A Survey on UAV Network for Secure Communication and Attack Detection: A focus on Q-learning, Blockchain, IRS and mmWave Technologies

Madhuvanthi T[1*], and Revathi A[2]
[1,2] Department of Computational Intelligence, SRM Institute of Science and Technology, School of Computing Kattankulathur, Chengalpattu, India
[e-mail: mt9279@srmist.edu.in, revathia1@srmist.edu.in]
[*]Corresponding author: Madhuvanthi T

Received November 2, 2023; revised January 11, 2024; accepted March 2, 2024; published March 31, 2024

Abstract

Unmanned Aerial Vehicle (UAV) networks, also known as drone networks, have gained significant attention for their potential in various applications, including communication. UAV networks for communication involve using a fleet of drones to establish wireless connectivity and provide communication services in areas where traditional infrastructure is lacking or disrupted. UAV communication networks need to be highly secured to ensure the technology's security and the users' safety. The proposed survey provides a comprehensive overview of the current state-of-the-art UAV network security solutions. In this paper, we analyze the existing literature on UAV security and identify the various types of attacks and the underlying vulnerabilities they exploit. Detailed mitigation techniques and countermeasures for the protection of UAVs are described in this paper. The survey focuses on the implementation of novel technologies like Q-learning, blockchain, IRS, and mmWave. This paper discusses network simulation tools that range in complexity, features, and programming capabilities. Finally, future research directions and challenges are highlighted.

Keywords: Attack detection techniques, Intelligent Reflecting Surface, Q-learning, mmWave communications, Swarm communication, UAV networks.

1. Introduction

UAV, or Unmanned Aerial Vehicle, refers to any aircraft operated without a human pilot. UAVs can be controlled remotely by a human operator or programmed to fly autonomously. UAVs are used in various applications, including military reconnaissance and surveillance, mapping and scrutinizing, search and rescue operations, wildlife conservation, and commercial photography and videography. Advancements in technology have made UAVs smaller, lighter, and more affordable, leading to an increase in their popularity and usage. However, there are concerns about privacy and safety, and the potential for UAVs to be used for malicious purposes. Overall, UAVs have the potential to revolutionize various industries and provide benefits in terms of efficiency, safety, and cost-effectiveness. It is significant to study their use's ethical and legal implications carefully.

UAVs can be used for communication purposes in several ways, particularly in areas with limited or non-existent traditional communication infrastructure. UAVs should be provided with cellular base stations to make temporary or backup cellular coverage in areas affected by natural disasters or when the infrastructure for cellular communication does not exist. The UAV can be programmed to fly to the affected area and provide cellular coverage for a set period. Also, UAVs can be supported with Wi-Fi hot spots into wireless internet access in areas where traditional internet infrastructure is unavailable. It can be particularly useful in rural areas or developing countries with limited internet connectivity. UAVs are used as relay nodes for communication networks, extending the range of existing communication infrastructure. For example, a UAV is a relay node to connect a remote village to a regional communication network. In emergencies, such as natural disasters or search and rescue operations, UAVs provide communication links between first responders and victims or between different first responder teams.

UAV communication networks facilitate communication among multiple UAVs and GCS, enabling data exchange and commands. The choice of UAV communication network will depend on the specific requirements of the mission, such as the range of communication needed, the number of UAVs involved, and the sort of data being transmitted.

- Ad-hoc networks: Decentralized networks that would be created on-demand without needing a pre-existing infrastructure. It is commonly used in UAV networks where the network topology can change rapidly, and a fixed infrastructure may not be available.
- Mesh networks: Mesh networks are networks where each node transmits data through the relay. It enables the network to extend its range and overcome obstacles that otherwise block the signal. Mesh networks are commonly used in UAV networks where the UAVs need to communicate with the GCS over long distances.
- Cellular networks: Cellular networks provide long-range communication among UAVs and GCS. Cellular networks are commonly used when UAVs fly beyond the operator's line of sight or in remote areas where other methods are unavailable.
- Satellite networks: They provide global communication coverage for UAVs. Satellite networks are commonly used in military and scientific applications where UAVs must operate in remote areas where other communication methods have not existed.
- Wi-Fi networks: It is used to enable communication between UAVs and GCSs over short distances. Wi-Fi networks are commonly used in consumer-grade UAVs for real-time video transmission and basic commands.

UAV communication network protocols enable communication with multiple UAVs and GCSs and manage data exchange and commands. Depending on what the mission requires, such as the range of communication needed, the number of UAVs involved, and the kind of

data being transmitted. Regarding securing communication for UAVs, several considerations are accounted for verifying the confidentiality, integrity, and availability of the data transmission categorized as shown in **Fig. 1**. When there is communication between UAVs and their control stations, it is essential to implement proper security measures.

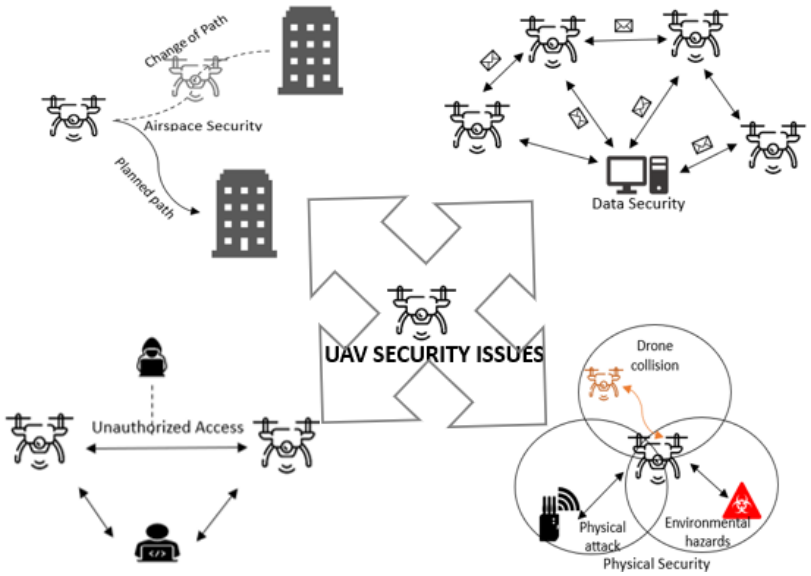

Fig. 1. Major security issues in UAV

The significant factors are the low cost of deployment of UAVs contributing to their success [1]. As prices and equipment downsizing change from exclusive military equipment to popularization in civil and commercial domains, the UAV market is increasingly opening, creating new beneficial chances for the future wireless communication industry [2]. The number has increased rapidly because of its extensive usefulness, UAV advancement, and research within the last decade. Recently, UAV networks have received much consideration for complicated and risky operations, including search and rescue, traffic monitoring, coastline surveillance, and land surveying [3]. The SENTINEL framework for UAV secure communication was developed in this [4] specially designed to reduce the computational and communication overheads associated with exchanges in certificate and computation of asymmetric cryptography, which are often necessary for authentication protocols. ProVerif, an automated cryptographic protocol verifier, was used to establish the privacy of SENTINEL.

[5] proposed a light mutual authentication approach on UAV-to-GCS authentication utilizing Physical Unclonable Functions (PUFs, “This protocol has a wide range of security features, for instance, user anonymity and mutual authentication, along with its resistance to network threats such as replay, masquerade, node manipulation, and clone attacks. Several authentication mechanisms exist throughout many unmanned aerial vehicles (UAV) systems [6], all vulnerable to handover delays and security complications for an attack. To address these challenges, the research concentrated on developing a unique optimized DL algorithm named FFUDAS to eliminate harmful assaults. The proposed FFUDAS model outperformed the others, achieving a throughput of 0.96 Mbps, a handover delay of 0.423 ms., and an execution time of 0.073 ms. Using the proposed MADDPG technique [7], it is possible to safeguard the transmitter of UAVs from wiretaps for HAPs by centralized training and distributed execution on all UAVs. This allows the collaboration of all UAVs to be entirely distributed.

