Fig. 24. Impersonation Attack.

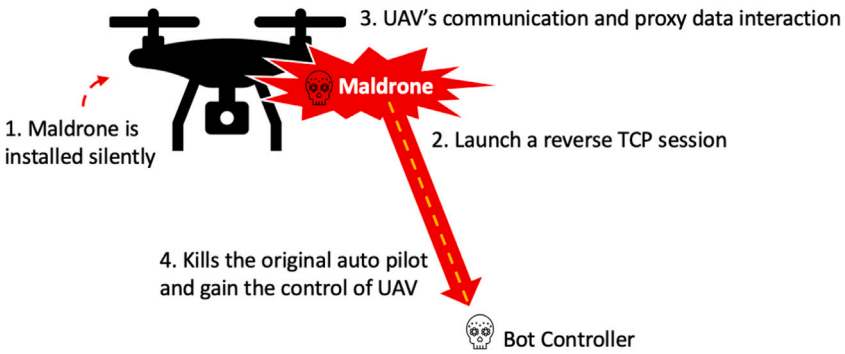


Fig. 25. Maldrone Attack.

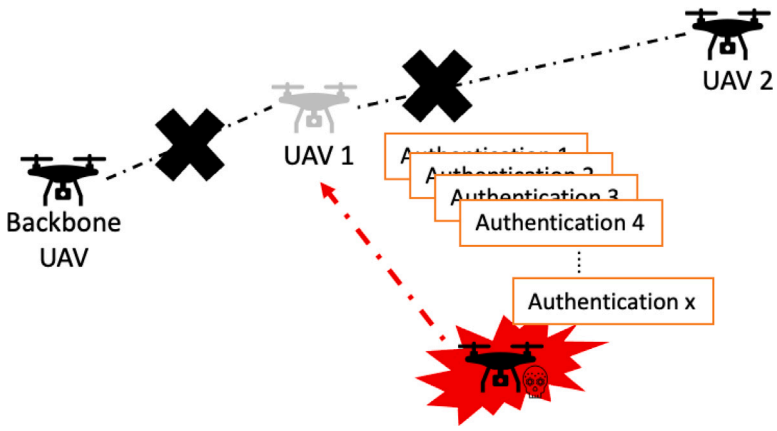


Fig. 26. DoS Attack.

Table 11
Threats on connections & nodes based on the STRIDE model.

Security Attacks/Threats	Threat Model					
	S	T	R	I	D	E
Connection Security						
C1						
Eavesdropping	✓			✓		✓
Insider		✓		✓	✓	
Replay	✓				✓	
C2						
Eavesdropping	✓			✓		✓
Jamming				✓	✓	
MITM	✓	✓		✓	✓	✓
Replay	✓				✓	
C3 & C4						
Eavesdropping	✓			✓		✓
Jamming				✓	✓	
MITM	✓	✓		✓	✓	✓
Replay	✓				✓	
Sybil		✓		✓	✓	
C5						
Impersonation	✓	✓		✓	✓	
Data tampering	✓	✓		✓	✓	
Eavesdropping	✓			✓		✓
Node Security						
GCS & Backbone UAV						
SPOF					✓	
Node - UAVs						
Backdoor		✓		✓	✓	
DoS					✓	
Flooding attack					✓	
Selfishness					✓	
Cloud Server & Storage						
Data tampering	✓	✓		✓	✓	

consume significant resources, meaning the UAV cannot accept new missions from the backbone UAV or UAV 2.

- *Flooding attack*. An attacker sends a large amount of packets to exhaust UAV resources and reduce network bandwidth. This process results in abnormal UAV operation, as their memory buffers and processing powers are significantly reduced [76].
- *Selfishness/selfish node*. As discussed earlier, UAVs have limited computational power. When a UAV is running low on power, they may not be able to process or transfer data very quickly. This situation is known as selfishness or selfish node [98], meaning the UAV continues to operate, but can downgrade the overall performance and availability of FANET [10,123]. Fig. 27 shows an example of a selfish node [124]. UAV S sends messages to UAV D, but due to the low power level of the selfish node in-between them, packets are not forwarded to UAV D.

Table 12
Taxonomy of security threats based on connections (Part I).

Security Attacks/Threats	Impact	Solutions			
	C/I/A/P	Network Types	Name	Year	Section
C1					
Eavesdropping	C, P	RW	mmWave-ULA [87]	2017	6.2.8
		5G	PA [88]	2018	
		F	LBE-Lite [17]	2018	
		IoD	CRP-PUF [77]	2020	
		F	CoMAD [32]	2021	
Insider	C, I, A, P	F	LWT-SEA [17]	2018	6.2.13
		IoD	GCACS-IoD [80]	2021	
		5G	IHP [79]	2021	
Replay	A	F	DNA-DAW [81]	2017	6.2.17
		5G	IHP [79]	2021	
		IoD	GCACS-IoD [80]	2021	
		F	CoMAD [32]	2021	
C2					
Eavesdropping	C, P	RW	mmWave-ULA [87]	2017	6.2.8
		5G	PA [88]	2018	
		F	LBE-Lite [17]	2018	
		IoD	CRP-PUF [77]	2020	
		F	CoMAD [32]	2021	
Jamming	C ,A, P	WLAN	FHSS [99,100]	1996	6.2.1
		WLAN	DSSS [10]	2016	
		WLAN	UFH [57]	2008	
		F	JarmRout [78]	2018	
		F	HID-RS {83}	2018	
		F	AFRL [92]	2020	
		F	FLBD [101]	2020	
MITM	C, I, A	5G	PA [88]	2018	6.2.15
		F	DroneSig [75]	2021	
		IoD	GCACS-IoD [80]	2021	
		5G	IHP [79]	2021	
		F	CoMAD [32]	2021	
Replay	A	F	DNA-DAW [81]	2017	6.2.17
		5G	IHP [79]	2021	
		IoD	GCACS-IoD [80]	2021	
		F	CoMAD [32]	2021	

Cloud server and storage — data tampering. To enhance UAV payload ability, some commercial UAVs store data in Cloud databases [17]. Any unauthorised modification of this data [125] might reveal private information or affect FANET operations.

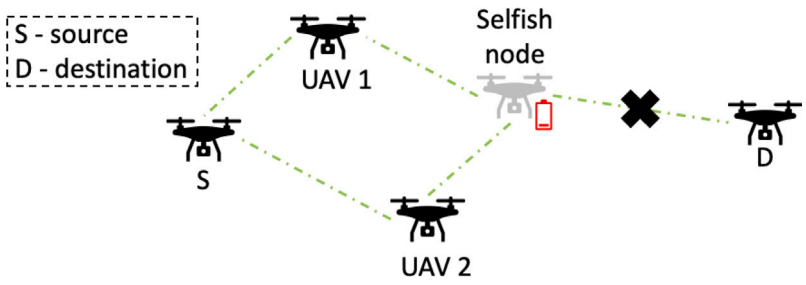


Fig. 27. Selfish Node.

Table 13
Taxonomy of security threats based on connections (Part II).

Security Attacks/Threats	Impact	Solutions			
	C/I/A/P	Network Types	Name	Year	Section
C3 & C4					
Eavesdropping	C, P	RW 5G F IoD F	mmWave-ULA [87] PA [88] LBE-Lite [17] CRP-PUF [77] CoMAD [32]	2017 2018 2018 2020 2021	6.2.8
Jamming	C ,A, P	WLAN WLAN WLAN F F F F	FHSS [99,100] DSSS [10] UFH [57] JarmRout [78] HID-RS [103] AFRL [92] FLBD [101]	1996 2016 2008 2018 2018 2020 2020	6.2.1
MITM	C, I, A	5G F IoD 5G F	PA [88] DroneSig [75] GCACS-IoD [80] IHP [79] CoMAD [32]	2018 2021 2021 2021 2021	6.2.15
Replay	A	F 5G IoD F	DNA-DAW [81] IHP [79] GCACS-IoD [80] CoMAD [32]	2017 2021 2021 2021	6.2.17
Sybil	C, I, A, P	WSN	ETS [84]	2017	6.2.21
C5					
Impersonate	C, I, A, P	A IoD F	ARAN [109] GCACS-IoD [80] CoMAD [32]	2005 2021 2021	6.2.12
C6					
Data tampering	C, I	F F	DNA-DAW [81] LBE-Lite [17]	2017 2018	6.2.5
Eavesdropping	C, P	RW 5G F IoD F	mmWave-ULA [87] PA [88] LBE-Lite [17] CRP-PUF [77] CoMAD [32]	2017 2018 2018 2020 2021	6.2.8

Table 14
Taxonomy of security threats based on nodes.

Security Attacks/Threats	Impact	Solutions			
	C/I/A/P	Network Types	Name	Year	Details
GCS & Backbone UAV					
SPOF	A	✗	Not found	✗	6.2.20
UAVs					
Backdoor malware	C, I, A, P	✗	Not found	✗	6.2.2
DoS	A	F	CoMAD [32]	2021	6.2.7
Flooding attack	A	IoD	Lids [76]	2021	6.2.9
Selfishness	A	WLAN F F	CUSUM [96] FBTM [98] TBC [89]	2013 2018 2020	6.2.19
Cloud Server & Storage					
Data tampering	C, I, A, P	F F	DNA-DAW [81] LBE-Lite [17]	2017 2018	6.2.5

Table 15
IoD characteristics compared to standard networks.

Characteristic	IoD	Standard Network
Energy	Limited	Unlimited
Mobility	Mobile	Static
Architecture	Hierarchical	Hierarchical
Communication Range	Short	Long
Routing Connections	Element-to-element	End-to-end
Packet Delivery	Broadcast	Guaranteed

4.5. Security threats on the IoD

There are many significant privacy and security issues that need addressing in the IoD, as drones are not necessarily designed with security in mind. We outline concerns regarding data confidentiality and leakage, as well as malicious interference [126]. Table 15 summarises the differences in characteristics between the IoD and standard networks. Due to hardware constraints, the IoD relies on lightweight protocols for data encryption and processing, especially with miniature, economical devices. Airspace is a common resource shared by drones, which is divided into zones. These zones are connected by inbound and outbound gates. Every zone has a path map, containing airways, nodes and intersections. To aid drones, zone service providers (ZSPs) supply navigational information, together with IoD service providers (IoDSP) that assist adjacent ZSPs in managing gates. Fig. 28 provides an overview of the IoD communication system.

4.5.1. Confidentiality

The IoD can generate a significant amount of personally identifiable or sensitive data. These data can include items such as geographical locations, drone owners, travel routes, and drone identities. This type of data can aid a physical attack on important buildings. Whilst the true identity of the drone can be protected, relevant authorities (such as the FAA or CAA) should be able to trace and identify individual drones. Malicious IoD drones can collude to record target positions then obtain its real identity by monitoring. Insider attacks should also be considered, for example employees, such as a ZSP manager who can access sensitive drone data, then collaborate with external attackers [126].

4.5.2. Integrity

Resource restrictions within drones and ZSPs mean that tasks requiring significant computational power are often outsourced to the cloud. If drone data is not encrypted, it could be accessed by malicious actors, such as employees of the cloud service provider. Drones or ZSPs may be unable to encrypt large datasets, for example, real-time video streams. Even if the data was encrypted, drones or ZSPs may not have the computational power to fully search or index it. Challenges regarding

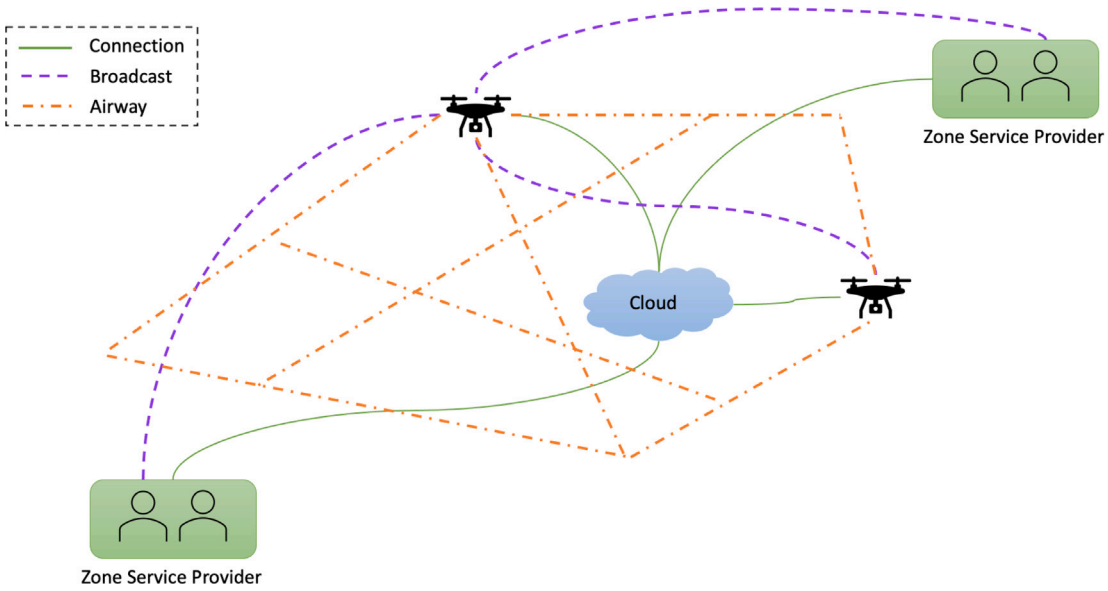


Fig. 28. IoD Communication System Overview.

authentication and authorisation with collaborated data can also arise in the IoD [126].

4.5.3. Availability

IoD architecture is controlled by ZSPs, meaning the control systems between them and drones are tempting targets for attackers, who wish to jeopardise the system. Attackers could use methods such as DoS or spoofing attacks and malicious injection of data. These attacks may require third-party auditing or inspection services to be properly detected. Trusted computing platforms can be used to prevent unauthorised software and hardware modifications, but these may have high latency or false alarm rates [126].

5. A taxonomy of security threats based on OSI layers

This section provides a taxonomy of FANET security threats based upon the OSI layers. We focus on the four lowest OSI layers, namely Physical, Data Link, Network, and Transport Layers. Fig. 29 illustrates a taxonomy of 12 security threats, along with their 28 corresponding security solutions. There are three security threats in the Physical Layer, three in the Data Link Layer, five in the Network Layer, and one in the Transport Layer. The existing solutions are over five network types: 5G, FANET, other types of Ad-Hoc Networks, RW, and WLAN. In addition, we review threats and solutions related to routing protocols in FANETs. In particular, we consider six types of routing protocols and compare 21 related security solutions.

Tables 16 and 17 categorise security threats on four OSI layers. Firstly, the FANET security impact is identified in relation to Confidentiality (C), Integrity (I), Availability (A), and Privacy (P). Secondly, a chronological sequence introduces the existing solutions over the six network types, indicating conventional and novel solutions. The corresponding solutions are identified and categorised later in Section 6.

5.1. Physical layer (radio and antenna)

The wireless signal encoding and decoding, transmission and reception of bits, frequency band as well as transmission medium are related to the physical layer [1,9]. A great distance between UAVs can mean their signal is prone to interference. Signal transmission and reception are achieved by antennas, which are either directional or omni-directional. Directional antennas transmit in a specific direction; when they are positioned correctly they provide long ranges, low latency and high capacities. Omni-directional antennas send signals to all directions, hence there is no need for node positioning to target other UAVs. However, their transmission range is short, latency is high and capacity is low [1]. Fig. 30 illustrates the difference between the coverage of omni-directional and directional antennas.

Eavesdropping. In Section 4.3, eavesdropping is identified in four communication channels (C1, C2, C3 & C4 and C6). In the physical layer, consideration is given to the disruption and secrecy of the

Table 16
Threat categorisation based upon four OSI layers and five network types (Part I).

