

# Towards Secure Wireless Mesh Networks for UAV Swarm Connectivity: Current Threats, Research, and Opportunities

Martin Andreoni Lopez, Michael Baddeley, Willian T. Lunardi, Anshul Pandey and Jean-Pierre Giacalone  
Secure Systems Research Center (SSRC), Technology Innovation Institute (TII)  
Abu Dhabi, United Arab Emirates  
{martin, michael, willian, anshul, jean-pierre}@ssrc.tii.ae

**Abstract**—UAVs are increasingly appearing in swarms or formations to leverage cooperative behavior, forming flying ad hoc networks. These UAV-enabled networks can meet several complex mission requirements and are seen as a potential enabler for many of the emerging use-cases in future communication networks. Such networks, however, are characterized by a highly dynamic and mobile environment with no guarantee of a central network infrastructure which can cause both connectivity and security issues. While wireless mesh networks are envisioned as a solution for such scenarios, these networks come with their own challenges and security vulnerabilities. In this paper, we analyze the key security and resilience issues resulting from the application of wireless mesh networks within UAV swarms. Specifically, we highlight the main challenges of applying current mesh technologies within the domain of UAV swarms and expose existing vulnerabilities across the communication stack. Based on this analysis, we present a security-focused architecture for UAV mesh communications. Finally, from the identification of these vulnerabilities, we discuss research opportunities posed by the unique challenges of UAV swarm connectivity.

**Index Terms**—UAVs, Swarm, Mesh Networks, Security

## I. INTRODUCTION

The precise location of objects, real-time mapping of unknown or difficult environments, and task time reduction when compared with single devices make the UAV swarm attractive for commercial and military use. In addition, UAV swarms can help to facilitate the requirements of future networks, providing high availability, greater connection density and low end-to-end delay in the form of Aerial Access Networks [1]. Such scenarios, however, introduce significant challenges in the form of device mobility, ad hoc network formation, and limited device energy, that should be combined with self-organization, robustness through redundancy, and task coordination requirements of UAV Swarms.

Existing wireless mesh technologies have the potential to address these issues, and both the IEEE 802.11 [2] and IEEE 802.15.4 [3] standards have popularized mesh protocols for household and industrial use-cases. Indeed, while IEEE 802.15.4 is a wide-ranging standard typically focusing on low-power, low-rate communications, the IEEE 802.11s and Independent Basic Service Set (IBSS) amendments included as part of the IEEE 802.11-2012 revision enable Wi-Fi-based mesh networks capable of supporting high throughput appli-

cations across the mesh, such as image or video – a common focus of many UAV scenarios.

Nevertheless, despite considerable advances mesh communications still face several of the complex challenges identified within seminal works [4, 5]. Specifically, within the context of this paper, we identify key weaknesses in current state-of-the-art (SOTA) mesh solutions that present critical security challenges within the context of UAV swarms – a relatively new research area in comparison to much of the initial mesh research. For example, while distributed routing protocols can adapt relatively easily to static or slow topology changes in community or industrial mesh networks, the highly mobile environments of UAV swarms, with speeds ranging from 30 to more than 400 km/h [6], present a significant challenge.

We argue that the unique conditions arising from UAV swarm connectivity requires a comprehensive analysis of security and resilience in wireless mesh networks, with key considerations for future research. In this paper, we aim to survey the current SOTA of secure UAV Swarm communications and examine how underlying assumptions in current wireless mesh protocols and standards invite key vulnerabilities and expose significant threats to UAV swarm communications. We also provide a comprehensive overview of these security challenges, from the physical to the application layer, showing how current solutions leave the entire communication system subject to different attack vectors. While we describe specific threat areas that can be mitigated through existing techniques, there is significant exposure within Layers 1 (physical) to 3 (networking) that remains unsolved with current solutions. We identify key research challenges and opportunities and propose a security-focused mesh networking architecture for secure UAV mesh communications that can be used by the research community to address vulnerabilities in UAV swarm communication.

This paper is structured as follows. In Section II we introduce background on wireless mesh communications and recent research on routing protocols for UAV mesh networks. Section III presents the main threats and vulnerabilities on UAV swarm communication, from the physical to the application layer. An architecture that addresses the mentioned issues is presented in Section IV. In Section V we discuss the current and future research, open issues, and challenges. Finally, Section VI concludes our work.

arXiv:2108.13154v1 [cs.NI] 12 Jul 2021

## II. BACKGROUND

Fundamental capacity limitations complicate the application of mesh networks within UAV use-cases. As highlighted in [4], when considering half-duplex radios (such as those commonly found in commercial drones) every forwarding action by an intermediate node reduces the maximum end-to-end wireless throughput by at least  $1/N$ . Furthermore, routing nodes serving as relays for nodes further away in the mesh are forced to share their bandwidth with child branches. Such bottlenecks present difficulties for the network in responding to changing topology or react to threats. Therefore, while protocols have evolved to mitigate these challenges, the distribution of intelligence within the mesh is a complex trade-off between optimization and scalability. Centralizing control allows optimal solutions with global visibility but generate considerable overhead when forwarding control signaling across multiple hops. Distributing control solves this issue and improves responsiveness, but then suffers from reduced visibility of the network state [7].