This paper's main objective is a comprehensive survey of UAV secure communication strategies. There is a need for a survey that examines UAV communication from conferences, journals, and magazines. The suggested survey offers a thorough review of the most cutting-edge UAV network security solutions available right now. The survey also focuses on the application of cutting-edge technologies including Q-learning, blockchain, IRS, and mmWave. The survey also compares current performance measures and approaches.

2. Research Gap

Despite the multiple safe UAV communication techniques, there are still a lot of challenges to be solved before effective results can be obtained. Under traditional approaches, a number of current techniques for UAV secure communication are provided. In [8] HetNets, overhead communication was high, and scalability was poor. These modifications reduce the quantity of data delivered and the system's latency. For UAV communication to be secure and effective, new communication protocols must be created to address these issues. The TDMA protocol was used for communication between the UAV and ground users [9]. This approach was not used with non-orthogonal multiple access protocols. Furthermore, a powerful algorithm for cancelling interference among several users effectively reduced interference. To address these issues, new communication protocols that use non-orthogonal multiple access protocols must be created and implemented and incorporate a successful interference cancellation algorithm. Through RIS-supported UAVs, secure communication protects privacy. It was crucial to boost the signal strength because the RIS [10] was moving. Additionally, base station and single and multiple-user scenario optimization were completed. However, the optimization procedure was more difficult because of several base stations and users.

3. UAV Attacks and Detection Techniques

UAVs bring a number of efficiency and convenience advantages, but they also raise a number of security issues. UAVs are susceptible to unauthorized access and control by cybercriminals who can commandeer the drone's flight route or get access to private information the UAV's sensors have acquired. UAVs are capable of gathering and transmitting copious amounts of data, including pictures, videos, and other sensor data. The private or sensitive information included in this data may be jeopardized by the possibility of interception, theft, or hacking. UAVs are governed by air operations regulations; however, some operators may flout them, endangering other aircraft and ground personnel. UAVs can be used maliciously to carry out assaults, smuggle goods, or secretly monitor people or groups without their knowledge or agreement. When used to transport bombs or other potentially hazardous payloads, or when they collide with buildings or other structures, they can pose a security concern in and of themselves. These networks transmit sensitive data that is vulnerable to a variety of dangers. An open wireless channel, such as the internet, is used by a UAV's ground station to control it, and it is also rife with security threats. Communication channels used by UAVs may be subject to various cybersecurity concerns. In **Table 1**, an overview of existing detection methods and their attack types were highlighted.

Table 1. Attacks and existing detection techniques

Attack Type	Detection Method	Drone / Simulator
Spoofing attack [11]	Game-based spoofing detection with multi-agent reinforcement learning MADDPG-based Spoofing Detection	-
GPS Spoofing [12, 13]	Pyramidal LK algorithm	DJI Phantom 4 drone
Jamming attack [14]	Simultaneous Localization of Multiple Jammers and Receivers algorithm	-
Black hole attack [15]	Detection and presentation of a black hole attack AODV routing protocol	VANET
Jamming attack [16]	Kalman Filter	-
Malicious adversary attacks [17]	Zonotope based attack detection	-
Jamming Attack [18]	CNN-LSTM Seasonal and Trend decomposition using Loess	-
False data injection attack ADS-B attack Bad & Good mouthing GPS spoofing attack Gray hole attack Black hole attack [19]	BRUIDS UAV detection agent - UAV node level	NS3 simulator
Sybil attack Blackhole attack Flooding attack [20]	SID-UAV HIS algorithm	NS-3 emulator
Black hole attack Gray hole attack [21]	Optimized Enhanced ad hoc On-demand Distance Vector (OEAODV) protocol	VANET
Jamming attack [22]	MCR decoding method	Matlab
Jamming attack [23]	Kullback-Leibler-Divergence	-
Worm hole attack [24]	k-NN SVM	VANET - NS2 SUMO simulator
Jamming attack [25]	Jamming detection mechanism	-
GPS Spoofing [26]	Artificial Neural Network	GPS SMA
Jamming attack [27]	ACS properties based blind algorithm Post sorting algorithm	
False data injection DOS attack Random attacks [28]	Modified sliding innovation sequences	Quadrotor - 6DOF dynamics model
Emerging threats [29]	Random Forest Classifier SVM KNN	COOJA Simulator
GPS sensor attack Ramp attack [30]	Kalman filter algorithm Chi-square test	Unmanned Autogyro
Single and multi-transmitter GPS spoofing attack [30]	Kullback–Leibler divergence	Pixhawk
Botnet attack DDoS attack Brute force attack HTTP DOS	Logistic Regression Linear Discriminant Analysis K-nearest Neighbor Decision Tree	Python coded environment

Network infiltration attack [31]	Gaussian Naive Bayes Stochastic Gradient Descent K-means	
GPS Spoofing attack [32]	Linear regression anti-spoofing model	Quadrotor jMAVSim

3.1 Eavesdropping

An eavesdropping attack [33], which occurs when personal information is collected illegally, is an attack on privacy and confidentiality. This involves a malevolent UAV listening in on the confidential communications with other UAVs also doing not anything about it. [34] As a form of passive MiM attack, it mainly snoops the vulnerable communication links on the data. There are two basic types of wireless surveillance, passive and proactive eavesdropping, depending on legitimate monitor's strategy. Legitimate monitors can passively eavesdrop on suspect links by simply listening to them [35] and deploy far away from suspecting transmitters. In proactive eavesdropping, [36] despite an imperfect eavesdropping channel related to the suspicious link, the legitimate monitor is yet able to successfully decode all suspicious messages.

3.2 DoS Attack

An attack on a website involving a denial-of-service attempts to stop legitimate users from using it. By flooding UAVs with data, such as replicas and fake authentication messages, attackers overload them with data [37]. A logic attack and a resource attack are the two main types of attacks. A logic attack is an attack that exploits existing software defects to instigate a server to collide or to significantly decrease in performance. Attacking a victim's resources by sending many spurious requests, causing their memory, CPU, or network to overflow.

3.3 Blackhole Attack

Upon receiving data packets from a malicious node, it does not forward them to any other node. A malicious node releases the data packets. Hence it is named as Black-hole attack [38]. Attacks on black holes fall into two categories [39]: those perpetrated by an external adversary against some nodes and those perpetrated by an internal adversary against everyone else. In a single black hole attack, the malevolent nodes can drop the packets they receive or selectively advances them, thus causing disruption in the network. A cooperative black hole attack, numerous malicious nodes work together to form a black hole and start dropping all the packets they receive, which can lead to a complete network disruption.

3.4 Man-in-the-middle Attack

This involves intercepting then modifying the UAV's communication signal in real-time [40], allowing the attacker to manage the UAV's aircraft path or steal sensitive information. The attacker positions themselves between the UAV and its GCS, usually by setting up a rogue wireless access point or using a radio jammer to force the UAV to connect to their own network. Attacker intercepts the communication signal in the UAV and GCS, then begins to manipulate the data being transmitted. The attacker can then send commands to the UAV that appear to be coming from the GCS, or modify the data being sent from UAV to GCS, in order to deceive the GCS into believing that everything is normal. With control of the UAV, the attacker can then manipulate its flight path, causing it to crash or fly off course.

3.5 Spoofing

The purpose of RF spoofing attacks is to deceive networks or users, gain access to services or information, disrupt communications through the use of signals or channels. GPS spoofing is defined as by sending out false signals, the attacker can deceive the GPS receiver and cause it to display inaccurate information. The attacker may also be able to interfere with navigation systems and cause them to provide incorrect routes or incorrect decisions. In these experiments, UAVs, especially civilian UAVs, are seriously affected when facing GPS spoofing attacks. The act of impersonating and masquerading as a suitable user in the UAV network is referred to as Identity Spoofing.

