DESIGN AND DEVELOPMENT OF A SECURE DATA TRANSMISSION PROTOCOL FOR UAV

Sandya Rani Vadlamudi[1*], Dr. A M Viswa Bharathy[2]

Article History: **Received: 05.06.2023** **Revised: 02.07.2023** **Accepted: 01.08.2023**

Abstract—
Rapid technological advancements have made it possible for unmanned aerial vehicles (UAVs) to be used in a variety of applications, and since they are so mobile, UAV systems may work together to complete a wide variety of missions. UAVs have a variety of applications in both military and commercial sectors. UAVs can also be deployed in civil sectors like search and rescue operations. In recent years, UAVs were used illegally. These attacks are becoming more common and can have far-reaching consequences. As a result, associated industries and standards agencies are investigating potential solutions for protecting UAV infrastructure. Researchers have been looking for robust and secure protocols to protect UAVs from cybercriminals. However, hackers can easily exploit many vulnerabilities in the existing protocols. Therefore, it is essential to research and examines the current security protocols employed in UAVs to identify and fix their flaws. The goal of this survey is to uncover more about the secure protocol for UAV data transmission. The survey examines the existing methods described in the literature to solve the security issues that arise during data transmission between UAVs and base stations. Each protocol's advantages and disadvantages are detailed, along with suggestions for future research that could improve UAV security. Researchers and professionals in the area will find this survey a valuable resource, which provides a brief description of the secure data transmission protocols used in UAVs.

Keywords— Unmanned Aerial Vehicle, Communication, Data Transmission, Authentication, Cloud Secure, Protocol, Routing, Networking

[1*]Research Scholar, Dept of Computer Science and Engineering, GITAM School of Technology, GITAM University, vs.sandya@gmail.com
[2]Assistant Professor, Dept of Computer Science and Engineering GITAM School of Technology, GITAM University, viswabharathy86@gmail.com

***Corresponding Author:** Sandya Rani Vadlamudi
*****Research Scholar, Dept of Computer Science and Engineering, GITAM School of Technology, GITAM University, vs.sandya@gmail.com

DOI: - 10.48047/ecb/2023.12.si10.00525

I. INTRODUCTION

A UAV is a plane, helicopter, or other flying machine that is piloted by no human being [1]. You can use both the control system and the GCS when flying a UAV. The pilot of a UAV controlled remotely looks either at the aircraft itself or through a camera installed on the UAV. The UAV's flight instructions are sent in real-time. The purpose of the communication module connecting the controller and UAV is to allow for communication between the two parties via predefined protocols [2]. Networking technologies like telemetry, Wi-Fi, ZigBee, and others are widely utilized for conversation. However, when the UAV is controlled from GCS, a computer is used to link the software to the UAV, and the UAV then carries out the mission instructions that were uploaded by the user. Because of all the sensors installed in the UAV, GCS is always aware of its altitude, distance, geographical position, and true mission status [3]. The numerous parts of an unmanned aircraft system are controlled by electronic equipment on board or on the ground. Components include sensor payloads and GCS or stations. RPA-style UAVs need stable wireless connectivity because they are piloted by humans on the ground. However, GCSs are necessary for close control of large UAVs due to range and communication limitations.

The popularity and effectiveness of UAVs have both increased dramatically during the past two decades. These are commonly employed in security-related activities like monitoring and investigation [4]. Traffic surveillance [5], infrastructure observation, environmental monitoring [6], disaster administration [7], photography, agriculture [8], entertainment [9], search, and rescue operations [10] are just a few of the many uses for UAVs beyond the military and defence. Numerous studies have shown, for instance, that civilian uses of UAVs, especially in smart cities and the Internet of Things, will soon outnumber military uses and may eventually supplant the military's need for UAVs in the future [11]. Due to their popularity and security flaws, UAVs present a tempting target for hackers and attackers. There are many ways in which the owners of a hacked UAV could be harmed. Research into the best ways to secure UAVs is still in its infancy because of their novelty. Most of these solitons are either suggestions or brand-new creations. If there is a security breach, vital data could be lost or buildings and people could be destroyed [12]. The economic and social repercussions are severe. Insecure communication networks are the root source of most problems and dangers.

A UAV can only be attacked from the outside unless the attacker has physical access to the UAV's system. Due to the inherent dependence of its wireless communication technology on such inputs, UAVs are highly dependent on human control. This opens up a wide variety of possible vectors for assault. The most susceptible area of the system is the communication system and the GCS. Second, only to the UAV sensors themselves, environmental data transport is a crucial part of the system. Both of these connections are very malleable. The sensors' reliability is also questionable. The host's knowledge of the components' responsiveness to orders is crucial for maintaining control of a UAV during a cyberattack.

The following is the outline for this survey paper. Section I introduces UAVs and their applications in a variety of disciplines. Section II described the numerous attacks as well as the operation of communication protocol principles. Section III goes into more detail about how UAV networking protocol can be used for both short- and long-distance communication. Section IV addresses the various UAV routing protocols. Section V examines the security needs for UAV communications. Section VI describes the evolving technologies for secure UAV communications that are now available. Section VII discusses the future direction and challenges. Section VIII wraps up the survey with a brief summary.

II. UAV VULNERABILITIES AND PROTOCOL PRINCIPLES

Most UAVs have remote communication and control capabilities. Wireless communication poses serious risks when used for command and control (C2) purposes. Most studies, however, have concentrated on the UAVs' ability to fly autonomously. Common targets for the UAV-to-ground challenge include "out of line-of-sight" or "long-range communications" problems. Unfortunately, the security of communication protocols used by UAVs is often overlooked. Finding security flaws in UAV designs requires an in-depth familiarity with the various parts of such systems and the means of communication used to link them. Additionally, UAVs have a high potential for technical malfunction. Basic UAV elements and data flows are shown in Figure 1.

