DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

Survey of UAV Security Authentication and Cryptography Protocols

Manar H. Abed[1], Shatha H. Jafer[2], Soukaena H. Hashem[3]
[1,2,3] Computer Science Department, University of Technology, Bagdad, Iraq
[1]Nawarahasan79@gmail.com, [2] Shatha.h.jafer@uotechnology.edu.iq,
[3] Soukaena.h.hashem @uotechnology.edu.iq

Abstract— *Unmanned aerial vehicles, or UAVs, are gaining significant attention because of the strategic and financial information and value involved in aerial applications, as well as the sensitive data collected through embedded sensors. UAVs are rapidly developing in various fields and find widespread utility in military applications for effective target tracking, battlefield surveillance, radiation monitoring, and sports. UAVs are useful and advantageous, but they can also be attacked by a variety of techniques, including jamming, fuzzing, false data injection, and zero attacks. Researchers were looking on robust security mechanisms to protect UAVs from attackers in order to combat such security risks. However, there is a large number of vulnerabilities in designed protocols that hackers could take advantage of. For the identification and addressing of those vulnerabilities and weaknesses, it is becoming highly important to study and analyze current security protocols that are used in the UAVs. In this study, a thorough survey will be introduced on authentication and cryptography that are used in the UAV protocols, as well as describing architecture, procedure, and security of Micro Aerial Vehicle Link (MavLink) protocol. We will explain as well the cryptography and authentication approach that has been developed by the use of the MavLink protocol.*

Index Terms— *UAV, Unmanned Aerial Vehicles, MavLink, Zero attack.*

I. INTRODUCTION

Drones, which are also referred to as the UAVs, are used for various purposes, which include recreation, aerial surveillance, and military operations. They could operate both without and with a human pilot and could be controlled remotely over wireless networks like radio or Wi-Fi. UAVs could include other flying objects like quadcopters and gliders [1]. UAVs could function autonomously or collaborate to establish a network. The number of UAVs utilized as well as their travel distances vary substantially based on the type of application. Yet, we need several UAVs positioned effectively for monitoring areas affected by disasters. Since numerous networked drones may do tasks which a single drone cannot, using multiple drones is commonly favored. UAV networks are often ad hoc wireless networks which enable communication between UAVs and/or between UAVs and the ground. They give critical information for disaster aid, environmental monitoring, recovery and rescue operations, and emergency. Because the majority of IoT-based networks depend on wireless communication and have severe resource constraints, they need specialized security solutions. Additionally, because they lack the resources to install any durable hardware form to guard against wireless medium infiltration, UAVs depend only on wireless communication. They operate in dangerous areas, which increases the possibility that the assailant will also physically catch them. The attacker might access the secret keys stored in device memory and initiate numerous attacks on the UAV networks [2]. It was demonstrated that the current standard primitives and cryptographic protocols are ineffective with regard to time consumption and energy for small aerial drones which run on

Received 04/February/2024; Accepted 23/April/2024

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

microprocessors with limited resources, despite the fact that they could be used to deliver basic security services. As a result, it is now clear that the only practical ways to offer security services like authentication, confidentiality, and integrity are through lightweight protocols. UAVs must also be equipped with tamper-resistant features which impose authenticated policies and are unchangeable. In the event that an adversary tries to probe or manipulate the circuit, this will permanently change the small physical differences in integrated circuit, which must stop sensitive data from regenerating, including secure session keys [3]. UAV and the GCS often interact via a variety of protocols, including UAVCan, MavLink, and UranusLink. Of such protocols, MavLink is the most popular and extensively utilized, and it is supported by numerous UAVs as well as the ground station [4]. MavLink protocol, which is utilized as communication protocol between GCS and UAV, will be the only subject of this study. The work is structured as follows. The definition and design of MavLink protocol, together with security requirements and associated threats, are covered in the section that follows. In Section III, various methods for UAV security, including authentication and encryption, were reviewed and listed. Section IV the discussion is produced. The study is concluded in section V.