The authors of [8] present high-level overviews on security issues in wireless mesh networks: identifying how mesh constraints such as processor performance, battery life, mobility, and limited bandwidth present unique security challenges. Many of these constraints occur due to the complexities of routing information across a distributed multi-hop network. However, while many routing protocols have been proposed for wireless mesh networks, most approaches neglect to address security.

Better Approach To Mobile Ad-hoc Networking (BATMAN) [9], and Optimized Link State Routing (OLSR) [10] are two widely used routing protocols that assume security will be implemented in the upper layers [6], while asymmetrical key encryption techniques sign every message, but consume resources that can be expensive in UAV swarm networks [11]. While symmetric key solutions such as CASTOR [12] avoid the high processing of asymmetrical encryption, they require secure key exchange between source and destination, which can be complex to implement in a highly dynamic UAV swarm environment. PASER is a position-aware routing protocol specifically focused on UAV wireless mesh networks [13]. PASER uses hybrid cryptography schemes, asymmetric key for mutual node authentication and key exchange, and symmetric for routing message authentication solving inherent mesh wireless network issues such as blackhole and wormhole attacks. Unfortunately, protocols using Public Key Infrastructure (PKI) assume a Certification Authority (CA) to provide certificates with the public and the private key. While this assumption is feasible within the UAV swarm (since the CA can be accessed through connection to the cloud), it is desirable to avoid a centralized solution to support a fully autonomous swarm and mitigate loss in connectivity to a backbone infrastructure. JarmRout is a jamming-resilient multipath routing protocol, based on three features: i) link quality scheme, analyzing received signal strength indication (RSSI) of received packets; ii) traffic load scheme, the packets stored in the queues; and iii) spatial distance between source and destination [14]. This work only focus on secure routing without providing any

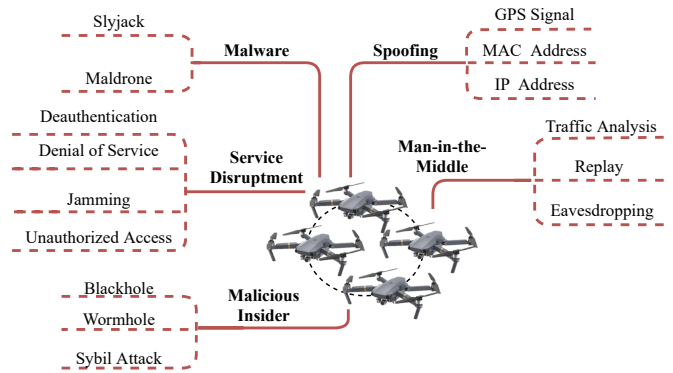


Fig. 1. Classification of threats faced by UAV wireless mesh networks.

solution to other secure aspects.

While the flexibility offered by wireless mesh makes such networks an ideal candidate for intra-drone communication in UAV swarms, these fundamental challenges present vulnerabilities within SOTA mesh networks that introduce many attack vectors that bad actors could exploit.

## III. VULNERABILITIES AND THREATS

Many mesh protocols are designed with no security or assume security issues are handled on the above layers. This assumption, and the absence of a central controller, make the protocol layers vulnerable to several threats. Suppose an attacker's objective is to disrupt the communication between drones in the swarm. Thus, without access to the network, an external attacker can control or disrupt communications within the network. On the other hand, an attack can be internal – once an attacker compromises benign nodes or network credentials through cryptanalysis or physical attack. We systematically identify vulnerabilities faced by UAV mesh communications at each networking layer and show how exploitation of these weaknesses presents a specific threat. We classify these in Figure 1, and provide a high-level summary in Table I.

### A. Physical Layer

**Vulnerabilities.** The broadcast nature of the wireless channel makes transmissions at the physical layer susceptible to various attacks and malicious activities. Broadly, the threats at the physical layer can be classified as either passive or active attacks [15]. Passive attacks are mainly categorized as eavesdropping and traffic analysis, while active attacks mainly include jamming and interference. There may also be a case of hybrid attack where the malicious node may behave according to the wireless channel conditions. All the attacks presented at the physical layer are considered external to the UAV swarm.

**Threats.** In a multi-hop UAV swarm communication, eavesdropping is the simplest form of passive attack to perform. The attacker only needs to overhear the information broadcast over the wireless channel. This may expose confidential network information. Traffic analysis is another type of passive attack at the physical layer. Herein, the attacker is not interested in the data. Instead, the attacker looks to capture network information

TABLE I  
SUMMARY OF THREATS AND VULNERABILITIES FOR UAV MESH SWARM CONNECTIVITY.

| Layer       | Threat/Vulnerability                   | Exploits   | Defense/Opportunity   |
|-------------|--|--|---|
| Physical    | Passive Eavesdropping<br>RF Jamming    | Broadcast Nature of Wireless Channels<br>Wireless contention | Strong Encryption<br>Avoid Interference Zones                       |
| Link        | Spoofing<br>Frame Modification         | Intentional Collision<br>MAC Spoofing                        | Intrusion Detection Systems (IDS)<br>Encryption                     |
| Network     | Routing Forwarding<br>Data Forwarding  | Selfish Attacks<br>Collusion Attacks                         | Intrusion Detection Systems (IDS)<br>Firewall                       |
| Transport   | Packet Corruption<br>Protocol Weakness | Denial of Service (DoS)<br>Session Hijacking                 | Intrusion Detection Systems (IDS)<br>Transport Layer Security (TLS) |
| Application | ROS2 Bugs<br>Open Protocols            | Malware<br>Injection/Modification                            | Authentication<br>Encryption  |

such as the location of key network entities, routing, and other involved behavior patterns to carry out more sophisticated attacks. The challenge is to detect such passive attacks, which are generally mitigated through strong encryption.

