Article

Not peer-reviewed version

Communication Security for UAV in Military

Rashid Alshamsi and Mohammad Naouss *

Posted Date: 18 April 2025

doi: 10.20944/preprints202504.1585.v1

Keywords: drone communication; security; UAV networks; inter-drone authentication; drone's authentication doi:10.20944/preprints202504.1585.v1

Article

Communication Security for UAV in Military

Rashid Alshamsi and Mohammad Naouss *

College of Information Technology, United Arab Emirates University, Al Ain, United Arab Emirates
* Correspondence: m.naouss@uaeu.ac.ae

Abstract: Unmanned Aerial Vehicles (UAVs) are essential in a variety of fields, including emergency rescue, security patrol, and agricultural planting. UAVs present benefits like allowing ground communications even in situations where connectivity is restricted by physical barriers. Conversely, they expand the area that can be attacked. For example, physical drone attacks give the attacker credentials to introduce fake data into the Internet of Things (IoT) network, compromising user safety as well as security. Authentication is essential in this situation to ensure security. One major obstacle to UAV communications is privacy and security concerns. UAVs can potentially give an increase in security concerns due to their open-access communication environments. These concerns may include threats to authentication and the potential for location and other sensitive data to be leaked to unauthorized parties. However, security against drone attacks cannot be ensured by the authentication schemes that are currently in place. Because of its performance and security, elliptic curve cryptography (ECC) is frequently used in the design of authentication protocols. So, in this paper, an elliptic curve cryptography-based scheme is presented. ECC is particularly preferred because it can provide complete safety with shorter key lengths, which is suitable for drones with limited resources. The mathematical properties of elliptic curves strengthen the algorithm's resilience to various cryptographic attacks, ensuring a high level of security.

Keywords: drone communication; security; UAV networks; inter-drone authentication; drone's authentication

1. INTRODUCTION

One of the main issues that might restrict the advancement of information-based technologies and services in the future is security. Certain situations, such nuclear power plants, aerospace, and defense, make even small security flaws intolerable because of their effects on the country or the world. IoT is clearly having a significant impact on our society, and since so many diverse items are present, it is easy for IoT and its many applications to offer a wide range of services. But the exponential rise in connected devices also brings up some very severe difficulties, particularly those related to security and privacy, which end up being the main roadblocks to the widespread implementation and use of IoT. Two factors may be used to describe the primary causes of these security flaws [1].

First, the IoT system is more vulnerable to many incidents due to its wireless communication environment, including data manipulation, identity spoofing, leaking of private information, and message eavesdropping. Second, the processing power, storage capacity, and network capacity of various IoT device types are usually constrained, which makes the system challenging to deploy sophisticated security solutions and, consequently, vulnerable to a variety of security threats. These weaknesses might be inconvenient or possibly have detrimental effects on people's lives. Moreover, IoT is classified as a system of systems as its many use case scenarios capture its heterogeneity [2]. However, integrating the additional services and scenarios is challenging due to the various security needs of each individual application scenario. To overcome the challenges, it is necessary to integrate various security technologies and solutions. Even if centralized security solutions like public-key infrastructure (PKI) are effective, they still have major scaling problems in an IoT system this complex. Therefore, new security solutions should be offered to address such vulnerabilities and guarantee that new devices or users may easily integrate with new services and that the system can only be used by those who have been verified and allowed.

To increase security, several block ciphers have been suggested by different researchers up to this point, all based on separate internal structures and operating ideas. The United States officially adopted the Data Encryption Standard (DES) cipher as a Federal Information Processing Standard (FIPS) in 1977. With a low degree of security, it gains less property and throughput per security level. The International Data Encryption Algorithm (IDEA) [3], initially suggested in 1991, is based on the XOR, furthermore, and modular multiplication operations. In this instance, unsigned 16-bit integers are used for all data operations. The Advanced Encryption Standard (AES) block cipher, which is great for high rates and minimal data overhead, was authorized by FIPS in 2001. Additionally, it can use cryptographic keys of 128, 192, and 256 bits to encrypt and decode data in blocks of 128 bits [4]. Involutional structure and cyclic key timetable characterize the iterated block cipher CURUPIRA, developed in 2007 by Paulo S. L. M. Barreto and Marcos A. Simplicio Jr. [13]. It recognizes keys with a configurable number of rounds of 96, 144, or 192 pieces and uses a 96-piece information block.

Another block cipher, called PRESENT, was proposed by A. Bogdanov et al. in 2007 [14]. Its ultra-lightweight primary equipment provides a level of safety commensurate with its small size. The 31-round SPN consists of a replacement layer, a stage layer, and a round key expansion. It was designed to function with low-cost devices such as RFID labels. A Light Encryption Gadget (LEG) cipher with fundamental cutoff points on the number of dynamic S-boxes during a block cipher encryption was suggested by Jian Guo et al. in 2011 [7] considering AES-like design specifications. The ELWC (what means ELWC?) approach is suggested by the authors Madavi K P, Sowjanya K as a means of securing data produced by Internet of Things devices [8]. Rather than considering 64 bits for each piece of device data, the data is combined based on bit-requirement size to form a single plain text that can be encrypted and decrypted. The suggested approach with embedded data is contrasted with the conventional LWC method, or PRESENT. Comparing the encryption and decryption times of the two methods, the ELWC approach outperformed the conventional way using the non-embedded data format.

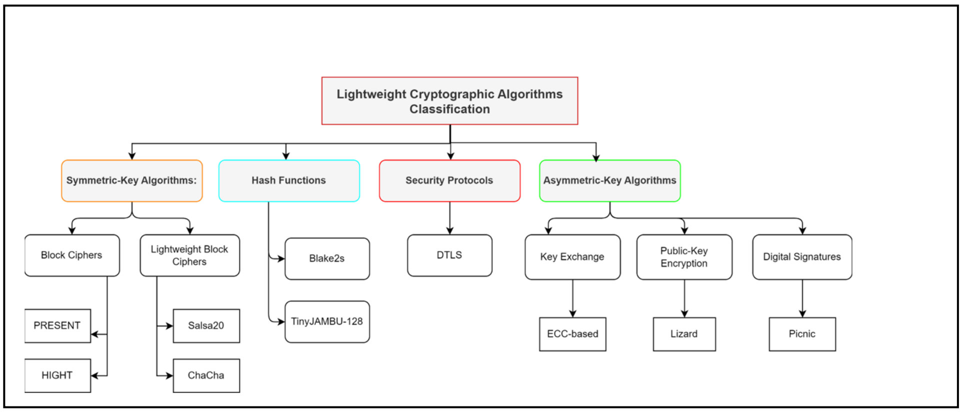
The piece-cut lightweight block cipher square form was proposed by Wentao Zhang et al. in 2015 [9]. It is extremely equipment-well-disposed and can be conducted on various stages promptly. The ARX-based block cipher SPARX, which belongs to the LTS-based family of block ciphers, was suggested by Daniel Dinu et al. [10]. SPARX has exceptional performance on many inserted stages, such as the 16-bit TI MSP430 and the 32-digit ARM Cortex-M3. The 64-digit block ciphers Secure IoT (SIT), a low-cost encryption algorithm that needs a 64-bit key to encode data, was suggested by Muhammad Usman et al. [11]. Symmetric key block ciphers, such as SIT, use a 64-bit key and plain text.