II. MAVLINK COMMINATION PROTOCOLS

A. Commination Requirement

This protocol was first created by Lorenz Meier in the year 2009 under a GPL license. UAV and GCS can communicate back and forth thanks to MavLink. UAV transmits telemetry as well as other status data to GCS, whereas GCS receives commands and control messages from UAV. Moreover, MavLink is used for linking UAVs via the internet. Various UAVs and a number of autopilot systems, including PX4 and Ardupilot, which are open-source and the best autopilots for controlling any kind of unmanned vehicle, even unmanned submarines, support the MavLink protocol. MavLink is specified as a lightweight, cross-platform networking protocol that is available as open source. There are three versions available: MavLink 1.0 and 2.0 [5, 6], and a prototype version that is called sMavLink. Timestamped hash-based message authentication codes (HMAC) were employed in MavLink 2.0 for authentication and integrity. The platform-independent serialization regarding system states' messages and commands that are necessary for them to execute in a specific binary format characterizes MavLink's structure as a Marshaling library. In comparison with other serialization techniques, such as JSON and XML, MavLink's binary serialization method is lightweight and has minimal overhead. sMavLink draft version is specified as a stable version that uses symmetric key authenticated encryption of pertinent details to guarantee integrity and confidentiality. As far as we are aware, sMavLink has not yet been put into practice. Also, because of its Binary Serialization characteristics, MavLink messages are often small and may be sent across a variety of wireless networks, such as WiFi or even serial telemetric systems with low data rates. The packet header's message accuracy and durability are ensured by double checksum verification. Those features make the MavLink protocol the most common amongst its peers for unmanned system-to-GCS communication. MavLink communication protocol, although robust and extensively utilized, is susceptible to many security breaches, including DDoS attacks, man-in-the-middle attacks, and eavesdropping, due to its absence of a subtle security mechanism. Since the MavLink protocol doesn’t encrypt communication messages, such vulnerabilities are readily visible. This indicates that an unencrypted channel is being used for binary communications between GCS and UAV, leaving it vulnerable to various security threats. hence jeopardizing UAV security [4].

Received 04/February/2024; Accepted 23/April/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

B. MavLink Protocol (MavLink System Architecture)

There are 2 types of MavLink messages, which are: (a) commands and control messages transferred from the GCS to UAV, (b) state information messages (such as, heartbeat, position, and system status information) sent from the UAV to the GCS. *Fig. 1* illustrates MavLink 2.0 packet structure. MavLink protocol is intended to be light-weight due to the fact that it is utilized for real-time communications [7].

STX	LEN	INC FLAGS	CMP ID	SE Q	SYS ID	COMP ID	MSG ID 3Bytes	PAYLOAD (0-255) Bytes	CHECKSUM 2Bytes	SIGNATURE 13Bytes

FIG. 1. MAVLINK 2.0 PACKET STRUCTURE.

Early in 2017[8], MavLink 2.0 has been released, and it represents the most recent version which is advised. It is backwards compatible with the MavLink 1.0 and has significant enhancements over that version. Table I explanation of MavLink 2.0 frame acronyms along with its contents.

TABLE I. MAVLINK 2.0 FRAME ACRONYMS AND ITS CONTENTS

Acronyms	Contents	Description
STX	OXEF	Describe start of the frame
SEQ	0 - 255	Used to represent packet Sequence
LEN	0 - 255	Payload Length
COMP	0 - 255	This field to knowing which component sending the message
SYS	1 - 255	This value represents unmanned system ID
Payload	0- 255 1- bytes	Contain the real data which depend on the type of message
MSG	0 - 255	Describe message type
CKA and CKB (CRC) or checksum	2bytes content	This field (CKA, CKB) knowing as checksum

MavLink 2.0 employs a 13-byte optional Signature field to make sure the link cannot be tampered with. The ability to authenticate messages and confirm that they come from a reliable source greatly enhances the security features of MavLink 1.0. In the event that incompatibility flags are set to 0×01, the message signature is attached. The next fields are contained in the 13bytes of message signature:

• LinkID is a single byte which serves as a representation of the link (or channel) that the packet was sent over. Wi-Fi and telemetry links and channels could be mixed. Each data transmission channel ought to have a unique LinkID. It offers a way to use MavLink 2.0 for multi-channel unmanned system control.

• Since January 1, 2015 GMT, the timestamp has been encoded with six bytes every ten microseconds. With each communication delivered over the channel, it rises. Every stream that has its definition defined by tuple (SystemID, ComponentID, LinkID) is subject to it. The timestamp serves as a defense against replay attacks.

Received 04/February/2024; Accepted 23/April/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

- The entire message, the secret key, and the time-stamp are used to compute the 6-byte signature for the message. The first 6bytes (48bits) of SHA-256 hash applied to the MavLink 2.0 message—which does not include the signature—are included in the signature. The ground station and autopilot, or MavLink API, store a shared symmetric key consisting of 32bytes, which is the secret key.

Processing incoming MavLink messages is affected by MavLink 2.0 message signature. In the case when a message is signed, after that it is discarded if (a) the received message timestamp is older than previous packet that is received from same stream that is identified by the tuple (SystemID,ComponentID, LinkID), (b) the calculated signature at reception differs from the signature appended to the message. This could suggest that (c) the timestamp differed by more than a minute from the local system's timestamp, or that there was a change in the message. The rejection or acceptance of the packet is implementation-specific if the message is not signed [8]

C. Security Requirements for MavLink

In general, a lot of study was done on the security regarding unmanned aerial systems; however, less was done on the security of communication at the communication level, specifically with regard to MavLink protocol. The phrase "prevention is better than cure" is a medical one, and it fits the security requirements the best. It is crucial to comprehend security requirements and steer clear of such undesirable circumstances in order to prevent security dangers and attacks. To safeguard communication between GCS and UAV and avert threats, the MavLink needs to be secure in terms of integrity, confidentiality, authentication, non-repudiation, availability, privacy, and authorization. The security requirements for MavLink are shown in *Fig. 2* below [4].