Security Threats	Impact	Solutions			
	C/I/A/P	Network Type	Name	Year	Details
Physical Layer					
Eavesdropping	C, P	RW	mmWave-ULA [87]	2017	6.2.8
		5G	PA [88]	2018	
		F	IBE-Lite [17]	2018	
		IoD	CRP-PUF [77]	2020	
		F	CoMAD [32]	2021	
GPS spoofing	A	WLAN	CUSUM [96]	2013	6.2.10
		F	HID-RS [103]	2018	
Jamming	C, A, P	WLAN	FHSS [99,100]	1996	6.2.1
		WLAN	DSSS [10]	2016	
		WLAN	UFH [57]	2008	
		F	HID-RS [103]	2018	
		F	JarmRout [78]	2018	
		F	AFRL [92]	2020	
		F	FLBD [101]	2020	
Data Link Layer					
Collisions	A	F	LODMAC [104]	2015	6.2.4
		F	CF-MAC [95]	2016	
		F	ZSP [17]	2018	
De-authentication	A	WLAN	S-RSSI [110]	2008	6.2.6
Low link quality and high latency	A	WLAN	MPR [106]	1988	6.2.14
		WLAN	AMUAV [93]	2010	
		F	TBP [108]	2012	
		F	CADA [94]	2014	
		F	LODMAC [104]	2015	
		F	RLSRP-PPMAC [90]	2018	
		F	LTA-OLSR [105]	2018	

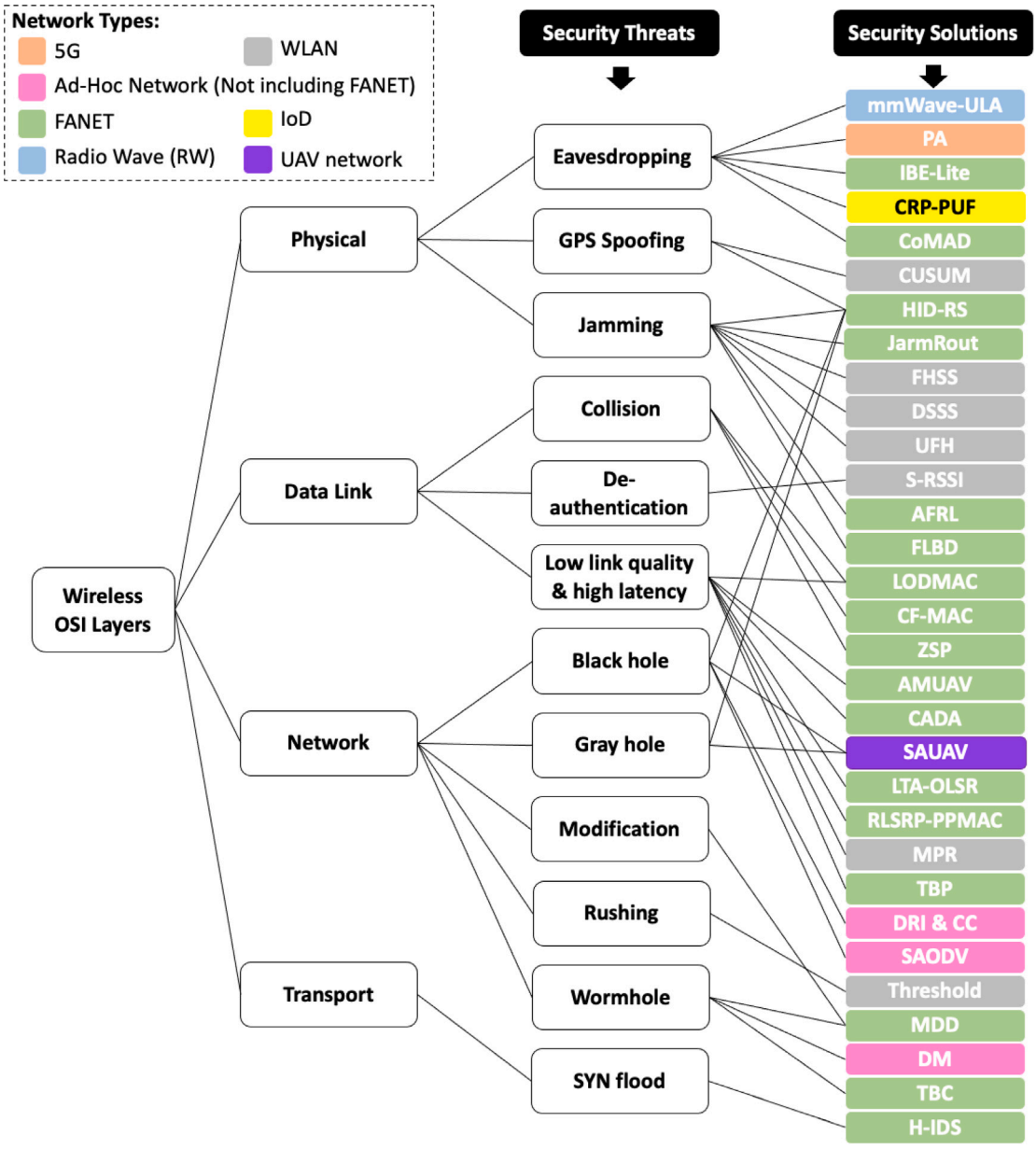


Fig. 29. A taxonomy of security threats, with their corresponding solutions, based on the lowest four layers of the OSI model.

transmitted messages [87]. This is likely to happen on both directional and omni-directional antennas.

GPS spoofing. GPS spoofing was presented in 2012 by researchers at the University of Texas [128]. In 2015, the U.S. border surveillance UAVs were hijacked using GPS spoofing [129], as their GPS signals were not encrypted or authenticated [130]. Fig. 31 shows how GPS spoofing works. An attacker sends false data on a counterfeit signal using a GPS simulator with a power amplifier and antenna. This process deceives the UAV flight controller, providing it with misleading directional information. GPS spoofing could result in safety issues such as UAV hijacking, operational failures or crashes [12].

Jamming. As introduced in Section 4.3, a jammer can interfere with the radio signal between two nodes. As signals from omni-directional antennas are sent in all directions, they are more likely to be found jammed than those from directional antennas. Signal jamming [32] is the main physical layer issue and can cause FANETs to disconnect. To mitigate jamming, self-organisation or self-recovery schemes can be applied that maintain FANET availability. Fig. 32 illustrates signal jamming on omni-directional antennas.

5.2. Data link layer

The data link layer controls the speed of data being sent and received in order to prevent network devices from becoming overloaded. The layer has two sub-layers: media access control (MAC) and logical link control (LLC). MAC focuses on error detection, medium access and data assembly, whereas LLC manages errors as well as flow control [131].

Collisions. Collisions occur when two or more nodes simultaneously send data in a half-duplex network environment. As nodes are unaware of data transmissions from others, the flow of packets can become interrupted [132,133]. Fig. 33 illustrates a situation where collisions could occur [134]. Backbone UAV and UAV 2 can both communicate with UAV 1. Backbone UAV and UAV 2 are not aware of each other, so collisions occur when Backbone UAV and UAV 2 simultaneously send data to UAV 1.

De-authentication. An attacker sends de-authentication packets to the target UAV which disrupt the original UAV pilot connection [110,135]. The attacker can take control of the UAV and often disturbs normal

Table 17
Threat categorisation based upon four OSI layers and five network types (Part II).

Security Threats	Impact	Solutions			
	C/I/A/P	Network Type	Name	Year	Section
Network Layer					
Blackhole	A	A	DRI & CC [97]	2011	6.2.3
		A	SAODV [107]	2015	
		F	HID-RS [103]	2018	
		UAV	SAUAV [82]	2020	
Grayhole	A	F	HID-RS [103]	2018	6.2.11
		UAV	SAUAV [82]	2020	
Modification	C, I, A	F	MDD [85,86]	2015	6.2.16
Rushing	A	A	Threshold [127]	2013	6.2.18
Wormhole	C, I, A, P	A	DM [83]	2008	6.2.23
		F	MDD [85,86]	2016	
		F	TBC [89]	2020	
Transport Layer					
SYN flood	A	F	H-IDS [102]	2018	6.2.22

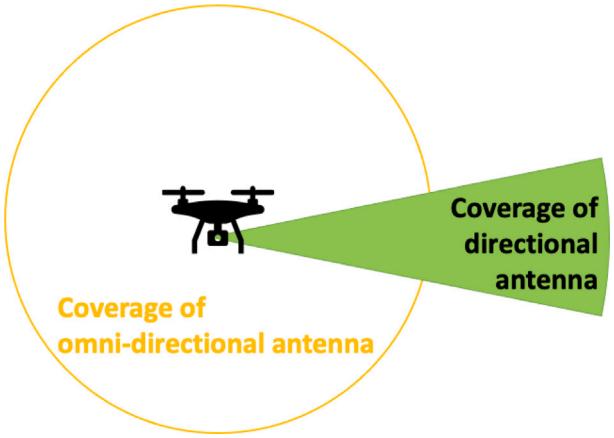


Fig. 30. Omni-directional and Directional Antenna Coverage.

FANET operation. Fig. 34 shows Client-A piloting the UAV. An attacker sends a de-authentication message spoofing the source IP address of Client-A. The connection between UAV and Client-A is lost and the attacker assumes UAV control [136].

Low link quality and high latency. Link quality indicates the condition of a communication channel, based on the amount of data packets it receives [137,138]. Latency is the time duration between action and response of a network or packet [139]. The high mobility and varying distances between UAVs might create low link quality and high packet latencies, which could result in FANET availability or capacity issues.

5.3. Network layer

The network layer is in charge of forwarding data packets via suitable network routes [131]. In this subsection, we introduce their security threats and related routing protocols.

Blackhole. In FANETs, every UAV acts as a router to transfer packets. In a blackhole attack, a malicious UAV deceives legitimate UAVs into sending packets to it, by pretending to have the shortest network destination route [97]. These packets are then dropped by the malicious UAV [107]. Fig. 35 describes a blackhole attack. S and D denote the source and destination UAVs, respectively. M denotes a malicious UAV. In the figure, S sends a route request (RREQ) to its neighbours: UAV 1, UAV 4, and M. Normally, UAV 1 forwards RREQ to UAV 2 and UAV 3, whilst UAV 4 forwards RREQ to D. However, while other UAVs forward RREQ to next hop, M responds to S with a route reply (RREP) containing a high destination sequence number. A route is built between M and S. M drops the packets received from S.

Grayhole. In a grayhole attack, a malicious UAV alters the packets within its network route. The malicious UAV chooses a random time to change its behaviour, at this point it drops packets that are normally sent onto other UAVs. After an arbitrary period, the malicious UAV switches back to standard operation and forwards packets as normal. Due to the unpredictable nature of the malicious UAV, grayholes are more difficult to detect than blackholes [140,141]. Fig. 36 shows an example of a grayhole. At the top of the diagram, M drops packets that should have been sent to D. In the bottom diagram, M changes its behaviour and forwards packets like a legitimate UAV.

Modification. Modification is also known as an *injection attack* [85, 142]. An unauthorised third party manipulates messages to deceive the receiver or flood the network with fake messages. Fig. 37 illustrates an example of a modification attack, where the malicious UAV sees message contents and changes the location, for example, from York Minster to Manchester. As the UAV is sent to the wrong location, this attack makes the FANET topology unavailable.

Rushing. A rushing (also known as rush) attack involves route discovery packets being sent by an attacker faster than from other nodes. By doing this, the attacker obtains access rights to process further work then can replace legitimate routes for UAV services [10,127]. Fig. 38 illustrates a rushing attack. When S sends RREQ to D, it should normally pass through UAV-1, UAV-2, and then reach D. However, when M is present it replies to S with a higher transmission rate than the other UAVs. When D receives packets from M, it ignores any subsequent RREQs. As a result, D takes the route via M as being valid and uses it for communication.

Wormhole. Also referred to as a *tunnelling attack*, one or more malicious nodes deceive other nodes into sending packets to them. They then use tunnels which relay packets to another network in order to steal data for analysis. In the meantime, the malicious nodes might allow or drop destination packets. Due to the high mobility characteristic of FANETs, the wormhole attack is difficult to detect. This characteristic also means determining actual packet delivery and speed is also problematic [83,86,89]. Fig. 39 shows two malicious cooperating UAVs: M1 and M2. They deceive other UAVs into believing that they are legitimate to receive data from UAV 1 and UAV 4. M1 and M2 then use a private network tunnel to transfer data between themselves in order to steal information.

5.4. Routing protocols at network layer

In this subsection, we divide routing protocols into five main categories: static, proactive, reactive/on-demand, geographic-based, agent-based as well as hybrid, expanding surveys [9,12]. Routing protocols are used to solve specific issues or to improve aspects related to FANET; for example, throughput, security, bandwidth, or data transfer. Routing protocols are also used to choose the FANET best path based on different criteria, such as quality of service, security, or number of hops [9,143]. Fig. 40 illustrates common protocols relevant to UAV communication [9,12]. We consider four different network types. We observe that some routing protocols were designed by the authors specifically for UAV communication and cannot be used in FANET. Below, we describe the routing protocol based on the aforementioned five categories.

Static Protocols. When a mission starts, each UAV calculates its own routing table. This could be advantageous if the UAV was to join a FANET, as there is no initial delay for routing table construction. It is known that static protocols do not provide the flexibility to accept unpredictable failures or changeable environments. FANET topologies alter very quickly and UAV's have high mobility, so FANET is not suitable for static protocols [9,16]. Some of the listed protocols are experimental and not suitable for real-world deployments yet.

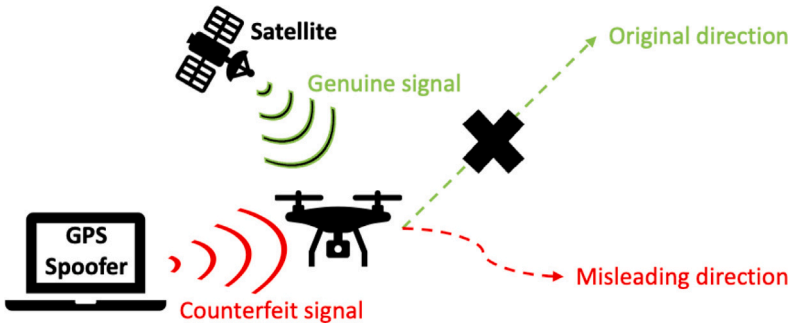


Fig. 31. GPS Spoofing.

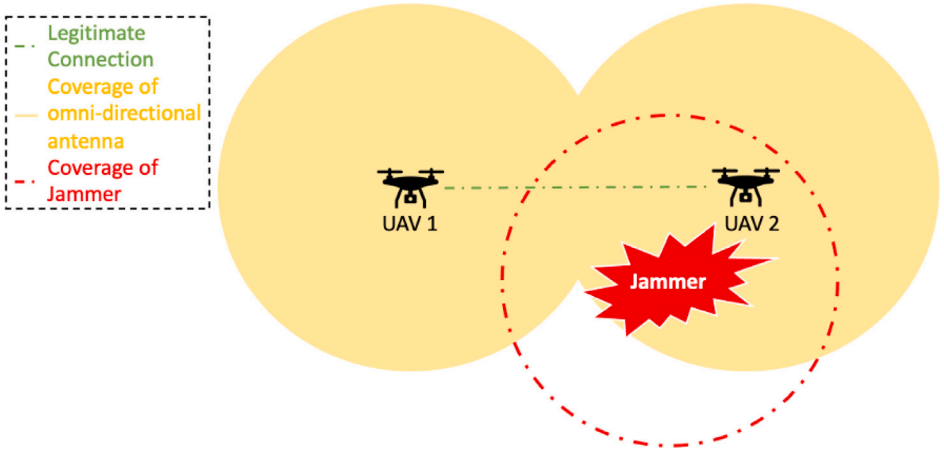


Fig. 32. Omni-Directional Jamming.

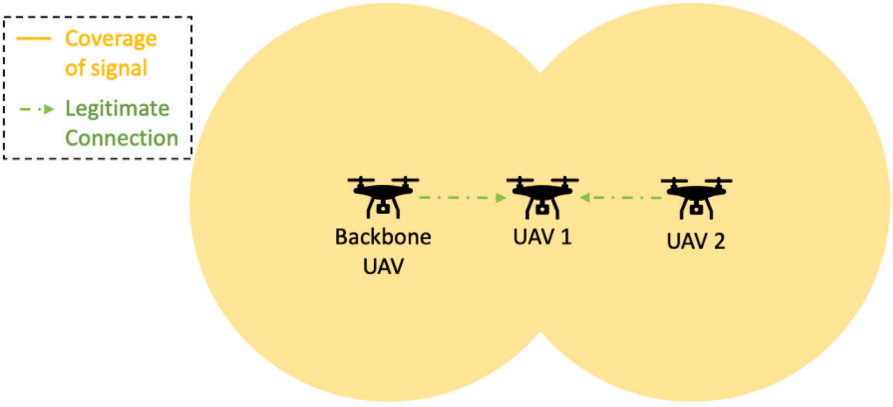


Fig. 33. Collision Situation.

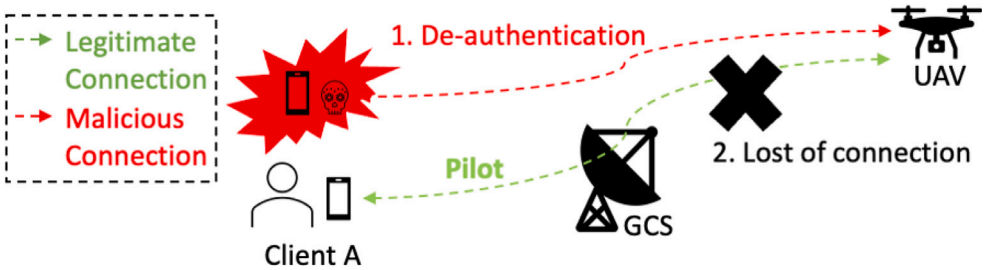


Fig. 34. De-authentication Attack.

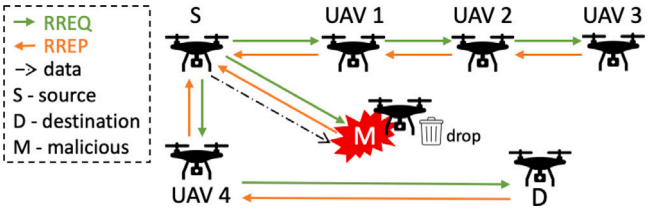


Fig. 35. Blackhole attack.

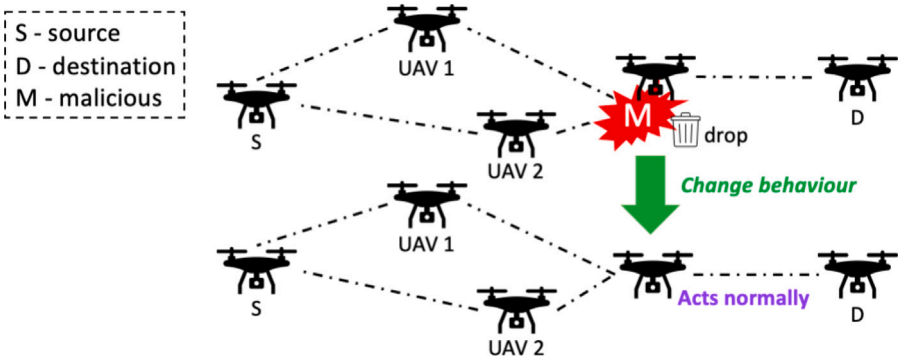


Fig. 36. Grayhole attack.

Fig. 37. Modification Attack.