3.6 Jamming

Among the dangerous threats against UAVs today is the jamming attack, which disrupts the communication among UAVs and more legitimate entities. Using multiple radio frequencies, jamming attacks disrupt the UAV network and behave like Internet Denial of Service (DOS) attacks [41]. These frequencies overwhelm the UAV's receivers and interfere with proper communication, potentially leading to system failure and data loss [42]. Through the use of noise radio signals, they seek to degrade UAV communication performance by broadcasting ongoing communication. There are four categories of jamming attack: constant, deceptive, random, and reactive. An attack which continuously transmits a high-power noise signal is called a constant jamming attack. Despite not following any protocol, it uses the receiver's power to transmit data. As a result of a deceptive jamming attack, authentic packets are sent constantly to confuse additional aircraft. In the random jamming attack, resource is kept active and idle at the same time so that the power can be properly preserved.

3.7 Greyhole - Wormhole - Sinkhole Attack

Partial packet dropping is the term used to describe a technique that drops only the specific data packets destined for the targeted recipients during transmission. This is an active attack type that results in messages being dropped. In an attack, the attacker agrees to send packets but fails to send them. It is also known as grave attack, at one part in the network, packets are intercepted by the attacker, tunneled to another point, and re-repeated across it. [43] VANETs and other wireless networks are often attacked by this type of attack. Sinkhole attacks cause a sinkhole [44] in the center of the network by luring all the traffic from the neighboring area towards the compromised node. All the data of its neighbors is stolen by the attacker or compromised node. In an attempt to appear as the most attractive relay in the neighborhood, the attacker presents itself as the most reliable one.

3.8 Sybil Attack

An attacker pretends to be another UAV in order to gain the network resources [45] unjustly and also to undermine network security. They also make false claims that they are to blame for the identity theft of other UAVs.

3.9 False data injection and dissemination attack

The intruder modifies the UAV network's routing algorithm [46] by adding false bandwidth data. The primary goal of introducing false bandwidth is to obstruct data transmission routing. There are two kinds of false bandwidth injection: low bandwidth injection attacks and high bandwidth injection attacks. An attacker can broadcast false information to neighbors through a UAV that broadcasts environmental conditions [19].

Addressing these security concerns will require a combination of technical solutions, such as encryption and secure communication protocols, as well as policy and regulatory measures to ensure responsible use of UAVs. It will also require collaboration between stakeholders in the UAV industry, including manufacturers, operators, and government agencies responsible for regulating UAV use.

4. Secure Communication for UAVs Utilizing Various Techniques

4.1 Q-Learning Based UAV Secure Communication

Q-learning is a reinforcement learning technique that has been successfully applied to a variety of issues, including decision-making in autonomous systems. As opposed to this, Q-learning may be used to optimize the behavior of the UAV in safe UAV communication to ensure trustworthy communication. In **Table 2**, comparison, we provided an overview of existing Q-learning based secure UAV communication systems and information on the sorts of attacks that may be employed in conjunction with Q-learning based secure communication systems. In **Table 2**, under the validation section: S denotes simulation, M denotes mathematical and P denotes Python coded environment. To use Q-learning to UAV safe communication, first define a state space, then an action space, and lastly a reward function. The state space may contain elements like the UAV's present location, the caliber of the communication channel, and the existence of any possible threats. A UAV's actions, such as increasing its altitude or altering its course, can be included in an action space. The goal of the incentive function should be to encourage the UAV to adopt activities that enhance communication while avoiding those that would jeopardize security. The Q-learning technique may be used to train the UAV once they have been defined.

Table 2. Secure communication with q-learning based on different attacks

Techniques	Type of Attacks	Validation			Advantages	Disadvantages
		S	M	P		
Stackelberg game; HQLA [47]	Multiple adaptive Eavesdroppers	✓	✓	✗	Transmit power is optimized for transmission of legitimate users	Eavesdropping cost is high; Not utilized in real time environment
DQN; DDQN [48]	Malicious eavesdropper	✗	✗	✓	Convergence speed is faster	Only when number of episodes increases secrecy rate increases, hence at the beginning of the trajectory eavesdropping is however possible
Q learning; Rician fading model [49]	Passive Eavesdroppers	✓	✓	✗	Less computation time; Less probability of hybrid outage	Interception is high
Q Learning algorithm for Stackelberg equilibrium strategy [50]	Multiple UAV active eavesdroppers	✗	✓	✓	Probability of attacking mode is shown	Uncertainties; change of environments is difficult

Noncooperative game theory; NE strategy [51]	Eavesdroppers Jamming Spoofing Keeping Silent	✓	✓	✗	Attack rate decreases; Satisfies the convergence	Accuracy of channel estimation is degraded; Rationality is not satisfied;
GEVD-based beamforming method [52]	-	✗	✗	✓	Physical layer security is achieved	Only partial CSI is considered; Beam is not pointing accurately towards the large-scale array of antenna
Spiral placement algorithm; Nash Q-learning [53]	Eavesdropper	✗	✗	✓	System utility is higher; better offloading	Less coverage; High energy consumption
Multi-agent deep reinforcement learning; JDTNP algorithm; DDPG algorithm [54]	Smart UAV eavesdropper	✗	✗	✓	Actual problem is considered as TZSG problem and it is solved by DRL, which achieves better performance	Non-stationarity is increased by each agent perceptive

As the UAV explores the state space during training, the present Q-values are put to use. Feedback from the environment is received when the UAV interacts with it, and the Q-values are changed to reflect its experience. The UAV can utilize the learnt policy to make choices in real time after the Q-values have converged to their ideal levels. By following this strategy, you can make sure that the UAV takes measures that maximize communication quality while reducing the possibility of security issues. Generally speaking, Q-learning offers a solid foundation for optimizing UAV behavior in secure communication. Utilizing machine learning techniques, we can make sure that UAVs can adapt to changing situations and real-time-optimize their behavior to ensure dependable and secure communication.

4.2 Blockchain based UAV Secure Communication

Blockchain has the prospective to revolutionize how UAVs communicate securely. Using a blockchain-based communication system, UAVs can securely exchange data with GCS and UAV-to-UAV without the risk of unauthorized access, tampering, or hacking. The use of blockchain-based technology for secure communication is compared in **Table 3**, along with its existing objective, platform/validation for experimenting, and the type of attack provided, they verify whether this technique satisfies specific communication criteria. Moreover, in [55] secure authentication framework with key agreement architecture for 5G-enabled UAVs is presented using Permissioned Blockchain technology. At first, authentication was carried out between Edge to Cloud server, UAV to Edge server, and UAV to UAV mutually, and then the key agreement was supported. Here data is protected from attacks by a permissioned blockchain framework.

