Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Secure Communication Frame for Aerial Networks

Onss Dhurgham Hashim Hani [a], *Abbas Abdulazeez Abdulhameed* [b]

[a]*Department of Computer Science, Collage of Science, Mustansiriyah University, Baghdad, 10052, Iraq.Email ons.dhurgham@uomustansiriyah.edu.iq*
[b]*Department of Computer Science, Collage of Science, Mustansiriyah University, Baghdad, 10052,Iraq.Email:abasabdulazeez@uomustansiriyah.edu.iq*

ARTICLE INFO

Article history:
Received: 12 /11/2024
Rrevised form: 1 /12/2024
Accepted : 24 /12/2024
Available online: 30 /12/2024

Keywords:

Internet of Things,

Internet of Drones,

Aerial Networks,

Connection Protocols,

Drones,

MAVLink.

ABSTRACT

This research explores the seamless integration of the Internet of Things (IoT) within the realm of Unmanned Aerial Vehicles (UAVs), resulting in the paradigm of the Internet of Drones (IoD) to create a unified framework that connects both aerial and ground-based systems, enabling an interconnected system. The primary objective is to enhance the operational efficiency, scalability, and innovation potential of drone systems while addressing critical challenges related to connectivity, data management, and security in this emerging paradigm. Securing IoD is essential to protect against a wide range of cyber threats. Moreover, secure communication channels will strengthen the resilience of IoD systems, enabling them to operate safely in dynamic and potentially hostile environments. As IoD systems will rely on continuous communication between drones and IoT devices, securing these exchanges without compromising performance is a primary concern. The research aims to set a foundation for the practical implementation of IoD systems, ensuring secure and efficient operations in diverse applications. The feasibility of implementing a virtual drone framework should be evaluated using open-source simulators or network simulators before deploying the IoD in real-world applications. The Mission Planner simulator, as an open-source tool, offers a wide range of capabilities, including motion capture, collision detection, ease of programming, and support for multiple sensor types, making it ideal for initial tests. In addition, designing a secure IoD communication framework is essential to ensure safe data transfer between IoD endpoints with minimal impact on system performance. To achieve this, the study reviews several secure IoD communication frameworks that incorporate advanced cryptographic techniques. These frameworks are crucial for safeguarding the integrity, confidentiality, and authenticity of data exchanged within the IoD network.

https://doi.org/10.29304/jqcsm.2024.16.41788

1. Introduction

The Internet of Things refers to the interconnection of electronic devices embedded into physical things, enabling them to communicate and interact with one other and the external world [1]. In the near future, IoT technology provide enhanced levels of services and fundamentally transform people's everyday routines [2]. The Internet of Things (IoT) has made significant progress in several fields such as medical, power, gene treatments, agriculture, smart cities, and smart homes [3].

Integration of internet and electronic devices allows for remotely operation and management from any location. This also increases data reachable across multiple devices, rather than being limited to a single device [4]. The essential components necessary for operation IoT system include Cloud, Gateway, User Interface, Analytics, Database, Standards & Protocols, Device Connectivity, and Automation. IoT focuses on being able to detect things and responding regarding environmental requirements. Growth of internet and smart sensor systems has revolutionized this field [1].

∗Corresponding author: Onss Dhurgham Hashim Hani

Email addresses: ons.dhurgham@uomustansiriyah.edu.iq

Communicated by 'sub etitor'

Integration of drones into (IoT) represents a technology shift, offering a myriad of opportunities and challenges [4]. Drones, also called unmanned aerial vehicles (UAVs), equipped with various sensors and communication devices, become integral nodes in the IoT network. This convergence holds potential for enhancing efficiency, data collection, and real-time decision-making across many sectors [5].

The Internet of Drones has lately gained traction as a result of its high adaptability to a wide range of difficult scenarios, due to technological and practical advantages such as high mobility, the ability to extend wireless coverage areas, or the ability to reach places inaccessible to humans [6]. Unmanned Aerial Vehicles (drones) successfully used in a variety of applications such as search and rescue missions, agriculture, mission-critical services and surveillance systems [3]. Furthermore, usage of drones enhances the performance aspects of various network topologies, such as dependability, connection, throughput, and delay [6]. Usage of drones is a beneficial tool for dealing with concerns in standard procedures [4]. Connecting drones to develop (IoD) is a desired trend to enhance flight safety and quality due to the rising numbers of UAVs in low-altitude airspace.

IoT integration and drones accomplished via a device known Autopilots. Which is a tiny electronics system designed for control UAVs (drones). Initially designed for full automation of drones, autopilot systems today include sensors and processors necessary for drone to cloud in-built connectivity [1].

However, there are still concerns about IoD security, privacy, and communication [2]. The IoD deployment involves a number of difficulties, especially with regard to operational safety. Attackers have targeted the IoD to do damage because it is used in a variety of application industries. The drones might be the object of an assault, or a tool used to carry out crimes and attacks. As a result, researchers have focused more on IoD security, including how to handle it safely and deal with physical and cyberattacks that target it.

2. Related Works

Several studies extensively discuss various aspects of Internet of Drones (IoD), particularly focusing on the security challenges and solutions in aerial networks. These studies explore key topics related to securing communication, integrity of data, and authentication within IoD system.

- In 2018 (Dey, Pudi et al.): Authors proposed many tactics and projects to enhance the security of drone communication. Responding to sensitivity of drones GPS spoofing, anti-spoofing and anti-jamming transmitters created. Research has proposed numerous effective methods for detecting and circumventing GPS anti-spoofing and anti-jamming techniques, which are (cryptography and non-cryptography) technique. These strategies were either difficult to implement or required acquiring of cost technology [7].
- In 2018 (Bunse and Plotz): Authors investigated a standard UAV contact and control protocol. They discussed conventional attack strategies, assumptions, and protocol security. Utilizing on message a brute force attack, radio chip employed. They recommended utilizing a secret of maximum length, specifically at least 6 bytes. This complicates brute force attacks further and enhances the authentication of the legitimate owner. They approved the implementation of cryptographic technology. Due to the limited availability of commercial communication components, these discoveries can be applied to different protocols [8].
- In 2019 (Allouch, Cheikhrouhou et al.): Authors identified MAVLink vulnerabilities and presented MAVSec, an enhanced MAVLink that utilizes encryption methods to protect transmission of MAVLink signals between Ground Control Stations and Unmanned Aerial Vehicles. Ardupilot was employed to evaluate MAVSec and analyzed efficacy of chosen algorithms (including ChaCha20, RC4, AES-CBC, and AES-CTR) regarding memory usage and consumption of CPU. The results indicate ChaCha20 exceeds existing encryption algorithms in performance and efficiency. This research mostly concentrates on establishing control over drones via authentication between drones and ground stations. Research lacks a comprehensive comparison of unsecured MAVLink and secured MAVSec implementations either performance or latency. Authors did not assess other lightweight encryption methods that could be good for resource-constrained environments [9].
- In 2020 (Chaari, Chahbani et al.): Authors present a secure communication framework, MAV-DTLS, to improve security of UAV-GCS communication. It is based on the Datagram Transport Layer Security (DTLS) protocol, adapted for use with MAVLink. MAV-DTLS addresses key security challenges and is evaluated for computational overhead and latency, showing it enhances security with minimal impact on communication efficiency. The framework is suitable for UAV operations, ensuring secure data exchange between UAVs and GCS. However, the study has limitations, including a lack of exploration into its adaptability to evolving cyber threats and how it integrates with existing UAV communication protocols [10].
- In 2020 (Nayyar, Nguyen et al.) and (Abdelmaboud 2021): Authors present an IoD architecture that seeks to address the issue of airspace allocation and management. The suggested architecture offers versatile services that may be utilized by various applications in which drones are capable of performing tasks. The studies discuss many obstacles that hinder the efficiency of the Internet of Drones in order to suggest potential areas for future study in this field [11,12].