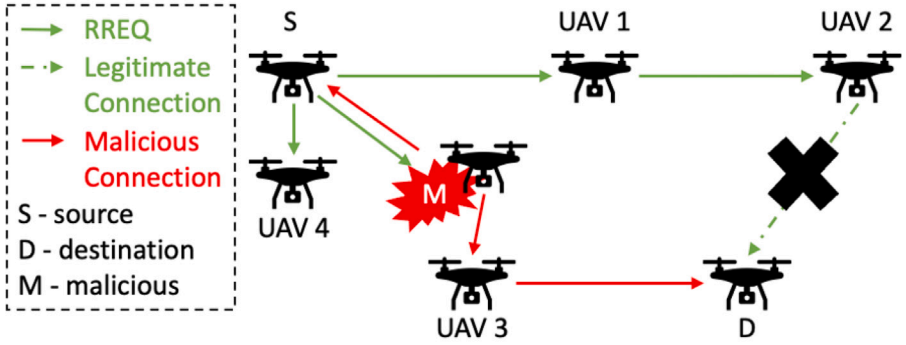


Fig. 38. Rushing Attack.

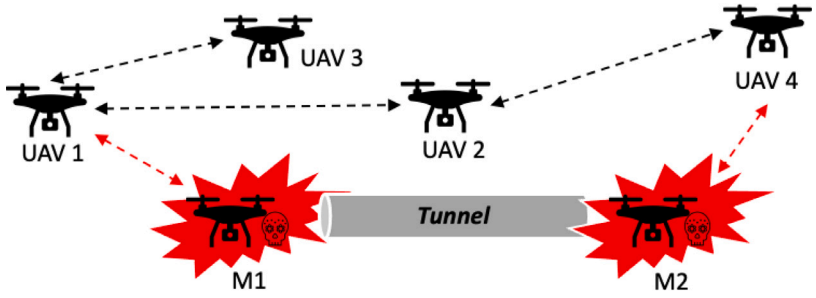


Fig. 39. Wormhole Attack.

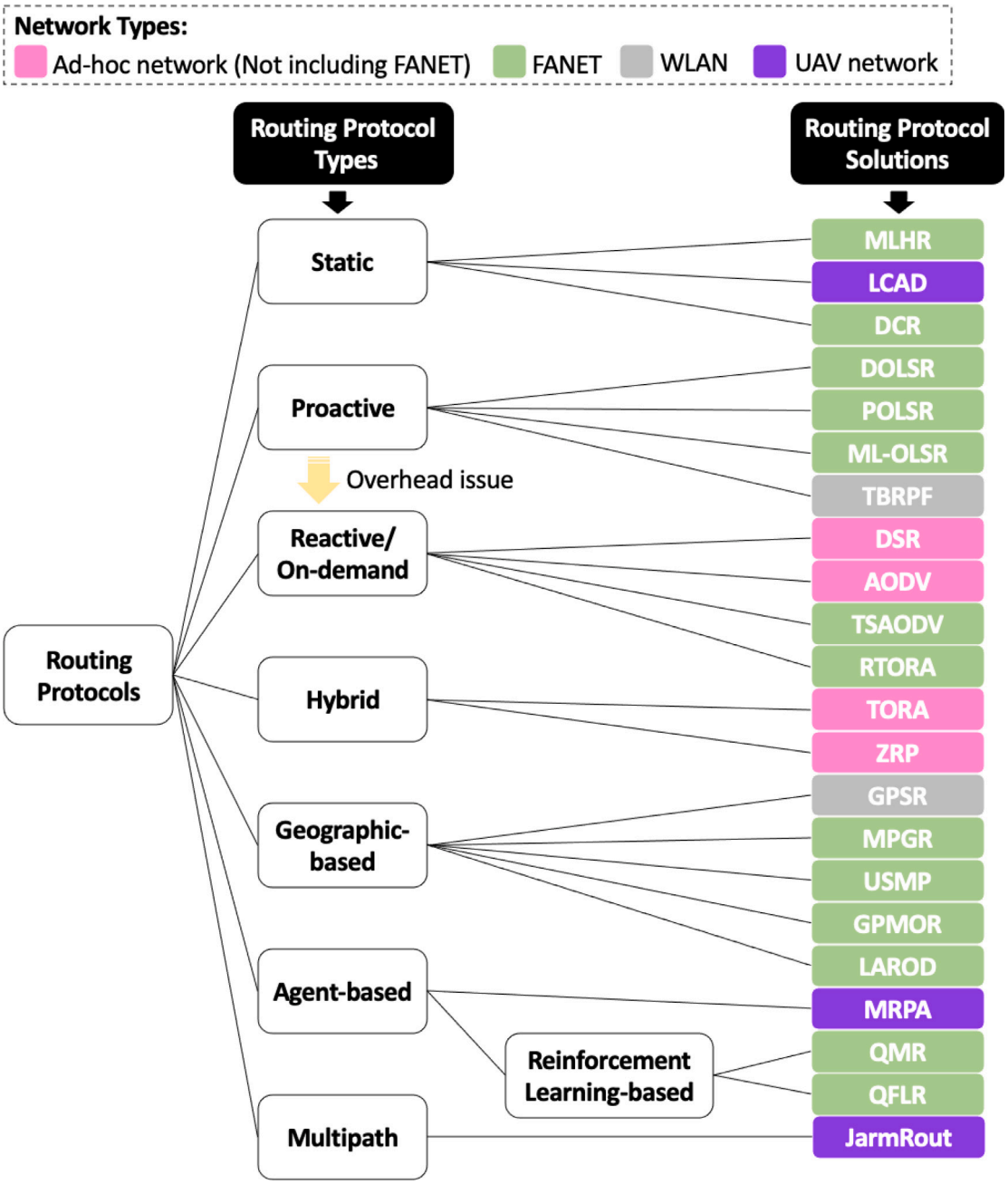


Fig. 40. A taxonomy of routing protocols.

- Load-carry-and-deliver (LCAD) was introduced in 2007 [144]. When a UAV receives GCS data packets, it carefully calculates time and flight plans for maximum throughput, high security, and minimal delay to data being transferred in relay networks between GCSs.
- Multi-level hierarchical routing (MLHR) is based on [145,146]. MLHR separates UAVs into multiple clusters, each cluster having a cluster head (CH) that acts as a leader and stands for the whole cluster when it operates. MLHR uses the UAV upper layer to communicate with GCS and the UAV lower layer within the clusters. MLHR is suitable for three-dimensional spaces used in FANET communications; it provides management for different UAV types and flexibility to scale up to large UAV groups [16,147].
- Data centric routing (DCR). Research indicated that multi-node communication is preferred to one-to-one communication. Efficiency gains are made when data is transferred on-demand, which provides a suitable environment for cluster architectures by using attributes for data access instead of UAV IDs [147].

Proactive Protocols. A routing table stores the routing data or network area relating to all nodes prior to initial data transmissions. If the topology changes, this table is automatically updated by nodes that broadcast link-state data, meaning the routing data is always current. Network bandwidth is decreased by route update messages; this could slow down FANET operations as its topology changes frequently due to UAVs having high mobility levels [9,16]. Below, we outline the proactive protocols.

- Optimised link state routing (OLSR) is used in MANET which sends topology control and hello messages; these keep ad-hoc networks operating by understanding their neighbouring nodes. A multipoint relay (MR) can be selected to reduce overhead [9,16].

With FANET, this data exchange would create significant overheads; these can be mitigated by extension protocols which we now consider: directional OLSR (DOLSR) decreases transmission overheads and delays. At the start of transmission, the source calculates the distance to destination. If this distance is greater than the maximum reached by directional antenna, DOLSR is chosen [9,16]. Otherwise, OLSR is deployed with omni-directional antennas [10]. Predictive-OLSR (POLSR) — UAV link speed and quality is monitored by its GPS data. POLSR selects the highest quality link to carry out the mission [9]. Mobility and load aware OLSR (ML-OLSR) considers the speed between neighbour nodes. To prevent network congestion, each UAV packet load is evaluated to find the most optimal route [9].

- Topology broadcast based on reverse-path forwarding (TBRFP) was introduced in 2002 [148]. It broadcasts link-state updates by deploying reverse-path forward, instead of using shortest path first method, the shortest hop paths are chosen which minimise network changes and lower overheads.

Reactive/On-Demand Protocols. Each route is created when a node wants to join the network, solving overhead issues created by proactive protocols that exchange RREQ and RREP messages. A RREQ is transferred using flood techniques that collect all possible network paths. A RREP is sent using unicast [9,16]. Each mission determines its own path, meaning the routing table does not have to be updated. As not all connections are known, comprehensive routing tables can take time to construct; these tables do not scale or recover from unpredictable failures easily. Below, we outline the reactive protocols.

- Dynamic source routing (DSR) was introduced for ad-hoc networks in 1996 [149] and was updated to RFC 4728 in 2007 [150]. Dynamic source routing is used when topologies change frequently. Route data is contained in RREQ and records hop sequences during route discovery. The first version of the DSR protocol did not consider any security mechanisms. A later update included route maintenance features such as packet rescue, broken link, and route error message dissemination. The update also incorporated loop detection and route caching.
- Ad-hoc on-demand distance vector (AODV) was designed for MANETs in 2003 [151]. A sequence number is used to verify routing data freshness in order to create a loop-free route. Suitable routes are selected based upon having the highest sequence number and shortest hop count [97]. AODV can be vulnerable to blackhole attacks, as it does not include authentication or other security mechanisms.
- Time-slotted AODV (TSAODV) extends the AODV protocol. Whilst data is being sent, a specific time slot is selected for each UAV. The protocol can prevent packet collisions, which enhances FANET availability and increases bandwidth use [9].
- Rapid re-establish temporally ordered routing algorithm (RTORA) uses a reduced overhead mechanism to decrease overheads due to TORA link reversal failures. These failures can flood the network with control packets [9].

Hybrid Protocols. Integrating proactive and reactive protocols can overcome their shortcomings. Integration can reduce initial routing discovery process latencies and control message overheads. The integrated protocols can be easier to adapt to large-scale networks and provide greater network capacity. We now discuss the relevant hybrid protocols [9].

- Temporally-ordered routing algorithm (TORA) was first proposed in 1997 [152] and was updated by the IETF MANET Working Group in 2001 [153]. TORA provides four main route functions: creation, maintenance, removal, and optimisation. These functions select the most optimal route, to reduce network overheads a long path is sometimes chosen, instead of a short one.
- Zone routing protocol (ZRP) was introduced for MANETs in 1997, and updated in 2002 [154]. Nodes are grouped into zones, intra-zone communications use proactive protocols for route maintenance. Inter-zone communications use reactive protocols to transfer data amongst other zones. A border-casting concept is implemented to increase efficiency by using a straight query to the other side of the overlapping routing zone [16].

Geographic Based. They find the optimal path based upon node location. There are two strategies: greedy forwarding and backup method. Greedy perimeter stateless routing (GPSR) uses position and destination to decide the forwarding path [155]. GPSR keeps an up-to-date topology related to the geo-location of neighbours; data is then greedily forwarded to the closest geographical hop. This increases mobility and the routing control messages have less overheads than the DSR protocol. Mobility prediction geographic routing (MPGR) integrates GPSR with a mobility prediction mechanism to compensate for the high mobility of FANETs. UAV search mission protocol (USMP) implements two features to determine UAV location and prevent collisions [9]. A protocol using similar concepts is geographic position mobility oriented routing (GPMOR), where the next hop is decided using the Gaussian–Markov model which estimates UAV actions [156]. In the location aware routing for opportunistic delay tolerant network (LAROD) [157], both the greedy forwarding and store-carry-forward principles are deployed which are suitable for high mobility environments. The protocol was designed with a delay-tolerant network (DTN) model, whenever the greedily forwarding is sent to the destination UAV and further movement is impossible, the protocol preserves the package for a short period of time.

Agent Based. An agent senses and reacts to the surrounding environment in response to a specific situation [158]. Agent-based solutions implement agents to solve specific issues. For example, the mission route planning agent (MRPA) [12,158] was designed to solve route planning issues. MRPA helps UAVs complete their operations in the most efficient manner. Situational awareness algorithms are implemented which record environmental states, forwarding actions are then decided based on data collected by the agents. *Reinforcement learning-based* is a type of agent-based protocol. Reinforcement learning (RL) is a type of training model for machine learning (ML). RL includes an agent for effective learning in changeable and complex environments [13,159]. In 2020, Liu et al. [13,69] suggested a Q-learning based multi-objective optimisation routing protocol (QMR). In QMR, the Q-learning is balanced which gives low latency and power consumption, making it suitable for high mobility FANET. Yang et al. [13,70] proposed a Q-learning-based fuzzy logic algorithm for the FANET routing protocol (QFLR). By using both link-level and path-level parameters, it provides a low hop count, saves computational power, and extends network lifetime duration.

Multipath. The authors in [78] proposed a jamming-resilient multipath routing protocol (JarmRout) to enhance FANET performance. Three main schemes are implemented — link quality, traffic load, and spatial distance. JarmRout improves packet delivery ratios and latency as well as reducing the end-to-end communication disruption rate. If a source UAV cannot find a network route to its destination, a RREQ packet is broadcast to intermediate UAVs. These UAVs rebroadcast the RREQ packet with information regarding the link quality and traffic load along the route. To ensure that a destination UAV receives enough RREQ packets to create multipaths, intermediate UAVs cannot send RREP packets back to the source UAV. When the destination UAV receives the RREQ packets, it updates its routing table and discards packets not meeting the node-disjoint path requirement. The UAV routing table prioritises the network path containing the least number of source to destination hops. A route error RERR packet is sent back to the source UAV, this removes any incomplete routing table paths. When compared to the DSR and OLSR protocols, JarmRout provides a higher packet delivery ratio and lower end-to-end communication outage rates even when under significant network loads.

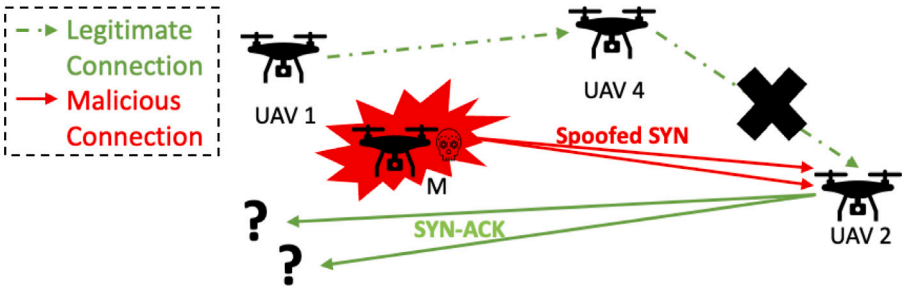


Fig. 41. SYN Flood Attack.

5.5. Transport layer

The transport layer coordinates end-to-end communication across the network by using error-checking and data flow controls [131]. Below, we discuss two most important security threats at the Transport Layer.

SYN flood. A SYN flood attack is based upon the TCP 3-way handshake, whereby the sender sends a large amount of SYN packets with spoofed source IP addresses to the receiver. The receiver then replies with a SYN-ACK to show it is ready for the handshake. Next step then waits for an ACK packet. As the source IP is spoofed, when receiver replies, it never gets an ACK packet as the address might not exist or a SYN packet with the corresponding SYN-ACK does not exist on the specific device [10,160]. Fig. 41 illustrates a SYN flood attack. A malicious UAV (M) sends spoofed SYN packets to UAV 2, which replies with a SYN-ACK to destinations that do not exist. Using its own resources, UAV 2 waits for ACK packets. A subsequent request from UAV 4 is rejected as UAV 2's resources are now occupied.

Message reliability Message reliability is very important to FANET as it often has multiple applications and UAVs in operation at the same time. This reliability should incorporate data control to prevent reduced packet delivery ratios or latency increases and optimisation between fast moving UAVs or multiple senders [1].

6. Security solutions and standards

In this section, we identify and compare appropriate security solutions that have been proposed to mitigate FANET security threats. In particular, 15 security threats are considered, six of the reviewed solutions mitigate more than one threat. In addition, we classify 22 security threats based on 7 security requirements and then compare the 32 proposed security solutions. Finally, we compare six existing standards and identify their limitations.

6.1. Security solutions

Table 18 shows security solutions identified in Sections 4 and 5 that defend against two security threats or more. One effective solution to consider when implementing FANETs is CoMAD [32], which can prevent a number of security threats. CoMAD mitigates five security threats: DoS, eavesdropping, impersonation, MITM, and replay. HID-RS [103] mitigates four security threats: blackhole, GPS spoofing, grayhole, and jamming. Some of the solutions proposed in [17] were identical, but the authors had given them different names. These solutions prevent collisions, data tampering, eavesdropping, and insider attacks. IHP [79] focused on insider, MITM, and replay attacks. GCACS-IoD [80] protects against impersonation, insider, MITM, and replay attacks. The remaining security solutions [81,82,85,86,88,96], protect against two security threats. As each proposed solution used different measurements during their simulations, identifying their efficiency was not always possible.

Table 19 categorises the solutions into agent-based and, as with most solutions, agent-less. The former category uses a device agent to solve specific issues whilst the latter has no background device service, daemon, or process. The majority of agent-based solutions rely upon autonomous ML algorithms: FLBD [101], AFRL [92], RLSRP-PPMAC [90], QFLR [13,70], and QMR [13,69]. Table 19 is a reference for security solutions and routing protocols used with lightweight or high computational power UAVs that deploy different applications.

Based on the STRIDE model (as outlined in Fig. 8), Fig. 42 shows twenty-three security threats with seven security requirements (impacts) and thirty-two security solutions for different network types.

Table 20 breaks down Fig. 42, to give a clearer view of the security requirements of each threat. Fig. 42 and Table 20 indicate that the most prevalent FANET security requirement is availability, followed by confidentiality, privacy, integrity, authentication, authorisation, and non-repudiation.

6.2. Specialised solutions

In this section, security solutions are given that correspond with threats discussed in Sections 4 and 5.