Table 3. Comparison of secure communication methods based on blockchain

Approach	Objective	Platform	Attack Type	Advantages	Disadvantages
Elliptic Curve Diffie-Hellman [56] One time pad	Authorizing the transactions with higher security level	Private	-	Allows transactions without encrypting the messages;	Generally, focuses on CIA properties but doesn't include scalability, storage, performance of the network
Consensus algorithm Hash generation algorithm [57]	To give a solution for the harmful cyber-attacks To prevent data loss	MATLAB Python	Malicious cyber-attacks	Automatically interacts Bloom filter	Data congestion
Permissioned Blockchain POA consensus algorithm [55]	To provide a security for services like session-key security, mutual authentication, and credential privacy using key agreement framework	Ethereum Rinkby blockchain platform	Poisoning attack Impersonation attack Insider attack MITM and replay attack	It makes the data temperproof, also trustable. Data can be rescued from poisoned attack by blockchain-enabled distributed cloud	Uses DY model which not only alter, delete, intercept the data however it can also add any harmful data In CK-adversary model may hijack the live session by stealing credentials and session state
Admission control algorithm [58] Hashing algorithms	To provide a security by means of computational needs	MATLAB 2019b	-	Transactions are not stored since end-users are isolated	Extreme rise on delay even though it is in acceptable range
PoA consensus algorithm [59]	To obtain a security for transmission on data in wireless communications To identify and block all the fake buoys and UAVs	Ethereum Blockchain Ganache tool MATLAB tool with Python IDE	Hijacking GPS Spoofing Malicious Buoys DDoS Attack	impersonating attacks are avoided by the authentication mechanism; Fake buoys are blocked from further communication	-
Consortium blockchain mechanism [60]	To enhance sensing data's integrity To recognize malicious sensors	MATLAB tool with Python IDE	Forged identity Spoofing False data injection	Mining complexity is reduced for UAV swarm communication	Data sensing is difficult; cost of dataset collection is high;
Smart contract program Consensus algorithm [61]	To secure the communication process and the decrease of	Ethereum network MATLA	Spoofing attack MitM attack	Authenticates on each level; Storage capacity is	Communication overhead

	communication's consumption costs	B Remix IDE	DOS attack	fully feasible	

4.3 Intelligent Reflecting Surface Based UAV Secure Communication

IRS is a potential technique for improving wireless communication networks by reflecting signals in a regulated and adaptable manner. IRS improves the communication security when used with UAVs. One possible use is to place the IRS on the ground to reflect signals from a UAV in a certain direction, limiting signal leakage and enhancing communication security. Additionally, an IRS may selectively boost or weaken the signal strength in particular directions by adjusting the reflectivity of the surface, adding an extra layer of protection against jamming or eavesdropping assaults. A UAV can also be equipped with IRS to increase its communication range and signal dependability. The UAV can safely connect with the base station even in places where signals are weak or obstructed thanks to the IRS on the UAV, which can reflect signals from the base station to the UAV and vice versa. An analysis of existing UAV communication systems with Intelligent Reflecting Surfaces (IRS) has been conducted to compare their performance in the **Table 4**. Overall, the use of IRS and UAVs has great potential to increase security. To control IRS effectively, accurate models must be developed for predicting signal propagation in dynamic environments. Models can be used to anticipate and mitigate potential IRS security threats. Reflected signals must be secured and unauthorized access must be prevented. For IRS deployment and operation to be widely adopted, clear standards and regulations must be established. The practical use of this technology and the technical difficulties in combining IRS with UAVs, however, both call for more study.

Table 4. Comparison of secure communication methods based on IRS

Security Issue	Model	Design Analysis	IRS Located	Advantages	Disadvantages
Blockage in mmWave networks Eaves droppers	Beamforming model Semidefinite relaxation [62]	UAV-BS and IRS Positions UAV-BS Beamforming and IRS Passive Beamforming	On outer UAVs	Improved performance gains	Optimization of position is challenging; Network secrecy is less
-	Iterative algorithm [63]	IRS-assisted UAV position	Between BS and users.	Finding location is simple	More attenuation; Degradation in system performance
Passive eaves-dropper	Iterative algorithm - SCA [64]	IRS from the physical layer security Phase Shifter With trajectory	Mounted on the building wall	-	Requires more power as number of elements increases
Severe blockage	Genetic algorithm based AO algorithm [65]	Multiaccess edge computing Joint optimization with active beamforming IRS passive beamforming	UAV - UIRS hovering	Task latency is reduced; Runs on hardware with limited memory	Computational offloading issue arises for multiuser

-	DF based RIS assisted [66]	RIS-Assisted G2A Link A2G Link Outage probability	On a building	Capacity and coverage improved for communication	Less reliable
Decoding error rate	Gradient-descent optimization [67] Nelder-Mead simplex	Passive beamforming Coherence and Maximal Channel Gain	On a building	Highly reliable; Better convergence; less computation time	Mobility of UAV
Eaves dropper	Low-complexity alternating algorithm [68]	Convex approximation technique Fractional programming	On outer wall	Maximum secrecy is achieved even in high UAV mobility	Power transmission is high; Number of elements are high
Passive eaves dropper	SCA [69]	User Scheduling optimization Trajectory optimization Power optimization	Between UAVs	Better power control, user scheduling, security on physical layer	-
Air-ground interference	[70]	Cellular Downlink and Uplink Communication IRS passive beamforming	Outer UAVs	Less transmission power due to usage of hybrid IC	Number of elements are high

4.4 mmWave UAV secure communication

mmWave (millimeter wave) communication is a wireless communication technology that operates at high frequencies, typically between 30 GHz and 300 GHz [71]. mmWave UAV communication is a promising technology enabling high-speed, low-latency, and high-capacity data transmission between UAVs and other devices. mmWave frequencies have high bandwidth, allowing for quickly transmitting large amounts of data. This makes it ideal for UAVs that require real-time data communication for navigation, control, and data transmission. However, mmWave communication has a shorter range compared to other wireless communication technologies, and it is more susceptible to obstacles such as buildings, trees, and other structures. This means that mmWave UAV communication requires a clear line of sight between the transmitting and receiving antennas, which can be challenging in urban environments.

To ensure secure communication in mmWave communication, several measures can be taken. One such action is beamforming, which allows for directional transmission and reception of signals. By focusing energy in a specific direction, mmWave beam forming reduces interference and increases the signal-to-noise ratio. This is achieved by using an array of antennas that work together to create a beam of energy that can be steered in a specific direction. However, there are also challenges associated with using mmWave beam forming in UAVs, such as the need for high-powered antennas, the potential for signal attenuation in adverse weather conditions, and the need for precise beam steering to maintain a reliable

connection [72].

4.5 UAV swarm communication

UAV swarm communication refers to the communication protocols and techniques used by multiple UAVs [73] (also known as a swarm) to collaborate and perform tasks cooperatively. In a UAV swarm, communication between the individual UAVs is crucial to ensure that they can work together effectively and achieve their collective goals. There are several communication approaches that can be used in UAV swarms, including centralized, decentralized, and distributed communication. The term "UAV swarm algorithms" refers to the mathematical and computational methods used to coordinate the actions of several UAVs in order to accomplish group objectives. Programming languages and tools like MATLAB, Python, and ROS (Robot Operating System) can be used to create UAV swarm algorithms. Centralized communication [74] involves all the UAVs in the swarm communicating with a central control unit or a ground control station. This approach provides a single control point and enables efficient coordination of the swarm's activities. However, it can also create a failure at a single point, making the swarm vulnerable to disruption or attack. Decentralized communication [75] involves each UAV in the swarm communicating with its nearest neighbors, forming a mesh network. This approach can be more resilient to disruption or attack, as there is no single point of failure. However, coordinating and managing the swarm's activities can be more complex. Distributed communication [76] involves each UAV in the swarm communicating with all other UAVs, allowing for more comprehensive information sharing and coordination of activities. This approach can be highly resilient and efficient, but requires more processing power and bandwidth than centralized or decentralized communication.