Active attacks can exploit the physical layer by intentionally transmitting interfering signals. In particular, Radio Frequency (RF) jamming attempts to occupy legitimate channels and degrade the received signal-to-interference noise ratio (SINR). In the context of UAV mesh networks, such disruption could lead to loss of geospatial positioning, mission references, and even flight control [16]. While many wireless protocols are built to withstand external interference from other devices and networks, those widely used in UAV swarm communication typically operate over the 2.4 GHz ISM band, where deliberate and targeted jamming attacks can quickly disrupt communications. For the purposes of this paper we broadly categorize jammers into three types of attack: *constant*, *reactive*, and *cognitive*, for more in-depth analysis of RF jammers refer to [17].

*Constant* jammers are low-cost, and generate a constant or sweeping tone across a  $W$  MHz channel, allowing the jammer full coverage of a spectrum band within a short period of time. Communication schemes that employ frequency diversity through Frequency Hopping Spread Spectrum (FHSS), however, provide some defense. Within a UAV swarm, this (typically) low-powered attack can also be mitigated through spatial diversity.

*Reactive* jammers sense the spectrum before transmitting a blocking signal in response to a transmission from a nearby device. Thus, the jamming device can conserve energy – as a high-powered radio transmission will typically use more power than passively receiving.

*Cognitive* jammers are typically high-powered, military-grade jamming solutions able to actively monitor the spectrum for active communications and try to disrupt the underlying communications: such as beating the Forward Error Correction (FEC) schemes at the PHY and MAC level. Such sophisticated attacks are extremely difficult to detect as opposed to a constant tone. For instance, the attacker may listen passively when the wireless channel condition is favorable. If the channel is poor, it may disrupt the network communication by introducing the interfering signals [18].

### B. Link Layer

**Vulnerabilities.** The link layer is responsible for multiplexing data streams, error control, and medium access control. The main vulnerability at this layer lies in MAC Address Spoofing, where one station claims the identity of another member of the network. Other frame-level exploits and vulnerabilities include sniffing and broadcast storms.

**Threats.** *Link-layer jamming attacks* are a form of Denial of Service (DoS). The attacker repeatedly transmits the MAC frame header without payload. The benign node subsequently always finds the channel busy and will back-off for some time before sensing again. A more sophisticated version can be used to monitor the network activity of other layers and mimic the typical behavior such as packet size, protocol patterns, etc.

An *Intentional Collision Attack* is a feature of the link-layer protocol implementation. When two nodes attempt to transmit at the same frequency simultaneously, a packet collision occurs. In collision-avoidance MAC protocols (such as in IEEE 802.11), an exponential back-off is applied at both nodes. The attacker can take advantage of this feature and send continuously corrupted MAC packets. Both these attacks are considered external to the UAV swarm.

A *MAC Spoofing Attack* is a common wired and wireless link layer attack. As a MAC address is a unique identifier provided by the manufacturer, it is often used as an authentication factor to grant network privileges to a user. Wireless standards such as IEEE 802.11 do not provide any security against a MAC source address modification in the transmitted frames. MAC spoofing is a way to evade Intrusion Detection Systems (IDS) and Access Control lists, enabling the attacker to masquerade as a legitimate user and gain access to the network.

*Replay Attacks*, also known as Man-in-the-Middle (MitM) can be executed for internal or external nodes. Normally, this attack is executed together with MAC spoofing and eavesdropping. Initially, a node C will eavesdrop on the broadcast communication between two nodes, A and B. Node C will then spoof the MAC address to impersonate node B when communicating with node A.

### C. Network Layer

**Vulnerabilities.** This layer is responsible for IP packet encapsulation and routing of information across the network.

Specifically, in wireless mesh networks, by using multi-hop routing algorithms. Attacks to this layer target the routing mechanism of the UAV swarm communication and affect the packet forwarding [19].

**Threats.** A *Black-hole attack* consists of corrupting route discovery in the routing protocol to place the malicious node on the path of as many routes as possible. Once done, the attacker node may drop all or the majority (gray-hole attack) of data packets and thus significantly degrade routing performances.

A *wormhole attack* consists of two colluding nodes creating a wormhole, or a tunnel, within the network by corrupting the route discovery process to capture sensitive data. Both techniques imply forging false routing packets.

A *Sybil Attack* is named after the subject of the book *Sybil*, a case study of a woman diagnosed with multiple fake identities. These fake identities are known as Sybil nodes. The Sybil nodes can outvote the honest nodes in the system. Usually, multi-path systems are vulnerable to Sybil attacks. Cryptography is a broadly used technique to secure the underlying routing protocols against nodes' misbehavior by ensuring the integrity and authenticity of routing packets. Nevertheless, cryptography consumes significant network resources like processing, delay, and throughput and it can affect energy consumption in UAV networks [20]. All these attacks need to have at least one insider node to perpetrate the attack.