6.2.1. Active interfering (jamming)

In a wireless connection, active interfering can be seen as intentional jamming [9,12] which can affect FANET availability. In [161], the authors discuss mitigation techniques for interference whilst UAVs are being controlled with radio signals. Several solutions were proposed to deal with radio signal jamming whilst communicating on the physical layer, degrading availability. The frequency hopping spread spectrum (FHSS) [99,100] using the 802.11 WLAN standard was introduced in 1996. FHSS transmits radio signals by rapidly changing the channel frequency within a non-overlapping range. FHSS can reduce interference to neighbouring radio channels and decrease the possibility of jamming attacks by using random patterns to switch channels. Direct sequence spread spectrum (DSSS) [10] integrates RF carriers and pseudo-noise digital signals to create a wide transmission signal carrying more information using a large bandwidth. DSSS enhances confidentiality, as it is difficult for attackers to recover the RF carrier then original signal [100].

Uncoordinated frequency hopping (UFH) [57] was designed to allow two nodes to launch a key establishment protocol, despite not having a pre-shared key. Once their secret key is created, a secret hopping sequence is started and the nodes communicate using coordinated frequency hopping. This process makes it difficult for attackers to guess which frequency nodes are using [10]. [103] proposed an agent-based HID-RS with a rule-based intrusion detection method for UAV and GCS. The UAV carries an agent to gather packets within reachable radio coverage and checks the number and value of collected packets. When an instance of jamming is detected, the agent contacts the GCS with an *intrusion report* that includes data relating to the malicious UAV. [101] proposed an on-device federated learning-based detection (FLBD) to detect jamming and solve data privacy issues relating to single UAVs and unbalanced sensor data. FLBD provides real-time updates on non-IID and other issues, as well as determining UAV FANET validity; it is designed to be trained on lightweight UAV devices. [92] developed

Table 18
Solution categorisation with more than two threats.

Threats	CoMAD [32]	CUSUM [96]	HID-RS [103]	PA [88]	LBE-Lite/ ZSP/ LWT-SEA [17]	MDD [85,86]	DNA-DAW [81]	SAUAV [82]	IHP [79]	GCACS -IoD [80]
Blackhole			✓					✓		
Collisions					✓					
Data tampering					✓		✓			
DoS	✓									
Eavesdropping	✓			✓	✓					
GPS Spoofing		✓	✓							
Grayhole			✓					✓		
Impersonate	✓									✓
Insider					✓				✓	✓
Jamming			✓							
MITM	✓			✓					✓	✓
Modification						✓				
Selfishness		✓								
Replay	✓						✓		✓	✓
Wormhole						✓				

Table 19
Agent-based and agent-less security solutions and routing protocols.

Types	Security Solutions	Routing protocols
Agent-based	H-IDS [102], HID-RS [103], FLBD [101], AFRL [92], RLSRP-PPMAC [90], DroneSig [75]	MRPA [12,158], QFLR [13,70], QMR [13,69]
Agent-less	AMUAV [93], ARAN [109], CADA [94], CF-MAC [95], CoMAC [32], CUSUM [96], DM [83], DRI & CC [97], DSSS [10], ETS [84], FBTM [98], FHSS [100], IBE-Lite [17], LODMAC [104], LTA-OLSR [105], LWT-SEA [17], MDD [85,86], mmWave-ULA [87], MPR [106], PA [88], S-RSSI [110], SAODV [107], TBC [89], TBP [108], Threshold [127], UFH [57], ZSP [17], Lids [76], CRP-PUF [77], IHP [79], SAUAV [82], GCACS-IoD [80], DNA-DAW [81]	AODV [151], DCR [147], DOLSR [9,16], DSR [149], GPMOR [156], GPSR [155], LAROD [157], LCAD [144], ML-OLSR [9], MLHR [147], MPGR [9], POLSR [9,16], RTORA [9], TBRFP [148], TORA [152], TSAODV [9], USMP [9], ZRP [154], JarmRout [78]

Table 20
A classification of security threats based on security requirements.

Threat	Avail.	Authentic.	Authorisation	Confidential.	Integrity	Privacy	Non-repud.
Backdoor malware	✓			✓	✓	✓	
Blackhole	✓						
Collisions	✓						
Data tempering	✓	✓		✓	✓	✓	
De-authentication	✓						
DoS	✓						
Eavesdropping		✓	✓	✓		✓	
Flooding attack	✓						
GPS Spoofing	✓						
Grayhole	✓						
Impersonation	✓	✓		✓	✓	✓	✓
Insider	✓			✓	✓	✓	
Jamming/Active interfering	✓			✓		✓	
LLQ & HL	✓						
MITM	✓	✓	✓	✓	✓	✓	
Modification	✓			✓	✓	✓	
Replay	✓	✓					
Rushing	✓						
Selfishness	✓						
SPOF	✓						
Sybil	✓			✓	✓	✓	
SYN flood	✓						
Wormhole	✓			✓	✓	✓	

adaptive federated reinforcement learning (AFRL) to detect and defend against constant, random, and reactive jamming attacks using model-free Q-Learning methods. AFRL has two main components: multi-access edge computing (MEC) server and UAV. Each UAV maintains its own estimation of the parameter by collecting sensor data. UAVs train a local model and update the local weight by computing the collected data using a learning rate and then uploading it to the MEC. The global weight is initialised in the MEC with local updates from UAVs; this improves global model leveraging. To detect jamming in the neighbouring area, UAVs create a model by downloading the global weight from MEC then updating it to reflect the local training process.

6.2.2. Backdoor malware

Our research has not found a specific solution for UAV backdoor malware that enhances FANET confidentiality, availability, integrity and privacy. [162] developed a solution specifically for WSN mobile

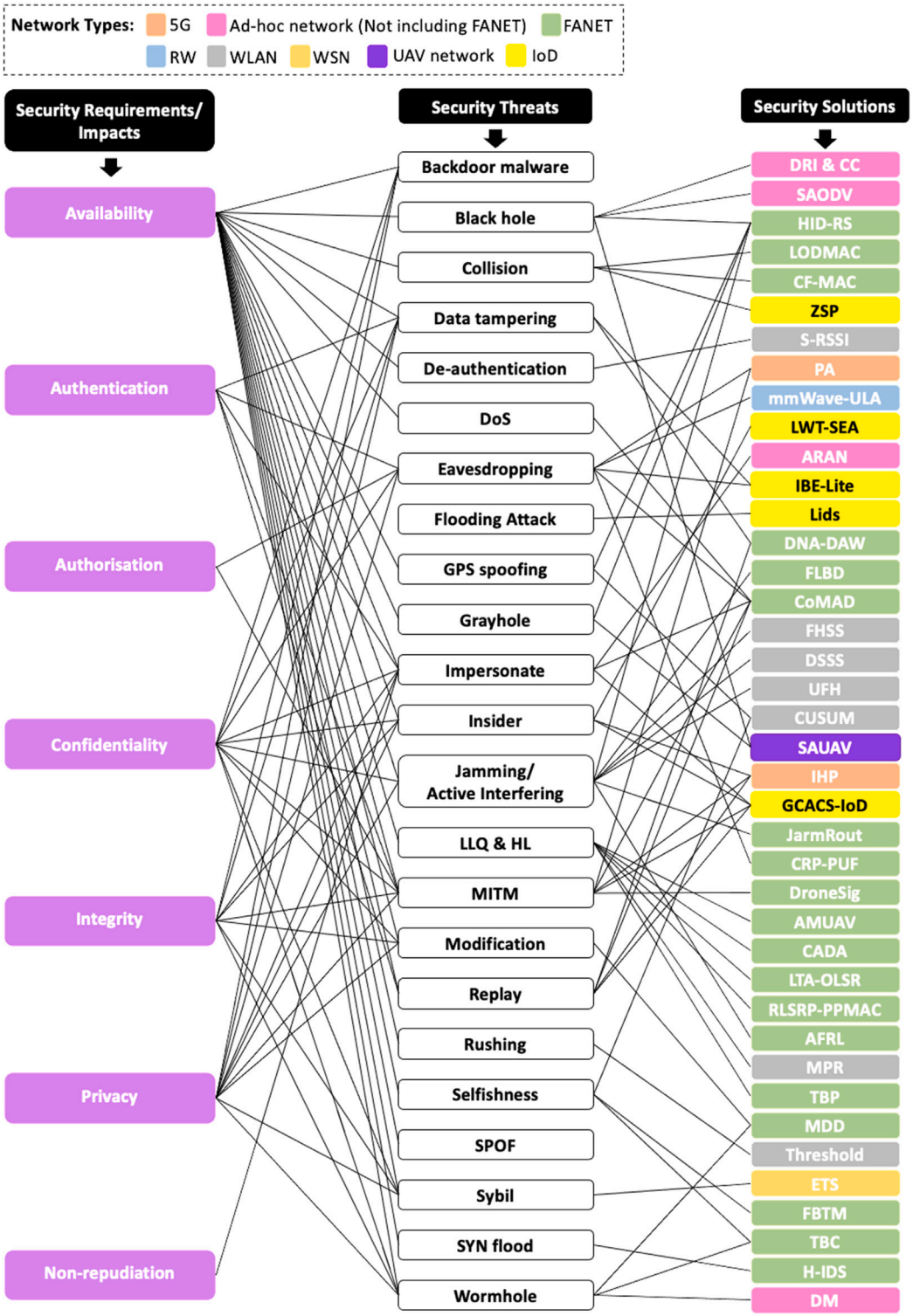


Fig. 42. Security threats and solutions based on security requirements.

nodes. This solution was not designed for FANET or UAV communications, however, this method could potentially resolve future issues by locating, tracking, and then curing infected nodes.

6.2.3. Blackhole

According to [97,107], the ad-hoc on-demand distance vector (AODV) protocol is vulnerable to blackhole attacks. The following solutions have been proposed to enhance FANET availability and prevent packets from being dropped by malicious nodes.

Faraji-Biregani and Fotohi [82] designed a secure agent unmanned aerial vehicle (SAUAV) on the AODV protocol. SAUAV has two phases to protect UAV networks, in the first phase a malicious UAV is identified then removed using a set of rules. The second phase implements a negotiation process with a mobile agent. This agent allows UAVs to discover neighbours that are one-hop away, and provides UAVs

in the network with information regarding malicious UAVs. When compared to other methods, such as BSUM-based, HVCR, CS-AVN or CST-UAS, SAUAV has high detection rates for malicious UAVs. In addition, SAUAV provides high residual energy and packet delivery rates with low levels of false positives.

[97] modified AODV to include MANET data routing information (DRI) tables and cross checking (CC). Each node preserves their own DRI to indicate where every packet is from and its route through other nodes. In CC, to find a suitable route, the source node broadcasts a RREQ during the route discovery process. The middle node, located between source and destination, sends a RREP with DRI entry and next hop data; the source node then verifies its reliability. To mitigate blackhole attacks in MANETs, a secure AODV (SAODV) was proposed in [107], under the assumption that malicious nodes always provide the first reply. In this protocol, only reply packets are counted, with the first source reply packet being ignored. [103] proposed an agent-based hierarchical detection and response system (HID-RS) which uses the GCS as a centralised and reliable node that monitors FANET packets. Firstly, each UAV needs to send a *neighbouring packet* to the GCS which includes the UAV's type (source or relay), as well as the next and the previous hop node. Secondly, the GCS differentiates UAVs based upon four categories: normal, suspect, abnormal, and malicious. The GCS only takes account of normal and suspect UAVs. Then the GCS verifies if the relay UAV actually has sent packets to the next hop node, and calculates the number of dropped packets. Finally, to identify intentional and unintentional (caused by collisions or interfering) dropped packets, a threshold value TH_{BH} is set and updated by an SVM algorithm.

6.2.4. Collisions

UAVs can operate in, join or leave half-duplex FANET networks which are characterised by high mobility levels and frequent topology changes. The MAC layer must, therefore, provide communication which is collision free and enhances FANET availability [95]. The location oriented directional MAC protocol (LODMAC) was introduced in [104]. FANET capacity and availability is increased by neighbouring UAV locations being integrated with directional antennas; this resolves collision and deafness issues. [95] proposed a collision-free MAC protocol (CF-MAC) which comprises the CSMA/TDMA MAC protocol using half-duplex radio channel and omni-directional antennas. To prevent collisions, time slots are used that arrange how UAVs join the FANET. [17] suggests that to maintain effective and real-time UAV navigation, only authorised UAVs should fly in aerial spaces. To this end, UAVs broadcast their location to a zone service provider (ZSP), rather than using self-organisation to heal the network. The ZSP detects, monitors and manages UAV operations, checking for abnormal behaviour such DoS, spoofing or data tampering attacks that could interrupt the normal network operation.

6.2.5. Data tampering

An encryption algorithm should be implemented to protect sensitive data from being altered. This algorithm will maintain confidentiality, availability, integrity, and privacy. [17] presented the lightweight identity-based (IBE-Lite) method that encrypts UAV data, preventing cloud service providers from reading the data, even if they have physical access to it. It is unlikely that an attacker could obtain sensitive data, given that only public parameters, such as big prime, prime order and elliptic curve base point are saved in UAV's sensors.

Sun et al. proposed a distributed network architecture with double-authentication watermark (DNA-DAW) [81]. In DNA-DAW, a collection UAV gathers data, then generates an authentication watermark embedded with a timestamp, which is sent to the cluster head UAV. The cluster head UAV authenticates data packets, generates a random sequence, embeds a watermark on part of the data, then sends it to the sink UAV. The sink UAV analyses data within the packets to confirm its authenticity and integrity.

6.2.6. De-authentication

CVE-2019-3944 [163] was published in 2020 and documented Wi-Fi de-authentication issues and a Parrot ANAFI vulnerability. The vulnerability allows remote unauthorised attackers to interrupt mid-flight connections then break FANET availability [110] proposes a method to avoid de-authentication attacks. Their method uses the physical layer signal signature with a received signal strength indicator (S-RSSI) to discover any conflicting requests to join the same target UAV.

6.2.7. Denial-of-Service (DoS)

There are many ways in which DoS attacks can cause serious damage to the availability of FANET normal operations. [32] presented two methods in the context-aware mutual authentication protocol (CoMAD) that can mitigate DoS attacks. Firstly, repeated data from the same source UAV is dropped. Secondly, UAVs that provide invalid passwords or authentication contexts are prohibited from operating.

6.2.8. Eavesdropping

Eavesdropping attacks can affect confidentiality and privacy. The following solutions aim to mitigate such attacks. Using a directional antenna on the millimetre wave (mmWave) band provides wide bandwidths and fast data rates. In 2017, a uniform linear array (ULA) was developed [87] that accesses the mmWave secrecy rate. Experimental results indicate that low frequency mmWave signals achieve higher secrecy rates using low transmit power when compared to high frequency signals with a higher transmit power. It was also found that to decrease attacker antenna gains, an increased number of transmitting node antennas are required.

To prevent both eavesdropping and MITM attacks while deploying 5G networks, a new framework was designed by the 3rd Generation Partnership Project (3GPP), called the primary authentication (PA) in 5G new radio (NR). The framework provides two mandatory authentication choices, extensible authentication protocol (EAP) as well as 5G authentication and key agreement (5G-AKA). 5G-AKA provides an in-built home control that verifies if the device is valid in a specific network. Secondary authentication is used that validates the data network not in the mobile operator domain. Privacy concerns are dealt with by a public home network key being deployed to enhance the subscriber's identity privacy [88]. To protect UAV's identity and location privacy from eavesdropping or transferred messages, [17] proposed a lightweight identity-based (IBE-Lite) method. This method provides symmetric encryption, group signatures (GS), and zero-knowledge proofs to process mutual authentication between UAVs, meaning only authorised UAVs can access data. [32] proposed CoMAD to protect sensitive data during normal operation and authentication processes. To confirm if the UAV is still a legitimate member while authenticating, CoMAD implemented a symmetric session key and a public–private key pair with valid context data.

A lightweight authentication protocol was proposed by Pu and Li [77], whereby every UAV holds a circuit with a physical unclonable function (PUF). The challenge-response pair (CRP) of the PUF is used to start up the chaotic system then generate a session key which secures communications between UAV and GCS. This process can prevent adversaries manipulating the UAV, as hostile probes or modifications can invalidate the PUF challenge-response mapping, which will prevent UAV communications.

6.2.9. Flooding attack

Pu and Zhu [76] proposed a lightweight distributed detection method (Lids) to help both UAVs and GCSs identify flooding attacks. When a UAV joins the network, a certificate authority (CA) registration process is completed defining the threshold for packets that can be sent within a specific time period. UAVs then communicate with each other the number of packets they have each sent over a specific time period. Packets will be discarded by the UAV if the threshold is exceeded within a set time limit. The GCS collects UAV threshold reports when they connect to it. Any suspicious UAVs can be discovered which will result in an alarm packet being broadcast to all UAVs in the local network.

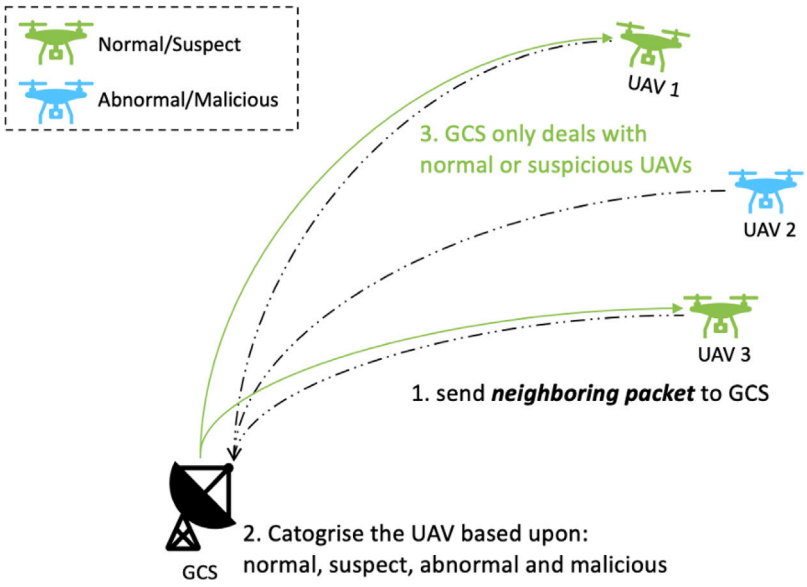


Fig. 43. Hierarchical intrusion detection and response scheme (HID-RS).