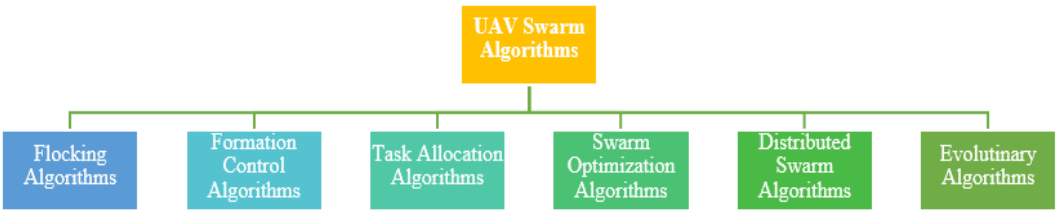

Fig. 2. Classification of UAV Swarm Algorithms

UAV swarm secure communication refers to the methods and techniques used to ensure the confidentiality, integrity, and availability of communication between multiple UAVs while performing tasks collaboratively. There are various algorithms used in UAV swarm applications are shown in **Fig. 2**. The secure communication of UAV swarm is essential to ensure the privacy of the data transmitted between the UAVs and to prevent unauthorized access and interference. SND is a protocol [77] for secure and efficient discovery of neighbors in a UAV swarm. It uses cryptographic techniques to provide integrity and authenticity of the messages exchanged between UAVs during the discovery process. For low-altitude UAV [78], secrecy performance outage in closed form is attained by the opportunistic relay. This experimented the communication architecture for swarm UAVs in the Low Earth Orbit environment to provide secure communication. The author developed the Hubenko architecture, a multi cast communication architecture.

5. Network Simulation Tools

There are several network simulation tools available for network modeling and simulation. These tools are used to design and analyze different types of network topologies and help in evaluating the performance of network protocols and applications under various conditions. From the **Fig. 3**, it can be understood that the Network simulator of versions such as NS-3 and NS-2 are the most widely used tools. Second most used tool is OPNET, followed by MATLAB users. Researchers use Python/C++ environment for attack detection, classification purposes. Others in the **Fig. 3**, include ONE simulator, SUMO, DJI INSPIRE, eMotion 2.0 flight simulator, etc.

5.1 OPNET

It is a commercial network simulation tool used to model and analyze types of communication networks in wired and wireless networks, LANs, WANs, and the Internet. It also provides a powerful simulation engine that allows users to simulate network behavior in various conditions and to analyze the performance by metrics like throughput, delay, and packet loss.

5.2 NS-2 & NS-3

It is an open-source network simulation tool that supports both wired and wireless networks. It provides an extensive set of tools and libraries for simulating network protocols at different layers, such as TCP, UDP, IP, and MAC. It is an open-source network simulation tool that is designed to replace NS-2. It provides a large set of models for different network layers such as packet level, MAC, and PHY layers, and supports both IPv4 and IPv6 protocols.

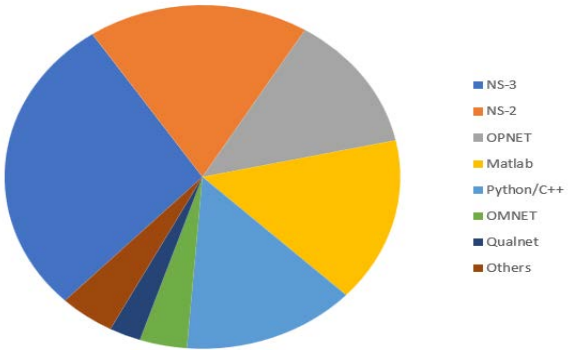

Fig. 3. Network simulators contribution to UAV applications

5.3 GNS3

GNS3 stands for Graphical Network Simulator-3 and is primarily used by network engineers and IT professionals to design, test, and troubleshoot network infrastructures without the need for physical hardware. It allows users to simulate complex networks using virtual machines (VMs) and real devices. GNS3 supports an extensive collective of network devices and OS, including Cisco routers and switches, Juniper routers, and various open-source operating systems like Linux and FreeBSD. It also supports a range of network protocols, including TCP/IP, OSPF, BGP, and VLANs.

5.4 OMNeT++

It stands for Objective Modular Network Testbed in C++, an open-source discrete event

network simulation framework. It supports a variety of network protocols and technologies, including TCP, IP, ATM, MPLS, Ethernet, Wi-Fi, LTE, and more. It also supports integration with other simulation tools and frameworks, such as MATLAB and Simulink.

5.5 PacketTracer

PacketTracer is a network simulation tool developed by Cisco. It allows users to simulate network traffic and test configurations without the need for physical hardware. It supports many types of protocols and devices, including routers, switches, firewalls, and servers. Users can create virtual networks, add devices, and connect them together using different types of network cables.

5.6 QualNet

QualNet is a commercial network simulation tool used to model and analyze various types of communication networks. It is widely used in the telecommunications industry for network planning, optimization, and deployment.

5.7 Cooja

Cooja is a network simulator specifically designed for WSNs and IoT systems. It is a component of the Contiki OS, which is an open-source, low-power, and flexible for networked embedded systems. Cooja simulates wireless nodes running Contiki, allowing users to test and evaluate various scenarios and protocols in a virtual environment. It also provides a range of tools for visualization, debugging, and analysis of simulated networks. Cooja is written in Java and runs on various platforms, including Linux, Windows, and macOS. It is widely used in research and development of wireless sensor networks and IoT systems.

From the **Fig. 3**, it can be understood that the Network simulator of versions such as NS-3 and NS-2 are most widely used tool. Second most used tool is OPNET, followed by MATLAB users. Researchers use Python/C++ environment for attack detection, classification purposes. Others in the **Fig. 3**, include ONE simulator, SUMO, DJI INSPIRE, eMotion 2.0 flight simulator etc.

6. Analysis of Performance Metrics

6.1 Packet Delivery ratio

It is an important networking performance metric used to evaluate effectiveness of a communication system, such as a wireless network, unmanned aerial vehicle [79] etc., PDR measures the ratio of transmitted packets successfully reach the intended destination without errors or losses. The PDR in UAV communication systems is altered by several factors, as well as the type of wireless technology used [80], the distance among the UAV and GCS, the presence of obstacles or interference, and the features of the communication link.

6.2 Average end-to-end delay

It is also a key metric in UAV communication systems, as it measures the time taken for a packet to be transmitted from the source UAV to the target UAV [81], including all the processing and transmission delays along the way. The propagation delay is termed as time taken for the signal to travel from the source to destination UAV, mainly defined by the distance of these two UAVs. The processing delay is the time taken for the UAVs and layers

like application layer, transport layer, and network layer protocols to process the data packets. The queuing delay is the time taken for a packet to wait in the transmission buffer before it is transmitted. Finally, the transmission delay is the time taken to transmit the packet over the wireless medium, which is determined by the proportion of the data and the wireless channel conditions.

6.3 Overhead

Routing overhead in UAV communication refers to the extra communication messages exchanged between UAVs or among the UAVs and GCS in order to establish and maintain the communication links and exchange data. This overhead includes the control messages, such as acknowledgements, route maintenance, route discovery, and congestion control, which are necessary for reliable and efficient communication.

6.4 Throughput

UAV throughput describes the transmitted amount of data over a communication link between two UAVs or among the UAV and GCS in a given period of time [82]. The throughput is calculated in terms of bits per second (bps) or bytes per second (Bps, “

6.5 Packet Loss Rate

UAV packet loss can be affected by several factors, including the strength and quality of the wireless signal and also the distance between the UAV and the GCS, and the presence of obstacles such as buildings or trees that can obstruct the signal. High packet loss rates can cause delays and interruptions in the transmission of critical information between the UAV and the GCS, leading to reduced performance and potentially endangering the safety of the UAV and its surroundings.

We include detailed technical scenarios for implementation and evaluation criteria in our paper [83], along with an overview of performance measures. Along with detailing the routing protocol, its kind, and its constraints, the study also compares the performance data. Lastly, guidelines for choosing the most appropriate performance measurements in a particular scenario are provided by the study.

7. Conclusion

Secure UAV communication is essential for safeguarding data, protecting privacy, ensuring operational safety, maintaining mission integrity, countering cyber threats, complying with regulations, and building trust in UAV technology. To protect sensitive information and prevent unauthorized access, UAVs and control stations should maintain secure communication. Using existing literature on UAV security, we identify the different types of attacks and the vulnerabilities they exploit in this paper. It provides comprehensive mitigation strategies and countermeasures for the defense of UAVs. A number of domain-based secure communication solutions are also examined, including Q-learning, blockchain, swarm, IRS, and mmWave-based specific communication strategies. In order to analyze and describe UAV communication in this article, many network characteristics are employed.