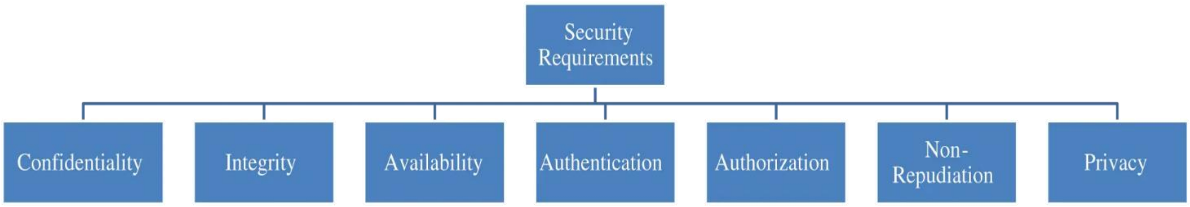

FIG. 2. MAVLINK SECURITY REQUIREMENTS.

D. Security Threats on MavLink

With the aid of the communication protocol, GCS and UAV are able to communicate via a wireless channel. Since Mavlink protocol lacks established security protocols, this communication is susceptible to security breaches. Checking whether the packet is valid and originates from legitimate source is the only security measure. Confidentiality and the other criteria of security aren't natively supported. The messages are neither encrypted by Mavlink, nor does it include a covert security feature, which indicates that there is a high security breach risk in communication between GCS and UAV. Any attacker or hacker could intercept communication and communicate with UAV if they have the right transmitter device. This vulnerability could be used by the attacker for their intended purpose, like taking full control of the UAV or inserting false commands into an already-running operation. Additionally, such attacks are categorized as follows [4] based on how they turn out. Table II has the classification.

Received 04/February/2024; Accepted 23/April/2024

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

TABLE II. SECURITY THREATS TO MAVLINK PROTOCOL

Security requirement	Threat	Mitigation
Confidentiality and Privacy	Intercepption Man in the Middle Identity spoofing Unauthorized Paccess Evesdroping Hijacking	Datalink encryption
Availibilty	Routing attack Command and control Jamming Flooding Denial of service	Authinication
Integrity	Packet injection Fabrication Man in the Middle Message deletion Replay attack Message modification	Hash MAC(MessageAuthinication Code) Authinication
Authenticity	Fabrication Gcs Spoofing	Authinication

Agreement protocol was initially performed between the UAV and GCS. A shared secret key is generated and agreed upon amongst participants during this step (GCS-UAV).

The comparative overview which summarizes the key differences among proposed protocols in section II is displayed in Table III below.

TABLE III. COMPASSION BETWEEN DIFFERENT PROTOCOLS

Schemes	Feature	Weakness	Strength
[4] 2021	Clarify MavLink communication requirements and security threat	Dont mentioned MavLink architecture	Define attack type
[5] 2017	Explain the MavLink packet structure and analyze network latency and data loss	Explain MavLink packet structure only no frame acronyms	Communication requirements, of the MavLink protocol has been analyzed
[6] 2015	Explain MavLink versions	Not mentioned communication requirement and security Threat	Explain MavLink development stage
[7] 2019	Define packet structure and frame acronyms of MavLink 2.0	Not mentioned MavLink packet structure of different versions of the MavLink protocol	Summarize MavLink 2.0 packet structure

III. UAV SECURITY

A. Security of Communication

Typically, UranusLink, MavLink, and UAVCAN are the communication protocols used for exchanges between GCS and UAVs. Messages are transferred using such protocols while GCS are in communication. There is a possibility that most security procedures in place were not meant for cases like this. They either don't utilize the resources efficiently or don't provide measures of safety when utilizing such communication platforms. MavLink is the most commonly utilized and popular protocol among these for GCS-UAV communication. Security is even more of a concern due to the unmanned nature of UAVs and remote wireless communication. The concerned UAVs are more likely to lose their communication paths in the case when attackers take over the cellular base stations. In addition, they could encounter serious interference issues when using the line-of-sight (LOS) links [9], so in situations where there is an open wireless communication channel, UAV communication security is highly necessary. UAVs have susceptibility to a wide range of cyberattacks, which try to undermine data and infrastructure privacy and integrity. Data in communication between GCS and UAV is vulnerable to

Received 04/February/2024; Accepted 23/April/2024

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

eavesdropping and keylogging attacks; different methods for securing UAV communication are shown in *Fig. 3*.