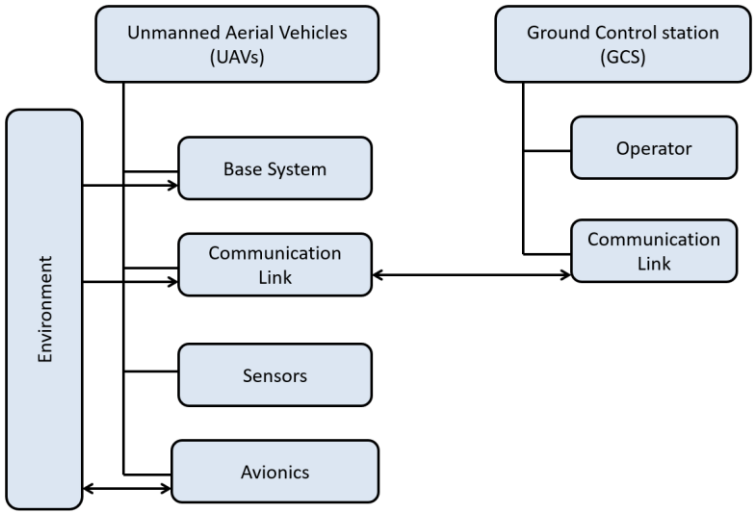

Fig. 1: UAV elements and data flows.

The potential risks and vulnerabilities of current UAVs are examined using information from a magazine [13] that gives details of general and specific cyber-attack strategies. Below, we discuss both general and specific ways in which UAVs can attack:

A. General Attack Scenarios:

After examining the data flow of the UAV, several potential avenues of generic cyber-attacks are described. Three categories of attacks exist:

Hardware Attack: An adversary can launch a hardware attack on a UAV's autopilot if they are able to physically access a crucial component of the system. After that, the attacker can either access the autopilot's internal storage or install malicious components that interfere with data transmission. At any point in the lifecycle of the UAV, from design to operation, these kinds of attacks are possible. To gain control of the UAV and the tactical data it collects, an attacker with such capabilities only needs to establish a direct link to the autopilot and destroy, reprogram, or install the necessary components. Attacks on the hardware of the UAV carry the risk of compromising its capacity to function autonomously, collect tactical data, and live.

Wireless attacks: When data stored in the autopilot of the UAV is tampered with via wireless communication channels, a wireless attack has taken place. In the worst case, the attacker can decode the protected channel of communication. If an attacker is aware of the UAV's communication protocol, full control of the aircraft is at their fingertips. Buffer overflow attacks, which affect onboard data or trigger operations, are another potential. The fact that wireless attacks can be launched remotely while the UAV is in flight is the biggest cause for concern.

Sensor spoofing: On-board sensors that gather data from the outside environment are frequently the target of spoofing attacks. Sensors include things like GPS receivers, radar, cameras, lidar, sonar, and infrared detectors. With the help of forged data sent over the GPS channels, an attacker can deactivate or trick any of the optical sensors [14]. The UAV autopilot's reliance on faulty sensor data for Guidance and Navigation is extremely risky.

B. Specific Attack Scenarios:

In addition, we found numerous attack scenarios that bring attention to vulnerabilities in the standard UAV setup. From a cybersecurity perspective, it was clear that the attacks are divided into two types:

Control System Security: Interference with the intended functioning of the hardware or CPU. Attacks of this type can involve hardware tampering or additions, input device buffer overflow attacks, and forced system resets to load malicious applications [15].

Application Logic Security: Manipulation of sensors or the environment with malicious intent to feed misleading data into the control system. When this occurs, the control system keeps running as usual, but the inputs are contaminated. One form of attack is to tamper with data used for C2, navigation, or senses.

In order to send and receive data wirelessly, UAVs use radio frequency communication technologies. So, we'll have a look at the typical structure and parts of radio protocol messages. Then, please describe in great detail the steps taken by the radio

chip when sending or receiving data. Encoding and modulating data is a prerequisite for transmission [16]. The many steps required to convey a message are visually represented in Figure 2. As we proceed, we shall refer to the message's bit sequence as "message bits" and the encoded message's bit sequence as "data bits." To protect data transmission from disruptions, Frequency Hopping Spread Spectrum (FHSS) is frequently employed.

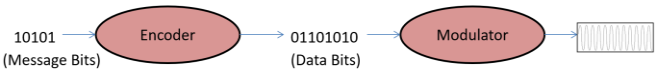

Fig.2. Sending messages

The actions outlined above are performed in reverse order when a message is received. The process of demodulating and decoding the incoming signal is repeated. It is depicted in Figure 3 how a message is received.

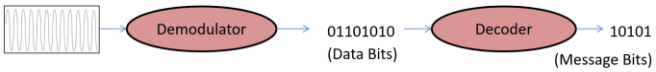

Fig 3. Receiving Message

III. UAV NETWORKING PROTOCOL

Data can be transferred from UAVs, to and from satellites and airborne control units, and from the air to the ground via a number of different communication protocols. Since the operation zone is frequently large and beyond the Line of Sight (LoS), the communication range of a single UAV, and networked UAV systems are required for a reliable connection. From a technical, feasible, and cost standpoint, the most essential design concern is selecting the most appropriate wireless technology with enough capacity and a suitable Quality of Service (QoS) [17].