Xu Yang, and Xuechao suggested a safe, low-cost IoT authentication method based on blockchain technology [12]. Their architecture creates and implements a decentralized, privacy-preserving, lightweight authentication system by fusing the blockchain with the MSR cryptography algorithm. Additionally, the suggested scheme's security is examined. They assess our scheme's effectiveness by putting it into practice on Remix and contrasting its communication and computation costs with those of other methods.

The contribution of this research is as follows:

1. Indicated an elliptical curve cryptography with optimal RSU distribution for privacy-aware secure routing to enhance UAV's performance.
2. The trusted authority is made extremely secure by elliptical curve cryptography, which enhances UAV's confidentiality and authentication.
3. The elliptic curve cryptography-based lightweight authentication technique is designed to enable secure message transmission between the drones that are in communication.

The structure of the research is as follows. Section 2 discusses the relevant works from an optimization and security-based perspective. The state of the art regarding the UAV subsystem and a comparison of cryptographic techniques are covered in Section 3 on cryptography methods. The current protocols for UAV authentication are compared in Section 4 Results and Discussions, along with their implementation on SW, HW, and hybrid systems. The research is concluded with future directions in Section 6. Implementation in just one domain and can be a section alone, then results and discussions.



Statement of Problem:

Benefits of UAVs include the ability to communicate with the ground even when physical obstacles are preventing connectivity. Precisely the opposite they increase the attackable area. One possible consequence of UAVs' open-access communication settings is a rise in security issues. Threats to authentication & the possibility of location and other private information being disclosed to unauthorized individuals are a few examples of these issues. That is why Elliptic curve cryptography (ECC) has been widely employed in authentication protocol design due to its performance and security. Because elliptic curves have certain mathematical properties, the technique is more resistant to various cryptographic attacks, which ensures a high level of security.

Objective:

One of the most important components of security is authentication as it protects against data theft and unauthorized access. However, there are several limitations to the current UAV authentication systems, including the need for specialized hardware, a lack of security, costly overhead, and more.

To achieve optimal drone communication security and privacy, advanced cryptographic approaches are essential. Since ECC can provide full safety with shorter key lengths, it is particularly recommended.

Because ECC is so successful at generating keys, exchanging keys, and enabling electronic signatures, it provides a practical and secure solution for safeguarding confidential data in drone communication networks. It satisfies the requirements for both reliable safety and efficient operation.

2. LETRATURE REVIEW

Lightweight Cryptographic (LWC)

Combining the terms "light" with "weight" results in lightweight encryption. In the context of asset obligated IoT devices, lightweight encryption is a component of an outdated cryptographic computation. For the Internet of Things to be secure, encryption is an essential development.

A method of protecting data and communication via programs that allows processing of the information only by the people for whom it is intended is called cryptography. Writing is identified by the term "graph," and hiding by the word "crypt." Two basic kinds of cryptographic keys exist: the first is symmetric, quick, and easy to use, while the second is asymmetric and requires laborious computation of both a public and private key. Public keys are not secret, but symmetric keys and private keys that are always secret are what primarily ensure the security of cryptographic applications.

These are further separated into hash functions from symmetric, stream ciphers, and block ciphers. This section provides an explanation of the SPN type, which is a type of block cipher. The categorization of the lightweight method is shown in Figure 1.

The two types of cryptographic algorithms are symmetric and asymmetric. Asymmetric encryption and decryption processes use two separate keys, whereas symmetric encryption and decryption processes use just one key. While symmetric key cryptography is quick and secure, key sharing between two parties can be problematic. Asymmetric utilizes two keys: a private key for authentication and a public key for secrecy and integrity [13].

Table 1. Standard Cryptographic Algorithms.

Algorithm	**Description**
AES	Block cipher encryption is a substitution-permutation network, and the number of rounds and key size have a significant impact on how safe the technique is.
DSS	It generates digital signatures using the Digital Signature Algorithm (DSA) and the SHA-2 family of hash functions.
Diffie-Hellman	To create a secret key that is shared between two parties across an unsecure channel, asymmetric key exchange method is employed. It serves as the basis for many cryptographic protocols' safe key exchange.
SHA-2	SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256 are among the hash functions in the family that are constructed using the Merkl-Damgard construction.
SHA-3	"Sponge construction" is used to build the hash function. A function called sponge creation may take any bit stream as input and produce an output bit stream with any length that is needed.
RSA	It is an asymmetric encryption method utilized for safe exchange of keys and digital signatures. RSA key pairs are made up of a key that is publicly accessible and a private key.
Speck	Block cipher encryption method, which functions similarly to ChaCha and has been fine-tuned for software implementation performance
Elliptic Curve Cryptography	This digital signature and asymmetric encryption technique makes use of elliptic curve mathematics. Comparing with other asymmetric algorithms, ECC provides good security with lower key lengths, making it appropriate for situations with limited resources.
Blowfish	It is a fast and straightforward symmetric-key block cipher. Even though it is thought to be safe, AES is now more frequently utilized instead of it.
3DES	an encryption system using symmetric keys that cascades using the Data Encryption Standard (DES) algorithm three times. It is still employed in older systems since it was intended to offer a better level of security than DES.
HMAC	a construction for employing a cryptographic hash function (SHA-256, for example) to generate a message authentication code. It is frequently employed for authentication and data integrity verification.
ChaCha	encryption system known as stream cipher, whose round operations are limited to modular addition, rotation, and xor
RC4	a symmetric stream cipher which was often employed in the past for wireless encryption and secure sockets layer (SSL). Nevertheless, it is now widely regarded as outdated and contains known weaknesses.