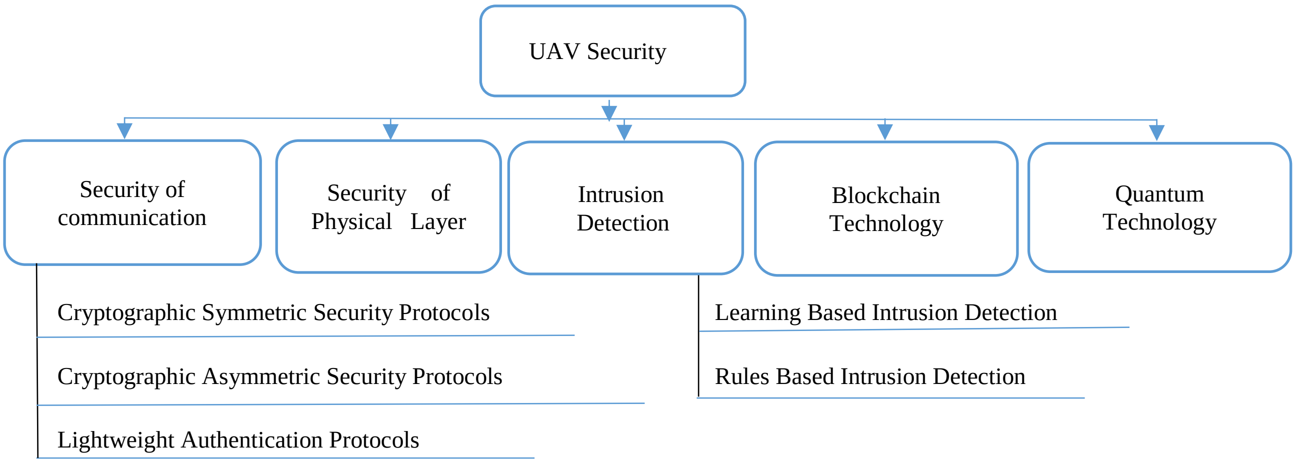

FIG. 3. VARIOUS TECHNIQUE TO SECURE UAV COMMUNICATION [10][11].

1. Cryptographic symmetric security protocols

Cryptographic protocols are widely utilized to assure integrity, availability, and confidentiality. Specifically, sensitive data including images, text, video, and audio are safeguarded via symmetric protocols. The receiver and transmitter need to have the same key so as to access original data when using symmetric security protocols, where the same key is utilized for encryption as well as decryption. Symmetric security mechanisms, such as (One Time Pad) or OTP, are frequently employed to safeguard transmissions. OTP needs the key size to match the data size for securing data. For instance, regarding images, the key needs to be $M \times N$, or the length of original image, in the case when the image has N columns and M rows of pixels. OTP encryption has been utilized in [12] to improve wireless communication MAV link security. Data transmission security is achieved by using an encryption-decryption function. There are numerous commands for controlling UAVs, like takeoff command, start UAV, and autopilot enable. Each of these commands is expressed as a bit, which has two possible values: 0 and 1. The many bits could be combined to produce a long text that could be encrypted and secured. Table III displays the most recent symmetric security protocols.

2. Cryptographic asymmetric security protocols

Asymmetric security protocols employ different keys. The private key is the other; one is the public key. With the use of private key and public key, respectively, the user at receiver and transmitter ends decrypts and encrypts data. Since information cannot be decrypted with the use of the same public key which has been utilized for encrypting it, the public key does not need to be kept secret. Public key cannot be utilized to obtain the data; instead, a secret (private) key needs to be utilized. The comparison between several cryptographic protocols is displayed in Table IV below.

TABLE IV. COMPASSION BETWEEN DIFFERENT CRYPTOGRAPHIC PROTOCOLS

Schemes	Cryptographic Type	Algorithm	Technique	Feature	Vulnerabilities
[13]2019	Symmetric	Lorenz Dynamic chaotic system	Data security protocols	More randomness	Insecure Because of absence of confusion part
[12]2015	Symmetric	one-time-pad encryption technique	OTP of securing communication link	Secure due to large key size	Required more bandwidth

Received 04/February/2024; Accepted 23/April/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

[14]2020	Asymmetric	successive convex flying trajectory	Convex Optimization	Improve The trajectory, decrease over heading,tr ansmitpo were simuleneously	Take more time to find system converges
[17]2019	Asymmetric	Atrust-based security mechanism	Trust based protocols For UAV and sensors	Authentic -iteto decide whether ornot sensors, are trusted	Packet sent as in original form which may be fabricated or stolen
[16]2017	Asymmetric	AES public key and random values based on time information	Authentication schema	Protecting Informati on even after attacking	High bandwidth,c ost,processing time when sending large data
[15]2013	Asymmetric	Diffie Hellman key exchange	Public key exchange protocols	Node Communi cate just after authentication process	Only one random number is chosen as public key

3. UAV Authentication Technique

The authentication process relates to message authentication as well as UAV-GCS authentication. Node authentication mandates the formation of network connections between registered and trusted UAV-GCS, the provision of access to network resources, and the confirmation of a UAV's identity. Successfully authenticating valid nodes keeps away unauthorized ones, maintaining privacy and security [18].