Nevertheless, the *Hello Flood Attack* can be performed for an external node. Nodes are required to send messages to other nodes to show proximity, routes, performance, among other metrics to decide the best path for communication. An attacker can flood the channel with small `hello` messages affecting the performance of an entire network. Machine Learning (ML) based Intrusion Detection Systems (IDS) [21] are employed for network threat detection.

#### D. Transport Layer

**Vulnerabilities.** This layer controls data flow within a communication stack. Vulnerabilities in this layer are related to packet corruption or exploiting weaknesses within protocols. Transport Layer Protocol (TCP) (connection-oriented), User Datagram Protocol (UDP) (connection-less), and Internet Control Message Protocol (ICMP) are the main transport layer protocols.

**Threats.** In TCP every time a packet is sent with the SYN flag enabled, a new connection is opened. This is exploited on the *TCP SYN Flood Attack* where an attacker creates a large number of TCP-SYN packets, creating a half-open connection to a target node spoofing the source address. On the victim side, every open connection exhausts memory, while the victim is not able to accept any other legitimate connection.

In a *UDP Flooding Attack* the attacker node sends a large number of UDP packets without payload to random ports on the victim, with a spoofed source IP address. On the victim side, when a service is not running on the port, a reply with an ICMP Destination Unreachable packet will be sent to the spoofed IP. Thus, the victim system sends many ICMP packets, being unreachable by other clients.

In *ICMP Flooding Attack*, also known as ping flooding, the attacker overwhelms the victim with ICMP echo requests, also known as pings. As this attack is very easy to reproduce using standard tools such as `hping3`, it is one of the reasons why corporations block ICMP packets in their network.

The *Session Hijacking Attack* exploits the vulnerability of the transport protocols that do not check security during ongoing sessions. Thus, an attacker spoofs the IP address of a victim node, correctly determines the current sequence number that is expected to be generated at the victim node, and then performs a DoS attack on the victim node. Network threats are normally detected using IDS. Also, for protection software firewall systems can be used. Moreover, Transport Layer Security (TLS) can be used to encrypt the communication over this layer.

#### E. Application Layer

**Vulnerabilities.** The Robot Operating System (ROS) is a framework widely adopted for robotic middleware, as an example of the application layer in UAV Swarms. Since ROS was mainly designed for research purposes, no security features were added during its implementation. The lack of security features such as data encryption and authentication make ROS a critical surface for different attack vectors in UAV networks [22]. ROS2 is built on the top of Data Distribution Service (DDS) with a Real-Time Publish Subscribe (RTPS) architecture and was designed to provide a solution for the vulnerabilities found in its earlier iteration – adding authentication, encryption, and process profile features, which rely on public key infrastructure. However, some vulnerabilities on the DDS system impacting the ROS2 key exchange were highlighted in White et al. [23].

**Threats.** Message Queuing Telemetry Transport (MQTT) is a lightweight, publish-subscribe protocol that transports messages between devices. Running on top of TCP/IP, it is typically used to send data from the drones to the cloud; its popularity is based on minimal bandwidth requirements and low memory consumption. Nevertheless, it has been shown that by default the MQTT protocol (i) allows anybody to subscribe to the broadcasted topic without any authentication; (ii) MQTT does not provide any data encryption and (iii) The attacker who has already known the data packets by sniffing the traffic can modify the data in transit [24]. Moreover, Mosquitto (a popular MQTT broker) allows a malicious client to supply invalid data as shown in CVE-2017-7653<sup>1</sup>. Additionally, [25] shows how in an open application protocols such as Telnet and FTP, an attacker can connect, execute commands, and transfer data [26]. With these features, a malware can be installed in the victim drone. A malware called *Maldrone* was created and tested in Parrot AR Drone 2.0 and a DJI Phantom. In the demo the author showed that after malware installation, the drone can be forced to land in a specific location. DDS uses a naming convention for its topics including information about software or data type such as `/my/image/raw_image`. Thus, an attacker can apply text recognition or natural language programming to fingerprint the

<sup>1</sup><https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7653>

device, un-patch or exploit versions of software/firmware, or even discover the network topology.

#### IV. SECURITY ARCHITECTURE FOR UAV MESH NETWORKS

The proposed security architecture addressing the issues highlighted in Section III is presented in Figure 2. This architecture is designed to fill all the requirements of a fully distributed UAV mesh network. It is divided into two main layers: the *Network Provisioning Layer* is responsible for managing the network aspects in a IEEE 802.11-based mesh network, while the *Mesh Security Layer* includes features related to the detection and protection of the main threats for UAV swarms.

**Network Provisioning Layer:** *Address Provisioning* is responsible to deliver a unique IP address to every participant node. In a fully distributed network where no central authority exists, address provisioning is a challenge. Filter-based techniques are proposed as a lightweight solution for mobile ad hoc networks in [27]. *Neighbor Discovery* should be a collaborative, latency, and energy-aware solution to determine the participants and the way they are distributed on the network. [28] propose a solution to combine these requirements in a group-based fast neighbor discovery algorithm (GBFA) by carrying neighbor information in a beacon packet.

*Node Blocking* must be a solution to avoid communication with any compromised node. Once the node is detected as compromised, a network countermeasure should be taken.