ECDSA	utilized in instances with asymmetric keys for digital signatures
zk-SNARKs	enable one party to prove possession of specific information without revealing the information itself.
MPC	allow different parties to collaborate on computing a result over the inputs they provide while maintaining the privacy of those inputs
Fully Homomorphic Encryption (FHE)	performs actions on encrypted data such as addition and multiplication. This sophisticated encryption method can handle increasingly intricate calculations while protecting the privacy of data.
Blockchain-Based Cryptography	Drone communication could gain from the integration of blockchain technology for safe and transparent data integrity verification, authentication, and logging. Frequently employed in blockchain-based systems are algorithms such as the Elliptic Curve Digital Signature Algorithm (ECDSA).
Hash-Based Signatures	Some signature schemes, like the Lamport and Merkle schemes, are considered into consideration because they can resist quantum attacks. They are involved in the PQC project at NIST.

Key size that raises the convolution is the sole issue with asymmetric encryption. Because of its small file size, it can be sent quickly, requires less storage space, and is the recommended block cipher for most devices with limited resources. Fixed size blocks are used in block ciphers for both encryption and decryption at the same time. Block sizes for most block ciphers are 64 or 128 bits.

Multiple cipher invocations are used to encrypt messages containing more than 128 bits. One division of the data is a four-by-four array. Each block has 128 bits overall since there are eight bits per byte, but a stream cipher continually receives bits as input.

To provide security in back-to-back communication within a device, LWC is often utilized in smaller, resource-constrained devices. The LWC algorithm protects transmitted data between the source and the destination by guaranteeing authentication, nonrepudiation, secrecy, and integrity. LWC adheres to cryptographic principles.

Millions of devices operating on various platforms provide odd issues for users and a significant change in resource-constrained devices, which also results in security issues with integrity, confidentiality, and authentication [18].

Because these devices have direct interface with the outside world and gather private data, they are easily targeted by attackers [17]. Though cryptography techniques are still inapplicable to tiny devices like RFID, tags, actuators, sensors, etc., they may be the best option in this case for storing and exchanging data over the internet. The problems may be fixed and the communications between the Unmanned Aerial Vehicles (Drones) secured with a lightweight cryptographic scheme.

The table below displays the most widely used hash algorithms and encryption techniques. High-security encryption methods like AES and dss enable several rounds of operations. ChaCha is more optimized for mobile devices and has a higher CPU efficiency. Hashing functions are essential for randomization in cryptography. The hash functions that are most often employed are SHA-3 and SHA-2. Even though SHA-3 is more secure, its slower software prevents it from being widely utilized [19].

2.1. Typical Applications

LWC relevance in many contexts where secure yet effective cryptographic solutions are required due to resource constraints. Internet of Things, or IoT, devices, embedded systems, networks of wireless sensors, wearable and mobile devices, unmanned aircraft (drones), limited in resources environments, low-power and battery-powered devices, safe authentication, and secure communication protocols are some examples of typical applications of lightweight cryptography.

Figure 2 illustrates the several common uses for lightweight cryptography, wherein approaches are used to safeguard data and provide secure communication in contexts with limited resources.

For the protection of protocols and communication interfaces in a variety of resource-constrained situations, lightweight cryptography provides a critical role. Application areas for this cryptography expertise include a range of communication interfaces and protocols.

it is particularly useful for tackling the difficulties posed by systems and devices with constrained memory, processing, and energy resources. Numerous scenarios are covered by the applications, such as IPv6 over A low-power Wireless Personal Area Networks (6LoWPAN), Bluetooth Low Energy, or BLE, the Zigbee RFID, near-field communications (NFC), CoAP, LoRaWAN, MQTT, and wireless sensor networks (WSNs).

Custom communication protocols catered to applications are also included. Within these interfaces, lightweight cryptography plays a critical role in maintaining communications security while reducing computational and memory overhead, guaranteeing the privacy, reliability, and authenticity of data transfer. The finding of suitable lightweight cryptography strategies and algorithms is an important research concern, depending on the interface, security needs, and limitations imposed by the devices or systems involved.

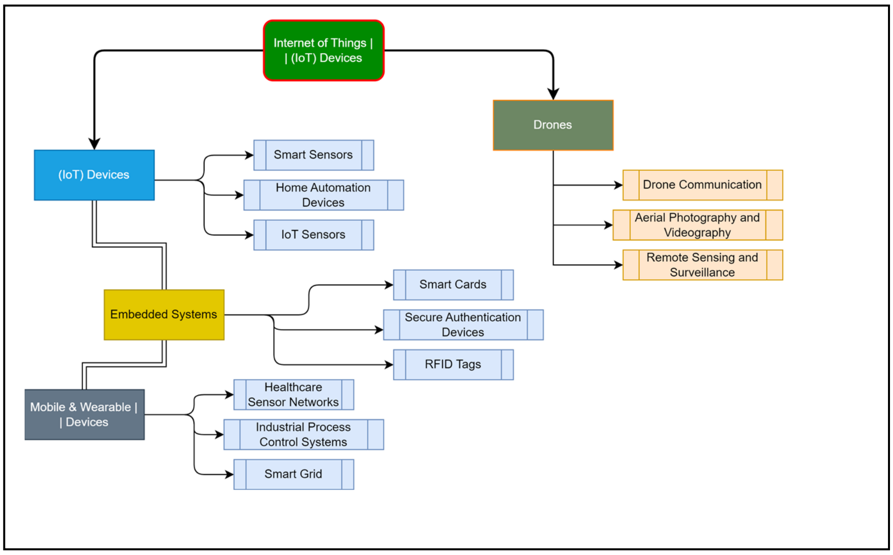

Internet of Things | | (IoT) Devices
Drones
(IoT) Devices
Smart Sensors
Home Automation Devices
IoT Sensors
Drone Communication
Aerial Photography and Videography
Remote Sensing and Surveillance
Embedded Systems
Smart Cards
Secure Authentication Devices
RFID Tags
Mobile & Wearable | | Devices
Healthcare Sensor Networks
Industrial Process Control Systems
Smart Grid

Figure 2. Applications of lightweight cryptography.

2.2. Communication Interfaces

Unmanned aerial vehicles (UAVs), commonly referred to as drones, use a variety of communication interfaces and protocols to guarantee efficient operation and data transmission. Drones frequently employ a variety of communication interfaces, such as: Telemetry Systems, Radio Control (RC), Wireless Communication, GPS (Global Positioning System), Cellular Networks, FPV (First-Person View), Satellite Communication, Secure Data Links, Mesh Networks. Radio waves in bands like HF (high frequency) and UHF (ultra-high frequency) are used in the most popular drone communication method. RF datalinks are still only available in line-of-sight (LOS) but have a longer range than Wi-Fi. They can be digital or analog. In the UAV communications system, range is determined by the size of the antenna, the strength of the transmitter, and the frequency; lower frequencies offer greater ranges but lower data rates [19]. SATCOM, offers exceptional uptime and coverage practically everywhere on Earth. Unfortunately, because of the equipment's relative mass, the approach is not currently appropriate for platforms with restricted SWaP (size, weight, and power).