6.2.10. GPS spoofing

GPS spoofing can result in UAV normal operations becoming unavailable which could lead to a UAV being hijacked. [96] proposed a detection method that deploys cumulative sum (CUSUM) algorithms that quickly discover GPS spoofing attacks. In their simulation, the hit-rate is monitored, if the time offset is greater than the no-hit zone, then it is determined that GPS spoofing is occurring. Moreover, the CUSUM detection method can also be used to detect selfish nodes and data injection attacks. [103] introduced HID-RS which implements rule-based intrusion detection methods on both UAV and GCS with detection and response schemes respectively. The attacker normally produces high signal strength intensity (SSI) to take over control of a UAV. Hence, in HID-RS a UAV carries an agent to gather SSI data sent from the initiating node. The SSI is analysed with the SSI's threshold to find out if GPS spoofing exists. The SSI's threshold is updated by using the support vector machines (SVMs) learning algorithm to maintain the proper detection function.

6.2.11. Grayhole

Grayhole attacks can significantly affect the FANET availability, but can be difficult to detect due their unpredictable behaviour. [103] proposed a hierarchical intrusion detection and response scheme (HID-RS) which monitors packets using the GCS as a centralised and reliable node. This solution is similar to that introduced for blackhole attacks. Fig. 43 illustrates the HID-RS process. Each UAV sends a *neighbouring packet* to the GCS which includes the UAV type (source or relay), as well as the next and the previous hop nodes. The GCS then classifies the UAV into abnormal, malicious, normal, or suspect, and then only interacts with the last two categories. The GCS confirms if the relay UAV has sent packets to the next hop node, then calculates the number of dropped packets. Dropped communication packets, which can be caused by collisions or interference, are identified and used to set a threshold value TH_{GH} which indicates Greyhole behaviour.

As outlined in Section 6.2.3 (SAUAV [82]), misbehaving UAVs can be removed from UAV networks by using the two phase method. A mobile agent shares notifications between the UAVs, meaning network packets from malicious UAVs are rejected.

6.2.12. Impersonation

Some FANET protocols deploy authentication to determine if a UAV has the right to join the FANET. Authentication can prevent unauthorised or malicious UAVs connecting to the network, attempting to steal data, decreasing availability or stopping operations. To enhance non-repudiation, once a UAVs identity is confirmed, data exchange should not be denied in later communications. Denying data exchange can affect not only the availability but also the confidentiality, integrity, and privacy [32,109]. Authenticated routing for ad-hoc networks (ARAN) was introduced in [109]. ARAN uses public-key encryption to prevent identity attacks. [32] demonstrated the context-aware mutual authentication protocol for drone networks (CoMAD). CoMAD re-organises swarms using predefined UAV ID and key pairs that authenticate their identity.

With the proposed solution GCACS-IoD [80], discussed in Section 6.2.13, certificates are issued using a control room. Attackers do not have permissions to obtain certificates which could spoof UAV or GCS identities.

6.2.13. Insider

Insider attacks involve the leakage of sensitive data and can create privacy issues. [17] proposed a lightweight symmetric encryption algorithm (LWT-SEA) to encrypt all navigation data from the source to the destination node.

Wu et al. [79] proposed an improved protocol based on Hussain et al.'s design (IHP). Their protocol contains the following phases: drone registration, user registration, logging, and authentication. During the first phase, the drone identity is sent to the server which calculates a value using it, together with a random number and secret key. This data is then sent to the drone database. In the second phase, the user's identity is sent to the server. The server selects a random number and a temporary user identity. The server then calculates values, such as temporary user identity, with a random number. These are passed back to the user, which stores them on a mobile device. The third phase involves a user sending an authentication request to the server, which confirms the message's freshness and verifies user legitimacy. When the message is verified, the server selects a random number with a timestamp and then sends the message to the drone. The drone verifies the message freshness using the server timestamp; if the verification is successful, the drone then sends the message to the user. The user confirms the freshness of the drone message with its timestamp, upon process completion authentication is concluded. Once this process is completed, the authentication is successfully finished. Insider attacks can be prevented by IHP. Even if an adversary has the server secret key, specific values are randomly generated, resulting in the overall session being unable to be computed.

After reviewing the design of Bera et al. [164], Chaudhry et al. [80] proposed a certificate-based generic access control scheme for Internet of drones (GCACS-IoD). In GCACS-IoD, before any communication commences, every UAV and GCS obtains an initialisation certificate by registering with a control room. The certificate uses predefined UAV credentials, UAVs are only allowed to join the IoD after being fully initialised. Insider attacks are not possible, as registration data cannot be accessed before deployment.

6.2.14. Low link quality and high latency (LLQ & HL)

LLQ & HL result in FANET availability and capacity issues. According to [9], the concept of using IEEE 802.11 with omni-directional antennas was originally deployed in FANET. Omni-directional antennas have short transmission range, high latency, and low capacity; therefore, they are more suited to use in MANETs and VANETs rather than in FANETs. As wireless transmitters and receivers cannot operate at the same time, directional antennas use full duplex radio circuits with multi packet reception (MPR) [106]. The adaptive MAC protocol for UAV (AMUAV) was introduced in [93] using GPS and IMU. An omni-directional antenna sends packets that control the UAV position. Data packets are sent using a directional antenna; this configuration increases network communication performance and enhances throughput. To achieve the QoS and high mobility, a token-based protocol (TBP) [108] was introduced with three key lists: code, channel gain, and delay requirements. When a token is received by a UAV, a code is taken out of the list in order to transfer the data. The channel gain of each link is updated in the channel gain list and the waiting time of the sender before transmitting data is added into the delay requirements list. The token is passed to the next UAV earlier than data starts to transmit.

[94] presented capacity analysis in directional antennas (CADA) which simulate different flight scenarios and distances between UAVs. The authors' results indicate that when the beam angle degree is increased, the number of UAV nodes drop. [104] also proposed a location oriented directional MAC protocol (LODMAC) which has two transceivers running in parallel on different frequencies. One of them probes phases, the other transmits data. The probing phase has two stages, location estimation and communication control. In the first stage, a sender broadcasts its location to UAVs in a specific transmission range. Listeners can delay their transmissions to prevent collisions. To alleviate the deafness issues associated with directional antennas, the second stage involves a new Busy to Send (BTS) being defined with Request to Send (RTS) and Clear to Send (CTS) packets. Usually when two UAVs exchange packets, nodes wanting to communicate using a RST packet are ignored. With LODMAC, a BTS will be sent to inform the sender that the node is transmitting data with another node. The sender then waits a specific amount of time, which is defined in BTS, then sends it again. Data transmission starts whenever sender and receiver exchange RTS/CTS. The receiver location is provided from a neighbouring directional database, the receiver points their antenna to the sender to transfer data quickly.

[90] proposed a position-prediction based directional MAC protocol (PPMAC) with a self-learning routing protocol, based upon reinforcement learning (RLSRP). This solution merges directional antennas and position prediction methods in the MAC layer to alleviate deafness issues. An up-to-date routing policy also provides low network latencies. [105] introduced a link-quality and traffic-load aware OLSR protocol (LTA-OLSR) to increase FANET reliability, availability, and efficiency. UAVs learn the status of other UAVs one-hop away by periodically broadcasting a *HELLO message* containing their address and traffic load. Each UAV then chooses a multipoint relay (MR) from the other one-hop away UAVs. To maintain link quality, UAVs not chosen to be a MR do not broadcast packets obtained from that UAV again. Traffic load is calculated based upon channel data and packet buffers.

6.2.15. Man-in-the-middle (MITM)

Unauthorised nodes can use MITM attacks to affect the connection confidentiality, integrity, and availability. In some cases, even the UAV identity is revealed, which then alters its privacy. Section 6.2.13 outlines the design of [80], whereby timestamps with random nonces assist in identifying malicious messages. The authors' design prevents MITM attacks from being launched, even when messages are intercepted.

Wu et al. [79] proposed an IHP protocol using a design outlined in Section 6.2.13. Certain communication values are locally calculated, then not transmitted between users and the server. This process prevents attackers from successfully authenticating to the network or intercepting messages.

A lightweight digital signal protocol called DroneSig [75] was developed by Li and Pu in 2020. DroneSig prevents UAV commands from being executed unless they contain a valid digital signature and come from a legitimate GCS. The digital signature is generated using a 3-step process, simulation experiments indicate better performance in terms of resources than Advanced Encryption Standard (AES), Data Encryption Standard (DES) or Triple DES (3DES).

In 2018, 3GPP designed a new framework, primary authentication (PA) to prevent both eavesdropping and MITM attacks while deploying 5G. [32] proposed CoMAD to guard against MITM attacks. CoMAD uses the following strategies: (i) UAV join or leave requests are encrypted, (ii) public keys secure communication messages, and (iii) timestamps and nonces are deployed to ensure message freshness.

6.2.16. Modification

Modification means an unauthorised third party manipulates the message to achieve its goal. This attack alters package contents to break FANET confidentiality, integrity, and availability. A model-driven design (MDD) was proposed in [85,86] for FANETs. An asymmetric encryption and one-way hash chain are deployed to prevent the package hop count and lifetime fields being altered.

6.2.17. Replay

To mitigate replay attacks, proper timestamps or nonces should be deployed that maintain FANET availability. [32] proposed CoMAD where fresh nonces are generated during the FANET initialisation process. A fresh nonce is used in FANET to guarantee that other UAVs are not receiving replay messages. Timestamps are implemented in backbone UAVs to ensure correct time synchronisation, messages are discarded when the timestamp expires.

In Section 6.2.13, we noted that GCACS-IoD adds a timestamp and random nonces to messages between UAVs. The timestamps are verified and nonces are confirmed using certificates. This process means UAVs can identify replay messages. As discussed in Section 6.2.13, Wu et al. [79] proposed the IHP protocol which utilises unique timestamps for UAV, server and user during the registration and authentication processes. Message freshness is constantly verified, any identified sessions containing reply messages are closed immediately. DNA-DAW [81] was outlined in 6.2.5, whereby reply attacks can be discovered by time-stamping the cluster head node watermark.

6.2.18. Rushing

Rushing results in the target UAV operating abnormally and also affects FANET availability. [127] analysed suitable techniques to prevent rushing attacks. One method uses a time threshold between sender and receiver. The receiver compares a known threshold with the actual packet arrival time. If the arrival time is less than threshold value, the packet is dropped.

6.2.19. Selfishness

Whenever a selfish UAV exists in the FANET, it can affect FANET availability. The CUSUM [96] detection method can be deployed to mitigate selfishness. A fuzzy-based trust model (FBTM) was proposed in [98]. FBTM calculates direct and indirect trust values to detect and separate UAVs that are non-cooperative, meaning they are selfish nodes, these are then marked as malicious. Another trust-based clustering (TBC) scheme was provided in [89] that uses a cluster voting concept to select members based on their fuzzy environment behaviour. TBC can mitigate malicious UAVs, such as misbehaved or selfish ones that affect FANET availability.

6.2.20. Single Point of Failure (SPOF)

According to [165], SPOF is an architectural design issue, where redundant systems are not provided [166]. SPOF can be prevented by developing redundant systems using load balancers and other high-availability methods. These systems automatically deploy working nodes when failures occur.

6.2.21. Sybil attacks

Sybil attacks affect confidentiality, availability, integrity, and privacy during normal transmissions. [84] proposed a detection method based on energy trust systems (ETS) for WSNs. In cluster architectures, this method verifies the identity and location at each level based on an energy threshold. If the rate is not constant, the UAV is suspected to be a Sybil node and the received message is deleted.

6.2.22. SYN flood

SYN flood attacks disrupt the operation of UAVs in FANET and affect FANET availability [10]. [102] proposed a hybrid intrusion detection system (H-IDS) with spectrum traffic analysis and a method to monitor FANET for abnormal behaviour.

6.2.23. Wormhole

Although wormholes can be difficult to be detected in ad-hoc networks, some detection methods have been proposed. A detection metric (DM) for MANETs was provided in [83]. The wormhole strength was defined by the number of end-to-end paths engaged by the malicious node. When a path length is shorter than normal, a malicious node is suspected. Another indicator of a wormhole is when one node remains the same even when the topology changes. A model-driven design (MDD) for FANETs was presented in [85,86]. The MDD analyses and compares differences between packet hop count and a hop count computed with path length. When the values are not equal, a wormhole attack is detected. During the route discovery process, messages are exchanged. Every UAV generates unicast route discovery packets to neighbouring UAVs containing the next hop node with a hash. This hash is compared with the one existing in the packet to confirm validity. TBC uses a voting system to select cluster members based on their behaviour in a fuzzy environment. This model can recognise malicious nodes and separate them from FANETs.

6.3. Generic solutions: Cross-layer

The cross-layer design has been proposed to deal with performance issues in wireless connections, this design shares data within the first three OSI layers (Fig. 44), namely physical, data link, and network layers [131,167]. Contention-based OLSR (COLSR) [168] deploys a systematic method to build better paths by selecting the next hop and optimum relay. To prevent collisions between UAVs, the distributed relay is selected using the MAC-physical cross-layer. Choosing geographic routes is based on MAC-network cross-layer. Intelligent MAC protocol for UAV (IMAC-UAV) with directional OLSR (DOLSR) was proposed in [169]. A specifically designed MAC Layer protocol named IMAC-UAV drives two directional and two omni-directional antennas. Data packets are sent via directional antennas. Omni-directional antennas listen for other UAVs and send heartbeats updating location data. Distances and bit error rates are monitored in case they affect UAV altitude or antennas. DOLSR extends the OLSR Network Layer; route decisions are based on collected data among layers. When packets are sent, if the distance is greater than maximum, D_{max}, the node uses DOLSR. Alternatively, if the distance is less than D_{max}, OLSR is used. Efficient power OLSR (EP-OLSR) was proposed in [167]. Fig. 45 illustrates how EP-OLSR works among different layers. An enhanced signal is sent from the physical layer to the network layer via a multi antenna relay. Hello messages are launched to inform neighbouring UAVs to choose the MPR and update the routes. EP-OLSR maintains link quality and reduces the chance of link cut-outs.

6.4. IoD solutions

We now describe some of the countermeasures that could be implemented against the IoD security threats described in 4.5. The focus is purely on technological means, rather than regulations or standards, which are not within the scope of this survey.

6.4.1. Confidentiality

Lightweight and energy-efficient symmetric-key cryptographic algorithms should be deployed on devices that are resource constrained. Ni et al. [170] implemented Elgamal and AES to encrypt location information, which provides confidentiality and traceability for mobile devices. Srinivas et al. [171] designed TCALAS, an temporal credential based anonymous lightweight user authentication mechanism for the IoD. This was proven to be resistant to known authentication attacks. Al et al. [172] improved TCALAS by using lightweight symmetric key primitives and temporal credentials to secure against traceability as well as stolen verifier attacks. The researchers proposed scheme, ITCALAS, is lightweight and can work with multiple IoD flying zones or clusters.

6.4.2. Integrity

Several IoD defence mechanisms can be deployed against malicious actors to prevent them from accessing drone data. Altawy et al. [173] cite IDS, strict access control policies, firewalls and logging as being the most important. Dawaliby et al. [174] proposed a block-chain based platform for managing IoD operations that maintains trust and security. Their testbed consisted of IoT devices, a drone and block-chain enabled gateways. Obtained results indicated decreased signalling and operation times, with autonomous drone management.

6.4.3. Availability

To safeguard drones from DoS or spoofing attacks, Altawy et al. [173] suggest an anonymous intrusion detection system that differentiates between genuine communications and those corrupted by DoS attacks. Arthur et al. [175] use an intelligent deep learning based IDS to distinguish between spoofed or original GPS signals. This allows drones to identify intruders and ensure a safe return-to-home if required. Simulations indicate the IDS can provide high levels of accuracy, sensitivity and specificity against a range of cyber security attacks.

6.5. Standards

In this subsection, we introduce the relevant UAS standards. These standards relate to UAV safety, design, communication, traffic management, flight controls and human training.

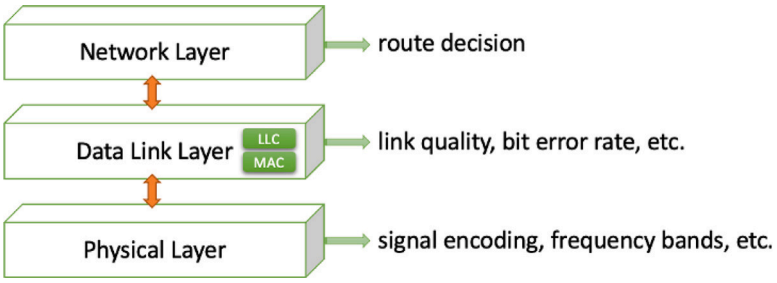


Fig. 44. Cross-Layer Design.