There are two broad categories of wireless technologies: those used for localized or immediate communication (*Short-Range Communication*), and those used for more extensive distances *(Long-Range Communication).*

A. Short-Range Communication Technologies

Despite focusing on local wireless access, short-range communication technologies offer lightweight, inexpensive communication links through the use of an unlicensed spectrum. Data can be sent from a few millimetres to hundreds of meters using short-range communication technology.

Bluetooth (IEEE 802.15.1): The range of a Bluetooth connection is 10-200 meters, and it runs in the unlicensed 2.4 GHz radio spectrum. Each generation of Bluetooth has a different maximum data transfer rate (often 1-3 Mbps). However, a maximum of 24 Mbps is achievable for data transfer. In [18], Bluetooth 5, you'll find the most up-to-date version of the Bluetooth specification. The next version of Bluetooth will improve upon its predecessor in several ways: speed, range, power consumption, and compatibility with other short-range protocols. Bluetooth 5 may communicate media files and URLs in addition to the usual location data.

Wi-Fi (IEEE 802.11): "Wireless Fidelity," or "Wi-Fi," refers to a collection of specifications for generating wireless local area networks (WLANs) that use the following frequency bands: frequency ranges of 2, 4, 5, and 60 GHz. IEEE 802.11 and its variations may be the ideal option for many UAV applications because of their quick throughput and capacity to carry big data sets such as films and images. The average Wi-Fi network has a range of about 100 yards for data transmission. However, the UAVs' transmission range could extend over a number of kilometres. The performance of a wireless connection between a UAV and GS was evaluated by looking at throughput, RSSI, and distance [19]. For a UAV-based network, establishing a wireless connection through 802.11a between the UAV and the GS is recommended.

ZigBee (IEEE 802.15.4): This protocol is often utilized in minimum data rate applications due to its long battery life, secure networking, and low transmission rate [20]. The effective radius is 10–100 meters. It's easier to use and cheaper than Wi-Fi and Bluetooth. It operates on the 2.4 GHz band and can transmit data at 250 kbps. The minimum bandwidth required is 5 MHz, with a maximum of 16 channels needed.

B. Long-Range Communication Technologies

Data communication services across vast distances can be provided between two locations using long-distance communication technologies as a backhaul. Direct connections between planes

might be possible with the use of U2U and U2I communication systems.

WiMAX (IEEE 802.16): It is a technical standard with the goal of providing broadband over extremely long distances through a number of different mechanisms, from point-to-point connections to fully mobile cellular-type access. This innovation is applicable to both mobile and fixed broadband deployments. Its top speed is 75 Mbps (20–30 Mbps per user), but the best mobile apps can only manage 30 Mbps (3–5 Mbps per user) [21]. The goal of WiMAX development is to provide reliable, high-quality audio and video streaming without degrading the expected QoS. According to the research [22], WiMAX is the best option for UAV-based rescue systems in dangerous atmospheres.

5G (Fifth Generation): Cellular mobile communication has progressed through several generations, with the most current being 5G (5th Generation or 5G). Previous generations include 2G, 3G, and 4G. It can move data quickly, has minimal latency, requires less energy, has more storage space, and is always accessible. According to the International Telecommunication Union, 5G mobile networks will be live by the year 2020. Such networks will offer 100 GB/s per user with scalability up to 1,000 times their current capacity [23]. As a result of these advantages, 5G technology will play an important role in UAV communication systems.

6G (Sixth Generation): As the demand for faster data transfer rates and larger network capacities increases, the arrival of 6G is imminent. 6G is projected to offer connections that are intelligent, secure, reliable, and unlimited at a speed 100 times faster than 5G [24]. We forecast that similar to 5G, 6G networks would include aerial nodes that better accommodate the varied needs of UAV networks, including reduced latency, dependability, and energy efficiency. A blockchain-based solution for UAV communications is just one example of the many connectivity-related applications that stand to gain from 6G network intelligence [25].

Satellite Communication (SATCOM): "Satellite communications" (or "SATCOM") refers to the transfer of electromagnetic signals between terrestrial stations and orbiting satellites. Multiple frequency bands are used for SATCOM (short for satellite communications). C-Bands are still used by some networks because of their 6-GHz uplink and 4-GHz downlink. Uplink and downlink frequencies in X-Bands are frequently utilized by government and military systems, 8 and 7 GHz, respectively. In the so-called Ku-Bands, the uplink frequency is 14 GHz, while the downstream frequency ranges from 11-12 GHz. Moreover, as these bands reach capacity, Ka-Bands are being progressively phased in as a replacement. Both the uplink and the downlink frequencies in Ka-bands are 30 GHz.

In light of the foregoing explanation, it is apparent that, based on the range and data rate, and UAV applications the type of communication is selected. The comparison of UAV networking protocol is given in Table 1.

Table 1. Comparison of UAV networking protocol.