- In 2021 (Boccadoro, Striccoli et al.): Authors provides a detailed description of the Internet of Drones and presents an architectural framework along with its applications, with a particular focus on those related to industrial IoT [13].
- In 2021 (Ismael): Authors examined the enhancement of drone communication security with the application of HIGHT lightweight algorithm for authentication and encryption. Author examines current weaknesses in communication networks and suggests HIGHT as a solution that provides effective encryption. The paper includes evaluations, showing that HIGHT can significantly improve security of drone communications without considerably reducing their efficiency [14].
- In 2022 (Kassim and Hashem): Authors present a novel method for encrypting data and communications on MAVLink utilizing a GIFTlightweight algorithm and dynamicDNA coding, resulting DMAV, an upgraded MAVLink protocol that integrates dynamic DNA coding to boost communication for UAVs. The authors recognize deficiencies in current standards concerning data security and transmission efficacy. Through the application of dynamic DNA coding, DMAV seeks to improve data integrity and mitigate the danger of unwanted access. DMAV exhibits enhanced efficiency and security relative to conventional MAVLink, positioning it as a promising alternative for resilient UAV communication across diverse applications [15].

3. Challenges and Considerations

IoD represents a complex and evolving field with numerous challenges and considerations. Addressing these challenges and considerations is essential for the successful development and deployment of the Internet of Drones. Some of these challenges are:

1. Privacy and security: arise due to the presence of multiple interconnected sensor devices in IoD. These devices are susceptible to a range of risks, such as hijacking, human mistake, and loss [14]. The drone applications design should prioritize these challenges. Communications networks are susceptible to jammer assaults that have the potential to immobilize or disrupt by altering their controls. In order to achieve this objective, it is imperative to utilize high integrity protected data lines between aircraft and controllers on ground. Technologies for data protection and augmented communications may prevent potential security risks [15,16].

2.Management of global resources: Efficient resource distribution crucial for enhancing IoD. It can be categorized into: global resource allocation and local resource allocation. Furthermore, IoD can achieve optimal worldwide productivity by utilizing a range of equipment, including edge computers, cloud servers, and UAVs. UAV applications must balance efficiency and cost. “Resource allocation” is the most popular economic activity since it involves conflicting interests of individuals, corporations, and services for resources. Another resource utilization challenge is setting priorities and pathways to minimize activity energy expenditure [17].

3. Sensor Communication: IoD sensor are meant to be lightweight and highly sensitive, which increases the likelihood of data loss or receiving incorrect data from other nodes. In addition, sensors encounter routing challenges when establishing communication with several drones through a network hub. In order to tackle these problems, future network technologies such as 5G, 6G, intelligent routing, narrowband Internet of Things, and LTE-M must be capable of accommodating many connection options [18,19].

4. Coordinating and scheduling tasks: Managing a large fleet of drones, particularly in urban environments, presents challenges in terms of coordination and collision avoidance. Integrating drones into existing air traffic management systems, particularly in congested airspaces, is a complex challenge. It requires collaboration between regulatory bodies, aviation authorities, and drone operators. Also developing systems for collision detection and avoidance is critical to ensure the safe operation of drones in shared airspace [20,21]

5. Distribution and Deployment of Drones: In addition to data confidentiality, the deployment of IoD also presents issues in terms of data exchange and access management. An ongoing difficulty in the application of using a group of drones to collect road traffic data from various places is how to securely and efficiently communicate this data. The goal is to ensure that only authorized entities may access the obtained data [22,23].

Hackers and individuals with malicious intent have consistently stayed ahead of security experts, creating a constant challenge for cybersecurity [24]. As a result, many techniques have been developed to protect against unauthorized access and harmful activities targeting drone systems.

4. Communication protocols

UranusLink, UAVCAN and MAVlink are communication protocols helping drones to operate with GCS, and are used to messages exchange between them. Messages contain information and control commands are sent from GCS to UAV and vice versa.

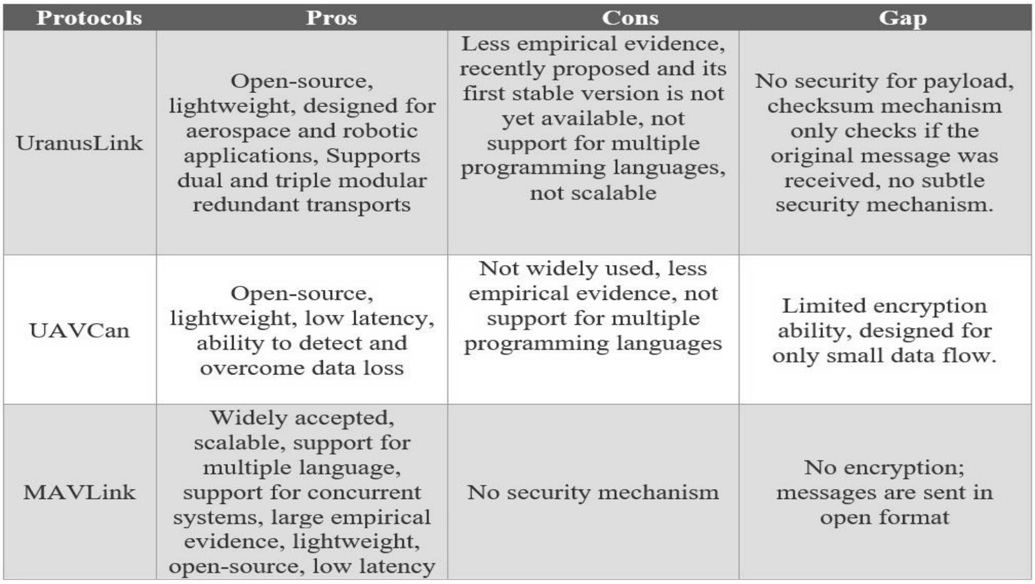
1. UranusLink protocol: is created to provide unreliable and reliable services as a packet-oriented protocol. The protocol determines packet structure and data representation transmitted. It is designed to use in radio ways [25].

2. UAVCAN protocol: lightweight, open-source protocol, ensure safe connection using reliable vehicle networks such as CANbuses in aerospace and robot applications. There is no master node, and all nodes possess equal privileges, this functionality supports numerous nodes and interfaces, which is typically necessary for applications with safety concerns. This protocol can be readily executed and verified. It's designed for resource-constrained and real-time systems [26].

3. MAVlink protocol: lightweight, open-source protocol, used for bidirectional communication in drones and GCSs. It's most important protocol [27].

Table (1) below shows pros and cons among communication protocols mentioned above.

Table (1):



Protocols	Pros	Cons	Gap
UranusLink	Open-source, lightweight, designed for aerospace and robotic applications, Supports dual and triple modular redundant transports	Less empirical evidence, recently proposed and its first stable version is not yet available, not support for multiple programming languages, not scalable	No security for payload, checksum mechanism only checks if the original message was received, no subtle security mechanism.
UAVCan	Open-source, lightweight, low latency, ability to detect and overcome data loss	Not widely used, less empirical evidence, not support for multiple programming languages	Limited encryption ability, designed for only small data flow.
MAVLink	Widely accepted, scalable, support for multiple language, support for concurrent systems, large empirical evidence, lightweight, open-source, low latency	No security mechanism	No encryption; messages are sent in open format

comparison of UAV protocols [27]

5. MAVLink and Attacks on IoD

It is largely employed for bidirectional communication between drones and GCSs, and specifies a comprehensive message exchanged between them. This protocol is widely used in major autopilot systems. Its key features include managing, monitoring, and controlling UAS, as well as enabling UAS integration with the internet [25]. MAVLink protocol enables management by facilitating exchange data between different components. It is commonly used for managing drones and serves as a communication bridge between various components on drone (autopilot, sensors) and GCS [27]. It's designed as a "Marshaling library" (serializes messages) into particular binary format (bytes stream) of system's states and commands that must execute [28]. Nature of binary serialization (minimal overhead) of MAVprotocol makes it lightweight as compared to other serialization strategies. MAVmessages are typically small sizes and can reliably, consistently sent across various wireless media [27]. MAVprotocol most popular among its peers because all these features for communication between drones and GCS, it supports a wide range of transport layers and communication mediums, enabling data transmission through various channels such [29]:

- Serial telemetry low bandwidth channels operating at sub-GHz frequencies. SubGHz frequencies provides for long communication ranges and remote control of UAS.
- Network interface (WiFi or Ethernet) MAVmessages are routed using IP networks.