On the other hand, a total exclusion from the network should be avoided, since it would be interesting to return the drone to the control base for forensic analysis. MAC address blocking is an effective solution using *eatables*, however, it is susceptible to MAC spoofing attacks. Ferraz et al. [29] propose a method to exclude a malicious node both locally within the mesh and globally within the whole network.

The *secure routing* approach is a way to ensure that packets are not modified while passing the network, avoiding routing attacks. The simplest solution is to sign all the routing packets. This approach, however, can consume considerable resources within in a UAV swarm environment. Sbeiti et al. [13] propose a combination of symmetric and PKI infrastructure for packet signing.

The *end-to-end Quality of Service (QoS)*, needs to be applied to ensure that main services in the mission have priority over the network without suffering any delay. Generic Routing Encapsulation (GRE) and Virtual eXtensible Local Area Network (VXLAN) are encapsulation methods in layers 2 and 3 used in traditional networks. Nevertheless, these approaches add an important overhead in the network traffic that can be harmful to UAV swarm networks. Thus, a lightweight solution must be used. *Smart Defense* applies all countermeasures to avoid threats and intrusion to the network.

*Node Re-Inclusion* is a network method applied under situations where a node disappeared, returned, and must then be re-included in the network. Measures should be taken to verify if the node has been compromised. For example, all mesh parameters can be renewed to avoid data exfiltration. It

is necessary to measure the impact of the parameter renewal when the drones are in the mission.

**Mesh Security Layer:** *Certificate Provisioning* must avoid communicating with the Certificate Authority during the mission. Initially, the certificate can be provisioned during the manufacturing process and key pairs are stored in Physical Unclonable Function (PUF), a hardware tamper-resistant approach. If the certificates are provisioned by the manufacturer, it is assumed the delegated trust route, trusting the entire web of trust until the producer root. Durand et al. [30] propose a decentralized web-of-trust using blockchain.

The *Authentication* should use the certificates provisioned in the previous step. Furthermore, the authentication must be on both sides, each node should authenticate with its immediate neighbor mutually. Zhu et al. [31] propose a lightweight algorithm to authenticate all packets in hop-by-hop authentication. Moreover, Jan et al. [32] suggest a mutual payload authentication method in a four-way handshake to avoid overhead in UAV swarm networks. Mutual Authentication is directly related to the neighbor discovery in the network layer since the nodes must know their neighbors to start the authentication process. The Control Access, Node Trusting, and Network exclusion are related to the node blocking scheme. Once a particular node A authenticates a neighboring node B, it will be responsible for the entrance of node B in the network. If a node presents malicious or selfish behavior,

*Control Access* is mandatory for nodes' cooperation and the correct operation of the network. Therefore, a delegation chain of responsibility between node A and node B is created with access control. In the UAV swarm environment, the fog drone will be responsible for the authentication and control access of all nano-drones.

*Node Trust* is a mechanism to measure the misbehaving degree of the nodes to improve the network performance and needs to be collaborative between nodes.

*Network Exclusion* is the final step to remove a malicious node. In this step, a voting mechanism can be used to avoid malicious node collusion in the network. These three previous characteristics are addressed by [29], which proposes an entire framework for control access based on node reputation. Encryption is necessary to protect the network from any kind of information leakage. Since UAV swarms can execute confidential missions, it is necessary to protect the packet payload but also the header information to avoid network and mission recognition. As mentioned before, traditional encryption methods can be energy intensive. Hence, Lightweight Cryptography (LWC) with smaller keys sizes and energy-awareness must be used in UAV swarm environments [33]. This feature is related to secure routing since the packet must be signed to fulfill the non-repudiation requirement.

*Secure Quality of Service* is directly related to the end-to-end QoS in the network layer. The objective of the Secure QoS is to provide end-to-end security to special services. To this end, tunnels can be created from the source to the destination. Dynamic tunnel creation is proposed in [34] with a combination of Virtual Private Network (VPN) and the IPsec protocol for

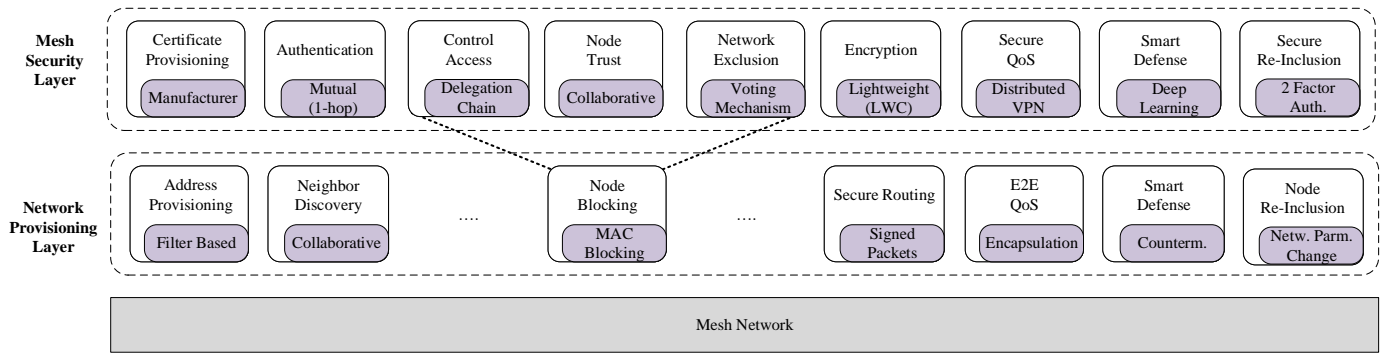


Fig. 2. Secure architecture for future UAV swarm deployment. The architecture is composed of two layers: The Mesh Security Layer includes features for resilience and the Network Provisioning Layer is responsible for the implementation of the security features in the network stack.

smart IoT objects. The dynamic tunnel creation is applicable in the UAV swarm environment, but an energy analysis must be performed.