Communication Technology	IEEE Standard	Spectrum Type	Range (m)	Frequency (Hz)	Latency (ms)	Data Rate (bps)	Advantages	Drawbacks
Bluetooth	802.15.1	Unlicensed	40–200	2.4 G	3	2 M	Energy-efficient	Low data rate
Wi-Fi	802.11	Unlicensed	20–100	2.4 G	<5	2 M	High speed and cheap	Limited range
ZigBee	802.15.4	Unlicensed	10–100	2.4 G	15	250 K	Low cost	Low data rate
WiMAX	802.16a	Licensed	48 k	2 to 11 G	30	75 M	High throughput	Interference issues
5G	-	Licensed	Wide Area	28 G	1	20 G	High data rate	Expensive
6G	-	Licensed	Wide Area	10 T	<1	25 G	High speed and High data rate	Expensive
SATCOM	-	Licensed	World Wide	40 G	550	30 G	Wide coverage	High delay and high cost

C. AI in UAV networking

When applied to UAV networks, AI can provide data-driven solutions to problems like interference control, cyber threats, mobility management, and authentication, all of which contribute to the reliability, connectivity, and security of wireless communication. For instance, AI may be used to foretell the success or failure of a gearbox. Based on the requirements of the application, the most appropriate communication protocol can be selected from those presented above. There have been several attempts to build new networking

algorithms on top of these protocols, and some have even been implemented, however, the vast majority of these innovations have not yet been brought to market. To increase the range of UAV connections for rapid, temporary service in areas with robust wireless coverage, for instance where Wi-Fi and Cellular networks are merged, spectrum sharing and leasing have been proposed [26]. Beamforming's ability to increase communication range while simultaneously decreasing interference is another perk.

IV. UAV ROUTING PROTOCOL

Several routing techniques for UAV networks are suggested in journals [27-32]. Initially, UAV network testbeds used MANET and VANET routing protocols [33]. However, it quickly became clear that the routing protocols developed for mobile ad hoc networks (MANETs) and vehicular ad hoc networks (VANETs) were unsuitable for UAV networks. As a result, new ideas for UAV-specific routing protocols have emerged.

UAV routing protocols are classified into two types: those based on network architecture and those based on data forwarding. Routing protocols in networks are divided into two types: topology and position-based. Deterministic and stochastic routing protocols are two types of data-forwarding routing systems. All divisions and sub-divisions of UAV routing protocol is illustrated in Figure 4.

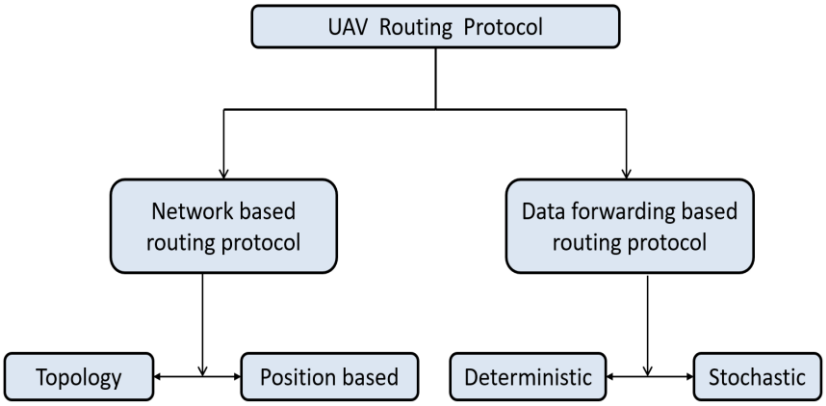

Fig. 4: Types of UAV routing Protocol.

Topology-based routing protocols: This makes use of the data already collected from the nodes to transfer packets around the network. Topology-based routing solutions use IP addresses in a network to identify each node in the network. Because of the excellent mobility and frequent topological changes in UAV networks, developing a routing protocol is difficult [34]. The four major types of routing protocols are static, reactive, proactive, and hybrid routing protocols.

Position-based routing protocols: Nodes are defined using GPS coordinates, making it geographically dependent. This routing considerably benefits highly dynamic UAV networks [35]. This protocol is categorized into two types: single and multi-path. Subcategories of single- and multi-path-based routing technologies include heterogeneous networks, Delay, and Non-Delay Tolerant Networks.

Deterministic routing protocol: Neighbouring nodes in deterministic routing are aware of a node's future path before it occurs. This protocol could be useful in UAV networks because UAVs often fly in structured formations. If all nodes have access to the availability, mobility, and motion data of all other nodes, a tree-based approach for particular routes might be established. The source node is believed to be the parent of all other nodes in the tree. Which branches to take are determined by the shortest time to the target node [36]. This protocol will be useful if you know where and when the nodes will be available in the future.

Stochastic routing protocols: If the behaviour of your network is unexpected, you should utilize a stochastic routing protocol [37]. Under these conditions, the location of a packet is critical. One alternative is to send the information to the next node in the chain and hopes that it is within network range. In this situation, different factors are considered during the routing process. It is a protocol for modifying the topology of a network dynamically in order to reduce latency and increase delivery rates. Stochastic routing protocols that are based on epidemics, estimations, node movements, controls, and encodings are some examples.

V. SECURITY REQUIREMENTS OF UAV

The security needs of UAV systems are discussed here, along with the features that make them vulnerable to attack. We define the parameters for the confidentiality of data, authentication of

access, availability of the system, integrity of the information, and dependability of conduct [38-41].

A. Data confidentiality:

Both military and civilian uses of UAVs necessitate the delivery of data. This means that no outsider may view the contents of a packet in real-time or intercept a live transmission. Data communications are vulnerable to insidious eavesdropping and grey-hole attacks. Information security measures must be robust to counter such threats.

B. Access authentication:

Preventing unauthorized users from making use of technology necessitates a reliable method of authentication. Users must present a valid identification for re-authentication after a disconnection before they can operate a UAV. Security holes in the Wi-Fi can be utilized in a de-authentication attack to take command of a UAV. De-authentication attacks from malicious actors make strong authentication at the point of access a must for defence.