Securing IoD is a challenging endeavor owing to the diverse range of communication protocols and the wide array of applications involved. Drones may be attacked in a variety of ways [28,29,30]. Figure 1 illustrate typical attacks classification of Internet of Drones.

1. Confidentiality and privacy attacks: when intercepting commands, or messages that are being sent through network between parties, examples of this type:

- Eavesdropping
- Identity spoofing
- Traffic analysis
- Unauthorized accessibility

2. Integrity attacks: when modifying data being sent. Violation of MAVLink integrity. Examples of this type:

- MITM
- Hijacking
- Replay attack
- Message modification
- False location update

3. Availability attacks: Attacks that impact availability of MAVLink can be executed by disrupting the data exchange link between drone and ground station. There are multiple ways in which these attacks can be performed such:

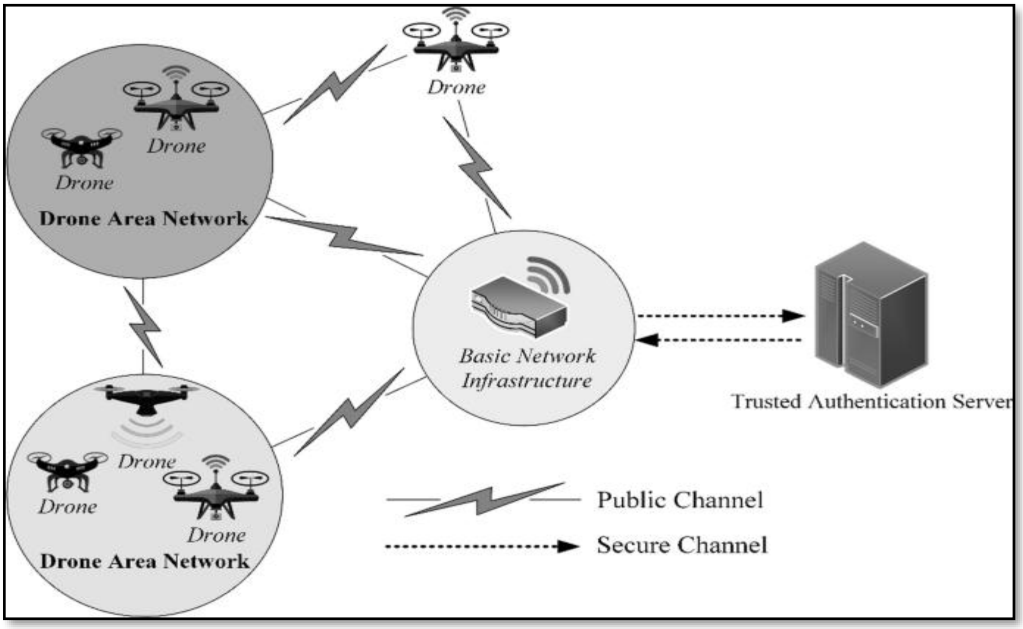
- Jamming
- DoS
- Flooding

4. Authenticity attacks: When an attempt is made to mislead GCS or UAV into believing that fake data is authentic, authenticity of MAVmessages can be compromised, and this can occur through:

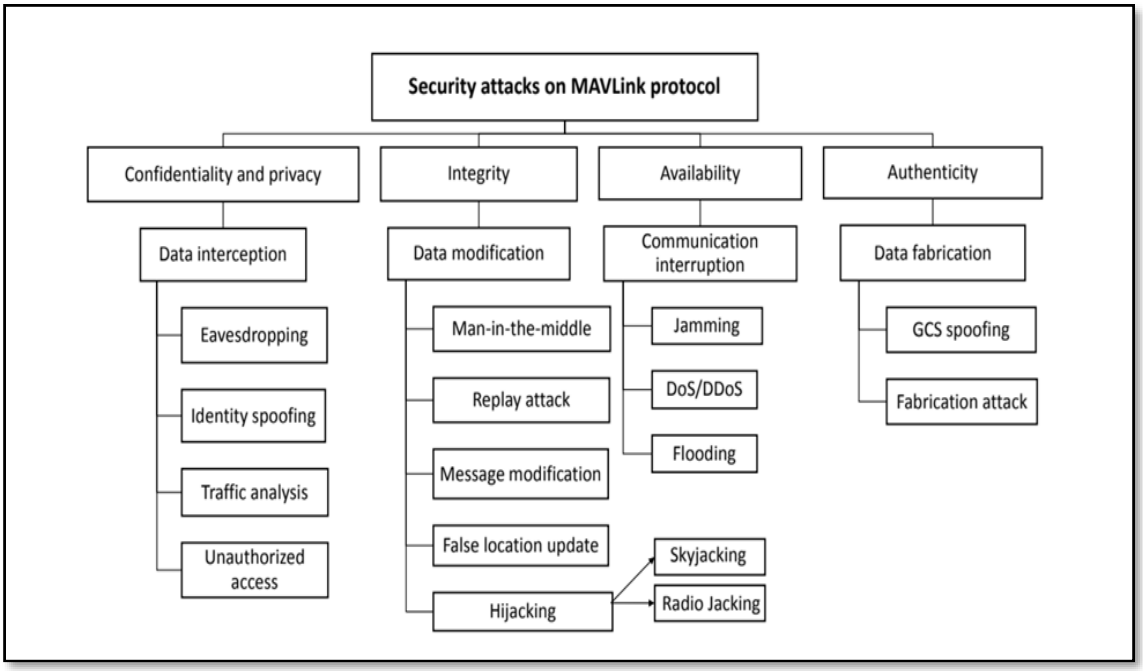
- Data fabrication

- GCS spoofing

Fig (1): MAVLink security attacks [30]



6. Secure IoD Communication



IoD are processing and transmitting enormous amounts of data. These data are susceptible to hackers and dangerous malware. Therefore, it is necessary to maintain security and effectiveness of data processing, storage, and transfer through communication protocols, which involves ensuring data confidentiality, integrity, authenticity, and real-time performance [30]. The IoD comprises a network of drones communicating with each other and ground stations over potentially insecure channels, necessitating robust security mechanisms [27]. Lightweight cryptography is one of techniques that can offer safe data transfer in an IoD network.

Secure keys must first be established in both entities, the two entities should be authenticated before any data is transmitted between them. Figure 2 illustrates that while a secure channel cannot be intercepted, a public channel may.