3.1 Authentication Obstacles in UAVs

One important component of the UAV network is authentication. The majority of eavesdroppers employ fake information to take control of UAVs. This fake information manifests itself as signals like GPS and Wi-Fi signals. UAVs are often distracted by spoofing methods. Furthermore, authentication plays a critical role in determining which signal the UAVs are receiving correctly. Scholars are working hard to investigate this field of study. Even though numerous information authentication procedures were put out, the current works still want improvement. For example, a single random integer is utilized for the authentication in several of the current authentication methods. Using a brute force attack, it is simple to predict a single random number. Thus, to create distinct random numbers, chaotic maps with a suitable key should be utilized rather than a single random number. More random numbers as well as more random substitution boxes cannot be generated by less dimensional chaos. High-dimensional chaotic maps, like the hyperchaotic map, could be used to address the problem of producing random numbers [1].

3.2 Lightweight authentication protocols for UAV

With the use of lightweight authentication and encryption mechanisms is another technique to keep sensitive information hidden from hackers. It could be possible to encode the data faster by using such lightweight techniques. Additionally, it uses less software memory, which enables UAV to operate more quickly. Table V illustrates the level of compassion among various authentication techniques.

Received 04/February/2024; Accepted 23/April/2024

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

TABLE V. THE COMPASSION BETWEEN DIFFERENT AUTHENTICATION TECHNIQUE

Schemes	Algorithm	Feature	Light weight Authentication	Mutual Authentication	MAVLINK Protocol
[18] Gada Emad	D-GIFT,D-hash,lightweight digital signature	Vulnerable to different security attacks like Eavesdropping, DDoS and GPS Spoofing.	√	√	√
[19] Anthony Demeri et al.	Elliptic curve Diffie-Hellman, Advanced Encryption Standard	Component are incorporated by using extensible and moldable APIs	√		
[20]jian Wang et al.	Block chain	Provide support for 5G network	√	√	√
[21] Cong Pu et al.	Duffing map	Using challenge response pair of Physical unclonable function p	√	√	√
[22] Hani M.Ismael et al.	Chaotic map, HIGHT	Minimize computational lower consumption	√	√	√

B. Security of Physical Layer

Secrecy rate [23] represents a widely utilized parameter of performance in physical layer security architecture, which indicates how securely information may be transmitted. To obtain highest secrecy rate regarding transmitted data between the two separate nodes, physical layer security, or PLS, is often utilized. It is, necessary for all communication and security equipment installed in UAV. PLS, in contrast to traditional cryptographic security techniques, leverages cellular channel properties, like interference, noise, and fading to increase legitimate receiver's signal reception at the same time as decreasing the eavesdropper's received signal quality [24], [25]. Although there are several cryptographic security methods available that offer a high level of security, no framework exists that delivers perfect security. PLS is thus receiving a lot of attention. For enhancing and maximizing the secrecy rate regarding wireless communication in UAVs, various studies were suggested on PLS [26–28]. Static relay-based communication systems have been used in the last few decades to enhance PLS schemes that are currently in use. UAV-enabled mobile relaying is a new type of depending approach that gained value due to the exciting advancements in autonomous vehicles. The authors of [29] have suggested a better PLS technique that takes advantage of the mobility reliance that is afforded by UAVs. Buffer-aided mobile relay that enables data to arrive in a more independent and quick manner and is helpful for the real-time applications, is used to increase the security of communication systems.

C. Intrusion Detection in UAV

Real-time network traffic analysis is necessary for the identification of intrusions targeting UAVs throughout a flight mission. By putting in place an intrusion detection system (IDS), UAVs can identify several types of intrusions, including routing attacks, malware, signal modification, and message forging [63]. Determining attack patterns also heavily depends on the creation of anomaly detection frameworks for monitoring malicious attacks. In addition, implementing honeypots and honeynets in conjunction with the IDS could aid in safeguarding the flight mission against malicious entities. Since UAV networks are intricate systems made up of many parts, in order to improve performance, intrusion detection techniques must take into account a variety of information-gathering sources. There are two different kinds of intrusion detection: learning-based intrusion detection, UAVs

Received 04/February/2024; Accepted 23/April/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

could use learning-based approaches to identify intrusions using pattern recognition. Once taught, the UAV can identify the pattern of the incursion; rules-based intrusion detection is the second method. When it comes to UAVs, distinct rules are programmed into the device's chip for every task, along with acceptability thresholds for each regulation. Table VI emphasize the most recent studies on various intrusion detection methods.