C. System availability:

The authorized user must give specific instructions for the UAV system to follow in order for it to operate or gather data. The primary goal of these assaults is not information theft from UAVs, but rather disruption of their normal operations. UAVs may lose communication with ground control stations (GCS) if they encounter extreme environmental conditions such as flooding or black holes. These assaults render the UAV inoperable and, in extreme cases, can bring the aircraft crashing to the earth. Therefore, it is crucial to guarantee the UAV system's accessibility.

D. Information integrity:

Particularly important for UAV control orders is the security of data transmitted via UAVs. When adversaries tamper with sensor data, the UAV's mission is compromised due to false information, and when control orders are tampered with, the UAV may fail to perform as intended. For a security system to be effective, it must maintain the integrity of its data.

E. Behavior reliability:

During an assault, UAVs often act in unexpected ways. Flooding attacks can render the UAVs uncontrollable, while attacks on vision and GPS sensors can lead to faulty photographs or wrong geolocation data. Therefore, we ask that the UAV exhibit stable behaviour that is unaffected by noise, inaccurate information, or external factors.

VI. EMERGING TECHNOLOGIES FOR SECURE UAV COMMUNICATION

This essay will examine four of the most exciting new approaches to UAV communication that are now in use or under active investigation. Software-Defined Networking (SDN), blockchain, fog computing, and ML are at the centre of the conversation over how to keep UAV communications safe and it is depicted in Figure 5.

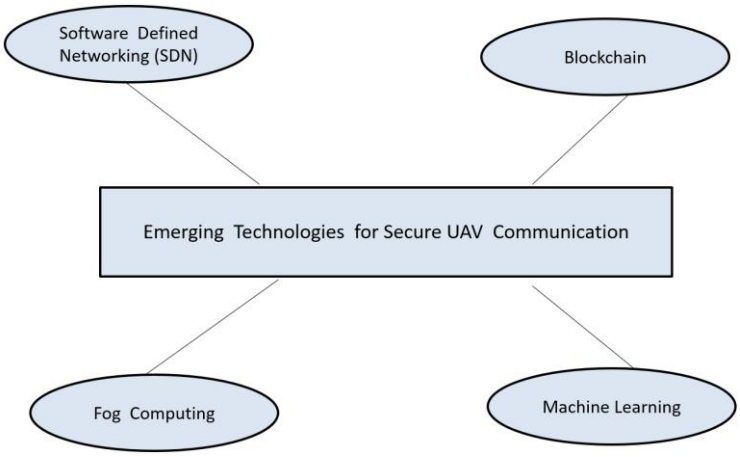

Fig. 5: Emerging Technologies of Secure UAV Communication.

A. Software-Defined Networking (SDN)

A networking architecture known as SDN allows for centralized management of software applications and network programming. Because all network components are centrally designed with SDN, consistent network administration is made easier. In a typical SDN-based UAV communication network, each UAV functions as a switch. High-level network operations are implemented via the SDN application plane, which relies on a centralized controller. The control plane, which handles data and command transmission between UAVs, resides in the CPU as well. The UAVs themselves are the data plane

since they execute the controller's directives. Various protocols and standards exist for completing specific network operations [42]. Protocols at various network layers can be implemented independently thanks to SDN's decoupling of the data and control planes. The configuration of an SDN-based network for UAV communications benefits greatly from this degree of flexibility.

In addition to boosting network reliability, centralised network control is made possible by SDN. In addition, SDN permits directly programmable network control by unbundling the data, control, and application layers. Deploying an SDN is a natural way to enhance service quality [43,44] as more and more UAV applications depend on real-time video streaming. With SDN, the controller can keep a close eye on data traffic and prevent many attacks that would otherwise be possible on a UAV despite its limited resources. The aforementioned SDN configurations improve the security of the network as a whole.

B. Blockchain

According to the study, including blockchain technology in UAV communication can boost safety by making it more difficult for unauthorized individuals to access or manipulate given data [45]. Blockchain data is dispersed over the network, making it difficult for a thief to compromise a single node and steal everything.

A continuous expansion of blocks linked together by cryptographic hash functions [46]. The importance of privacy protection, efficiency, and security in UAV-user interactions grows as UAV technology advances. Using blockchain technology to deploy real-time UAV applications is an intriguing prospect [47]. Once a transaction has been logged on the blockchain, it can't be altered by anyone else. In addition, smart contracts can be a helpful tool for ensuring that business deals are conducted in a secure and efficient manner. It is possible to construct public, private, consortium, and hybrid blockchain networks, each tailored to the specific requirements of a given use case. In addition, other consensus techniques are used across the blockchain network. UAV communications can benefit from blockchain's immutability, security, and decentralized ledger, making them more effective and affordable.

C. Fog Computing

In 2014 [48], CISCO was the pioneer in introducing the idea of fog computing. It's generally agreed that fog adds a lot of value and promise to cloud computing. Rather than being a replacement for cloud computing, fog is a strong augmentation of it. Between the edge devices and the cloud, there is an intermediary layer called the fog layer. Deploying servers to the cloud is challenging because it is both time-consuming and expensive. So, in 2014, a new idea emerged to help lessen the burden of cloud computing. Fog is a type of cloud that can be hosted in proximity to the actual endpoints. When an end device user sends a query to collect or publish data, the mobile network creates a link to the nearest fog node. Accessing and storing data in the cloud is now simple. In order to employ cloud services, you'll need a WAN connection to the internet, which is both more expensive and slower than using a LAN, like the fog does. Therefore, fog computing is incredibly useful in terms of efficiency, speed, and safety.