Network simulation tools for UAV communication networks help researchers, engineers, and operators analyze and optimize the performance of the network. They allow for testing different communication protocols, network configurations, and traffic patterns without the need for physical deployment, which can be costly and time-consuming. Difficulty in UAV

secure communication is a challenge that refers to the various obstacles and problems that hinder the establishment and maintenance of secure and reliable communication links between UAVs and other devices. UAV secure communication faces difficulty due to several factors. With multiple orientations and altitudes, UAVs create a highly complex and dynamic network topology, requiring algorithms for routing and resource allocation. UAVs suffer from various performance metrics that depend on channel conditions, network traffic, mobility patterns, interference, etc., such as throughput, delay, jitter, packet loss, energy consumption, etc. UAVs' communication and computation capabilities are limited by their limited battery life and power consumption. Energy consumption and performance need to be balanced when it comes to UAVs. A UAV's high mobility, environmental factors, node failure, and other factors can result in frequent link breaks and network partitions. The UAV must be capable of reliably delivering data and connecting to the network. High throughput can enable faster data

References

[1] X. Sun, C. Shen, D. W. K. Ng, and Z. Zhong, “Robust Trajectory and Resource Allocation Design for Secure UAV-Aided Communications,” in *Proc. of IEEE ICC Workshops*, 2019. Article (CrossRef Link)

[2] X. Chen, J. Tang, and S. Lao, "Review of unmanned aerial vehicle swarm communication architectures and routing protocols," *Applied Sciences*, vol. 10, p. 3661, 2020. Article (CrossRef Link)

[3] L. Chaari, S. Chahbani, and J. Rezgui, “Vulnerabilities assessment for unmanned aerial vehicles communication systems," in *Proc. of International Symposium on Networks, Computers and Communications (ISNCC)*, 2020. Article (CrossRef Link)

[4] G. Cho, J. Cho, S. Hyun, and H. Kim, "SENTINEL: A secure and efficient authentication framework for unmanned aerial vehicles," *Applied Sciences*, vol. 10, p. 3149, 2020. Article (CrossRefLink)

[5] T. Alladi, Naren, G. Bansal, V. Chamola, and M. Guizani, "SecAuthUAV: A Novel Authentication Scheme for UAV-Ground Station and UAV-UAV Communication," *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 15068-15077, 2020. Article (CrossRef Link)

[6] B. Doraswamy, K. L. Krishna, and M. Giriprasad, "A Secure Unmanned Aerial Vehicle Service for Medical System to Improve Smart City Facilities," *International Journal of Advanced Computer Science and Applications*, vol. 13, 2022. Article (CrossRefLink)

[7] Y. Zhang, Z. Zhuang, F. Gao, J. Wang, and Z Han, “Multi-Agent Deep Reinforcement Learning for Secure UAV Communications,” in *Proc. of IEEE WCNC*, 2020. Article (CrossRef Link)

[8] A. R. Wani, S. K. Gupta, Z. Khanam, M. Rashid, S. S. Alshamrani, and M. Baz, "A novel approach for securing data against adversary attacks in UAV embedded HetNet using identity based authentication scheme," *IET Intelligent Transport Systems*, vol. 17, no. 11, pp. 2171-2189, 2023. Article (CrossRef Link)

[9] S. Li, B. Duo, M. Di Renzo, M. Tao, and X. Yuan, "Robust secure UAV communications with the aid of reconfigurable intelligent surfaces," *IEEE Transactions on Wireless Communications*, vol. 20, pp. 6402-6417, 2021. Article (CrossRefLink)

[10] D. Wang, Y. Zhao, Y. He, X. Tang, L. Li, R. Zhang, et al., "Passive beamforming and trajectory optimization for reconfigurable intelligent surface-assisted UAV secure communication," *Remote Sensing*, vol. 13, p. 4286, 2021. Article (CrossRef Link)

[11] Y. Wu, T. Jing, Q. Gao, Y. Wu, and Y. Huo, "Game-theoretic physical layer authentication for spoofing detection in internet of things," *Digital Communications and Networks*, 2023/01/04/ 2023. Article (CrossRef Link)

[12] D. He, Y. Qiao, S. Chan, and N. Guizani, "Flight Security and Safety of Drones in Airborne Fog Computing Systems," *IEEE Communications Magazine*, vol. 56, pp. 66-71, 2018. Article (CrossRef Link)

[13] Y. Qiao, Y. Zhang, and X. Du, “A Vision-Based GPS-Spoofing Detection Method for Small UAVs," in *Proc. of CIS*, 2017. Article (CrossRef Link)
[14] S. Bhamidipati and G. X. Gao, "Locating Multiple GPS Jammers Using Networked UAVs," *IEEE Internet of Things Journal*, vol. 6, pp. 1816-1828, 2019. Article (CrossRef Link)
[15] A. Malik, M. Z. Khan, M. Faisal, F. Khan, and J.-T. Seo, "An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs," *Sensors*, vol. 22, p. 1897, 2022. Article (CrossRef Link)
[16] S. Bhunia and S. Sengupta, "Distributed adaptive beam nulling to mitigate jamming in 3D UAV mesh networks," in *Proc. of 2017 International Conference on Computing, Networking and Communications (ICNC)*, pp. 120-125, 2017. Article (CrossRef Link)
[17] S. Qiu and H. Liu, “A new zonotope-based attack detection method for UAV," in *Proc. of CCC*, 2022. Article (CrossRef Link)
[18] J. Viana, H. Farkhari, L. M. Campos, P. Sebastião, F. Cercas, L. Bernardo, Rui Dinis, “Two methods for Jamming Identification in UAV Networks using New Synthetic Dataset," in *Proc. of VTC2022-Spring*, 2022. Article (CrossRef Link)
[19] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, pp. 1594-1606, 2018. Article (CrossRef Link)
[20] R. Fotohi, M. Abdan, and S. Ghasemi, "A Self-Adaptive Intrusion Detection System for Securing UAV-to-UAV Communications Based on the Human Immune System in UAV Networks," *Journal of Grid Computing*, vol. 20, p. 22, 2022/07/15 2022. Article (CrossRef Link)
[21] S. Younas, F. Rehman, T. Maqsood, S. Mustafa, A. Akhunzada, and A. Gani, "Collaborative Detection of Black Hole and Gray Hole Attacks for Secure Data Communication in VANETs," *Applied Sciences*, vol. 12, p. 12448, 2022. Article (CrossRef Link)
[22] M. Sliti, W. Abdallah, and N. Boudriga, “Jamming Attack Detection in Optical UAV Networks," in *Proc. of ICTON*, 2018. Article (CrossRef Link)
[23] A. Krayani, A. S. Alam, L. Marcenaro, A. Nallanathan, and C. Regazzoni, "Automatic Jamming Signal Classification in Cognitive UAV Radios," *IEEE Transactions on Vehicular Technology*, vol. 71, pp. 12972-12988, 2022. Article (CrossRef Link)
[24] P. K. Singh, R. R. Gupta, S. K. Nandi, and S. Nandi, "Machine Learning Based Approach to Detect Wormhole Attack in VANETs," in *Proc. of WAINA 2019: Web, Artificial Intelligence and Network Applications*, Cham, pp. 651-661, 2019. Article (CrossRef Link)
[25] P. Mykytyn, M. Brzozowski, Z. Dyka, and P. Langendoerfer, “Jamming Detection for IR-UWB Ranging Technology in Autonomous UAV Swarms," in *Proc. of MECO*, 2021. Article (CrossRef Link)
[26] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, “Detection of GPS Spoofing Attacks on Unmanned Aerial Systems," in *Proc. of CCNC*, 2019. Article (CrossRef Link)
[27] D. Darsena, G. Gelli, I. Iudice, and F. Verde, "Detection and Blind Channel Estimation for UAV-Aided Wireless Sensor Networks in Smart Cities Under Mobile Jamming Attack," *IEEE Internet of Things Journal*, vol. 9, pp. 11932-11950, 2022. Article (CrossRef Link)
[28] J. Xiao and M. Feroskhan, "Cyber Attack Detection and Isolation for a Quadrotor UAV With Modified Sliding Innovation Sequences," *IEEE Transactions on Vehicular Technology*, vol. 71, pp. 7202-7214, 2022. Article (CrossRef Link)
[29] R. T. Mehmood, G. Ahmed, and S. Siddiqui, “Simulating ML-Based Intrusion Detection System for Unmanned Aerial Vehicles (UAVs) using COOJA Simulator," in *Proc. of ICOSST*, 2022. Article (CrossRef Link)
[30] Y. Luo, Y. Liao, S. Ni, A. Zhang, and L. Cheng, “Research on UAV Sensor Attack Detection Based on Kalman Filter," in *Proc. of ICSIP*, 2021. Article (CrossRef Link)
[31] R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim, "Machine-Learning-Enabled Intrusion Detection System for Cellular Connected UAV Networks," *Electronics*, vol. 10, p. 1549, 2021. Article (CrossRef Link)