TABLE VI. INTRUSION DETECTION TECHNIQUE

Schema	Type of Intrusion Detection	Technique	Advantage	Disadvantage
[28]2018	Learning based	Deep reainforcment learning	Estimate power of jamming signal	High Error rate and time
[32]2020	Learning based	Attack detection schema	Fast process	Feature selected are least because of compromised accuracy
[33]2018	Rules based	Intrusion detection	Reduce the number of false Negative prediction detection, defend UAV by false information injected	High number of rules because of high time to decision made by the UAV
[34]2017	Rules based	Intrusion detection, malicious node ejection	Using Bayesian game technique	More round is needed if positive rate increase

D. Blockchain Technology

A variety of cyberattacks, which include eavesdropping, masquerade, jamming, linking, fabrication, and access control attacks, can target centralized solutions. The blockchain (BC) is a significant solution for the previously described problems. It is a collection of blocks linked together by the preceding block's hash [35]. A blockchain-based architecture that is referred to as BHEALTH was suggested by [36] as a way to secure UAV-based healthcare systems. After that, a blockchain-based Healthcare 4.0 architecture with UAV path planning has been described by Aggarwal et al. [37]. The suggested architecture offers secure data transmission while defending private medical records against online threats. Table VII presents a comparative study of the state-of-the-art approach that is currently in use for secure UAV communications with blockchain technology.

TABLE VII. COMPARATIVE ANALYSIS OF SECURE UAV COMMUNICATIONS USING BLOCKCHAIN TECHNOLOGY

Application	Security Algorithm	Objective	Results
Semi-autonomous UAVs [40]	UAVNet Cybersecurity threats	secure and operatea network of semi-autonomous Unmanned Aerial Vehicles	POG Consensus algorithm utilizes UAV group partitioning
Healthcare [36]	Classic algorithm	For securing UAV-based Health-care system using blockchain that is referred to as BHEALTH	
Networked Swarms of UAVs [41]	Immutable Ledger technology	Blockchain Technology for Networked UAV Swarms	Developers will be capable of designing trustworthy UAV systems

Received 04/February/2024; Accepted 23/April/2024

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

UAV communication [39]	Blockchain	Presented a blockchain-based decentralized andsecure architecture for the mitigation of the cyberattacks	SDN-based secure UAV nrtwork management
Blockchain Military [38]	Blockchain	Presented blockchain technologyrole in prospects of military applications	It is a survey of blockchain benefit in military applications
Healthcare [37]	Blockchain base	UAV Path Planning for Health-care 4.0	Architecture offers data transfer approach and protecting sensitive health-care information
Military [42]	Blockchain	Blockchains and UAV-assisted secure communications for military applications	Prevention of cyberattacks in Internet of military things networks

E. Quantum Cryptography-as-a-Service

A method of performing cryptographic operations that utilizes the quantum mechanical phenomenon is called quantum cryptography. A perfect quantum cryptography method that addressed the exchange key problem while maintaining data security was quantum key distribution. Cryptography is the study of applying quantum mechanical concepts to security concerns. The most popular type of cryptography is quantum cryptography [43], which takes advantage of quantum key distribution and provides information-theoretically safe solutions to the underlying exchange problems. Quantum cryptography in UAV communication. Because of their increased mobility, drones are being used more frequently, which has created a research need for safe cryptography for drone-to-drone and drone-to-ground station communication. Conventional cryptography has its shortcomings in terms of communication security. Here, quantum cryptography could perform more effectively. Quantum cryptography needs to be implemented to support applications where drone data collecting is a vital resource. Utilize the features of quantum cryptography and networks that go beyond 5G [11] to increase the security of drone communications and the data being transferred. Specifically, it contained BB84, a quantum cryptography algorithm that differs from the currently used classical cryptography methods and is extremely safe. The unique architecture that this research proposes improvising for UAV-to-GCS and UAV-to-UAV communications is at the core of it.

IV. DISCUSSION

We produce the comparison of the current survey with the existing survey and review papers by using many categories and sub-categories like Secure communication and sub-categories (Symmetric security protocol, Asymmetric security protocol), Intrusion detection system and sub-categories (learning-based, Rules-based) and UAV network and sub-categories (Wireless,5G,6G) and many other parameters as shown in Table VIII.