Fog Computing is a style of computing that allows for low-latency, high-throughput access to and processing of data [49]. An intermediary between the user's device and distant servers. Fog computing is well-suited to enhancing QoS and QoE thanks to the near-instantaneous nature of data retrieval in the fog. Fog computing can ease the burden on cloud storage while simultaneously improving data dissemination's efficacy and dependability. With a decentralized model, information is spread out amongst a number of different fog levels. Data in the fog is safer than data kept in a centralized location since no single organization possesses the complete data set. Because the flaw was identified in time, the cloud server is now immune to attacks. For these reasons [50], fog computing is a crucial technique for protecting UAV communication.

D. Machine-Learning

Without being expressly programmed, machine learning (ML) allows machines to learn from their own experiences and improve over time. ML is able to learn and predict results automatically with little to no human intervention when given the right input data. In order for ML algorithms to produce reliable results, enormous amounts of training data are necessary. Both supervised (where labels are present in the training dataset) and unsupervised (where the data is not labelled) ML algorithms have been developed [51]. Multiple ML methods can be used to protect UAV transmissions. Furthermore, ML algorithms can be used to identify UAV communication issues, with the resulting recovery strategies relayed to the UAV for safety purposes [52]. A classification system can detect DoS and other attacks that use forged or stolen data packets to disrupt a network. Intruders can be prevented by promptly determining whether or not a data packet is secure.

These various ML applications can help develop highly secure UAV communication systems.
The capacity of ML algorithms to study from training data and enhance their performance over time is a major benefit since it allows for more efficiency and precision to be achieved with little to no human interaction. Attacks such as man-in-the-middle [53] and spoofing can be mitigated with the help of ML algorithms that detect harmful UAVs in the network. These algorithms improve in intelligence and accuracy over time, leading to better and better outcomes. In addition, the models can be trained to self-diagnose and fix faults [54]. Multidimensional and heterogeneous data pose little of a challenge for ML algorithms.

VII. FUTURE DIRECTION AND OPEN CHALLENGES

Some promising areas for further study in this area are listed below.

- UAVs are constrained by a lack of resources and storage room. Security methods like blockchain require additional UAV storage and processing power to be implemented in a fleet of UAVs. If that happens, we might be able to cut back on our flying time. Additionally, while the use of blockchain for non-critical communication may be acceptable at the moment, blockchains can cause high latency for the most important things, such as location coordinates. Due to the limited capabilities of UAVs, more study is needed to enable security measures.
- Connectivity points among UAVs, ground controllers, and satellites are of particular interest to cybercriminals. If the network's gateways are compromised, it doesn't matter how secure the endpoint devices are. The security of UAV hop-in-hop-out gateways requires further study.
- Unfortunately, inter-fog sharing of resources and tasks is not possible with the current design of fog computing. Some communication hubs for UAVs (fog nodes) may have lower throughput than others. The fog nodes in such a network would be able to work together and distribute the workload. The less data that travels from fog to the cloud, the safer the system.
- Both the potential number of nodes in permission-ed networks and the potential throughput of permission-less networks are severely constrained by the current blockchain design. Diverse consensus algorithms are being developed to sustainably serve a large number of nodes or users.
- To address the issue of the controller being a singular point of malfunction in SDN topologies, multiple distributed controllers have been proposed by some studies. To guarantee secure, near-real-time communication across SDN's multiple controllers, however, more work is needed.

VIII. CONCLUSION

The UAV has advanced rapidly in recent decades. Because of their low cost, UAVs are becoming increasingly popular, but a lack of security measures has left them open to a variety of risks. The complicated nature of UAV software and hardware presents significant problems in privacy and security. In this review, we examine the security issues of UAVs by categorizing them into two classes: general and specific attacks. We specifically survey the most prevalent vulnerabilities producing potential UAV attacks in every category. Next, we'll look at the protocols used for networking and communicating with UAVs over both short and long distances. Then, we will have a lengthy discussion about the routing protocol for UAVs. We also describe the existing mitigation approaches and security requirements for UAVs in depth. For secured UAV communication, the solution architecture section discusses cutting-edge technologies including blockchain, ML, SDN, and fog computing. The survey report has examined the communication protocol and security needs for UAVs in-depth in order to provide greater insight. Finally, we outline the remaining questions that need to be answered, point out the limitations imposed by current UAV protocols, and suggest a few possibilities for future study. To better understand how to construct and develop safe UAV systems, the research community ought to use our survey.

REFERENCES

1. Fahlstrom, Paul G., Thomas J. Gleason, and Mohammad H. Sadraey. Introduction to UAV systems. John Wiley & Sons, 2022.
2. Li, Jun, Yifeng Zhou, and Louise Lamont. "Communication architectures and protocols for networking unmanned aerial vehicles." In 2013 IEEE Globecom Workshops (GC Wkshps), pp. 1415-1420. IEEE, 2013.
3. Marty, Joseph A. Vulnerability analysis of the mavlink protocol for command and control of unmanned aircraft. Air Force Institute of Technology Wright-Patterson AFB Oh Graduate School of Engineering And Management, 2013.
4. Konert, Anna, and Tomasz Balcerzak. "Military autonomous drones (UAVs)-from fantasy to reality. Legal and Ethical