[32] L. Meng, L. Yang, S. Ren, G. Tang, L. Zhang, F. Yang, et al., "An Approach of Linear Regression-Based UAV GPS Spoofing Detection," *Wireless Communications and Mobile Computing*, vol. 2021, p. 5517500, 2021/05/07 2021. Article (CrossRef Link)
[33] A. S. Abdalla, K. Powell, V. Marojevic, and G. Geraci, "UAV-Assisted Attack Prevention, Detection, and Recovery of 5G Networks," *IEEE Wireless Communications*, vol. 27, pp. 40-47, 2020. Article (CrossRef Link)
[34] T. M. Hoang, N. M. Nguyen, and T. Q. Duong, "Detection of eavesdropping attack in UAV-aided wireless systems: Unsupervised learning with one-class SVM and k-means clustering," *IEEE Wireless Communications Letter*, vol. 9, no. 2, pp. 139-142, 2020. Article (CrossRef Link)
[35] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," *IEEE Transactions on Wireless Communications*, vol. 16, pp. 4585-4599, 2017. Article (CrossRef Link)
[36] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE transactions on wireless communications*, vol. 16, pp. 2790-2806, 2017. Article (CrossRef Link)
[37] Y. Ko, J. Kim, D. G. Duguma, P. V. Astillo, I. You, and G. Pau, "Drone secure communication protocol for future sensitive applications in military zone," *Sensors*, vol. 21, p. 2057, 2021. Article (CrossRef Link)
[38] A. Kumar, V. Varadarajan, A. Kumar, P. Dadheech, S. S. Choudhary, V. D. A. Kumar, et al., "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocessors and Microsystems*, vol. 80, p. 103352, 2021. Article (CrossRef Link)
[39] D. Sheela, V. Srividhya, B. Asma, and G. Chidanand, "Detecting black hole attacks in wireless sensor networks using mobile agent," in *Proc. of ICAIES*, 2012.
[40] N. A. Khan, S. N. Brohi, and N. Jhanjhi, "UAV's Applications, Architecture, Security Issues and Attack Scenarios: A Survey," in *Intelligent Computing and Innovation on Data Science, Singapore*, 2020, pp. 753-760. Article (CrossRef Link)
[41] F. Alrefaei, A. Alzahrani, H. Song, and S. Alrefaei, "A Survey on the Jamming and Spoofing attacks on the Unmanned Aerial Vehicle Networks," in *Proc. of IEMTRONICS*, 2022. Article (CrossRef Link)
[42] M. R. Manesh, M. S. Velashani, E. Ghribi, and N. Kaabouch, "Performance comparison of machine learning algorithms in detecting jamming attacks on ADS-B devices," in *Proc. of EIT*, 2019. Article (CrossRef Link)
[43] S. Sharma and A. Kaul, "A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud," *Vehicular communications*, vol. 12, pp. 138-164, 2018. Article (CrossRef Link)
[44] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," *Computers & Security*, vol. 89, p. 101664, 2020. Article (CrossRef Link)
[45] M. M. Singh, N. Dutta, T. R. Singh, and U. Nandi, "A technique to detect wormhole attack in wireless sensor network using artificial neural network," in *Proc. of ICECMSN*, pp. 297-307, 2021.
[46] V. Anandkumar and P. Ganapathi, "A Study on Various Cyber-Attacks and their Classification in UAV Assisted Vehicular Ad-Hoc Networks," in *Proc. of ICC3*, Coimbatore, India, pp. 124-131, 2017.
[47] J. Liu, N. Sha, W. Yang, J. Tu, and L. Yang, "Hierarchical Q-Learning Based UAV Secure Communication against Multiple UAV Adaptive Eavesdroppers," *Wireless Communications and Mobile Computing*, vol. 2020, p. 8825120, 2020. Article (CrossRef Link)
[48] Y. You, R. Zhao, and H. Sun, "Deep Reinforcement Learning-Based Trajectory Planning for Secure UAV Communication," in *Proc. of ICICSP*, 2021. Article (CrossRef Link)
[49] S. I. Alnagar, A. M. Salhab, and S. A. Zummo, "Q-Learning-Based Power Allocation for Secure Wireless Communication in UAV-Aided Relay Network," *IEEE Access*, vol. 9, pp. 33169-33180, 2021. Article (CrossRef Link)
[50] J. Liu, W. Yang, S. Xu, J. Liu, and Q. Zhang, "Q-Learning Based UAV Secure Communication in Presence of Multiple UAV Active Eavesdroppers," in *Proc. of WCSP*, 2019. Article (CrossRef Link)