In *Smart Defense*, all the countermeasures to protect the UAV mesh network after the detection of threats are applied. Stream processing [21] and lightweight Deep Learning approaches are used for network anomaly detection [35] and are combined with smart firewalls to protect the network.

Finally, *Secure Re-Inclusion* is the complement to re-incorporate a node into the network, avoiding spoofing or impersonation attacks. The PUFs can be used as the first factor of authentication and a pre-shared key as the second factor [36].

## V. CHALLENGES AND OPPORTUNITIES

While Section III demonstrates that many attacks and exploits can be mitigated with existing security mechanisms, we identify (i) *high mobility*, (ii) *vulnerability to jamming*, (iii) *susceptibility to compromised nodes*, and (iv) *positional awareness and security* as presenting immediate and critical vulnerabilities within UAV mesh networks as key areas for future research.

**High UAV mobility.** Distributed routing protocols such as OLSR [10] and BATMAN [9] provide a measure of support for mobility through local decision making on neighbors and forwarding. While these solutions are typically employed within IEEE 802.11-based mesh networks and are theoretically able to handle the high throughput application traffic required in UAV mesh networks, such protocols were not designed for the extreme mobility experienced in (relatively recent) UAV use-cases; constantly changing topology and channel conditions can present significant challenges to mesh networks. While routing techniques can certainly be applied to static UAV formations, exploration of recent research into flooding techniques could allow reliable network-wide broadcast of mission and flight information within a swarm.

Within the low-power wireless community Synchronous Flooding (SF) protocols have been used to *intentionally* let multiple relaying nodes forward packets without fear of collision by synchronously and simultaneously broadcasting them on the same carrier frequency [37]. This enables protocols based on SF to reliably flood a mesh with *the minimum possible latency dictated by the physical layer*. Through exploitation of non-destructive interference and the capture effect, this flooding

technique has consistently been shown to outperform routing solutions in terms of reliability and latency in low-power mesh networks [38]. While SF is limited to frequency demodulated physical layers [39] and thus cannot support high-throughput applications such as video, the promise of interference mitigation, low-latency, network-wide synchronization, and agnosticism to mobility, make it a promising candidate for time-critical control communications within a UAV swarm.

**Vulnerability to RF jamming.** The growing hardware power and falling cost of Software Defined Radio (SDR) kits alongside the widespread availability of ML techniques make sophisticated *reactive* and *cognitive* jamming attacks far more accessible. However, there still exist limitations in the capability of many RF jamming approaches. *Reactive* jammers will take a few milliseconds to ramp up their radio in response to a transmission. As such, a small amount of data will be demodulated at the receiving device before the reactive jamming signal kicks in. For example, 1 byte of data transmitted over a 1 Mbps physical layer (PHY) has an on-air time of  $8 \mu\text{s}$ . Non-standard PHY and MAC implementations could therefore avoid such jamming techniques by keeping packets short in time, combined with standard diversity techniques such as frequency, space, time. Furthermore, while the addition of FHSS-based MAC options to standards such as IEEE 802.15.4 [3] have resulted in many protocols that can escape external interference through channel hopping across a spectrum band, this may still be insufficient to defend against deliberate jamming attacks. However, multi-radio approaches could allow swarm communications across multiple bands and therefore mitigate this threat.

**Susceptibility to compromised nodes.** The highly dynamic environments associated with UAV use-cases lend weight to a need for flexible and decentralized security infrastructure. Traditional authentication schemes authenticate devices upon joining a network: deciding whether it is authenticated or not. Therefore, they are vulnerable to security threats such as hijacking, which take control of active sessions. To address this, Continuous Authentication (CoA) has been seen as a solution to maintaining authentication of UAV node identity [40]. However, as CoA is performed frequently and the IoT devices are resource-constrained, it is necessary to adopt a lightweight mechanism to reduce their energy consumption [41]. This

further complicates with the consideration of multi-hop traffic within a wireless mesh network.

Physical layer security (PHY-security) techniques are seen as a possible solution to achieve this. These techniques exploit the inherent random characteristics of the wireless channel (such as multipath fading, interference, propagation delay, etc.) to realize key-less secure transmissions through various coding and signal design and processing techniques [42], and ML-based approaches [43]. These solutions guarantee information security by degrading the channel capacity of the adversary, and does not need any third party intervention. In the context of UAV mesh communications, PHY-security solutions can provide mutual authentication [44], lightweight encryption [45], and anti-eavesdropping strategies [18, 46]. Specifically, physical layer-assisted CoA schemes are designed by exploiting the unique features of a specific transceiver pair (channel state information, received signal strength indicator (RSSI)) and/or analog front-end imperfections. Moreover, the inherent randomness of the wireless channels and the reciprocity principle can be used for physical layer-assisted key generation to provide continuous point-to-point encryption. Furthermore, techniques like beamforming and precoding [47], multi-user and multi-relay diversity [48], relay cooperation [18], and artificial noise generation [46] can degrade the channel quality of the malicious users and thus reduce information leakage. Thus, PHY-security is a potential solution to strengthen the security infrastructure in UAV wireless mesh networks.