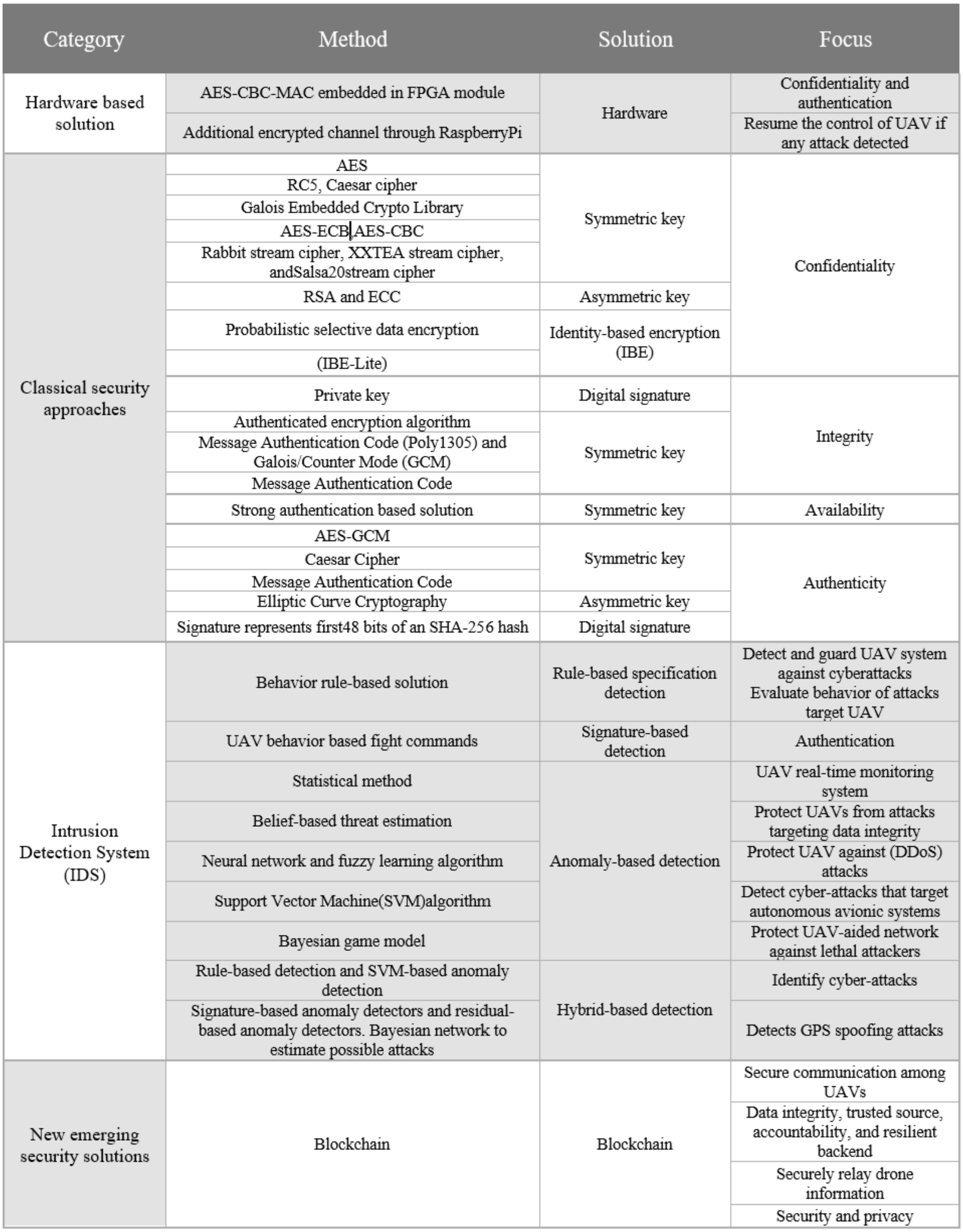
Fig (2): Secure communication in Internet of Drones [27]

Lightweight cryptography is a modern branch of cryptography that has appear in response to instant growth of ubiquitous and emerging technologies [14]. It is specifically designed for devices with low computing power, limited battery life, small memory, compact size, and constrained power supply [15]. As a result, traditional cryptographic methods may not be suitable for resource-limited smart devices. Lightweight encryption combines efficiency and security, achieving high levels of protection while operating with minimal computing power and resources. In context of securing MAVLink using lightweight algorithms becomes crucial.

Several strategies and solutions have already been presented to mitigate IoD vulnerabilities [31]. Current solutions are shown in table 2 they are typically hardware and software methodologies [27]. Hardware-based solution developed to safeguard connection protocols, a solution is provided to encrypt communication between GCS and drone. Another way is integrated FPGA module with drone incorporates symmetric key cryptography functionality.

Hardware solution impacts system performance and power consumption due to additional hardware weight. Also, an auxiliary secured channel of communication to enhance UAV data safety via RaspberryPi is introduced. Software-based solution such classical security strategies, Intrusion Detection System, and Blockchain technology [27,32]. Table (2) illustrate existing solution for securing IoD connection protocols.

Table (2):



Category	Method	Solution	Focus
Hardware based solution	AES-CBC-MAC embedded in FPGA module	Hardware	Confidentiality and authentication
	Additional encrypted channel through RaspberryPi		Resume the control of UAV if any attack detected
Classical security approaches	AES	Symmetric key	Confidentiality
	RC5, Caesar cipher		
	Galois Embedded Crypto Library		
	AES-ECB,AES-CBC		
	Rabbit stream cipher, XXTEA stream cipher, andSalsa20stream cipher		
	RSA and ECC	Asymmetric key	
	Probabilistic selective data encryption	Identity-based encryption (IBE)	
	(IBE-Lite)		
	Private key	Digital signature	Integrity
	Authenticated encryption algorithm	Symmetric key	
	Message Authentication Code (Poly1305) and Galois/Counter Mode (GCM)		
	Message Authentication Code		
	Strong authentication based solution	Symmetric key	Availability
	AES-GCM	Symmetric key	Authenticity
	Caesar Cipher		
	Message Authentication Code		
	Elliptic Curve Cryptography	Asymmetric key	
	Signature represents first48 bits of an SHA-256 hash	Digital signature	
Intrusion Detection System (IDS)	Behavior rule-based solution	Rule-based specification detection	Detect and guard UAV system against cyberattacks Evaluate behavior of attacks target UAV
	UAV behavior based fight commands	Signature-based detection	Authentication
	Statistical method	Anomaly-based detection	UAV real-time monitoring system
	Belief-based threat estimation		Protect UAVs from attacks targeting data integrity
	Neural network and fuzzy learning algorithm		Protect UAV against (DDoS) attacks
	Support Vector Machine(SVM)algorithm		Detect cyber-attacks that target autonomous avionic systems
	Bayesian game model		Protect UAV-aided network against lethal attackers
	Rule-based detection and SVM-based anomaly detection	Hybrid-based detection	Identify cyber-attacks
	Signature-based anomaly detectors and residual-based anomaly detectors. Bayesian network to estimate possible attacks		Detects GPS spoofing attacks
New emerging security solutions	Blockchain	Blockchain	Secure communication among UAVs
			Data integrity, trusted source, accountability, and resilient backend
			Securely relay drone information
			Security and privacy

Existing security solutions [27]

7. Security Requirements

The communication between drone and GCS is established through a wireless channel using a communication protocol. However, when using MAVLink protocol, this communication is susceptible to vulnerabilities due to lack of built-in standard security measures [30]. To mitigate potential threats and attacks, it is crucial to thoroughly understand security requirements and take proactive measures to address these vulnerabilities. Security requirements for MAVLink include confidentiality, integrity, availability, authentication, non-repudiation, authorization, and privacy [31].

Enhancing security of MAVLink can be achieved by integrating an encryption mechanism into its existing framework. However, this approach highlights the importance of incorporating security considerations during initial design of system. Adjust security features can lead to compatibility issues and complicate implementation. Overall, security is a fundamental aspect of any communication protocol, ensuring safe and reliable message transmission across network. [33,34]. Figure 3 shows security requirements for IoD.