Received 04/February/2024; Accepted 23/April/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

TABLE VIII. COMPARISONS OF CURRENT SURVEY WITH THE EXISTING SURVEY AND REVIEW PAPER

Categories	Sub-categories	Arslan et al. [1]	Yass Ine et al. [31]	Alaa et al. [45]	KhaN et al. [44]	J. Mc Coy et al. [46]	Current survey
Secure communication	Symmetric security protocol	√		√	√		√
	Asymmetric security protocol	√		√	√		√
	Authenticati on protocol	√			√	√	√
Intrusion detection system	Learning based	√	√			√	√
	Rule based	√	√			√	√
Security requirement			√				√
Security threat			√	√	√	√	√
Block chain technology							√
Quantum technology							√
UAV network	Wireless	√	√	√	√		√
	5G						√
	6G						√
MavLink security	Vulnerabilities	√					√
	Security mechisim	√		√	√	√	√

V. CONCLUSIONS

In this paper, we have presented a detailed survey on Security Authentication and Cryptography Protocols of Unmanned Aerial Vehicles, it concentrates on presenting the recently utilized cryptographic algorithms that work on providing secure communication in drones using the MavLink communication protocol.

Because UAV-generated and -transferred data is widely applied across multiple areas, it is seen as valuable. The actual difficulties in the management of data security and transfer in today's cryptography environment need to be addressed. To make UAV communication safe, this work examined many factors. It also offers the research community a useful resource for learning about the development as well as the design of secure UAV architectures.

REFERENCES

[1] A. Shafique, A. Mehmood, and M. Elhadef, "Survey of security protocols and vulnerabilities in unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 46927–46948, 2021.

[2] T. Alladi, V. Chamola, and N. Kumar, "PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks," *Comput. Commun.*, vol. 160, pp. 81–90, 2020.

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

[4] N. A. Khan, N. Z. Jhanjhi, S. N. Brohi, A. A. Almazroi, and A. A. Almazroi, "A secure communication protocol for unmanned aerial vehicles," *Comput. Mater. Contin.*, vol. 70, no. 1, 2021.

[5] S. Atoev, K.-R. Kwon, S.-H. Lee, and K.-S. Moon, "Data analysis of the MAVLink communication protocol," in *2017 International Conference on Information Science and Communications Technologies (ICISCT)*, IEEE, 2017, pp. 1–3.

[6] I. Mellado-Bataller, J. Pestana, M. A. Olivares-Mendez, P. Campoy, and L. Mejias, "MAVwork: a framework for unified interfacing between micro aerial vehicles and visual controllers," *Front. Intell. Auton. Syst.*, pp. 165–179, 2013.

Received 04/February/2024; Accepted 23/April/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

[7] A. Allouch, O. Cheikhrouhou, A. Koubâa, M. Khalgui, and T. Abbes, "MAVSec: Securing the MAVLink protocol for ardupilot/PX4 unmanned aerial systems," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, IEEE, 2019, pp. 621–628.

[8] A. Koubâa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui, "Micro air vehicle link (mavlink) in a nutshell: A survey," *IEEE Access*, vol. 7, pp. 87658–87680, 2019.

[9] G. Panice *et al.*, "A SVM-based detection approach for GPS spoofing attacks to UAV," in *2017 23rd International Conference on Automation and Computing (ICAC)*, IEEE, 2017, pp. 1–11.

[10] R. Gupta, A. Nair, S. Tanwar, and N. Kumar, "Blockchain- assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges," *IET Commun.*, vol. 15, no. 10, pp. 1352–1367, 2021.

[11] V. K. Ralegankar *et al.*, "Quantum cryptography-as-a-service for secure UAV communication: applications, challenges, and case study," *IEEE Access*, vol. 10, pp. 1475–1492, 2021.

[12] S. Atoev, O.-J. Kwon, C.-Y. Kim, S.-H. Lee, Y.-R. Choi, and K.-R. Kwon, "The secure UAV communication link based on OTP encryption technique," in *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, IEEE, 2019, pp. 1–3.

[13] V. V Kirichenko, "Information security of communication channel with UAV," *Electron. Control Syst.*, no. 3, pp. 23–27, 2015.

[14] Y. Li, R. Zhang, J. Zhang, and L. Yang, "Cooperative jamming via spectrum sharing for secure UAV communications," *IEEE Wirel. Commun. Lett.*, vol. 9, no. 3, pp. 326–330, 2019.

[15] O. K. Sahingoz, "Multi-level dynamic key management for scalable wireless sensor networks with UAV," in *Ubiquitous Information Technologies and Applications: CUTE 2012*, Springer, 2013, pp. 11–19.

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

[17] V. Valentin-Alexandru, B. Ion, and P. Victor-Valeriu, "Energy efficient trust-based security mechanism for wireless sensors and unmanned aerial vehicles," in *2019 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, IEEE, 2019, pp. 1–6.

[18] G. E. Kasim, "Secure Channel Protocol for Unmanned Aerial VehiclesTitle," University of Technology, 2022.