**Positional awareness and security.** Global Navigation Satellite System (GNSS) services have traditionally provided positioning and synchronization for UAVs, both of which are critical for mission and flight control. However, such services are designed for outdoor scenarios with direct satellite links, therefore precluding them from indoor environments. Furthermore, with low SNR, they are particularly vulnerable to malicious jamming and/or spoofing [49, 50]. To address these issues, several works have examined Computer Vision-based odometry [51] to augment traditional GNSS. Recently, several works have shown how, by using relatively low-power Ultra Wideband (UWB) devices, one can achieve centimeter accurate localization and outperform BLE as well as Wi-Fi devices. Such accuracy has been demonstrated as sufficient to efficiently navigate quadrotors and robots in indoor settings. However, it has been shown that the single or double-sided two-way ranging (TWR) schemes typically employed in UWB localization do not scale a key challenge in the context of UAV swarms. Inspired by the SF techniques [37] previously mentioned in this section, many researchers are investigating how to exploit UWB-based concurrent transmissions for secure and scalable localization services. Specifically, it has been demonstrated that it is feasible to exploit this technique together with channel impulse response information for ranging, allowing passive self-localization to support countless targets [52].

## VI. CONCLUSION AND FUTURE WORK

UAV swarms employ wireless mesh to provide ad hoc networking infrastructure, both in simple applications such

as geographical mapping or complex events like climate disasters or military missions. However, weaknesses inherent within mesh protocols and standards, have introduced new attack surfaces and presents novel security challenges. In this paper, we have therefore highlighted the main vulnerabilities and threats across in the entire UAV mesh communication stack – from the physical to the application layer. In addition, we have discussed the fundamental challenges and open issues currently faced by UAV swarm communications and provide a road map for future research opportunities within this area. From this analysis, we have proposed a secure mesh communication architecture, consisting of the specified requirements for resilience and network improvement. It is composed of both a network provisioning and mesh security layer, and details solutions for improving security at all layers within UAV swarm communication stack. As a future work, we will implement the proposed architecture and address the open challenges discussed within this paper. Moreover, this work will also extend the proposed architecture to address several categories of UAVs with different resource constraints and use-case scenarios.

## REFERENCES

- [1] N. N. Dao *et al.*, “Survey on aerial radio access networks: Toward a comprehensive 6G access infrastructure,” *IEEE Communications Surveys & Tutorials*, 2021.
- [2] *IEEE Std 802.11-2020 (Rev. of IEEE Std. 802.11-2016)*, IEEE 802.11 Working Group, 2020.
- [3] *IEEE Std 802.15.4-2020 (Rev. of IEEE Std 802.15.4-2015)*, IEEE 802.15.4 Working Group, 2020.
- [4] P. Gupta *et al.*, “The capacity of wireless networks,” *IEEE Trans. on information theory*, vol. 46, no. 2, 2000.
- [5] I. Akyildiz *et al.*, “Wireless mesh networks: a survey,” *Computer Networks*, vol. 47, no. 4, 2005.
- [6] M. Y. Arafat *et al.*, “Routing protocols for unmanned aerial vehicle networks: A survey,” *IEEE Access*, 2019.
- [7] M. Baddeley, “Software Defined Networking for the Industrial Internet of Things,” Ph.D. dissertation, 2020.
- [8] M. S. Siddiqui and C. S. Hong, “Security issues in wireless mesh networks,” in *MUE Conf. IEEE*, 2007.
- [9] A. Neumann *et al.*, “Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.),” 2008.
- [10] T. Clausen *et al.*, “Optimized Link State Routing Protocol (OLSR),” 2003.
- [11] O. K. Sahingoz, “Multi-level dynamic key management for scalable wireless sensor networks with uav,” in *Ubiquitous Information Technologies and Applications*. Springer, 2013, pp. 11–19.
- [12] W. Galuba *et al.*, “Castor: Scalable secure routing for ad hoc networks,” in *INFOCOM Conf. IEEE*, 2010.
- [13] M. Sbeiti *et al.*, “Paser: secure and efficient routing approach for airborne mesh networks,” *IEEE Trans. on Wireless Comms.*, vol. 15, no. 3, 2015.
- [14] C. Pu, “Jamming-resilient multipath routing protocol for flying ad hoc networks,” *IEEE Access*, vol. 6, 2018.