[51] C. Li, Y. Xu, J. Xia, and J. Zhao, "Protecting Secure Communication Under UAV Smart Attack With Imperfect Channel Estimation," *IEEE Access*, vol. 6, pp. 76395-76401, 2018. Article (CrossRef Link)
[52] R. Dong, B. Wang, and K. Cao, "Deep Learning Driven 3D Robust Beamforming for Secure Communication of UAV Systems," *IEEE Wireless Communications Letters*, pp. 1643-1647, 2021.
[53] W. Lu, Y. Mo, Y. Feng, Y. Gao, N. Zhao, Y. Wu, et al., "Secure Transmission for Multi-UAV-Assisted Mobile Edge Computing Based on Reinforcement Learning," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 3, pp. 1270-1280, 2023. Article (CrossRef Link)
[54] C. Wen, Y. Fang, and L. Qiu, "Securing uav communication based on multi-agent deep reinforcement learning in the presence of smart uav eavesdroppe," in *Proc. of WCNC*, 2022. Article (CrossRef Link)
[55] R. Kumar, A. Aljuhani, P. Kumar, A. Kumar, A. Franklin, and A. Jolfaei, "Blockchain-enabled secure communication for unmanned aerial vehicle (UAV) networks," in *Proc. of ACM Mobicom Workshop on Drone Assisted Wireless Communications for 5G and Beyond*, pp. 37-42, 2022.
[56] E. Ghribi, T. T. Khoei, H. T. Gorji, P. Ranganathan, and N. Kaabouch, "A secure blockchain-based communication approach for UAV networks," in *Proc. of IEEE EIT*, 2020. Article (CrossRef Link)
[57] M. Golam, J. M. Lee, and D. S. Kim, "A UAV-assissted Blockchain Based Secure Device-to-Device Communication in Internet of Military Things," in *Proc. of ICTC*, 2020. Article (CrossRef Link)
[58] M. ÖZÇEVİK, "Two-layered blockchain-based admission control for secure UAV networks," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 30, pp. 2165-2178, 2022. Article (CrossRef Link)
[59] P. Rahimi, N. D. Khan, C. Chrysostomou, V. Vassiliou, and B. Nazir, "A secure communication for maritime iot applications using blockchain technology," in *Proc. of DCOSS*, 2020. Article (CrossRef Link)
[60] T. Faika, "WIP: Consortium Blockchain for Secure Data Acquisition using UAVs as Sensing Devices," in *Proc. of UEMCON*, 2022. Article (CrossRef Link)
[61] Z. Wu and J. Liu, "Blockchain-Based Trusted Avionics Authentication for Secure Ground-to-Air Communication," in *Proc. of DASC*, 2022. Article (CrossRef Link)
[62] G. Sun, X. Tao, N. Li, and J. Xu, "Intelligent Reflecting Surface and UAV Assisted Secrecy Communication in Millimeter-Wave Networks," *IEEE Transactions on Vehicular Technology*, vol. 70, pp. 11949-11961, 2021. Article (CrossRef Link)
[63] J. Fang, Z. Yang, N. Anjum, Y. Hu, H. Asgari, and M. Shikh-Bahaei, "Secure Intelligent Reflecting Surface Assisted UAV Communication Networks," in *Proc. of ICC Workshops*, 2021. Article (CrossRef Link)
[64] S. Fang, G. Chen, and Y. Li, "Joint optimization for secure intelligent reflecting surface assisted UAV networks," *IEEE wireless communications letters*, pp. 276-280, 2020.
[65] C. He and J. Xiao, "Joint Optimization in Intelligent Reflecting Surface-Aided UAV Communication for Multiaccess Edge Computing," *Wireless Communications and Mobile Computing*, vol. 2022, 2022. Article (CrossRef Link)
[66] L. Yang, F. Meng, J. Zhang, M. O. Hasna, and M. Di Renzo, "On the performance of RIS-assisted dual-hop UAV communication systems," *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 10385-10390, 2020. Article (CrossRef Link)
[67] A. Ranjha and G. Kaddoum, "URLLC facilitated by mobile UAV relay and RIS: A joint design of passive beamforming, blocklength, and UAV positioning," *IEEE Internet of Things Journal*, vol. 8, pp. 4618-4627, 2021. Article (CrossRef Link)
[68] W. Wang, H. Tian, W. Ni, and M. Hua, "Intelligent reflecting surface aided secure UAV communications," *arXiv preprint arXiv:2011.04339*, 2020.
[69] Z. Ye, G. Su, B. Chen, M. Dai, X. Lin, and H. Wang, "Secrecy Rate Optimization for Secure communication in IRS-Aided UAV Systems," in *Proc. of WOCC*, 2022. Article (CrossRef Link)
[70] X. Pang, W. Mei, N. Zhao, and R. Zhang, "Intelligent reflecting surface assisted interference mitigation for cellular-connected UAV," *IEEE Wireless Communications Letters*, pp. 1708-1712, 2022.

[71] L. Yang, Y. Zeng, and R. Zhang, "Channel Estimation for Millimeter-Wave MIMO Communications With Lens Antenna Arrays," *IEEE Transactions on Vehicular Technology*, vol. 67, pp. 3239-3251, 2018. Article (CrossRef Link)
[72] D. Diao, B. Wang, K. Cao, R. Dong, and T. Cheng, "Secure Transmission of mmWave NOMA UAV-Assisted Relay System against Randomly Located Eavesdroppers," *Security and Communication Networks*, vol. 2022, 2022. Article (CrossRef Link)
[73] M. Campion, P. Ranganathan, and S. Faruque, "UAV swarm communication and control architectures: a review," *Journal of Unmanned Vehicle Systems*, vol. 7, pp. 93-106, 2018. Article (CrossRef Link)
[74] Y. Dong, X. Xiaojia, L. Jie, and L. Zhenyi, “Research on Ad-hoc Network for UAV Swarm Based on OPNET Simulation," in *Proc. of ICCT*, 2020. Article (CrossRef Link)
[75] S. Khaliq, S. Ahsan, and M. D. Nisar, “Multi-Platform Hardware In The Loop (HIL) Simulation for Decentralized Swarm Communication Using ROS and GAZEBO," in *Proc. of WoWMoM*, 2021. Article (CrossRef Link)
[76] D. Liu, J. Wang, K. Xu, Y. Xu, Y. Yang, Y. Xu, et al., "Task-driven relay assignment in distributed UAV communication networks," *IEEE Transactions on Vehicular Technology*, vol. 68, pp. 11003-11017, 2019. Article (CrossRef Link)
[77] M. M. Alam and S. Moh, "Survey on Neighbor Discovery and Beam Alignment in mmWave-Enabled UAV Swarm Networks,".
[78] H. Liu, S. J. Yoo, and K. S. Kwak, "Opportunistic relaying for low-altitude UAV swarm secure communications with multiple eavesdroppers," *Journal of Communications and Networks*, vol. 20, pp. 496-508, 2018. Article (CrossRef Link)
[79] T. Kim, S. Lee, K. H. Kim, and Y.-I. Jo, "FANET Routing Protocol Analysis for Multi-UAV-Based Reconnaissance Mobility Models," *Drones*, vol. 7, p. 161, 2023. Article (CrossRef Link)
[80] M. Zhang, C. Dong, P. Yang, T. Tao, Q. Wu, and T. Q. S. Quek, “Adaptive Routing Design for Flying Ad Hoc Networks,” *IEEE Communications Letters*, pp. 1438-1442, 2022.
[81] Y. J. Chen, K. M. Liao, and Y. F. Chen, "End-to-End Delay Analysis in Aerial-Terrestrial Heterogeneous Networks," *IEEE Transactions on Vehicular Technology*, vol. 70, pp. 1793-1806, 2021. Article (CrossRef Link)
[82] A. Khakimov, E. Mokrov, D. Poluektov, K. Samouylov, and A. Koucheryavy, "Evaluating the Quality of Experience Performance Metric for UAV-Based Networks," *Sensors*, vol. 21, p. 5689, 2021. Article (CrossRef Link)
[83] T. Madhuvanthi and A. Revathi, “Survey on Current Developments in UAV Secure Communication Techniques and Protocols," in *Proc. of RMKMATE*, 2023. Article (CrossRef Link)

Ms. Madhuvanthi T is a Research Scholar at Department of Computational Intelligence, College of Engineering and Technology, SRM Institute of Science and Technology, KTR Campus, Chengalpattu, Tamilnadu. She holds a M.E (CSE) degree from Kongu Engineering College, Perundurai, Erode and B.E (ECE) degree from Hindusthan Institute of Science and Technology, Coimbatore. Her fields of study interest range widely, including Network Security, Communication, Path Planning, Machine Learning, Deep Learning and Unmanned Aerial Vehicles. At present, she is active in the field of Unmanned Aerial Vehicle path planning and communication security. Email: mt9279@srmist.edu.in

Dr. Revathi A is a Assistant Professor at Department of Computational Intelligence, College of Engineering and Technology, SRM Institute of Science and Technology, KTR Campus, Chengalpattu, Tamilnadu since 2020. She holds a Ph.D in the field of Information and Communication Engineering, from Anna University, Chennai. M.E and B.E degree in Computer Science and Engineering from Madras University. Dr. Revathi has previously taught sensor networks, computer networks and programming for problem solving. With almost 19 years of teaching and research experience in computer science, she has made major contributions to the discipline. Her fields of study interest range widely, including Data Science, Machine Learning, Deep Learning, Network Security, Wireless Sensor Networks, Artificial Intelligence and Unmanned Aerial Vehicles. At present, she is active in the field of Unmanned Aerial Vehicle communication security. Additionally, she is a reviewer on top journals. Email: revathia1@srmist.edu.in