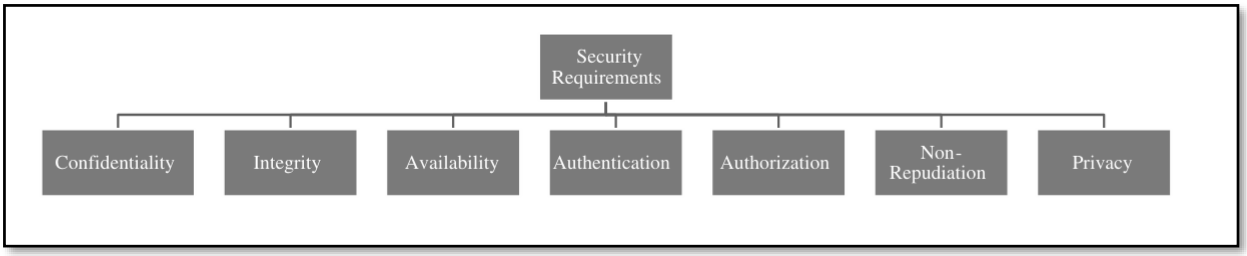


Fig (3): Internet of Drones security requirements [29]

MAVlink protocol enables management by facilitating exchange data between different components. It is commonly used for managing drones and serves as a communication bridge between various components on drone and GCS. MAV protocol supports different types of transport layers and mediums [35]. To address cybersecurity issues in drones, a three-step scheme should be applied for ensuring security. Figure 4 illustrating process.

1. First level of security addresses the wireless attack,
2. Second level addresses hardware attack on autopilot and calls for development,
3. A simulator which allows detailed analysis of threats and its mitigation.

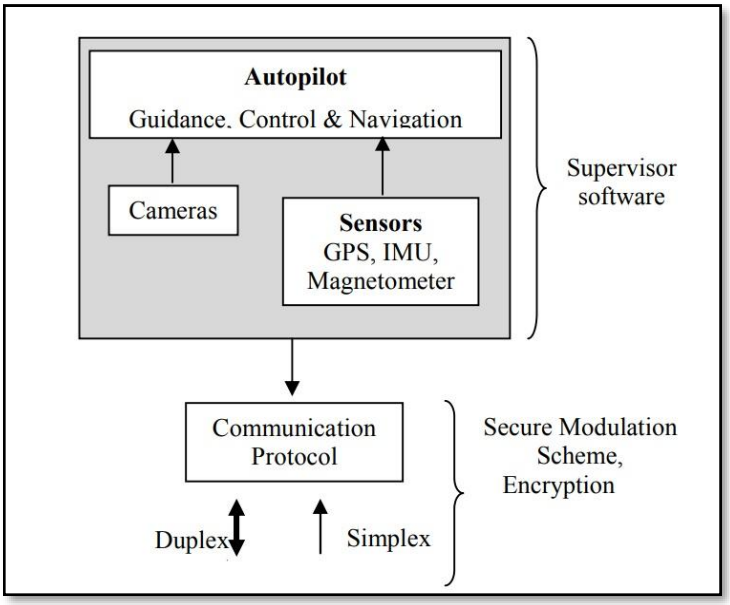


Fig (4): Security scheme to secure MAVlink [30]

8. Suggested Securing Method

Proposed method aims to establish verification of identity between drones and GCS, by using chacha20-poly1305 lightweight algorithm with key generation. Encrypt aircraft session key of the registry in a compiled dataset at GCS in order to improve the security of proposed approaches, ultimately enhancing the protection of payload data for MAVLink protocol. The main goal is to manage a single GCS and one drone throughout several flying missions. Figure 5, illustrate general phases (Initialization, authentication and encryption/decryption). Adding security features requires additional steps. first Define Security Requirements such (Encryption: Protect the confidentiality of messages to prevent unauthorized access), and (Integrity: Ensure that messages are not tampered with during transmission. Authentication: Verify the identity of the sender to prevent spoofing). ChaCha20-Poly1305 together, provide authenticated encryption. ChaCha20 is a stream cipher for encryption, and Poly1305 is a message authentication code (MAC) used for integrity and authenticity.

Integration ChaCha20-Poly1305 into MAVLink provides a robust cryptographic solution for securing UAV communications, addressing critical security concerns and maintaining efficiency in resource-constrained environments. Figure 6 illustrate overall structure. Critical requirements to take in considerations:

a. Key Management: First Use a secure key management system to generate and distribute keys. Each pair of communicating entities should have shared secret key. Second Use a secure key exchange method to establish shared keys by using a secure initial setup phase.

b. Message Encryption & Authentication: Prepare Message: Construct MAVLink message, Encrypt Message using ChaCha20 to encrypt payload. encryption key should be derived from shared secret key. Generate a nonce for each message to ensure that encryption is unique per message. Generate Authentication Tag:use Poly1305 to create an authentication tag over encrypted message and any additional data (like nonce). Tag will help verify integrity and authenticity of message. Now msg.format (Payload: Encrypted message, Tag: Poly1305 authentication tag, Nonce: Unique nonce for each message)

c. Message Decryption:

- Extract Encrypted Payload and Authentication Tag: From received MAVmessage.
- Verify Tag: Use Poly1305 received message.
- Decrypt Payload: Use ChaCha20 to decrypt payload if tag is valid.

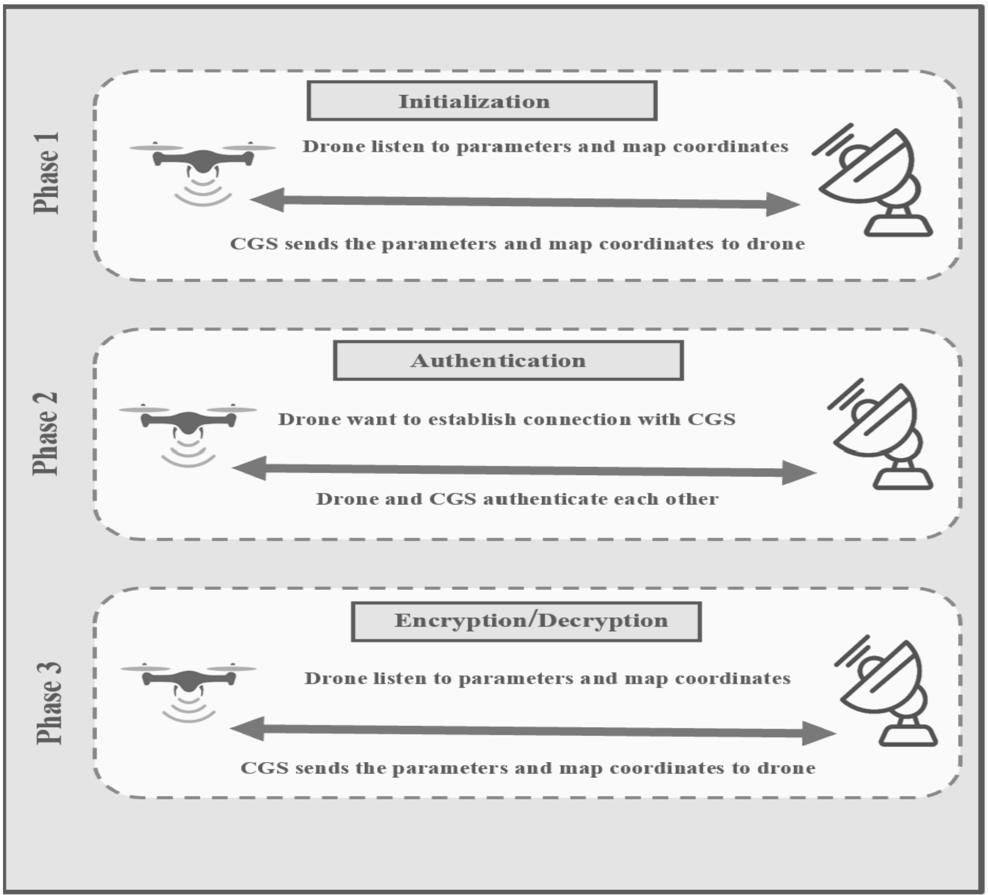

Phase 1
Initialization
Drone listen to parameters and map coordinates
CGS sends the parameters and map coordinates to drone
Phase 2
Authentication
Drone want to establish connection with CGS
Drone and CGS authenticate each other
Phase 3
Encryption/Decryption
Drone listen to parameters and map coordinates
CGS sends the parameters and map coordinates to drone