implications." Transportation research procedia 59 (2021): 292-299.
5. Puri, Anuj. "A survey of unmanned aerial vehicles (UAV) for traffic surveillance." Department of computer science and engineering, University of South Florida (2005): 1-29.
6. De Biasio, Martin, Thomas Arnold, Raimund Leitner, Gerald McGunnigle, and Richard Meester. "UAV-based environmental monitoring using multi-spectral imaging." In Airborne Intelligence, Surveillance, Reconnaissance (ISR) Systems and Applications VII, vol. 7668, pp. 331-337. SPIE, 2010.
7. Erdelj, Milan, and Enrico Natalizio. "UAV-assisted disaster management: Applications and open issues." In 2016 international conference on computing, networking and communications (ICNC), pp. 1-5. IEEE, 2016.
8. Yinka-Banjo, Chika, and Olasupo Ajayi. "Sky-farmers: Applications of unmanned aerial vehicles (UAV) in agriculture." Autonomous vehicles (2019): 107-128.
9. Kim, Si Jung, Yunhwan Jeong, Sujin Park, Kihyun Ryu, and Gyuhwan Oh. "A survey of drone use for entertainment and AVR (augmented and virtual reality)." Augmented Reality and Virtual Reality: Empowering Human, Place and Business (2018): 339-352.
10. Naidoo, Yogianandh, Riaan Stopforth, and Glen Bright. "Development of an UAV for search & rescue applications." In IEEE Africon'11, pp. 1-6. IEEE, 2011.
11. Khan, Navid Ali, Noor Zaman Jhanjhi, Sarfraz Nawaz Brohi, and Anand Nayyar. "Emerging use of UAV's: secure communication protocol issues and challenges." In Drones in smart-cities, pp. 37-55. Elsevier, 2020.
12. Al-Turjman, Fadi. "A novel approach for drones positioning in mission critical applications." Transactions on Emerging Telecommunications Technologies 33, no. 3 (2022): e3603.
13. Kim, Alan, Brandon Wampler, James Goppert, Inseok Hwang, and Hal Aldridge. "Cyber attack vulnerabilities analysis for unmanned aerial vehicles." In Infotech@ Aerospace 2012, p. 2438. 2012.
14. Davidson, Drew, Hao Wu, Robert Jellinek, Vikas Singh, and Thomas Ristenpart. "Controlling UAVs with Sensor Input Spoofing Attacks." In WOOT. 2016.
15. Chen, Chin-Ling, Yong-Yuan Deng, Wei Weng, Chi-Hua Chen, Yi-Jui Chiu, and Chih-Ming Wu. "A traceable and privacy-preserving authentication for UAV communication control system." Electronics 9, no. 1 (2020): 62.
16. Bunse, Christian, and Sebastian Plotz. "Security analysis of drone communication protocols." In Engineering Secure Software and Systems: 10th International Symposium, ESSoS 2018, Paris, France, June 26-27, 2018, Proceedings 10, pp. 96-107. Springer International Publishing, 2018.
17. Khan, Muhammad Asghar, Ijaz Mansoor Qureshi, and Fahimullah Khanzada. "A hybrid communication scheme for efficient and low-cost deployment of future flying ad-hoc network (FANET)." Drones 3, no. 1 (2019): 16.
18. Bluetooth Core Specification, Bluetooth Special Interest Group (SIG). 2016. Available online: https://www.bluetooth.com/specifications/bluetooth-core-specification (accessed on 6 October 2018)
19. Cheng, Chen-Mou, Pai-Hsiang Hsiao, H. T. Kung, and Dario Vlah. "Performance measurement of 802.11 a wireless links from UAV to ground nodes with various antenna orientations." In Proceedings of 15th International Conference on Computer Communications and Networks, pp. 303-308. IEEE, 2006.
20. Safaric, Stanislav, and Kresimir Malaric. "ZigBee wireless standard." In Proceedings ELMAR 2006, pp. 259-262. IEEE, 2006.
21. Banerji, Sourangsu, and Rahul Singha Chowdhury. "Wi-Fi & WiMAX: A Comparative Study." arXiv preprint arXiv: 1302.2247 (2013).
22. Dalmasso, Ilaria, Irene Galletti, Romeo Giuliano, and Franco Mazzenga. "WiMAX networks for emergency management based on UAVs." In 2012 IEEE first AESS European conference on satellite telecommunications (ESTEL), pp. 1-6. IEEE, 2012.
23. Jiang, D., and G. Liu. "An Overview of 5G Requirements. 5G Mobile Communications; Xiang, W.; Zheng, K.; Shen, X." (2017): 3-26.
24. Saad, Walid, Mehdi Bennis, and Mingzhe Chen. "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems." IEEE network 34, no. 3 (2019): 134-142.
25. Aggarwal, Shubhani, Neeraj Kumar, and Sudeep Tanwar. "Blockchain-envisioned UAV communication using 6G networks: Open issues, use cases, and future directions."