Additionally, SATCOM needs an ongoing service, which might be costly. UAV communications also take advantage of 4G and 5G cellular connections. Cellular datalinks can facilitate BVLOS (beyond visual line of sight) operations, albeit coverage may vary, especially outside of metropolitan areas. 5G offers several benefits including ultra-low latency and increased data throughput. 5G is ideal for applications that require a lot of bandwidth, such streaming HD video [17]. Additionally, Drone-to-drone communications can facilitate drone swarms when several UAVs collaborate to complete tasks more successfully. Every drone might function as a node in a mesh network, utilizing mobile ad hoc networking, or MANET, technologies to provide flexible routing and drone mobility. Drones may be able to serve as a communications relay thanks to this setup, offering internet and wireless connection in previously unconnected rural places.

Modern advancements in wireless communication and device technologies have resulted in a significant rise in the global number of linked nodes in use. Fitness trackers, speakers, headphones, automobiles, bicycles, and other nodes may communicate with one another because of the Internet of Things, networks. vehicular networks, which enable communication between vehicles (vehicle-to-vehicle, or V2V) and between vehicles and various infrastructures (vehicle-to-infrastructure, or V2I) have become a crucial component of the Internet of Things and next-generation networks (i.e., networks that operate beyond 5 G and 6 G) [4]. According to a recent prediction by Research and Markets (RM), the vehicle-to-everything (V2X) market is expected to reach $1, 692.7 billion by 2030, growing by around 64.6% year between 2020 and 2030 due to the growing need for safe and fully autonomous cars [5]. Considering this, scientists have lately begun to make progress in the analysis and development of next-generation communication technology, or beyond 5 G (B5G), also referred to as sixth generation (6 G) systems. These systems are expected to support V2X communications and offer data rates in the range of Terra bps, trillion-level user access, and ultra-low latency with ultra-high efficiency. As a result, 6 G communications are starting to become crucial for large-scale V2X networks.

2.3. Drone Interfaces

The serial ports (RS232, RS422, and RS485) were all developed to increase transmission distance, speed, and the number of devices that could be connected at once. A two-wire connection can only be made with an RS232 port; a four-wire connection can connect to 32 devices in a bidirectional full-duplex mode; a two-wire connection can connect to 10 devices in a bidirectional half-duplex mode; and a four-wire connection can connect to 32 devices in a bidirectional full-duplex mode.

Because technology is advancing so quickly, intelligent appliances may gather data and utilize IoT to share it with other internet-connected devices. In Internet of Things networks, time synchronization, system localization, and data validity are considered irrelevant. A communication or network is only considered secure if certain requirements are met. These essential elements include non-repudiation, availability, integrity, privacy, and secrecy [1].

- Confidentiality: The information sent between the devices needs to be kept secret. The person with access should be the only one to whom the information is disclosed. While keeping sensor data safe from unauthorized access, confidentiality also allows authorized users to access it.
- Integrity: Data is considered to have integrity if it is accurate, consistent, and uncompromised. It is the guarantee that data hasn't been inadvertently or purposely tampered with or changed. Stated differently, integrity is the veracity and accuracy of information that has been obtained.
- Availability: When needed, authorized users should be able to quickly access the data. It makes no difference how accurate and private the data is if the user is unable to access it.
- Authorization: Information is made available to individuals who have been allowed access through the procedure of authorization.
- Authentication: Using predetermined credentials, the authentication process entails interacting with various people and their devices to verify the authenticity of the device.
- Non-Repudiation: In an Internet of Things (IoT) context, certain nodes may send data utilizing two or more identities. There is a serious security danger here. The reputable source is referred to as non-repudiation.

- Privacy: Since the Internet of Things (IoT) is a network of interconnected applications, it is critical to protect data against unauthorized access and leaking of any personal information about users, devices, or networks. The user must be able to provide the outside world access to a significant amount of data.

Must protect data transfer security on several levels from all potential risks. If even one of the previously listed factors is compromised, the entire network is at risk [2].

[14] describes the FPGA hardware implementation of two lightweight cryptographic algorithms: PRESENT and DM-PRESENT. The performance of the implemented cores is assessed by the authors in terms of throughput, latency, and resource use, and they also make a comparison between the developed cores and other current implementations.

[15] investigates the requirement for LWC algorithms in IoT devices to protect limited items. They examine the most recent state-of-the-art LWC algorithms and assess how well they work in terms of memory, energy usage, and security. They evaluate these algorithms' performance in comparison to established cryptographic algorithms like RSA, AES, and SHA. The authors conclude that IoT devices with limited resources can benefit from lightweight cryptographic algorithms like PRESENT, PRINCE, and SIMON, which offer a high level of security with little resource usage. They do point out that the final algorithm selection is determined by the needs and constraints of the IoT device in use.

A comparison of many lightweight cryptographic hash algorithms is presented in [8], together with information on implementation factors, performance measurements, and security features. The writers assess these hash functions' performance across a range of platforms, such as embedded systems, mobile phones, and Internet of Things gadgets, and contrast it with those of other hash functions already in use.

A summary of the many kinds of lightweight cryptographic protocols, such as key agreement protocols, message authentication codes, and symmetric and asymmetric encryption algorithms [5]. The efficacy of these protocols in fulfilling the security needs of Internet of Things applications, including device authentication, data secrecy, and data integrity, is assessed by the authors.

In contrast to WSNs, VANETs, and MANETs, UAVs have special qualities. distributed networks are more able to resist security breaches than unmanned aerial vehicles (UAVs). Unmanned aerial vehicle (UAV) usage has been limited by several security concerns.

An RFID-based authentication system is explained in [20]. This method uses cryptographic IDs to guarantee device uniqueness and privacy. There is a basic drawback to the work since there is no mutual verification.

A method of anonymous mutual authentication with TPMs (Trusted Platform Modules) was given in [21]. The solution will cost more since TPMs are expensive, specialist security co-processors that must be added to the system. Additionally, the authors failed to investigate the UAV nodes' resistance to physical attacks and manipulation, which might allow an enemy to quickly acquire intelligence and launch an attack.

Similarly, in [32], a blockchain-based key management system for mixed UAV networks was put out. This plan was fully distributed, but it needed a strong cluster head drone to oversee the blockchain, which might not be sufficient in some circumstances.

3. PROPOSED METHODOLOGY

3.1. Unmanned Aerial Vehicles

UAVs can be utilized as a platform for a variety of functions, including pesticide spraying, picture and video shooting, air show production, transportation, and communication relay. It is also extensively utilized in military applications such as electronic countermeasures, targeted strikes, anti-radiation strikes, surveillance, and reconnaissance.