Fig (5): Suggested Method Phases

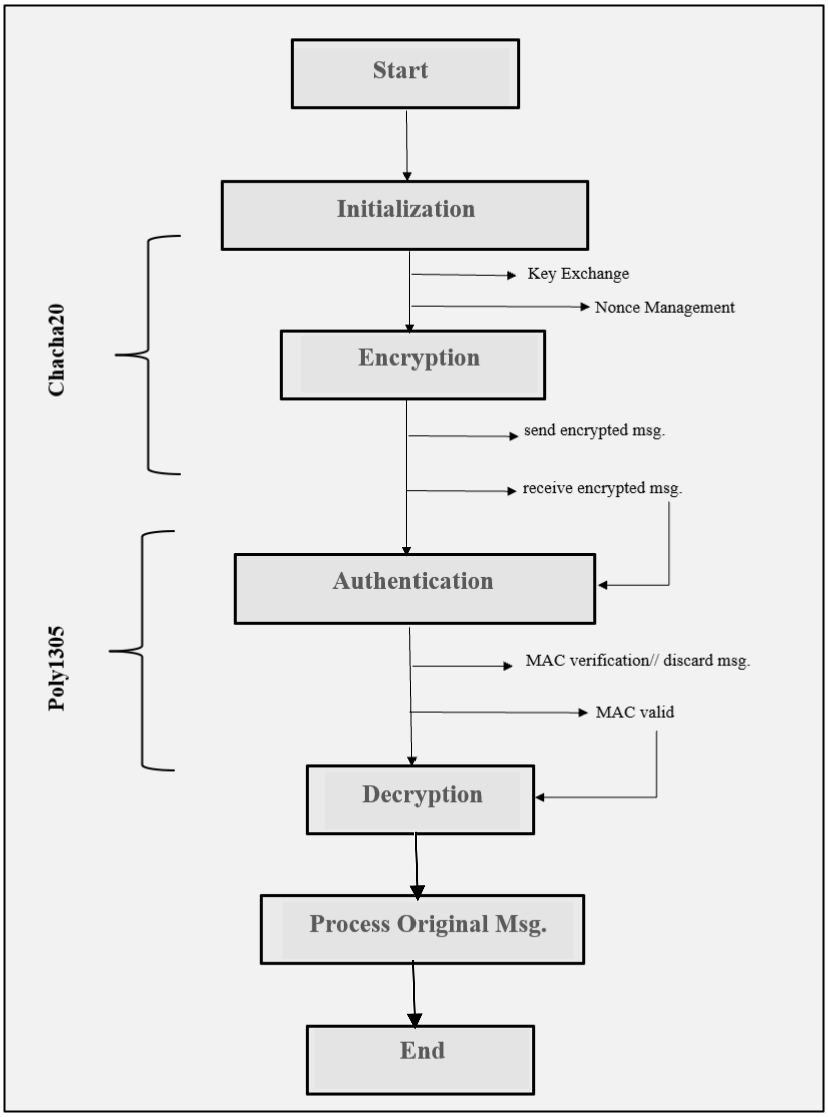


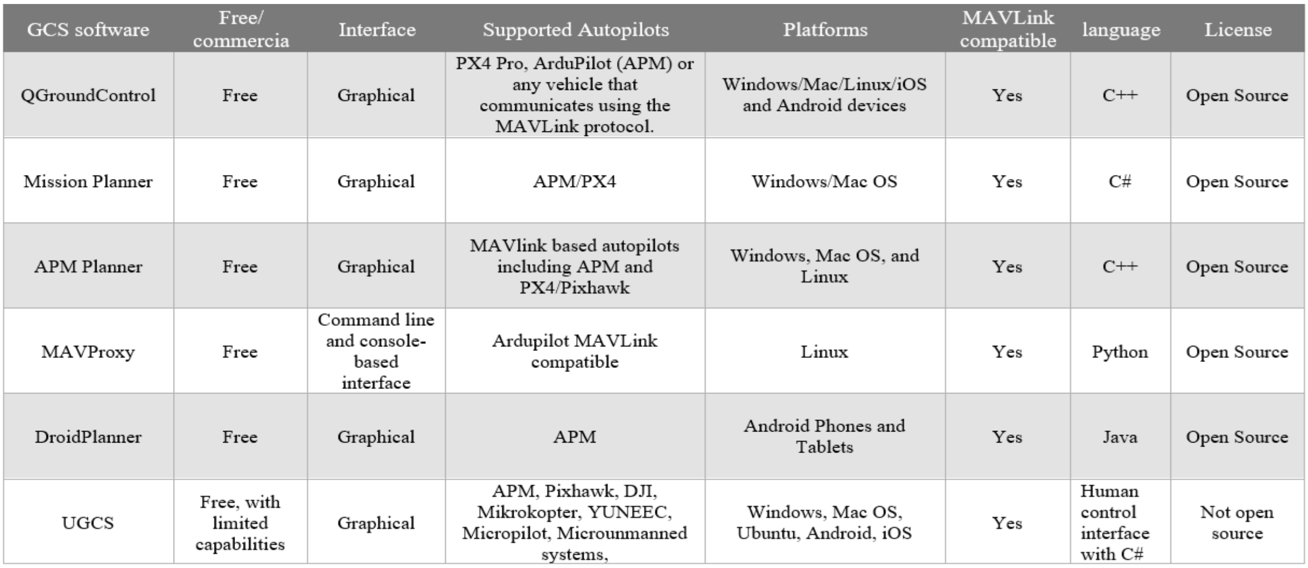
Fig (6): Integration Procedure

By combining ChaCha20 for encryption and Poly1305 for authentication, this approach secures the MAVLink communication between UAVs and GCS, making it resistant to various cyber threats such as interception, tampering, and unauthorized access.

9. Simulation Technique

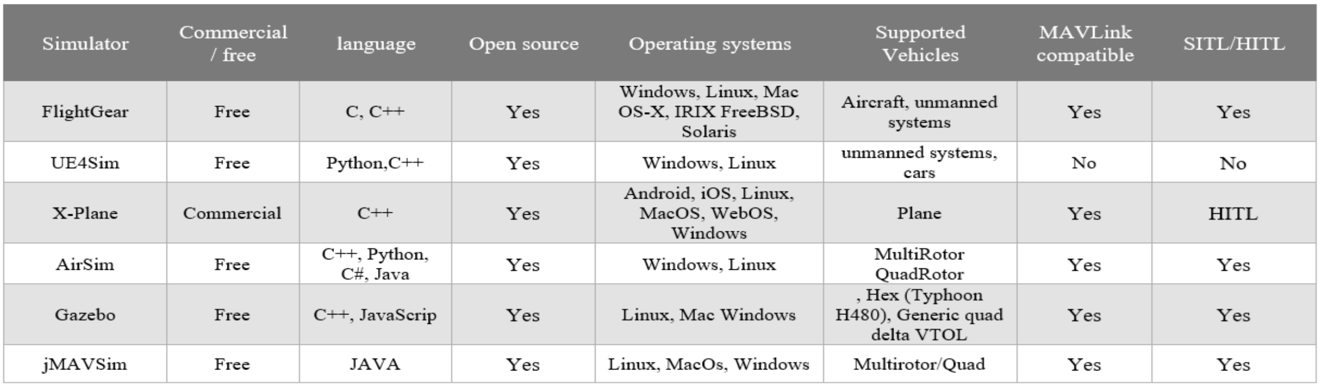
To mitigate drone threats, it is important to establish clear guidelines for drone usage, along with developing and implementing elective security measures. Simulation technologies replicate virtual environments to simulate drone flights in settings that closely resemble real-life scenarios. It offers the advantage of assessing efficiency of drone's networks in simulated environments at much reduced expenses and difficulties prior to conducting tests in actual situations. Selection of suitable simulator is contingent upon both testing purpose and array of features provided by each simulator [27,31]. Table 3 shows classification of simulation tools common to use with IoD. Moreover, simulators support real-time data analysis, allowing for immediate feedback and adjustments to system during simulations. This enables refined testing and optimization, improving accuracy of results before transitioning to field tests. As a result, simulation technologies are an essential part of the development IoD systems, facilitating safer, more cost-effective, and efficient operations for drone networks [27].