[19] A. Demeri, W. Diehl, and A. Salman, "Saddle: Secure aerial data delivery with lightweight encryption," in *Intelligent Computing: Proceedings of the 2020 Computing Conference, Volume 3*, Springer, 2020, pp. 204–223.

[20] J. Wang, Y. Liu, S. Niu, and H. Song, "Lightweight blockchain assisted secure routing of swarm UAS networking," *Comput. Commun.*, vol. 165, pp. 131–140, 2021.

[21] M. S. Haque and M. 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*, Springer, 2018, pp. 113–122.

[22] H. M. Ismael, "Authentication and encryption drone communication by using HIGHT lightweight algorithm," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 11, pp. 5891–5908, 2021.

[23] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, 2014.

[24] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Commun.*, vol. 14, no. 12, pp. 1–14, 2017.

[25] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, 2015.

[26] Y. Zeng, R. Zhang, and T. J. Lim, "Throughput maximization for UAV-enabled mobile relaying systems," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 4983–4996, 2016.

[27] D. H. Choi, S. H. Kim, and D. K. Sung, "Energy-efficient maneuvering and communication of a single UAV-based relay," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 50, no. 3, pp. 2320–2327, 2014.

[28] K. Li, R. C. Voicu, S. S. Kanhere, W. Ni, and E. Tovar, "Energy efficient legitimate wireless surveillance of UAV communications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2283–2293, 2019.

[29] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wirel. Commun. Lett.*, vol. 6, no. 3, pp. 310–313, 2017.

[30] G. Choudhary, V. Sharma, I. You, K. Yim, R. Chen, and J.-H. Cho, "Intrusion detection systems for

Received 04/February/2024; Accepted 23/April/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.3.4

networked unmanned aerial vehicles: a survey," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, IEEE, 2018, pp. 560–565.

[31] Y. Mekdad *et al.*, "A Survey on Security and Privacy Issues of UAVs. arXiv 2021," *arXiv Prepr. arXiv2109.14442*.

[32] X. Lu, L. Xiao, C. Dai, and H. Dai, "UAV-aided cellular communications with deep reinforcement learning against jamming," *IEEE Wirel. Commun.*, vol. 27, no. 4, pp. 48–53, 2020.

[33] W.-S. Ra, I.-H. Whang, and J. B. Park, "Robust weighted least squares range estimator for UAV applications," in *2008 SICE Annual Conference*, IEEE, 2008, pp. 251–255.

[34] M. B. Bejiga, A. Zeggada, A. Nouffidj, and F. Melgani, "A convolutional neural network approach for assisting avalanche search and rescue operations with UAV imagery," *Remote Sens.*, vol. 9, no. 2, p. 100, 2017.

[35] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, "Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review," *Comput. Electr. Eng.*, vol. 86, p. 106717, 2020.

[36] A. Islam and S. Y. Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," *Comput. Electr. Eng.*, vol. 84, p. 106627, 2020.

[37] S. Aggarwal, N. Kumar, M. Alhussein, and G. Muhammad, "Blockchain-based UAV path planning for healthcare 4.0: Current challenges and the way ahead," *IEEE Netw.*, vol. 35, no. 1, pp. 20–29, 2021.

[38] Y. Zhu, X. Zhang, Z. Y. Ju, and C. C. Wang, "A study of blockchain technology development and military application prospects," in *Journal of Physics: Conference Series*, IOP Publishing, 2020, p. 52018.

[39] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "A taxonomy of blockchain-enabled softwarization for secure UAV network," *Comput. Commun.*, vol. 161, pp. 304–323, 2020.

[40] A. Kuzmin and E. Znak, "Blockchain-base structures for a secure and operate network of semi-autonomous unmanned aerial vehicles," in *2018 IEEE International conference on service operations and logistics, and informatics (SOLI)*, IEEE, 2018, pp. 32–37.

[41] I. J. Jensen, D. F. Selvaraj, and P. Ranganathan, "Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs)," in *2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, IEEE, 2019, pp. 1–7.

[42] L. J. Min, "A UAV-assisted Blockchain Based Secure Device-to-Device Communication Using Bloom Filter in Internet of Military Things," 한국통신학회, 2020.

[43] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, pp. 3–28, 1992.

[44] N. A. Khan, S. N. Brohi, and N. Z. Jhanjhi, "UAV's applications, architecture, security issues and attack scenarios: A survey," in *Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2019*, Springer, 2020, pp. 753–760.

[45] A. N. Mazher and J. Waleed, "A Review of Recent Development of Security Schemes for UAVs Communication," *J. Al-Ma'moon Coll.*, no. 36, 2021.

[46] J. McCoy and D. B. Rawat, "Software-defined networking for unmanned aerial vehicular networking and security: A survey," *Electronics*, vol. 8, no. 12, p. 1468, 2019.

Received 04/February/2024; Accepted 23/April/2024