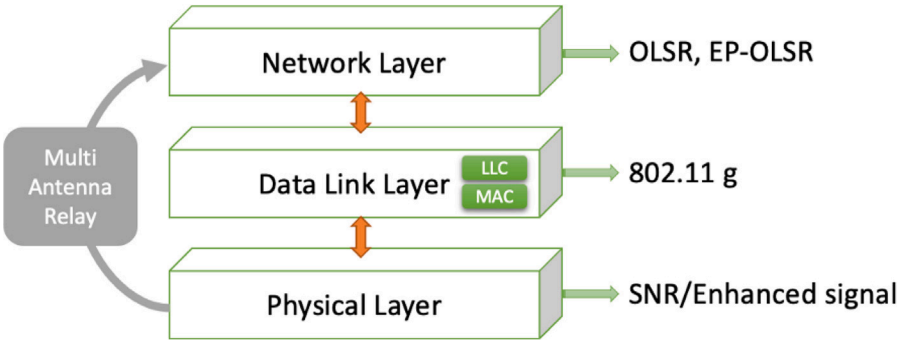


Fig. 45. EP-OLSR Operation.

6.5.1. 3GPP cellular standards

Alliance for Telecommunications Industry Solutions (ATIS) is the North American Organisational Partner for 3GPP. 3GPP Standards added some elements to mobile cellular networks to support UAV communication [176] using LTE and 5G radios. The related works are detailed in 3GPP Release 15 [177], 16 [178] as well as 17 [179] and includes UAVs ranging from low altitude to high altitude (8 km-50 km). These works cover issues such as up-link power control, interference detection, radio performance improvement, identification, initial UAV pilot authorisation, UAV traffic management, identity broadcasting when piloting BLoS.

6.5.2. ASTM F38

American Society for Testing and Materials (ASTM) F38 [180] is a committee that develops UAS standards and guidance, including topics relating to safety, performance as well as flight proficiency. There are thirteen active standards in subcommittee F38.01 [181] and five proposed new standards waiting for jurisdiction. In particular, these standards are UAS registration and marking (ASTM F2851-10) [182], small and lightweight UAS design (ASTM F2910-14) [183], construction and verification (ASTM F3298-19) [184], specification in designing command and control systems in small UAS (ASTM F3002-14a) [185], and detection as well as avoidance in small UAS BVLOS (ASTM WK62669) [186].

6.5.3. ISO/TC 20/SC 16

ISO Technical Committee (TC) 20, Subcommittee (SC) 16 are a set of standards in UAS areas containing, but not restricted to classification, design, manufacture and operation [187]. Since 2019, there are five published standards about commercial UAS operation requirements (ISO 21384-3:2019) [188], definition of relevant terms in UAS (ISO 21384-4:2020) [189], a classification tool of UAS (ISO 21895:2020) [190], a survey on UAS traffic management (UTM) (ISO/TR 23629-1:2020) [191] and methods for training people who operate UAVs (ISO 23665:2021) [192].

6.5.4. JAUS

Joint Architecture for Unmanned Systems (JAUS) is a standard message format for transferring data between UAVs, which was introduced in 1998 by NATO [193]. In 2007, AS5669a presented the JAUS transport specification for data communication among heterogeneous UAVs. JAUS supports TCP, UCP as well as serial, they are named as JTCP, JUDP and JSerial respectively. This communication is on top of TCP/UDP to support variable length data packets in low bandwidth serial links. Although JAUS provides a standard to follow, there might be hardware restrictions and real-time communication issues for UAVs. STANAG 4586 was introduced [194] to define a common Transport Layer protocol to support UAV communications. The Concept of Operations (CONOPS) was determined amongst NATO countries to provide a level of interoperability (LOI) between UAVs.

6.5.5. PODIUM

Providing Operations of Drones with Initial UAS traffic Management (PODIUM) [195] provides a U-space service (a European ecosystem assisting UAV operation), methods and technologies in three European countries. PODIUM gives advice regarding standards, regulations and future UAV use with partners like Airbus, DSNA, DELAIR, Drones Pari Region, and Unifly. PODIUM is contributed to by EUROCONTROL which is an organisation serving European aviation. EUROCONTROL also presents a series of projects and initiatives [196] about UAS operations, UTM, satellite navigation and flight control.

6.5.6. UASSC

Unmanned Aircraft Systems Standardization Collaborative (UASSC) was introduced by the American National Standards Institute (ANSI) [197] to help with safe integration of UAS by speeding up the development of relevant standards in the U.S. The standardisation roadmap was revealed in June 2020 which includes airworthiness, flight operations, personnel training, qualification and certification, infrastructure inspections, environmental applications, commercial services, workplace and public safety operations.

Based on the discussion above, we observe that although there are standards that support UAV communication, flight control, UTM, and human training, apart from JAUS there are no other novel standardised

communication protocols which can be deployed in heterogeneous UAVs. In this case, the communication between UAVs tends to be only between homogeneous UAVs. The design of small UAVs has been classified in ASTM F38, however, no encryption algorithms have been proposed among these standards.

7. Open research problems and challenges

7.1. Limitations

Although we have categorised 40 solutions to the identified threats, we expected to see more specifically designed FANET solutions. These designs would focus on a FANET with low node density, high node mobility, frequent topology changes, significant reliance on radio propagation, and restricted computational power. Our categorisation resulted in 19 solutions explicitly for FANETs, one for UAV network architecture, and five for the IoD. The remaining solutions are related to other types of ad-hoc networks, but unsuitable for UAVs that move at high speed. Currently, FANETs lack a standardised communication channel for authentication and authorisation of UAV communications. Time spent by UAVs within the FANET initialisation phase would decrease if a standard communication channel existed.

7.2. Future research

In terms of FANET security and privacy, we believe several different areas need further attention. Recently, novel security solutions related to software-defined networking (SDN) [198,199], machine learning, and 5G technologies have been proposed, some of these are not included in this survey. Furthermore, we note that our survey does not discuss research related to the multiple newly identified backdoor malware families which target UAVs and FANETs.

Because FANET is a subset of MANET, most of its routing protocols are designed around wireless communications. There are MANET protocols that can be modified to suit the characteristics of FANET, however, we observe that more security solutions exist for MANET than FANET. As UAVs become increasingly popular, we expect that research will concentrate on new protocol design, machine learning, and 5G technology. A large number of solutions exist that enhance FANET security. Whilst lightweight encryption is designed for resource constrained devices [200], reinforcement learning (RL) provides an agent to effectively learn in changeable and complex environments [13,159]. SDN can also improve network performance by automating network control [12].

7.3. Standardisation

FANET is a decentralised flexible network environment with both heterogeneous and homogeneous UAVs. We anticipated standardised communication protocols, facilitating cooperation between heterogeneous UAVs and FANETs would exist, but this was not the case. Therefore, future work could implement uniform protocols allowing heterogeneous UAVs to collaborate in commercial, agricultural, or military applications. Many industry-wide communication standards exist, for example, related to WiFi, Bluetooth, or Ethernet. We expected the UAV industry to follow this trend, and implement a clear set of standards across-the-board. To defend against security threats, we suggest UAV manufacturers set standards relating to authentication and encryption methods when equipped with an agent that has lightweight computational powers.

8. Conclusion

The aim of this survey was to provide a clear picture of recent FANET security threats, solutions, and their relevant techniques. We have surveyed complementary activities from academia, industries, and standardisation bodies and have identified twenty-three security threats over connections, nodes and the first four OSI layers, with the most significant issues explained using diagrams and easy-to-follow examples. In addition, we have classified forty security solutions over six network types, namely FANET, 5G, Ad-Hoc, RW, WLAN, and WSN. Twenty-one routing protocols are divided into six categories, namely static, proactive, reactive, hybrid, geographic-based, and agent-based. These solve specific issues and improve FANET usability. Finally, we also provide details regarding cross-layer routing protocols and UAV standards.

Existing surveys introduced FANET security solutions, however we have included other solutions not presented in those surveys. This survey includes traditional solutions as well as novel FANET solutions and protocols. The aim of this survey was to provide clear concepts regarding the formation of security threats with corresponding security impacts, together with their relevant solutions. Our target audience would be readers wishing to gain in-depth knowledge of UAV and FANET security and privacy threats with suitable solutions. For example, this survey would be a worthwhile read for anyone who wants to understand or start a new project regarding mobile vehicles. We provide a comprehensive overview of FANET security threats based on twelve threat vectors and four OSI layers. Finally, we also review existing standards related to UAV safety, design, communication, traffic management, and human training.

Agent-based or agent-less solutions can be deployed on UAVs or GCSs to detect or defend against security threats. Hardware limitations on certain UAV types could make them unsuitable for agent-based solutions unless an efficient machine learning algorithm is implemented. We believe that future work could compare agent-less with agent-based solutions. Most existing solutions aim to solve low link quality, high latency, and jamming issues. Future work could focus on security solutions that are more efficient and have low computational power, such as lightweight encryption, RL, and SDN. Instead of using MANET or VANET characteristics, FANET security solution design should consider its limitations — sparse, highly mobile nodes, frequent topology changes, significant reliance on radio propagation, and restricted computational abilities. We believe that FANET and IoD defence mechanisms are at a very early stage of development and we await to witness ongoing interest and progress in this area.

Nomenclature

AFRL Adaptive Federated Reinforcement Learning
AMUAV Adaptive MAC protocol for UAV
AN Autonomous Navigation
ANSI American National Standards Institute
AODV Ad-Hoc On-demand Distance Vector
ARAN Authenticated Routing for Ad-Hoc Networks
AS Authenticity Signal
ASTM American Society for Testing and Materials
ATIS Alliance for Telecommunications Industry Solutions
BLoS Beyond Line of Sight
BTS Busy To Send
BvLoS Beyond the Visual Line of Sight
CAA Civil Aviation Authority
CADA Capacity Analyse in Directional Antenna
CB Certificated-Based
CF-MAC Collision-Free MAC protocol
COLSR Contention-Based OLSR
CoMAD Context-aware Mutual Authentication protocol for Drone
CS Certificateless Signcryption
CUSUM Cumulative Sum
DCR Data Centric Routing

DM Detection Metrics
DOLSR Directional OLSR
DRI & CC Data Routing Information & Cross Checking
DSR Dynamic Source Routing
DSSS Direct Sequence Spread Spectrum
EP-OLSR Efficient Power Optimised Link State Routing
ETS Energy Trust Systems
FAA Federal Aviation Administration
FANET Flying Ad-Hoc Network
FBTM Fuzzy-Based Trust Model
FHSS Frequency Hopping Spread Spectrum
FLBD Federated Learning-Based detection
FRL Federated Reinforcement Learning
GCS Ground Control Station
GPMOR Geographic Position Mobility Oriented Routing
GPS Global Positioning System
GPSR Greedy Perimeter Stateless Routing
H-IDS Hybrid Intrusion Detection System
H-LWT Hybrid Lightweight
HID Hierarchical Identity-based
HID-RS Hierarchical Detection and Response System
IMAC UAV Intelligent Medium Access Control Protocol for Unmanned Aerial Vehicle
ISO International Organisation for Standardisation
JAUS Joint Architecture for Unmanned Systems
LAROD Location Aware Routing for Opportunistic Delay-tolerant network
LBA Location-Based Authentication
LBE-Lite Lightweight identity-based
LCAD Load-Carry-and-Deliver
LLSP Link-Layer Security Protocol
LODMAC Location Oriented Directional MAC protocol
LoS Line of Sight
LTA Link-quality and Traffic-load Aware
LTE Long-Term Evolution
LWT Lightweight
MANET Mobile Ad-hoc Network
MDD Model-Driven Design
MGUANET Multi-Group UAV Ad-Hoc Network
ML Machine Learning
ML-OLSR Mobility and Load aware OLSR
MLHR Multi-Level Hierarchical Routing
MLUANET Multi-Layer UAV Ad-Hoc Network
mmWave Millimetre Wave
MPGR Mobility Prediction Geographic Routing
MPR Multi Packet Reception
MR Multipoint Relay
MRPA Mission Route Planning Agent
OLSR Optimised Link State Routing
PA Primary Authentication
PODIUM Providing Operations of Drones with Initial UAS traffic Management
POLSR Predictive OLSR
PPMAC Position-Prediction-based directional MAC protocol
Q-MRP Q-learning-based fuzzy logic for Multiobjective Routing Protocol
QL Q-Learning
RC Remote-Controlled
RL Reinforcement Learning
RLSRP Reinforcement Learning Self-learning Routing Protocol
RREP Route Reply
RREQ Route Request
RTORA Rapid Re-establish Temporally Ordered Routing Algorithm
RTS Request to Send
S-RSSI Signalprint with Receive Signal Strength Indicator
SAODV Secure AODV
SAR Search And Rescue
SC Subcommittee
SDN Software Defined Network
SEAD Secure Efficient Ad-Hoc Distance
SSM Spread Spectrum Methods
TBC Trust-Based Clustering
TBP Token-Based Protocol
TBRFP Topology Broadcast based on Reverse-Path Forwarding
TC Technical Committee
TORA Temporally Ordered Routing Algorithm
TPPA Traceable and Privacy-Preserving Authentication
TSAODV Time-Slotted AODV
UASSC Unmanned Aircraft Systems Standardization Collaborative
UANET UAV Ad-Hoc Network
UAS Unmanned Aerial System
UAV Unmanned Aerial Vehicle
U-DSSS Uncoordinated Direct Sequence Spread Spectrum
UFH Uncoordinated Frequency Hopping
ULA Uniform Linear Array
USD-FH Uncoordinated Seed Disclosure in Frequency Hopping
USMP UAV Search Mission Protocol
UTM UAS Traffic Management
VANET Vehicle Ad-Hoc Network
ZRP Zone Routing Protocol
ZSP Zone Service Provider

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] I. Bekmezci, O.K. Sahingoz, S. Temel, Flying Ad-Hoc networks (FANETs): A survey, Ad Hoc Netw. 11 (3) (2013) 1254–1270.
[2] M. Satell, Ultimate list of drone stats for 2021, 2021, Philly By Air, 15th, Jan. 2021, URL https://www.phillybyair.com/blog/drone-stats/.
[3] Registering to use a drone or model aircraft, Civil Aviation Authority, URL https://register-drones.caa.co.uk/individual.
[4] 5 trends appear on the gartner hype cycle for emerging technologies, 2019, 2019, Gartner, 29th, Aug. 2019, URL https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019/.
[5] Flying in the open category, Civil Aviation Authority, URL https://www.caa.co.uk/Consumers/Unmanned-aircraft/Recreational-drones/Flying-in-the-open-category/.
[6] L. Schroth, The drone market size 2020–2025: 5 key takeaways, 2020, DRONEII, 22nd, Jun. 2020, URL https://droneii.com/the-drone-market-size-2020-2025-5-key-takeaways.
[7] Skies without limits, 2021, PwC, URL https://www.pwc.co.uk/intelligent-digital/drones/Drones-impact-on-the-UK-economy-FINAL.pdf.
[8] M. Satell, U.S. DRone survey reveals intriguing trends, 2020, Philly By Air, 28th, Jul.2020, URL https://www.phillybyair.com/blog/drone-study/.
[9] A. Chriki, H. Touati, H. Snoussi, F. Kamoun, FANET: Communication, mobility models and security issues, Comput. Netw. 163 (2019) 106877.
[10] I. Bekmezci, E. Sentürk, T. Türker, Security issues in flying ad-hoc networks (fanets), J. Aeronaut. Space Technol. 9 (2) (2016) 13–21.
[11] A. Bujari, C.E. Palazzi, D. Ronzani, FANET application scenarios and mobility models, in: Proceedings of the 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications, in: DroNet '17, Association for Computing Machinery, New York, NY, USA, 2017, pp. 43–46.
[12] J.-P. Yaacoub, H. Noura, O. Salman, A. Chehab, Security analysis of drones systems: Attacks, limitations, and recommendations, Internet Things 11 (2020) 100218.
[13] S. Rezwan, W. Choi, A survey on applications of reinforcement learning in flying ad-hoc networks, Electronics 10 (4) (2021).
[14] M.A. Khan, A. Safi, I.M. Qureshi, I.U. Khan, Flying ad-hoc networks (FANETs): A review of communication architectures, and routing protocols, in: 2017 First International Conference on Latest Trends in Electrical Engineering and Computing Technologies, INTELLECT, 2017, pp. 1–9.
[15] A. Riham, A.M. Youssef, Security, privacy, and safety aspects of civilian drones: A survey, ACM Trans. Cyber-Phys. Syst. 1 (2) (2016).