Table (3): Simulation tools [27]



GCS software	Free/ commercia	Interface	Supported Autopilots	Platforms	MAVLink compatible	language	License
QGroundControl	Free	Graphical	PX4 Pro, ArduPilot (APM) or any vehicle that communicates using the MAVLink protocol.	Windows/Mac/Linux/iOS and Android devices	Yes	C++	Open Source
Mission Planner	Free	Graphical	APM/PX4	Windows/Mac OS	Yes	C#	Open Source
APM Planner	Free	Graphical	MAVlink based autopilots including APM and PX4/Pixhawk	Windows, Mac OS, and Linux	Yes	C++	Open Source
MAVProxy	Free	Command line and console-based interface	Ardupilot MAVLink compatible	Linux	Yes	Python	Open Source
DroidPlanner	Free	Graphical	APM	Android Phones and Tablets	Yes	Java	Open Source
UGCS	Free, with limited capabilities	Graphical	APM, Pixhawk, DJI, Mikrokopter, YUNEEC, Micropilot, Microunmanned systems,	Windows, Mac OS, Ubuntu, Android, iOS	Yes	Human control interface with C#	Not open source

a- List of GCS software



Simulator	Commercial / free	language	Open source	Operating systems	Supported Vehicles	MAVLink compatible	SITL/HITL
FlightGear	Free	C, C++	Yes	Windows, Linux, Mac OS-X, IRIX FreeBSD, Solaris	Aircraft, unmanned systems	Yes	Yes
UE4Sim	Free	Python,C++	Yes	Windows, Linux	unmanned systems, cars	No	No
X-Plane	Commercial	C++	Yes	Android, iOS, Linux, MacOS, WebOS, Windows	Plane	Yes	HITL
AirSim	Free	C++, Python, C#, Java	Yes	Windows, Linux	MultiRotor QuadRotor	Yes	Yes
Gazebo	Free	C++, JavaScrip	Yes	Linux, Mac Windows	, Hex (Typhoon H480), Generic quad delta VTOL	Yes	Yes
jMAVSim	Free	JAVA	Yes	Linux, MacOs, Windows	Multirotor/Quad	Yes	Yes

b- List of simulators

10. Future Outlook

Researchers worked hard to improve security of IoD networks. However, since Ground Control Stations are a key part of these networks, it's important to secure data stored in GCS and protect commands sent to drones. Additionally, researchers should develop better systems to detect and prevent attacks, including identifying drones as potential attackers. Significant progress has also been made in improving IoD communication speed and storage efficiency [33].

Future Directions:

- Simulators and Security: Enhancing simulators like (Mission Planner) with secure IoD frameworks will make it easier to test drones communication and cryptography in realistic scenarios.
- 5G and IoT Integration: Future drones with 5G and IoT will play an important role in smart cities, but regulations need to be followed.
- AI and Security: Artificial intelligence, advanced communication technologies, and improved security will be critical for safer and smarter drone communication.

In the future, UAVs will expand beyond traditional uses like farming and construction to public safety and transportation.

11. Conclusion

Drones (UAVs) were mostly employed for military purposes. However, it is anticipated that the utilization of drones in civilian applications would soon surpass their military use. Due to the nascent stage of technological development and the continuous exploration of new application areas, hackers and attackers are increasingly targeting these systems to exploit their vulnerabilities for different malicious goals. Security threats against UAVs are directed the communication protocols inside the network. MAVLink is the predominant protocol for communication among UAVs. Despite its improved communication capabilities, MAVLink lacks a security method for encrypting messages, which can lead to significant repercussions. Hence, there is a requirement for a robust communication protocol that can effectively address the aforementioned problem. In conclusions the study highlights the significant risks associated with unencrypted and unauthenticated communication protocol in drones specially MAVLink which prioritizes safety and availability, where security should be essential in designing all systems and protocols. Considering security as core component of any software and hardware design, rather as a supplementary feature, will decrease capacity of malicious individuals to gain illegal access to remote systems, thus potentially defending surrounding communities.

Acknowledgements

Authors are thankful to Department of Computer Science, College of Science, Mustansiriyah University (https://uomustansiriyah.edu.iq/e-newsite.php), for supporting this work.