- [15] X. Sun *et al.*, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, 2019.
- [16] Q. Wu *et al.*, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wireless Communications*, vol. 26, no. 5, 2019.
- [17] N. Sufyan *et al.*, "Detection of Jamming Attacks in 802.11b Wireless Networks," *EURASIP Journal on Wireless Communications and Networking*, 2013.
- [18] L. Yang *et al.*, "Optimal relay selection for secure cooperative communications with an adaptive eavesdropper," *IEEE Trans. on Wireless Comms.*, vol. 16, no. 1, 2017.
- [19] J.-A. Maxa *et al.*, "Survey on UANET routing protocols and network security challenges." *Adhoc & Sensor Wireless Networks*, vol. 37, 2017.
- [20] I. Sultan *et al.*, "Analysis and optimization of advanced encryption standard for the internet of things," in *Signal Processing and Integrated Networks*. IEEE, 2020.
- [21] M. Andreoni Lopez *et al.*, "Toward a monitoring and threat detection system based on stream processing as a virtual network function for big data," *Concurrency and Computation: Prac. and Exp.*, vol. 31, no. 20, 2019.
- [22] J. McClean *et al.*, "A preliminary cyber-physical security assessment of the robot operating system (ROS)," in *Unmanned Systems Technology XV*, vol. 8741. Intl. Society for Optics and Photonics, 2013.
- [23] R. White *et al.*, "Network reconnaissance and vulnerability excavation of secure DDS systems," in *IEEE European Symposium on Security and Privacy Workshops*, 2019.
- [24] J. J. Anthraper *et al.*, "Security, privacy and forensic concern of MQTT protocol," in *SUSCOM Conf.*, 2019.
- [25] R. Sasi, "Maldrone the first backdoor for drones," 2015.
- [26] O. Westerlund *et al.*, "Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the IoT," in *1<sup>st</sup> Intl. Conf. on UVS*. IEEE, 2019.
- [27] N. C. Fernandes *et al.*, "An efficient filter-based addressing protocol for autoconfiguration of mobile ad hoc networks," in *IEEE INFOCOM Conf.*, 2009.
- [28] L. Wei *et al.*, "A fast neighbor discovery algorithm in WSNs," *Sensors*, vol. 18, no. 10, 2018.
- [29] L. H. G. Ferraz *et al.*, "An accurate and precise malicious node exclusion mechanism for ad hoc networks," *Ad hoc networks*, vol. 19, 2014.
- [30] A. Durand *et al.*, "Decentralized web of trust and authentication for the internet of things," in *7<sup>th</sup> Intl. Conf. on the Internet of Things*, 2017.
- [31] S. Zhu *et al.*, "LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks," in *23<sup>rd</sup> Intl. Conf. on Distributed Computing Systems*. IEEE, 2003.
- [32] M. A. Jan *et al.*, "A payload-based mutual authentication scheme for internet of things," *Future Generation Computer Systems*, vol. 92, 2019.
- [33] N. A. Gunathilake *et al.*, "Next generation lightweight cryptography for smart IoT devices: implementation, challenges and applications," in *IEEE 5th WF-IoT*, 2019.
- [34] M. Juma *et al.*, "Hybrid end-to-end VPN security approach for smart IoT objects," *Journal of Network and Computer Applications*, vol. 158, 2020.
- [35] R.-H. Hwang *et al.*, "An unsupervised deep learning model for early network traffic anomaly detection," *IEEE Access*, vol. 8, 2020.
- [36] P. Gope *et al.*, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, 2018.
- [37] M. Zimmerling *et al.*, "Synchronous Transmissions in Low-Power Wireless: A Survey of Communication Protocols and Network Services," *arXiv preprint 2001.08557*, 2020.
- [38] M. Schuß *et al.*, "A Competition to Push the Dependability of Low-Power Wireless Protocols to the Edge," in *Proc. of the 14th EWSN Conf.*, 2017.
- [39] M. Baddeley *et al.*, "The Impact of the Physical Layer on the Performance of Concurrent Transmissions," in *IEEE ICNP Conf.*, 2020.
- [40] A. Shoufan, "Continuous authentication of UAV flight command data using biometrics," in *IFIP/IEEE VLSI-SoC Conf.* IEEE, 2017.
- [41] M. Yahuza *et al.*, "An edge assisted secure lightweight authentication technique for safe communication on the internet of drones network," *IEEE Access*, vol. 9, 2021.
- [42] R. Chen *et al.*, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Wireless Communications*, vol. 26, no. 5, 2019.
- [43] J. Yu *et al.*, "Radio frequency fingerprint identification based on denoising autoencoders," in *WiMob Conf.* IEEE, 2019.
- [44] X. Wang *et al.*, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Communications Magazine*, vol. 54, no. 6, 2016.
- [45] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, 2015.
- [46] A. Sanenga *et al.*, "An overview of key technologies in physical layer security," *Entropy*, vol. 22, no. 11, 2020.
- [47] W. Zhang *et al.*, "Transmit beamforming for layered physical layer security," *IEEE Trans. on Vehicular Technology*, vol. 68, no. 10, 2019.
- [48] L. Fan *et al.*, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Trans. on Wireless Comms.*, vol. 15, no. 6, 2016.
- [49] G. X. Gao *et al.*, "Protecting gnss receivers from jamming and interference," *Proc. of the IEEE*, vol. 104, no. 6, 2016.
- [50] M. L. Psiaki *et al.*, "Gnss spoofing and detection," *Proc. of the IEEE*, vol. 104, no. 6, 2016.
- [51] F. Caballero *et al.*, "Vision-based odometry and slam for medium and high altitude flying uavs," *Journal of Intelligent and Robotic Systems*, vol. 54, no. 1, 2009.
- [52] B. Großwindhager *et al.*, "Snaploc: An ultra-fast uwb-based indoor localization system for an unlimited number of tags," in *18<sup>th</sup> (IPSN) Conf.*, 2019.