The most recent papers address a wide range of subjects, such as security for 6G communication, applications, and networking enhancements. UAV communication is heading toward 6G networks as technology develops, and during the past three years, study articles have increased in volume to varying degrees. By focusing on the study topic, we have selected, our research method enables us to gain a broad overview of the body of literature currently available on fundamental 6G UAV communication technology. UAV communication has potential in a range of fields, including academics, business, and even the military, due to the wider area of study. Since the creation of bitcoin, people all around the world have realized the immense value of a decentralized system that can be used in a variety of industries [22].

Nearly all Internet of Things, or IoT, gadgets are connected to legacy internet via a typical centralized infrastructure. The decentralized manner that these gadgets may now interact with one another thanks to the blockchain is a novel idea. This idea guarantees immutable data flow between nodes, eliminates a single point of failure, and strengthens the blockchain system. Compared to the traditional blockchain implementation that requires clusters and strong computers, the heterogeneous nature of IoT devices poses minimal hurdles for blockchain applications [23].

In a comparable manner, the Ethereum blockchain makes use of smart contract technology and is seen as a development of the fundamental blockchain concept [24]. The development of a smart contract, which allows for the decentralized implementation of code and goes beyond just storing record transactions in accounts, is bringing crucial aspects of blockchain technology to life. Smart contracts may be tailored to enable for contract enforcement and storage, enhancing the blockchain system's capacity to function as more than just a database.

A UAV 6G network's integration of blockchain technology may cause network dispersion, which is uncommon in traditional blockchains and mostly relies on wired networks. The present research [25] addresses the difficulties caused by the divides within swarms. The Swarm DAG method was developed to accurately control the network's splits and merges during the partitions to archive reliable partitions.

S. Okamoto, J. H. Lee, and S. Kawabata [26] look at drone use for structures and enterprises. Navigating becomes challenging when we consider deteriorating infrastructure and the incapacity to receive GPS signals. Therefore, a camera is used to trace the location of an algorithm for location estimation indoors. In the intended arrangement, the localization data and target points are determined and tested. To minimize obstacles on the journey path, a control system is also computed.

Low-range TUAVs, also known as tactical drones, are a type of small-to-medium drones designed primarily for military usage in high-risk areas. Their purposes include enhancing military operations, minimizing human mistake, guaranteeing security, and advancing defense tactics. Applications for it include logistical assistance for soldiers in temporarily inaccessible places, threat-prone area surveillance, and even shooting down an adversary from a distance [26]. These drones can cover many kilometers in range.

F. Ronaldo, D. Pramadihanto, and A. Sudarsono [27] investigate the many incidents against UAVs that are tasked with specific missions by the client and entrusted with privacy. Privacy may be jeopardized by trespassing and duplicate nodes. When it comes to the Internet of Drones, the target area is likewise unsafe for transmission and retrieval. UAV data transfer between the drones and servers needs to be reliable. AES, SHA, and ECC are multi-layer methods that have been utilized at each node to create a more secure architecture. Further paragraph illustrates the state of art of the Drone subsystem like hardware, software, and Hybrid method of secure the communications with their characteristics.

We reference the following publications about authentication methods created for SUAVs (drones) and UAVs in general. For drone-assisted 5G networks, Alladi et al. suggested a PUF-based authentication mechanism in [28]. Through the protocol, a base station and a drone may establish a secret key and mutually authenticate each other. Nevertheless, their protocol only uses PUF at the drone side, therefore it isn't a true mutual authentication. Teng et al. [29] presented an authentication system that makes use of the Public Key Infrastructure, or PKI, and Elliptic Curve Cryptography, for inter-drone communication. While their protocol could offer a degree of safety, it is highly resource-intensive for devices with limited resources, such as drones. A PUF-based authentication technique for IoD-based UAV settings was presented by Gope et al. in [30]. The protocol enables the establishment of a secret key and the sharing of private data between a UAV (or drone) and a UAV service provider (USP) through authentication utilizing PUFs. The USP's storage of the registered drones' CRPs is one of the protocol's security flaws. Therefore, the CRPs might be revealed or utilized to pose as the drones if the USP is maliciously abused (by an insider, for example).

A lightweight authentication method known as PCAP was introduced by Pu et al. [31] to enable mutual authorization among a UAV and a ground station as well as the creation of a secret key enabling secure communications. Duffing mapping and PUF technologies are used in the protocol. However, the protocol keeps the drones' CRPs in the control station's database in unencrypted. The enrolled CRPs may become public knowledge and the base station may pose as the authorized drone if the database is breached, or the grounds base is maliciously utilized (by an insider). Furthermore, the protocol employs a distinct CRP for every authentication session; that is, a previously used CRP will not be reused. Given that there is a limited number of CRPs, this is a form of design problem. The procedure could eventually run without CRPs. Using nonces to make each CRP unique and repeating the CRP several times might be one way to address this problem.

There are several difficulties and restrictions to UAV communication, such as:

a. Security and privacy: Unauthorized access, data manipulation, and spoofing attacks are just a few of the cyberthreats that UAV communication networks are susceptible to. Maintaining the authenticity and security of data requires ensuring private and secure interactions between UAVs and base stations.

b. Interoperability and Standardization: Interoperability issues arise because UAV communication systems frequently use diverse equipment and protocols. Standardization is necessary to enable smooth coordination and communication amongst UAVs made by various manufacturers or service providers.

c. Trust and Accountability: Several parties are involved in UAV communication, including service providers, regulatory bodies, and UAV operators. Efficient and transparent operations depend on these entities building confidence and accountability. Concerns concerning data tampering and the introduction of single points of failures are possible with centralized trust arrangements.

d. Spectrum management: For UAVs to communicate and be controlled, they need to have access to radio frequency spectrum. Effective spectrum management and allocation are essential to avoid interference, ensure dependable.

3.2. State of the Art About UAV Subsystem

UAV Hardware: Fixed wing systems and rotary wing systems are the two (2) categories into which drones are separated. There are notable variations in their volatile qualities. A fixed wing UAV is like a tiny version of a normal plane. It is a highly efficient system that can stay in the air for a long period relative to the energy it uses because of aerodynamic design and development. In its most basic configuration, a rotary wing unmanned aerial vehicle (UAV) replicates a smaller version of a helicopter with two rotors, much like manned helicopters.

A more thorough understanding of the UAV’s subsystems and their parts is provided by the detailed diagram.