References

1. Lakshman, S. A., & Ebenezer, D. (2021). *Integration of internet of things and drones and its future applications*. Materials Today: Proceedings, 47(4), 944–949. https://doi.org/10.1016/j.matpr.2021.05.039
2. Samanth, S., K. V., P., & Balachandra, M. (2022). *Security in Internet of Drones: A comprehensive review*. Cogent Engineering, 9(1), Article 2029080. https://doi.org/10.1080/23311916.2022.2029080
3. Abualigah, L., Diabat, A., Sumari, P., & Gandomi, A. H. (2021). *Applications, deployments, and integration of internet of drones (iod): a review*. IEEE Sensors Journal, 21(22), 25532-25546. https://doi.org/10.1109/JSEN.2021.3082595
4. Labib, N. S., et al. (2021). *The rise of drones in internet of things: A survey on the evolution, prospects, and challenges of unmanned aerial vehicles*. IEEE Access, 9, 115466–115487. https://doi.org/10.1109/ACCESS.2021.3070405
5. Sharma, A., Vanjani, P., Paliwal, N., Basnayaka, C. M. W., Jayakody, D. N. K., Wang, H.-C., & Muthuchidambaranathan, P. (2020). *Communication and networking technologies for UAVs: A survey*. Journal of Network and Computer Applications, 168, Article 102739. https://doi.org/10.1016/j.jnca.2020.102739
6. Ghamari, M., Rangel, P., Mehrubeoglu, M., Tewolde, G. S., & Sherratt, R. S. (2022). *Unmanned aerial vehicle communications for civil applications: A review*. IEEE Access, 10, 102492-102531. https://doi.org/10.1109/ACCESS.2022.3208571
7. Dey, V., Pudi, V., Chattopadhyay, A., & Elovici, Y. (2018). *Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study*. In 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID) (pp. 398–403). IEEE. https://doi.org/10.1109/VLSID.2018.97
8. Bunse, C., & Plotz, S. (2018). Security analysis of drone communication protocols. In *Engineering Secure Software and Systems: 10th International Symposium, ESSoS 2018, Paris, France, June 26-27, 2018, Proceedings* (Vol. 10953, pp. 96–107). Springer International Publishing. https://doi.org/10.1007/978-3-319-94496-8_7
9. Allouch, A., Cheikhrouhou, O., Koubâa, A., Khalgui, M., & Abbes, T. (2019). *MAVSec: Securing the MAVLink protocol for ardupilot/PX4 unmanned aerial systems*. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 621–628). IEEE. https://doi.org/10.1109/IWCMC.2019.8766667
10. Chaari, L., Chahbani, S., & Rezgui, J. (2020, November). *MAV-DTLS toward security enhancement of the UAV-GCS communication*. In 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall) (pp. 1-5). IEEE. https://doi.org/10.1109/VTC2020-Fall49728.2020.9348584
11. Nayyar, A., Nguyen, B. L., & Nguyen, N. G. (2020). *The Internet of Drone Things (IoDT): Future envision of smart drones*. In A. Luhach, J. Kosa, R. Poonia, X. Z. Gao, & D. Singh (Eds.), *First International Conference on Sustainable Technologies for Computational Intelligence: Advances in Intelligent Systems and Computing* (Vol. 1045, pp. 569–579). Springer. https://doi.org/10.1007/978-981-15-0029-9_45
12. Abdelmaboud, A. (2021). *The Internet of Drones: Requirements, taxonomy, recent advances, and challenges of research trends*. Sensors, 21(17), Article 5718. https://doi.org/10.3390/s21175718
13. Boccadoro, P., Striccoli, D., & Grieco, L. A. (2021). *An extensive survey on the Internet of Drones*. Ad Hoc Networks, 122, Article 102600. https://doi.org/10.1016/j.adhoc.2021.102600
14. Ismael, H. M. (2021). *Authentication and encryption of drone communication using the HIGHT lightweight algorithm*. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(11), 5891–5908. https://doi.org/10.17762/turcomat.v12i11.6875
15. Kassim, G. E., & Hashem, S. H. (2022). *DMAV: Enhanced MAVLink protocol using dynamic DNA coding for unmanned aerial vehicles*. International Journal of Online and Biomedical Engineering, 18(11). https://doi.org/10.3991/ijoe.v18i11.34085
16. Abdulhameed, A. A., Al-Azawi, R. J., & Al-Mahdawi, B. M. (2020). *Modeling Web Security Analysis Attacks with CySeMoL Tool*. Al-Mustansiriyah Journal of Science, 31(3), 101–109. DOI: http://doi.org/10.23851/mjs.v31i3.876
17. Omolara, A. E., Alawida, M., & Abiodun, O. I. (2023). *Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey*. Neural computing and applications, 35(31), 23063-23101. doi.org/10.1007/s00542-023-07601-3
18. Ali, H. H., Naif, J. R., & Humood, W. R. (2023). *A new smart home intruder detection system based on deep learning*. Al-Mustansiriyah Journal of Science, 34(2), 60–69. DOI: http://doi.org/10.23851/mjs.v34i2.1267

19. Kumar, A., & Mehta, P. L. (2021). *Internet of Drones: An engaging platform for IIoT-oriented airborne sensors*. In D. Gupta, V. Hugo C. de Albuquerque, A. Khanna, & P. L. Mehta (Eds.), *Smart Sensors for Industrial Internet of Things: Internet of Things* (pp. 275–289). Springer. https://doi.org/10.1007/978-3-030-52624-5_16

20. Chakraa, H., Guérin, F., Leclercq, E., & Lefebvre, D. (2023). *Optimization techniques for Multi-Robot Task Allocation problems: Review on the state-of-the-art*. Robotics and Autonomous Systems, 104492. https://doi.org/10.1016/j.robot.2023.104492

21. Yanmaz, E., Yahyanejad, S., Rinner, B., Hellwagner, H., & Bettstetter, C. (2018). *Drone networks: Communications, coordination, and sensing*. Ad Hoc Networks, 68, 1–15. https://doi.org/10.1016/j.adhoc.2017.09.001

22. Haider, S. K., Nauman, A., Jamshed, M. A., Jiang, A., Batool, S., & Kim, S. W. (2022). *Internet of Drones: Routing algorithms, techniques, and challenges*. Mathematics, 10(9), Article 1488. https://doi.org/10.3390/math10091488

23. Yaacoub, J.-P., Noura, H., Salman, O., & Chehab, A. (2020). *Security analysis of drone systems: Attacks, limitations, and recommendations*. Internet of Things, 11, Article 100218. https://doi.org/10.1016/j.iot.2020.100218

24. Majed, D. M., Abdulhameed, A. A., & Gaata, M. T. (2023). *Botnet creation, life cycle, infrastructure, and detection techniques*. In 2023 Second International Conference on Advanced Computer Applications (ACA) (pp. 25–29). IEEE. https://doi.org/10.1109/ACA57612.2023.1034666

25. Khan, N. A., Jhanjhi, N. Z., Brohi, S. N., & Nayyar, A. (2020). *Emerging use of UAVs: Secure communication protocol issues and challenges*. In F. Al-Turjman (Ed.), *Drones in Smart Cities* (pp. 37–55). Elsevier. https://doi.org/10.1016/B978-0-12-819972-5.00003-3

26. UAVCAN Development Team. (2019). *UAVCAN communication protocol*. Retrieved from https://uavcan.org.

27. Koubâa, A., Allouch, A., Alajlan, M., Javed, Y., Belghith, A., & Khalgui, M. (2019). *Micro Air Vehicle Link (MAVLink) in a nutshell: A survey*. IEEE Access, 7, 87658–87680. DOI: 10.1109/ACCESS.2019.2924410

28. Chen, H. H. (2024). *Developing a custom communication protocol for UAVs: Ground control station and architecture design*. Internet of Things, 27, Article 101319. https://doi.org/10.1016/j.iot.2024.101319

29. Khan, M. A., Kumar, N., Mohsan, S. A. H., Khan, W. U., Nasralla, M. M., Alsharif, M. H., & Ullah, I. (2022). Swarm of UAVs for network management in 6G: A technical review. IEEE Transactions on Network and Service Management, 20(1), 741-761. https://doi.org/10.1109/TNSM.2022.3213370

30. Dorave, J., & Sadiwala, R. (2022). A secure communication protocol for unmanned aerial vehicles using IoT protocols. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 14(04), 79-88. https://doi.org/10.18090/samriddhi.v14i04.13

31. Collins, J., Chand, S., Vanderkop, A., & Howard, D. (2021). A review of physics simulators for robotic applications. IEEE Access, 9, 51416-51431. https://doi.org/10.1109/ACCESS.2021.3068762

32. Rani, S., Chauhan, M., Kataria, A., & Khang, A. (2023). IoT equipped intelligent distributed framework for smart healthcare systems. In Towards the Integration of IoT, Cloud and Big Data: Services, Applications and Standards (pp. 97-114). Springer Nature Singapore. https://doi.org/10.1007/978-3-030-52624-5_16

33. Eskandaripour, H., & Boldsaikhan, E. (2023). Last-mile drone delivery: Past, present, and future. Drones, 7(2), 77. https://doi.org/10.3390/drones7020077

34. Abro, G. E. M., Zulkifli, S. A. B., Masood, R. J., Asirvadam, V. S., & Laouiti, A. (2022). Comprehensive review of UAV detection, security, and communication advancements to prevent threats. Drones, 6(10), 284. https://doi.org/10.3390/drones6100284

35. Mekdad, Y., Aris, A., Babun, L., El Fergougui, A., Conti, M., Lazzeretti, R., & Uluagac, A. S. (2023). A survey on security and privacy issues of UAVs. Computer Networks, 224, 109626. https://doi.org/10.1016/j.comnet.2022.109626

36. Mahato, P., Saha, S., Sarkar, C., & Shaghil, M. (2023). Consensus-based fast and energy-efficient multi-robot task allocation. Robotics and Autonomous Systems, 159, 104270. https://doi.org/10.1016/j.robot.2022.104270

37. Tlili, F., Fourati, L. C., Ayed, S., & Ouni, B. (2022). Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures. Drones, 6(10), 284. https://doi.org/10.3390/drones6100284