IEEE Internet of Things Journal 8, no. 7 (2020): 5416-5441.
26. Shamsoshoara, Alireza, Mehrdad Khaledi, Fatemeh Afghah, Abolfazl Razi, and Jonathan Ashdown. "Distributed cooperative spectrum sharing in uav networks using multi-agent reinforcement learning." In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 1-6. IEEE, 2019.
27. Ashraf, E., A. F. Hossam, and S. Hassanein. "Routing schemes for DTN-an applications perspective." Telecommunications Research Lab (TRL) School of Computing Queen's University Kingston, Ontario, Canada Technical Report (2012).
28. Cardei, Ionut, Cong Liu, and Jie Wu. "Routing in wireless networks with intermittent connectivity." Encyclopedia of Wireless and Mobile Communications (2007): 1-23.
29. Pu, Cong. "Jamming-resilient multipath routing protocol for flying ad hoc networks." IEEE Access 6 (2018): 68472-68486.
30. Zheng, Xueli, Qian Qi, Qingwen Wang, and Yongqiang Li. "An adaptive density-based routing protocol for flying Ad Hoc networks." In AIP Conference Proceedings, vol. 1890, no. 1, p. 040113. AIP Publishing LLC, 2017.
31. Lin, Lin, Qibo Sun, Shangguang Wang, and Fangchun Yang. "A geographic mobility prediction routing protocol for ad hoc UAV network." In 2012 IEEE Globecom Workshops, pp. 1597-1602. IEEE, 2012.
32. Hong, Jie, and Dehai Zhang. "TARCS: A topology change aware-based routing protocol choosing scheme of FANETs." Electronics 8, no. 3 (2019): 274.
33. Hussen, Hassen Redwan, Sung-Chan Choi, Jong-Hong Park, and Jaeho Kim. "Performance analysis of MANET routing protocols for UAV communications." In 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 70-72. IEEE, 2018.
34. Arafat, Muhammad Yeasir, Md Arafat Habib, and Sangman Moh. "Routing protocols for UAV-aided wireless sensor networks." Applied Sciences 10, no. 12 (2020): 4077.
35. Oubbati, Omar Sami, Abderrahmane Lakas, Fen Zhou, Mesut Güneş, and Mohamed Bachir Yagoubi. "A survey on position-based routing protocols for Flying Ad hoc Networks (FANETs)." Vehicular Communications 10 (2017): 29-56.
36. Ben Amarat, Samia, and Peng Zong. "3D path planning, routing algorithms and routing protocols for unmanned air vehicles: A review." Aircraft engineering and aerospace technology 91, no. 9 (2019): 1245-1255.
37. Cardei, Ionut, Cong Liu, and Jie Wu. "Routing in wireless networks with intermittent connectivity." Encyclopedia of Wireless and Mobile Communications (2007): 1-23.
38. Constantinides, Chris, and Paul Parkinson. "Security challenges in UAV development." In 2008 IEEE/AIAA 27th Digital Avionics Systems Conference, pp. 1-C. IEEE, 2008.
39. Haque, Md Samsul, and Morshed U. Chowdhury. "A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV)." In Security and Privacy in Communication Networks: SecureComm 2017 International Workshops, ATCS and SePrIoT, Niagara Falls, ON, Canada, October 22–25, 2017, Proceedings 13, pp. 113-122. Springer International Publishing, 2018.
40. Rodrigues, Mariana, Jean Amaro, Fernando Santos Osório, and Branco Kalinka RLJC. "Authentication methods for UAV communication." In 2019 IEEE Symposium on Computers and Communications (ISCC), pp. 1210-1215. IEEE, 2019.
41. Wang, Li, Yu Chen, Pu Wang, and Zheng Yan. "Security threats and countermeasures of unmanned aerial vehicle communications." IEEE Communications Standards Magazine 5, no. 4 (2021): 41-47.
42. Huang, Dijiang, Ankur Chowdhary, and Sandeep Pisharody. Software-Defined networking and security: from theory to practice. CRC Press, 2018.
43. McCoy, James, and Danda B. Rawat. "Software-defined networking for unmanned aerial vehicular networking and security: A survey." Electronics 8, no. 12 (2019): 1468.
44. Mertens, J. S., G. M. Milotta, P. Nagaradjane, and Giacomo Morabito. "SDN-(UAV) ISE: Applying software defined networking to wireless sensor networks with data mules." In 2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), pp. 323-328. IEEE, 2020.
45. Chamola, Vinay, Vikas Hassija, Vatsal Gupta, and Mohsen Guizani. "A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact." Ieee access 8 (2020): 90225-90265.
46. Zhang, Rui, Rui Xue, and Ling Liu. "Security and privacy on blockchain." ACM Computing Surveys (CSUR) 52, no. 3 (2019): 1-34.

47. Alladi, Tejasvi, Vinay Chamola, Nishad Sahu, and Mohsen Guizani. "Applications of blockchain in unmanned aerial vehicles: A review." Vehicular Communications 23 (2020): 100249.
48. F. Stroud, "Fog computing," https://www.webopedia.com/TERM/F/ fog-computing.html, online; accessed on 18 october 2019.
49. Peng, Mugen, Shi Yan, Kecheng Zhang, and Chonggang Wang. "Fog-computing-based radio access networks: Issues and challenges." Ieee Network 30, no. 4 (2016): 46-53.
50. Tan, Zhenjie, Hua Qu, Jihong Zhao, Shiyu Zhou, and Wenjie Wang. "UAV-aided edge/fog computing in smart IoT community for social augmented reality." IEEE Internet of Things Journal 7, no. 6 (2020): 4872-4884.
51. Bithas, Petros S., Emmanouel T. Michailidis, Nikolaos Nomikos, Demosthenes Vouyioukas, and Athanasios G. Kanatas. "A survey on machine-learning techniques for UAV-based communications." Sensors 19, no. 23 (2019): 5170.
52. Challita, Ursula, Aidin Ferdowsi, Mingzhe Chen, and Walid Saad. "Machine learning for wireless connectivity and security of cellular-connected UAVs." IEEE Wireless Communications 26, no. 1 (2019): 28-35.
53. Sarker, Iqbal H. "Machine learning: Algorithms, real-world applications and research directions." SN computer science 2, no. 3 (2021): 160.
54. Waheed, Nazar, Xiangjian He, Muhammad Ikram, Muhammad Usman, Saad Sajid Hashmi, and Muhammad Usman. "Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures." ACM Computing Surveys (CSUR) 53, no. 6 (2020): 1-37.