Advanced rotary wing unmanned aerial vehicles (UAVs) require systems with three, four, six, or eight rotors or more because they can only take off with their mechanical power. This system's ability to navigate in small areas is its key advantage. Rotating wing UAVs are the most customizable of the two UAV kinds, offering a greater degree of freedom in hardware customization. This is because altering the solid wing hardware in any way might affect its aerodynamics and negate its biggest benefit. Prior to every flight, a few basic items on every aircraft need to be inspected. These consist of batteries, telemetry module, landing frame, GPS, motors, propellers, chassis, compass, gimbal (for maintaining compass horizontal), and camera. However, depending on the requirements of their task, UAVs are adaptable systems that may also incorporate other gear.

Detailed table outlining the parameters for several cryptographic techniques—including lightweight ones—used for drone communication.

Table 3. Comparison between Cryptographic Technique.

Cryptographic Technique	Typical Use Cases	Key Criteria	Lightweight Criteria	Notable Examples
AES (Symmetric)	Secure Data Transfer	Strong Security	Efficient, Low Overhead	AES-128, AES-256
Lightweight Block Cypher	Resource-Constrained	Efficient	Designed for Constraints	PRESENT, HIGHT, Speck
Lightweight Stream	IoT, Low-Power Devices	Efficient	Designed for Constraints	Grain, Trivium, Salsa20
SHA-256 (Hash)	Data Integrity	Strong Security	Lightweight, Efficient	SHA-256, Blake2s
RSA (Asymmetric)	Secure Key Exchange	Strong Security	Not Lightweight	N/A
ECC (Asymmetric)	Key Exchange, Signatures	Strong Security	Lightweight, Short Keys	ECC-256, Curve25519
Salsa20 (Stream)	Secure Streaming	Strong Security	Lightweight, Fast	Salsa20, XSalsa20
Lightweight Public key encryption	Low-Resource IoT	Efficiency, Secure	Designed for Constraints	Lizard

3.3. *Cryptography Techniques:*

The selection of a communication method for drone applications, whether military or civilian, is contingent upon several elements, such as the needs, operating surroundings, and security considerations. Drones have limited resources; thus, lightweight cryptography is usually used. We talk about popular non-quantum-safe public-key cryptography systems as well as quantum-safe encryption techniques. In this section, lattice-based cryptography is highlighted.

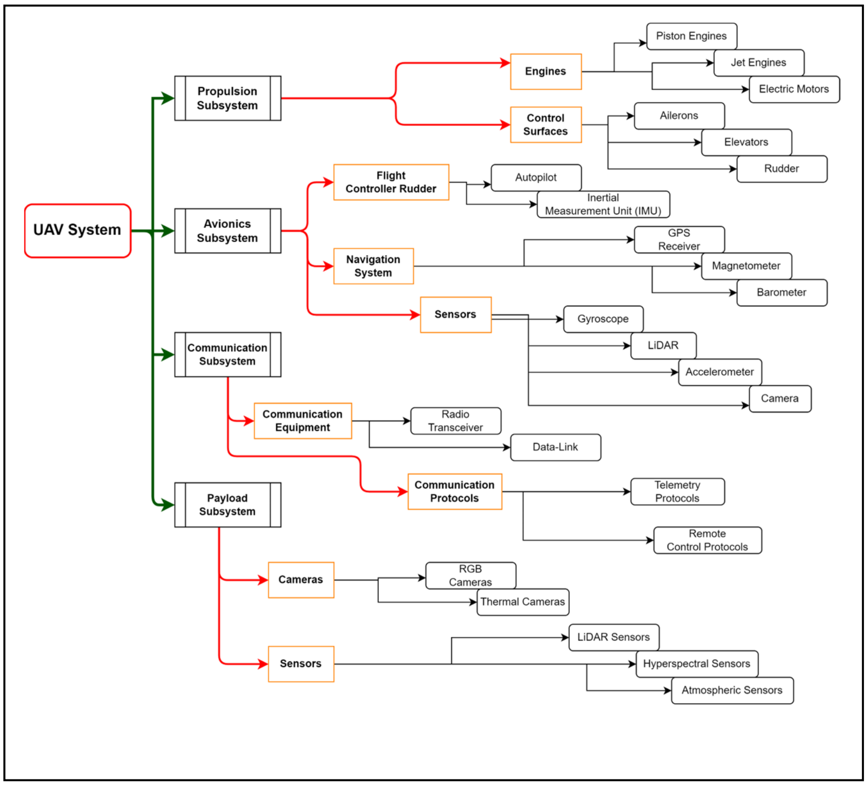


Figure 3. state-of-the-art in UAV subsystems.

Here are several low-power cryptography methods that may find use in drone applications:

3.3.1. Diffie–Hellman Key Exchange Protocol

In 1976, the Diffie-Hellman key exchange protocol was created. The main purpose of this is to allow Alice and Bob to create a mutual secret. Using this protocol, Bob receives $A \leftarrow ga$, which Alice computes using a random integer, a. After Bob receives A, he randomly selects b, computes $B \leftarrow gb$, and transmits it to Alice via the Internet. Note that Bob and Alice have predetermined that g is the group's generator. In the end, Bob computes $K \leftarrow Ab$ while Alice computes $K \leftarrow Ba$. In this instance, Alice and Bob may compute a shared secret K without disclosing an or b. The eavesdropper must extract either an or b, which solves the discrete logarithm problem precisely, to compute K. The discrete logarithm problem, which states that given y, finding x with $y=gx$modβ—where g is a generator and p is a huge prime—is regarded as a difficult issue. As a result, the eavesdropper has difficulty locating an or b.

An attacker with a sizable enough quantum computer may solve discrete logarithm and integer factorization problems in polynomial time, according to a method for quantum computers that Peter Shor proposed in 1994 [3]. The privacy associated with these public-key encryption protocols is vulnerable to a quantum computer because the RSA scheme [1] & the Diffie–Hellman protocols [2] rely on the difficulty of solving the factorization of integers and the discrete logarithm issue, respectively. As a result, researchers are already developing defense against prospective attackers using quantum technology soon. Since the Diffie–Hellman key transfer protocol and the algorithm known as RSA will no longer be able to provide the necessary security level when quantum computers become commonplace, we will be concentrating on the learning with mistakes (LWE) problem in this survey. This problem originates from lattice-based cryptography.

Table 4. Step-by-Step explanation of Diffie-Hellman algorithm.