[16] L. Gupta, R. Jain, G. Vaszkun, Survey of important issues in UAV communication networks, IEEE Commun. Surv. Tutor. 18 (2) (2016) 1123–1152.
[17] C. Lin, D. He, N. Kumar, K.-K.R. Choo, A. Vinel, X. Huang, Security and privacy for the internet of drones: Challenges and solutions, IEEE Commun. Mag. 56 (1) (2018) 64–69.
[18] M. Gharibi, R. Boutaba, S.L. Waslander, Internet of drones, IEEE Access 4 (2016) 1148–1162.
[19] M. Yahuza, M.Y.I. Idris, I.B. Ahmedy, A.W.A. Wahab, T. Nandy, N.M. Noor, A. Bala, Internet of drones security and privacy issues: Taxonomy and open challenges, IEEE Access 9 (2021) 57243–57270.
[20] Commission delegated regulation (EU) 2019/945, 2019, Official Journal of the European Union, 12th, Mar.2019, URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0945.
[21] T.F. Villa, F. Salimi, K. Morton, L. Morawska, F. Gonzalez, Development and validation of a UAV based system for air pollution measurements, Sensors 16 (12) (2016).
[22] M. Aljehani, M. Inoue, A. Watanbe, T. Yokemura, F. Ogyu, H. Iida, UAV communication system integrated into network traversal with mobility, SN Appl. Sci. 2 (2020) 1057.
[23] D. Giordan, M.S. Adams, I. Aicardi, M. Alicandro, P. Allasia, M. Baldo, P.D. Berardinis, D. Dominici, D. Godone, P. Hobbs, V. Lechner, T. Niedzielski, M. Piras, M. Rotilio, R. Salvini, V. Segor, B. Sotier, F. Troilo, The use of unmanned aerial vehicles (UAVs) for engineering geology applications, Bull. Eng. Geol. Environ. 79 (2020) 3437–3481.
[24] Unmanned aerial systems (UAS), 2020, SKYbrary, 8 December 2020, URL https://www.skybrary.aero/articles/unmanned-aerial-systems-uas.
[25] M. Vasylenko, I. Karpyuk, Telemetry system of unmanned aerial vehicles, Electron. Control Syst. (3) (2018) 95–100.
[26] H. Chao, Y. Cao, Y. Chen, Autopilots for small unmanned aerial vehicles: A survey, Int. J. Control Autom. Syst. 8 (1) (2010) 36–44.
[27] F. Höflinger, J. Müller, R. Zhang, L.M. Reindl, W. Burgard, A wireless micro inertial measurement unit (IMU), IEEE Trans. Instrum. Meas. 62 (9) (2013) 2583–2595.
[28] An introduction to unmanned aircraft systems, Civil Aviation Authority, URL https://www.caa.co.uk/Consumers/Unmanned-aircraft/Our-role/An-introduction-to-unmanned-aircraft-systems/.
[29] M.A. Khan, I.M. Qureshi, F. Khanzada, A hybrid communication scheme for efficient and low-cost deployment of future flying ad-hoc network (FANET), Drones 3 (1) (2019).
[30] Ad Hoc Network, NIST, URL https://csrc.nist.gov/glossary/term/Ad_Hoc_Network.
[31] M.R. Silva, E.S. Souza, P.J. Alsina, D.L. Leite, M.R. Morais, D.S. Pereira, L.B.P. Nascimento, A.A.D. Medeiros, F.H.C. Junior, M.B. Nogueira, G.L.A. Albuquerque, J.B.D. Dantas, Performance evaluation of multi-UAV network applied to scanning Rocket Impact Area, Sensors 19 (22) (2019).
[32] U.C. Cabuk, G. Dalkilic, O. Dagdeviren, CoMAD: Context-aware mutual authentication protocol for drone networks, IEEE Access 9 (2021) 78400–78414.
[33] H. Jahankhani, S. Yousef, Evolution of TETRA through the integration with a number of communication platforms to support public protection and disaster relief (PPDR), in: Cyber Crime and Cyber Terrorism Investigator's Handbook, Elsevier, 2014, pp. 259–273.
[34] Fact sheet – small unmanned aircraft systems (UAS) regulations (part 107), 2020, U.S Department of Transportation - Federal Aviation Administration, 6th, Oct.2020, URL https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=22615.
[35] J. Flynt, How fast can drones fly? 2018, 3DINSIDER, 19th, Oct.2018, URL https://3dinsider.com/drone-speed/.
[36] D.B. Johnson, D.A. Maltz, Dynamic source routing in ad hoc wireless networks, in: Mobile Computing, Springer, 1996, pp. 153–181.
[37] Z.J. Haas, A new routing protocol for the reconfigurable wireless networks, in: 6th International Conference on Universal Personal Communications, Vol. 2, ICUPC, 1997, pp. 562–566.
[38] J.-D.M.M. Biomo, T. Kunz, M. St-Hilaire, An enhanced Gauss-Markov mobility model for simulations of unmanned aerial ad hoc networks, in: 2014 7th IFIP Wireless and Mobile Networking Conference, WMNC, 2014, pp. 1–8.
[39] Y. Wan, K. Namuduri, Y. Zhou, S. Fu, A smooth-turn mobility model for airborne networks, IEEE Trans. Veh. Technol. 62 (7) (2013) 3359–3370.
[40] W. Wang, X. Guan, B. Wang, Y. Wang, A novel mobility model based on semi-random circular movement in mobile ad hoc networks, Inform. Sci. 180 (3) (2010) 399–413.
[41] O. Bouachir, A. Abrassart, F. Garcia, N. Larrieu, A mobility model for UAV ad hoc network, in: 2014 International Conference on Unmanned Aircraft Systems, ICUAS, 2014, pp. 383–388.
[42] E. Kuiper, S. Nadjm-Tehrani, Mobility models for UAV group reconnaissance applications, in: 2006 Int. Conference on Wireless and Mobile Communications, ICWMC'06, IEEE, 2006, p. 33.
[43] J. Sanchez-Garcia, J. Garcia-Campos, S. Toral, D. Reina, F. Barrero, A self organising aerial ad hoc network mobility model for disaster scenarios, in: 2015 International Conference on Developments of E-Systems Engineering, DeSE, IEEE, 2015, pp. 35–40.
[44] T. Camp, J. Boleng, V. Davies, A survey of mobility models for ad hoc network research, Wirel. Commun. Mob. Comput. 2 (5) (2002) 483–502.
[45] F. Bai, N. Sadagopan, A. Helmy, The IMPORTANT framework for analyzing the impact of mobility on performance of RouTing protocols for adhoc networks, Ad Hoc Netw. 1 (4) (2003) 383–403.
[46] A. Bujari, C.T. Calafate, J.-C. Cano, P. Manzoni, C.E. Palazzi, D. Ronzani, Flying ad-hoc network application scenarios and mobility models, Int. J. Distrib. Sens. Netw. 13 (10) (2017) 17.
[47] M. Sánchez, P. Manzoni, ANEJOS: A java based simulator for ad hoc networks, Future Gener. Comput. Syst. 17 (5) (2001) 573–583.
[48] E.M. Royer, P.M. Melliar-Smith, L.E. Moser, An analysis of the optimum node density for ad hoc mobile networks, in: IEEE International Conference on Communications, Vol. 3, ICC, 2001, pp. 857–861.
[49] F. Sun, Z. Deng, C. Wang, Z. Li, A networking scheme for FANET basing on SPMA protocol, in: IEEE 6th International Conference on Computer and Communications, ICCC, 2020, pp. 182–187.
[50] N.A. Khan, S.N. Brohi, N. Jhanjhi, UAV'S applications, architecture, security issues and attack scenarios: A survey, in: Intelligent Computing and Innovation on Data Science, Springer, 2020, pp. 753–760.
[51] T. Reed, J. Geis, S. Dietrich, Skynet: A 3G-enabled mobile attack drone and stealth botmaster, in: 5th USENIX Workshop on Offensive Technologies, WOOT 11, 2011.
[52] No fly zones for drones in the UK, URL https://www.noflydrones.co.uk.
[53] The STRIDE threat model, 2009, Microsoft Corporation., Dec. 2009, URL https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN.
[54] S. He, Q. Wu, J. Liu, W. Hu, B. Qin, Y.-N. Li, Secure communications in unmanned aerial vehicle network, in: International Conference on Information Security Practice and Experience, Springer, 2017, pp. 601–620.
[55] J. Kong, H. Luo, K. Xu, D.L. Gu, M. Gerla, S. Lu, Adaptive security for multilevel ad hoc networks, Wirel. Commun. Mob. Comput. 2 (5) (2002) 533–547.
[56] J. Won, S.-H. Seo, E. Bertino, A secure communication protocol for drones and smart objects, in: 10th ACM Symposium on Information, Computer and Communications Security, in: ASIA CCS, vol. 15, New York, NY, USA, 2015, pp. 249–260.
[57] M. Strasser, C. Popper, S. Capkun, M. Cagalj, Jamming-resistant key establishment using uncoordinated frequency hopping, in: 2008 IEEE Symposium on Security and Privacy, 2008, pp. 64–78.
[58] A. Liu, P. Ning, H. Dai, Y. Liu, USD-FH: Jamming-resistant wireless communication using frequency hopping with uncoordinated seed disclosure, in: 7th IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, IEEE MASS 2010, 2010, pp. 41–50.
[59] Y.-C. Hu, D.B. Johnson, A. Perrig, SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, Ad Hoc Netw. 1 (1) (2003) 175–192.
[60] J. Ren, T. Li, D. Aslam, A power efficient link-layer security protocol (LLSP) for wireless sensor networks, in: 2005 IEEE Military Communications Conference, Vol. 2, MILCOM, 2005, pp. 1002–1007.
[61] M. Strohmeier, V. Lenders, I. Martinovic, Intrusion detection for airborne communication using PHY-layer information, in: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2015, pp. 67–77.
[62] R. Mitchell, R. Chen, Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications, IEEE Trans. Syst. Man Cybern.: Syst. 44 (5) (2013) 593–604.
[63] S. Gil Casals, P. Owezarski, G. Descargues, Generic and autonomous system for airborne networks cyber-threat detection, in: 2013 IEEE/AIAA 32nd Digital Avionics Systems Conference, DASC, 2013, pp. 4A4–1–4A4–14.
[64] T. Kacem, D. Wijesekera, P. Costa, A. Barreto, An ADS-b intrusion detection system, in: 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 544–551.
[65] C. Rani, H. Modares, R. Sriram, D. Mikulski, F.L. Lewis, Security of unmanned aerial vehicle systems against cyber-physical attacks, J. Defense Model. Simul. 13 (3) (2016) 331–342.
[66] C. Li, Y. Xu, J. Xia, J. Zhao, Protecting secure communication under UAV smart attack with imperfect channel estimation, IEEE Access 6 (2018) 76395–76401.
[67] C.-L. Chen, Y.-Y. Deng, W. Weng, C.-H. Chen, Y.-J. Chiu, C.-M. Wu, A traceable and privacy-preserving authentication for UAV communication control system, Electronics 9 (1) (2020) 62.
[68] D. Sharma, A. Rashid, S. Gupta, S.K. Gupta, A functional encryption technique in UAV integrated HetNet: A proposed model, Int. J. Simul.–Syst. Sci. Technol. 20 (2019).
[69] J. Liu, Q. Wang, C. He, K. Jaffrès-Runser, Y. Xu, Z. Li, Y. Xu, QMR: Q-Learning based multi-objective optimization routing protocol for flying ad hoc networks, Comput. Commun. 150 (2020) 304–316.
[70] Q. Yang, S.-J. Jang, S.-J. Yoo, Q-learning-based fuzzy logic for multi-objective routing algorithm in flying ad hoc networks, Wirel. Pers. Commun. 113 (2020) 115–138.
[71] N.I. Mowla, N.H. Tran, I. Doh, K. Chae, Federated learning-based cognitive detection of jamming attack in flying ad-hoc network, IEEE Access 8 (2020) 4338–4350.

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

[73] I. Boureanu, A. Mitrokotsa, S. Vaudenay, Towards secure distance bounding, in: International Workshop on Fast Software Encryption, Springer, 2013, pp. 55–67.

[74] D.E. Denning, P.F. MacDoran, Location-based authentication: Grounding cyberspace for better security, Comput. Fraud Secur. 1996 (2) (1996) 12–16.

[75] Y. Li, C. Pu, Lightweight digital signature solution to defend micro aerial vehicles against man-in-the-middle attack, in: 2020 IEEE 23rd International Conference on Computational Science and Engineering, CSE, 2020, pp. 92–97.

[76] C. Pu, P. Zhu, Defending against flooding attacks in the internet of drones environment, in: 2021 IEEE Global Communications Conference, GLOBECOM, 2021, pp. 1–6.

[77] C. Pu, Y. Li, Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system, in: 2020 IEEE International Symposium on Local and Metropolitan Area Networks, LANMAN, IEEE, 2020, pp. 1–6.

[78] C. Pu, Jamming-resilient multipath routing protocol for flying ad hoc networks, IEEE Access 6 (2018) 68472–68486.

[79] T. Wu, X. Guo, Y. Chen, S. Kumari, C. Chen, Amassing the security: An enhanced authentication protocol for drone communications over 5G networks, Drones 6 (1) (2022).

[80] S.A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A.K. Bashir, Y.B. Zikria, GCACS-IoD: A certificate based generic access control scheme for internet of drones, Comput. Netw. 191 (2021) 11.

[81] J. Sun, W. Wang, L. Kou, Y. Lin, L. Zhang, Q. Da, L. Chen, A data authentication scheme for UAV ad hoc network communication, J. Supercomput. 76 (6) (2020) 4041–4056.

[82] M. Faraji-Biregani, R. Fotohi, Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles, J. Supercomput. 77 (5) (2021) 5076–5103.

[83] V. Mahajan, M. Natu, A. Sethi, Analysis of wormhole intrusion attacks in MANETS, in: IEEE Military Communications Conference, MILCOM, 2008, pp. 1–7.

[84] N. Alsaedi, F. Hashim, A. Sali, F.Z. Rokhani, Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS), Comput. Commun. 110 (2017) 75–82.

[85] J.-A. Maxa, M.S. Ben Mahmoud, N. Larrieu, Secure routing protocol design for UAV ad hoc networks, in: 2015 IEEE/AIAA 34th Digital Avionics Systems Conference, DASC, 2015, pp. 4A5–1–4A5–15.

[86] J.-A. Maxa, M.S. Ben Mahmoud, N. Larrieu, Joint model-driven design and real experiment-based validation for a secure UAV ad hoc network routing protocol, in: 2016 Integrated Communications Navigation and Surveillance, ICNS, 2016, pp. 1E2–1–1E2–16.

[87] Y. Zhu, L. Wang, K.-K. Wong, R.W. Heath, Secure communications in millimeter wave ad hoc networks, IEEE Trans. Wireless Commun. 16 (5) (2017) 3205–3217.

[88] A.R. Prasad, A. Zugenmaier, A. Escott, M.C. Soveri, 3GPP 5g security, 2018, 3GPP - A Global Initiative, 6th, Aug. 2018 URL https://www.3gpp.org/news-events/1975-sec_5g.

[89] K. Singh, A.K. Verma, TBCS: A trust based clustering scheme for secure communication in flying ad-hoc networks, Wirel. Pers. Commun. 114 (2020) 3173–3196.

[90] Z. Zheng, A.K. Sangaiah, T. Wang, Adaptive communication protocols in flying ad hoc network, IEEE Commun. Mag. 56 (1) (2018) 136–142.

[91] S. Han, M. Xie, H.-H. Chen, Y. Ling, Intrusion detection in cyber-physical systems: Techniques and challenges, IEEE Syst. J. 8 (4) (2014) 1052–1062.

[92] N.I. Mowla, N.H. Tran, I. Doh, K. Chae, AFRL: Adaptive federated reinforcement learning for intelligent jamming defense in FANET, J. Commun. Netw. 22 (3) (2020) 244–258.

[93] A.I. Alshbatat, L. Dong, Adaptive MAC protocol for UAV communication networks using directional antennas, in: 2010 International Conference on Networking, Sensing and Control, ICNSC, 2010, pp. 598–603.

[94] S. Temel, I. Bekmezci, Scalability analysis of flying ad hoc networks (FANETs): A directional antenna approach, in: 2014 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom, 2014, pp. 185–187.

[95] A. Jiang, Z. Mi, C. Dong, H. Wang, CF-MAC: A collision-free MAC protocol for UAVs ad-hoc networks, in: 2016 IEEE Wireless Communications and Networking Conference, 2016, pp. 1–6.

[96] Q. Zeng, H. Li, L. Qian, GPS spoofing attack on time synchronization in wireless networks and detection scheme design, in: IEEE Military Communications Conference, MILCOM, 2012, pp. 1–5.

[97] J. Sen, S. Koilakonda, A. Ukil, A mechanism for detection of cooperative black hole attack in mobile ad hoc networks, in: 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, 2011, pp. 338–343.

[98] K. Singh, A.K. Verma, A fuzzy-based trust model for flying ad hoc networks (FANETs), Int. J. Commun. Syst. 31 (6) (2018) e3517, e3517 IJCS-16-0655.R2.

[99] N. Chayat, Frequency hopping spread spectrum PHY of the 802.11 wireless LAN standard, 1996, 11th, Mar. 1996, BreezeCom - IEEE 802.Org.

[100] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, G. Pantziou, A survey on jamming attacks and countermeasures in WSNs, IEEE Commun. Surv. Tutor. 11 (4) (2009) 42–56.

[101] N.I. Mowla, N.H. Tran, I. Doh, K. Chae, Federated learning-based cognitive detection of jamming attack in flying ad-hoc network, IEEE Access 8 (2020) 4338–4350.

[102] J.-P. Condomines, R. Zhang, N. Larrieu, Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation, Ad Hoc Netw. 90 (2019) 101759.

[103] H. Sedjelmaci, S.M. Senouci, N. Ansari, A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks, IEEE Trans. Syst. Man Cybern.: Syst. 48 (9) (2018) 1594–1606.

[104] S. Temel, I. Bekmezci, LODMAC: Location oriented directional MAC protocol for FANETs, Comput. Netw. 83 (2015) 76–84.

[105] C. Pu, Link-quality and traffic-load aware routing for UAV ad hoc networks, in: 2018 IEEE 4th International Conference on Collaboration and Internet Computing, CIC, 2018, pp. 71–79.

[106] S. Ghez, S. Verdu, S. Schwartz, Stability properties of slotted Aloha with multipacket reception capability, IEEE Trans. Automat. Control 33 (7) (1988) 640–649.

[107] A.K. Jain, V. Tokekar, Mitigating the effects of black hole attacks on AODV routing protocol in mobile ad hoc networks, in: International Conference on Pervasive Computing, ICPC, 2015, pp. 1–6.

[108] Y. Cai, F.R. Yu, J. Li, Y. Zhou, L. Lamont, MAC performance improvement in UAV ad-hoc networks with full-duplex radios and multi-packet reception capability, in: 2012 IEEE International Conference on Communications, ICC, 2012, pp. 523–527.

[109] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, E. Belding-Royer, Authenticated routing for ad hoc networks, IEEE J. Sel. Areas Commun. 23 (3) (2005) 598–610.

[110] K. Bicakci, B. Tavli, Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks, Comput. Stand. Interfaces 31 (5) (2009) 931–941.

[111] T. Sakthivel, R. Chandrasekaran, Detection and prevention of wormhole attacks in MANETs using path tracing approach, Eur. J. Sci. Res. 76 (2) (2012) 240–252.