Alice	*Bob*
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b
Key generated = G^A modP	Key generated = G^b *modP*
Exchange of generated keys takes place	
Key received = y	key received = x
Generated Secret Key = $K_a = Y^a$ *modP*	Generated Secret Key = $K_b = Y^b$ modP
Algebraically, it can be shown that $K_a = K_b$	
Users now have a symmetric secret key to encrypt	

Algorithm 1: The Diffie-Hellman key exchange

```
import random[]
def mod_exp(base, exponent, modulus):
# Modular exponentiation for efficient computation
result = 1
while exponent > 0:
if exponent % 2 == 1:
result = (result * base) % modulus
base = (base * base) % modulus
exponent //= 2
return result

def generate_keys(prime, primitive_root):
# Step 1: Key Generation
private_key = random.randint(1, prime - 1)
public_key = mod_exp(primitive_root, private_key, prime)
return private_key, public_key

def compute_shared_secret(public_key, private_key, prime):
# Step 4: Shared Secret Key Computation
return mod_exp(public_key, private_key, prime)
def main():
# Example with prime number and primitive root
prime = 23
primitive_root = 5
# Alice's side
alice_private_key, alice_public_key = generate_keys(prime,
primitive_root)

# Bob's side
bob_private_key, bob_public_key = generate_keys(prime,
primitive_root)

# Key Exchange
shared_secret_alice = compute_shared_secret(bob_public_key,
alice_private_key, prime)
shared_secret_bob = compute_shared_secret(alice_public_key,
bob_private_key, prime)

# Both Alice and Bob should now have the same shared secret
print("Shared Secret (Alice's side):", shared_secret_alice)
print("Shared Secret (Bob's side):", shared_secret_bob)

if __name__ == "__main__":
main()
```

3.3.2. RSA Algorithm (Non-Quantum-Safe Public-Key Cryptography):

The foundation of this asymmetric encryption technique is the difficulty of factorizing a big number into its two prime components. The RSA algorithm consists of two primary components.

The process of creating the algorithm's public and private keys is known as key generation. The public key is represented by a pair of integers with positive values (e,n). The pair of integers with positive values that makes up the private key is (d,n). The value of n is calculated by multiplying two prime numbers, p and q:

$n=p\times q$

Large prime numbers p and q are selected at random. Since it is difficult to factor n to p and q, only n is known to the public. The other two values, p and q, are kept secret. Next, an integer d is randomly selected so that it is almost prime to both $p-1$ and $q-1$. From p, q, and d, the number e is calculated as the multiplicative reverse of d. Next, we have what follows.

$e\times d\equiv 1\mathrm{mod}(p-1)(q-1)$

Algorithms for encryption and decryption: these deal with how the data is encrypted and decoded. Initially, the message is expressed as an integer in the range of 0 to $n-1\}$. To acquire the ciphertext C, the encryption is performed by elevating the contents of the message M to its e-th value modulo n. Raise the ciphertext C to power d and mod n to decode it. The letters Enc and Dec stand for the encryption and decryption algorithms, respectively.

$\mathrm{Enc}(M)=Me\mathrm{mod}n$

$\mathrm{Dec}(C)=Cd\mathrm{mod}n$

Digital signatures and data encryption are both possible using the RSA technique. A secure connection is not required to exchange the secret key because previous key exchange is not required. However, the safety of this technique is vulnerable in the future since factoring n to p and q won't be difficult if quantum computers become accessible.

3.3.3. Lattice-Based Cryptography (Why not Included in the Table Above?)

One possible method for achieving quantum safety in cryptography is lattice-based encryption. We go into specifics of lattice-based cryptography here. The foundation of lattice-based cryptography constructs is the difficulty of the Shortest Vector Problem (SVP), which estimates a lattice vector's least Euclidean length. It is thought that lattice-based encryption is resistant to both traditional and quantum computers. FrodoKEM and NTRU Prime were chosen as alternate candidates, while five lattice-based encryption algorithms—CRYSTALS-KYBER, NTRU, SABER, CRYSTALS-DILITHIUM, and FALCON—were chosen as finalists in the third phase of the NIST post-quantum encryption standardization process.

Basic familiarity of lattices is required to fully comprehend the topic at hand. First, let's look at a vector space's mathematical representation:

$\mathrm{span}(B)=\{\sum aibi\text{: } ai\in\mathbb{R}\}$

Any combination of its base and any random real coefficients represents a vector space. An infinitely expanding collection of points known as a lattice ($\mathbb{L}$) may be expressed as linear combination of a vector known as the basis (B $\{b1,b2,\cdots,bn\}\}$). As a result, the mathematical representation of a lattice is

$\mathbb{L}(B)=\{\sum aibi : ai\in\mathbb{Z}\}$

A lattice & a vector space vary in that only integers may be coupled with the basis in a lattice, but any real coefficient can be mixed with the foundation of a vector space. As a result, the points in the space of lattices are discrete. Any point p in the vector field may be expressed in a distinct combination of B as follows: $p=a1b1+\cdots+anbn\in\mathrm{span}(B)$. This is because $b1,\cdots,bn$ are linearly independent. Next, if only if $a1,\cdots,an\in\mathbb{Z}$, then $p\in\mathbb{L}(B)$. B is the foundation for $\mathrm{span}(B)$ as it is a foundation for $\mathbb{L}(B)$ as well. But not every $\mathrm{span}(B)$ basis turns into a foundation for $\mathbb{L}(B)$ basis.

Matrix representations of this lattice specification with linearly separate columns are possible. Matrix representations have been used by cryptographers to study difficult lattice-based issues for decades. Higher dimensional lattices are considered in cryptography.

3.3.4. Hash-Based Authentication (Quantum-Safe Cryptography):

To reduce processing costs, basic hash cryptographic features were employed in [48]. A robust authentication system for the Internet of Things (IoD) was additionally suggested, utilizing randomized keys and the hash-based Secured Hash Algorithm (HMASHA1) function for message authentication. A Lightweight Privacy-Preserving Scheme (L-PPS) was developed in [49] as an effective way to preserve security against potential attacks while reducing the computing work and resource usage during encryption and decryption operations.

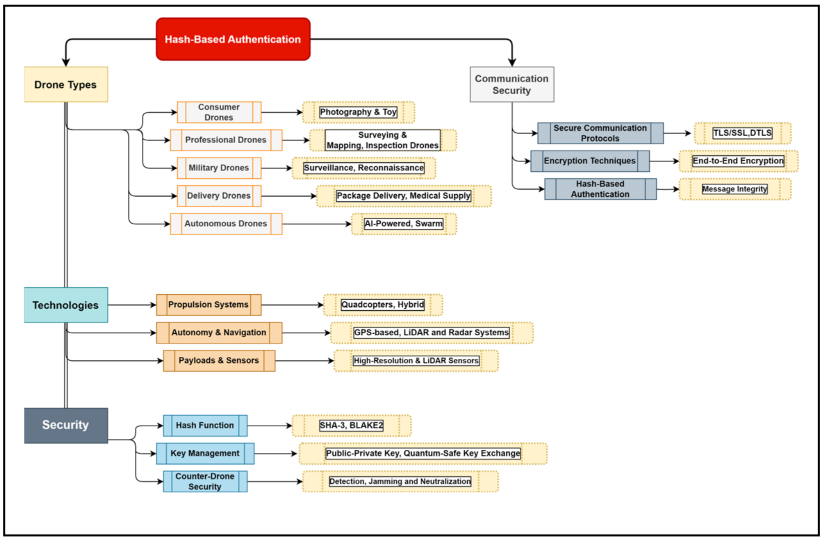


Figure 4. drone communication with hash-based authentication.