[112] J. Sen, S. Koilakonda, A. Ukil, A mechanism for detection of cooperative black hole attack in mobile ad hoc networks, in: Second International Conference on Intelligent Systems, Modelling and Simulation, 2011, pp. 338–343.

[113] J. Teng, W. Gu, D. Xuan, Chapter 10 - defending against physical attacks in wireless sensor networks, in: S.K. Das, K. Kant, N. Zhang (Eds.), Handbook on Securing Cyber-Physical Critical Infrastructure, Morgan Kaufmann, Boston, 2012, pp. 251–279, http://dx.doi.org/10.1016/B978-0-12-415815-3.00010-8.

[114] What is a replay attack? Kaspersky, URL https://www.kaspersky.com/resource-center/definitions/replay-attack.

[115] What are the spectrum band designators and bandwidths? 2018, 2nd. Sep. 2018, National Aeronautics and Space Administration.

[116] Man-in-the-Middle attack (MitM), National Institute of Standards and Technology, URL https://csrc.nist.gov/glossary/term/man_in_the_middle_attack.

[117] D. Förster, F. Kargl, H. Löhr, PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET), in: 2014 IEEE Vehicular Networking Conference, VNC, 19th, Jan.2015, 2015.

[118] A. Vasudeva, M. Sood, Survey on sybil attack defense mechanisms in wireless ad hoc networks, J. Netw. Comput. Appl. 120 (2018) 78–118.

[119] Cloud security guidance, 2018, National Cyber Security Centre, 17th, Nov. 2018, URL https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles/data-in-transit-protection.

[120] S. Khandelwal, MalDrone - First ever backdoor malware for drones, 2015, The Hacker News, 27th, Jan.2015, URL https://thehackernews.com/2015/01/MalDrone-backdoor-drone-malware.html.

[121] R. Sasi, Maldrone the first backdoor for drones, 2015, Fb1h2s Aka Rahul Sasi's Blog, 26th, Jan. 2015, URL http://garage4hackers.com/entry.php?b=3105.

[122] Denial of Service (DoS) guidance, National Cyber Security Centre, URL https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection.

[123] M. Li, S. Salinas, P. Li, J. Sun, X. Huang, MAC-Layer selfish misbehavior in IEEE 802.11 ad hoc networks: Detection and defense, IEEE Trans. Mob. Comput. 14 (6) (2014) 1203–1217.

[124] A. Shan, X. Fan, C. Wu, X. Zhang, S. Fan, Quantitative study on the impact of energy consumption based dynamic selfishness in MANETs, Sensors 21 (3) (2021).

[125] Tampering, Computer Security Resource Center, URL https://csrc.nist.gov/glossary/term/tampering.

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

[127] S. Shrivastava, Rushing attack and its prevention techniques, Int. J. Appl. Innov. Eng. Manag. 2 (4) (2013) 453–456.

[128] L. Vaas, Drone hijacked by hackers from texas college with $1,000 spoofer, 2012, Sophos Naked Security, 2nd, Jul.2012, URL https://nakedsecurity.sophos.com/2012/07/02/drone-hackedwith-1000-spoofer/.

[129] C. Thompson, Drug traffickers are hacking US surveillance drones to get past border patrol, 2015, Insider, 30th, Dec. 2015, URL https://www.businessinsider.com/drug-traffickers-are-hacking-us-border-drones-2015-12?r=US&IR=T.

[130] A. Khan, Hacking the drones, 2016, OWASP, Apr. 2016, URL https://owasp.org/www-chapter-london/assets/slides/OWASP201604_Drones.pdf.

[131] A. Froehlich, L. Rosencrance, K. Gattine, OSI model (Open Systems Interconnection), SearchNetworking, URL https://searchnetworking.techtarget.com/definition/OSI.

[132] T. Szigeti, J. Henry, F. Baker, Mapping diffserv to IEEE 802.11, 2018, Internet Engineering Task Force (IETF), Feb. 2018, URL https://datatracker.ietf.org/doc/html/rfc8325#section-6.

[133] Y. Cai, F.R. Yu, J. Li, Y. Zhou, L. Lamont, Medium access control for unmanned aerial vehicle (UAV) ad-hoc networks with full-duplex radios and multipacket reception capability, IEEE Trans. Veh. Technol. 62 (1) (2013) 390–394.

[134] Collision avoidance in wireless networks, 2019, GeeksforGeeks, 12th, Aug. 2019, URL https://www.geeksforgeeks.org/collision-avoidance-in-wireless-networks/.

[135] O. Westerlund, R. Asif, Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things, in: 2019 1st International Conference on Unmanned Vehicle Systems-Oman, UVS, IEEE, 2019, pp. 1–10.

[136] M. Tyagi, S. Narvare, C. Agrawal, A survey of different dos attacks on wireless network, 2018, CORE, Vol.9, No.5.

[137] Link quality, ScienceDirect, URL https://www.sciencedirect.com/topics/engineering/link-quality.

[138] D. Wu, P. Djukic, P. Mohapatra, Determining 802.11 link quality with passive measurements, in: 2008 IEEE International Symposium on Wireless Communication Systems, 2008, pp. 728–732.

[139] What is latency? | How to fix latency, Cloudflare, URL https://www.cloudflare.com/en-gb/learning/performance/glossary/what-is-latency/.

[140] R. Dey, H.N. Saha, Different routing threats and its mitigations schemes for mobile ad-hoc networks (MANETs)–A review, IPASJ Int. J. Electron. Commun. (IIJEC) 4 (3) (2016) 27–34.

[141] M. Tripathi, M.S. Gaur, V. Laxmi, Comparing the impact of black hole and gray hole attack on LEACH in WSN, Procedia Comput. Sci. 19 (2013) 1101–1107.

[142] S.K. Singh, M. Singh, D.K. Singh, A survey on network security and attack defense mechanism for wireless sensor networks, Int. J. Comput. Trends Technol. 1 (2) (2011) 9–17.

[143] I.U. Khan, I.M. Qureshi, M.A. Aziz, T.A. Cheema, S.B.H. Shah, Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET), IEEE Access 8 (2020) 56371–56378.

[144] C.-M. Cheng, P.-H. Hsiao, H.T. Kung, D. Vlah, Maximizing throughput of UAV-relaying networks with the load-carry-and-deliver paradigm, in: 2007 IEEE Wireless Communications and Networking Conference, 2007, pp. 4417–4424.

[145] P.P. Bonissone, Multi-criteria decision-making: The intersection of search, preference tradeoff, and interaction visualization processes, in: IEEE Symposium on Computational Intelligence in Multi-Criteria Decision-Making, 2007, p. 1.

[146] Z. Sun, P. Wang, M.C. Vuran, M.A. Al-Rodhaan, A.M. Al-Dhelaan, I.F. Akyildiz, BorderSense: Border patrol through advanced wireless sensor networks, Ad Hoc Netw. 9 (3) (2011) 468–477.

[147] O.K. Sahingoz, Networking models in flying ad-hoc networks (FANETs): Concepts and challenges, J. Intell. Robot. Syst. 74 (2014) 513–527.

[148] B. Bellur, R. Ogier, A reliable, efficient topology broadcast protocol for dynamic networks, in: IEEE Conference on Computer Communications, Vol. 1, INFOCOM, 1999, pp. 178–186.

[149] D.B. Johnson, D.A. Maltz, Dynamic source routing in ad hoc wireless networks, in: T. Imielinski, H.F. Korth (Eds.), Mobile Computing, Springer US, Boston, MA, 1996, pp. 153–181.

[150] Y.-C.H. David B. Johnson, The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4, 2007, IETF - RFC4728, Feb. 2007, URL https://datatracker.ietf.org/doc/rfc4728/.

[151] C.E. Perkins, Ad hoc on-demand distance vector (AODV) routing, 2003, IETF - Network Working Group, Jul. 2003, URL https://datatracker.ietf.org/doc/html/rfc3561.

[152] V.D. Park, C.M. Scott, Temporally-ordered routing algorithm (TORA) version 1 functional specification, 1997, IETF, 26th. Nov. 1997, URL https://datatracker.ietf.org/doc/html/draft-ietf-manet-tora-spec-00.

[153] V.D. Park, C.M. Scott, Temporally-ordered routing algorithm (TORA) version 1 functional specification, 2001, IETF MANET Working Group, 20th, Jul. 2001, URL https://datatracker.ietf.org/doc/html/draft-ietf-manet-tora-spec-04.

[154] P.S. Zygmunt J. Haas, The zone routing protocol (ZRP) for ad hoc networks, 2002, IETF - MANET Working Group, URL https://datatracker.ietf.org/doc/html/draft-ietf-manet-zone-zrp-04.

[155] B. Karp, H.T. Kung, GPSR: Greedy perimeter stateless routing for wireless networks, in: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, in: MobiCom '00, Association for Computing Machinery, New York, NY, USA, 2000, pp. 243–254.

[156] L. Lin, Q. Sun, J. Li, F. Yang, A novel geographic position mobility oriented routing strategy for UAVs, J. Comput. Inf. Syst. 8 (2) (2012) 709–716, Cited By :57.

[157] E. Kuiper, S. Nadjm-Tehrani, Geographical routing in intermittently connected ad hoc networks, in: 22nd International Conference on Advanced Information Networking and Applications, 2008, pp. 1690–1695.

[158] K. Tulum, U. Durak, S.K. Yder, Situation aware UAV mission route planning, in: 2009 IEEE Aerospace Conference, 2009, pp. 1–12.

[159] B. Osiński, K. Budek, What is reinforcement learning? The complete guide, 2018, Deepsense.Ai, 5th, Jul. 2018, URL https://deepsense.ai/what-is-reinforcement-learning-the-complete-guide/.

[160] SYN flood attack, Cloudflare, URL https://www.cloudflare.com/en-gb/learning/ddos/syn-flood-ddos-attack/.

[161] A. Takacs, H. Mahkonen, X. Lin, How mobile networks can support drone communication, 2017, Ericsson Blog, URL https://www.ericsson.com/en/blog/2017/11/how-mobile-networks-can-support-drone-communication.

[162] N.R. Zema, E. Natalizio, G. Ruggeri, M. Poss, A. Molinaro, MeDrone: On the use of a medical drone to heal a sensor network infected by a malicious epidemic, Ad Hoc Netw. 50 (2016) 115–127.

[163] CVE-2019-3944 detail, 2019, National Institute of Standards and Technology, URL https://nvd.nist.gov/vuln/detail/CVE-2019-3944.

[164] B. Bera, D. Chattaraj, A.K. Das, Designing secure blockchain-based access control scheme in IoT-enabled internet of drones deployment, Comput. Commun. 153 (2020) 229–249.

[165] Managing information security risk, 2011, National Institute of Standards and Technology, Mar. 2011, URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

[166] Single Point Of Failure, Avi Networks, URL https://avinetworks.com/glossary/single-point-of-failure/.

[167] H. Nawaz, H. Mansoor Ali, Implementation of cross layer design for efficient power and routing in UAV communication networks, Stud. Inf. Control 29 (1) (2020) 111–120.

[168] Y. Li, X. Luo, Cross layer optimization for cooperative mobile ad-hoc UAV network, Int. J. Digit. Content Technol. Appl. 6 (18) (2012) 367.

[169] A.I. Alshbatat, L. Dong, Cross layer design for mobile ad-hoc unmanned aerial vehicle communication networks, in: 2010 International Conference on Networking, Sensing and Control, ICNSC, 2010, pp. 331–336.

[170] J. Ni, X. Lin, K. Zhang, X. Shen, Privacy-preserving real-time navigation system using vehicular crowdsourcing, in: 2016 IEEE 84th Vehicular Technology Conference, VTC-Fall, 2016, pp. 1–5.

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

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

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

[174] S. Dawaliby, A. Aberkane, A. Bradai, Blockchain-based IoT platform for autonomous drone operations management, in: Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and beyond, in: DroneCom, vol. 20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 31–36.

[175] 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, 2019, pp. 1–5.

[176] Support for UAV communications in 3GPP cellular standards, 2018, Alliance for Telecommunications Industry Solutions (ATIS), Oct. 2018, URL https://access.atis.org/apps/group_public/download.php/42855/ATIS-I-0000069.pdf#page14.

[177] TR 38.811 v1.0.0 on study on NR to support non-terrestrial networks, 2018, Jun. 2018, 3GPP.

[178] Study on remote identification of unmanned aerial systems (UAS) specification #:22.825, 2018, 3GPP, Sep. 2018, URL https://www.3gpp.org/ftp/Specs/archive/22_series/22.825/.

[179] Study on supporting unmanned aerial systems (UAS) connectivity, identification and tracking, 2021, 3GPP, URL https://www.3gpp.org/ftp/Specs/archive/23_series/23.754//.

[180] M. Mikolajewski, Committee F38 on unmanned aircraft systems, American Society for Testing and Materials (ASTM), URL https://www.astm.org/COMMIT/SCOPES/F38.htm.

[181] Subcommittee F38.01 on airworthiness, American Society for Testing and Materials (ASTM), URL https://www.astm.org/COMMIT/SUBCOMMIT/F3801.htm.

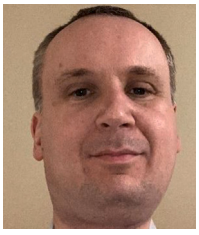
[182] Standard Practice for UAS registration and marking (Excluding Small Unmanned Aircraft Systems), American Society for Testing and Materials (ASTM), URL https://www.astm.org/Standards/F2851.htm.

[183] Standard Specification for Design and Construction of a Small Unmanned Aircraft System (sUAS), American Society for Testing and Materials (ASTM), URL https://www.astm.org/Standards/F2910.htm.

[184] Standard specification for design, construction, and verification of lightweight unmanned aircraft systems (UAS), American Society for Testing and Materials (ASTM), URL https://www.astm.org/Standards/F3298.htm.

[185] Standard specification for design of the command and control system for small unmanned aircraft systems (sUAS), American Society for Testing and Materials (ASTM), URL https://www.astm.org/Standards/F3002.htm.
[186] New test method for detect and avoid, American Society for Testing and Materials (ASTM), URL https://www.astm.org/DATABASE.CART/WORKITEMS/WK62669.htm.
[187] ISO/TC 20/SC 16 unmanned aircraft systems, International Organization for Standardization (ISO), URL https://www.iso.org/committee/5336224.html.
[188] ISO 21384-3:2019(en)unmanned aircraft systems — Part 3: Operational procedures, 2019, International Organization for Standardization (ISO), Nov. 2019, URL https://www.iso.org/obp/ui/#iso:std:iso:21384:-3:ed-1:v1:en.
[189] ISO 21384-4:2020(en) unmanned aircraft systems — Part 4: Vocabulary, 2020, International Organization for Standardization (ISO), May, 2020, URL https://www.iso.org/obp/ui/#iso:std:iso:21384:-4:ed-1:v1:en.
[190] ISO 21895:2020(en) categorization and classification of civil unmanned aircraft systems, 2020, International Organization for Standardization (ISO), Feb. 2020, URL https://www.iso.org/obp/ui/#iso:std:iso:21895:ed-1:v1:en.
[191] ISO/TR 23629-1:2020(en) UAS traffic management (UTM) — Part 1: Survey results on UTM, 2020, International Organization for Standardization (ISO), Apr. 2020, URL https://www.iso.org/obp/ui/#iso:std:iso:tr:23629:-1:ed-1:v1:en.
[192] ISO 23665:2021(en)unmanned aircraft systems — Training for personnel involved in UAS operations, 2021, International Organization for Standardization (ISO), Feb. 2021, URL https://www.iso.org/obp/ui/#iso:std:iso:23665:ed-1:v1:en.
[193] D. Serrano, Introduction to JAUS for unmanned systems interoperability - Joint architecture for unmanned systems, North Atlantic Treaty Organization.
[194] M.M. Marques, STANAG 4586 – Standard interfaces of UAV control system (UCS) for NATO UAV interoperability, North Atlantic Treaty Organization.
[195] Proving operations of drones with initial UAS traffic management, EUROCONTROL, URL https://www.eurocontrol.int/project/proving-operations-drones-initial-uas-traffic-management.
[196] Unmanned aircraft systems, EUROCONTROL, URL https://www.eurocontrol.int/unmanned-aircraft-systems.
[197] Unmanned aircraft systems standardization collaborative (UACCS), 2020, American National Standards Institute (ANSI), Jun. 2020, URL https://www.ansi.org/standards-coordination/collaboratives-activities/unmanned-aircraft-systems-collaborative.
[198] T. Girdler, V.G. Vassilakis, Implementing an intrusion detection and prevention system using software-defined networking: Defending against ARP spoofing attacks and blacklisted MAC addresses, Comput. Electr. Eng. 90 (2021) 106990.
[199] C. Birkinshaw, E. Rouka, V.G. Vassilakis, Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks, J. Netw. Comput. Appl. 136 (2019) 71–85.
[200] Lightweight Cryptography, Computer Security Resource Center, URL https://csrc.nist.gov/projects/lightweight-cryptography.

Kai-Yun Tsao received her BBA in Information Management from the National Taiwan University of Science and Technology in 2009. She recently completed a M.Sc. in Cyber Security at the University of York and is currently working in a computer software company. Her interests include emerging cyber defence practices, network and application security.



Thomas Girdler obtained a B.Sc. (Hons) in Computer and Network Engineering from Sheffield Hallam University in 2003. In 2019, he received an M.Sc. in Cyber Security from the University of York, and is employed in that field. His research interests are in network security, software-defined networks and malware detection.

Vassilios G. Vassilakis received his Ph.D. degree in Electrical & Computer Engineering from the University of Patras, Greece in 2011. He is currently an Assistant Professor in Cyber Security at the University of York, UK. He has been involved in government and industry funded R&D projects related to the design and analysis of future mobile networks and Internet technologies. His main research interests are in the areas of network security, Internet of things, next-generation wireless and mobile networks, and software-defined networks.