The Internet of Things network was made up of a strong server station, intermediate cluster heads, and clustered drone nodes that collected sensing data. By utilizing the Chebyshev Chaotic-Maps, the suggested plan circumvented challenging cryptographic procedures. To be more precise, this technique used bitwise exclusive-OR (XOR) operations, hash functions, and hash-based message authentication codes (HMAC) to create a secure channel, carry out mutual authentication between network nodes, and subsequently provide the safe transmission of sensing data. Due to the inherent dynamic nature of the Internet of Drones, this technique made use of an encrypted token exchange in every connection to authenticate the network nodes both quickly and persistently within the predetermined time frame.

Scyther and the Randomized Oracle Model (ROM) were used to test the L-PPS's performance [50]. The findings indicate that the L-PPS can outperform other pertinent current systems in several measures, including throughput rate, packet delivery ratio, end-to-end latency, and the amount of time needed for each drone to connect. A hash-based system that utilizes random labels was put forth in [51] for drone authentication in large-scale swarm deployments. In particular, the jobs' random labels were produced by utilizing the lightweight hash algorithms SHA-256 and SPONGENT-128, with consideration given to military applications. Using the OMNeT++ framework, a network simulation setting was built, and the latency and bandwidth of the previously specified authentication strategy tested. The accuracy of the authentication technique was confirmed.

To generate the public-private key pairs & the one-way hash functions, pairing cryptography was utilized. Furthermore, the Computational Diffie-Hellman Problem (CDHP) enabled the key exchange. To guarantee data integrity and secrecy, identity-based and aggregate based on signatures authentication systems were created.

Classifying the most recent developments in drone communication is necessary given the taxonomy that is primarily focused on this field and uses hash-based authentication.

4. RESULTS AND DISCUSSIONS

4.1. Overview of the Main Findings

We provide a quick overview of the most recent authentication techniques created specifically for unmanned aerial vehicles in this section.

4.1.2. UAV Authentication Protocols

For drone-assisted 5G networks, Alladi et al. suggested a PUF-based authentication mechanism in [52]. Through the protocol, a base station and a drone may establish a secret key and mutually authenticate each other. They do not, however, consider their protocol to be a true mutual authentication as this study claims, as PUF is only employed at the drone side.

Table 5. A Comparison of The Current Protocols for UAV's Authentication.

Method	Ref	Verification Tool	Pros	Limitations
ECC	54	N/A	Provide mutual Auth	Lacks confidentiality and traceability additional communication and computation
ECC	55	Burrows Abadi Needham (BAN) logic and seyther	Less communication computation and storage overhead	The initial identity of the mobile use can exposed on the fly due to the use of MS static identity resulting in a loss of anonymity
AEAD, SHA & ECC	56	Seyther, and ROR model	Protected against replay and man in the middle attacks	Does not address the issue of privacy leaking
Certificateless AKA	57	Seyther tool	Eliminated key escrow problem	No consider tempering or capturing risks
PUF	58	MAO Boyd Logic	Provided mutual auth	High computation cost
SDN	59	ROR model	Ensured the security of transmitted data	When SDN is used with 5G, it increases the performance
One way hash function	60	ROR model	Minimized computation overhead	Attacker can spoof any of the drone.
ECC	61	Seyther tool	Protected against impersonation attack	Not practical for UAVs due to the significant computation costs associated with ECC
Hash functions and XOR	62	ROR model	Provided mutual auth	Vulnerable to drone impersonation attack
Blockchain	63	ROR model AVISPA tool	Detecting unauthorized UAV	Missing the cover privacy and attack issues during the transfer of data from UAV to server.
Blockchain	64	ROR model AVISPA tool	Provided secure transactions among the drones	High computational cost due to ECC
ECC	65	AVISPA tool	Protected against drone impersonation attack	Not possess specific security credentials in order to participate in the auth protocol

Furthermore, kept in plaintext in the base station database are the drone's CRPs (Challenge-Response Pairs).

This poses a risk (such as CRP disclosure) as an insider with bad intentions might compromise or abuse the base station. Furthermore, the protocol is susceptible to denial-of-service attacks due to its architecture. The drone does several tasks before confirming that it is in contact with the authorized base station (till the drone validates the ounces). An attacker can pose as the base station and send out random answers to use this design weakness to deplete the drone's battery.

For IoD-based UAV settings, Gope et al. suggested a PUF-based authentication system in [53]. To create a secret key and share private data, the protocol enables an unmanned aerial vehicle (or drone) to authenticate itself to a UAV service provider (USP) via PUFs. This protocol's storage in the CRPs of registered drones by the USP is one of its security flaws. Thus, if the USP is illegally utilized (for example, by an employee), the CRPs may be made public or used to pose as drones.

4.1.3. Implementation (UAV’s Communication Systems)

Ground control systems, or grounds aircraft carriers, are used to remotely operate drones. These systems can be handled by human pilots or by autonomous systems like autopilot that work without the need for human interaction. UAVs were once intended for use in the military and for surveillance purposes, however quick research and development led to a huge drop in the cost of manufacturing UAVs. UAVs were once intended for defense and surveillance uses, however fast research and development greatly lowered the cost of producing UAVs. As a result, a wide range of business and non-military uses for UAV technology are emerging, including weather monitoring, intelligent cities surveillance, delivery services, agricultural, and search and rescue. The system can interact using drones in the following ways: drones to ground (D2G) you mean drone to drone via groud station or drone to GS?, drones to other drones (D2D), drones to satellites (D2S), and drones to cells (D2C).

Furthermore, a UAV swarms coordination algorithm's mathematical form involves organizing the essential actions and procedures in equation form.

Notations:

- UAVi represents the i-th UAV in the swarm.
- IDi is the unique identifier for UAV i.
- Posi(t) denotes the position of UAV i at time t, given by a vector (xi(t), yi(t), zi(t)).
- Hdgi(t) is the heading of UAV i at time t.
- Veli(t) is the velocity of UAV i at time t.
- CommRangei represents the communication range of UAV i.

Initialization:

- Assign unique identifiers: IDi ← Unique identifier for UAVi
- Initialize positions, headings, and velocities:
- Posi (0) ← Initial position of UAVi
- Hdgi (0) ← Initial heading of UAVi.
- Veli (0) ← Initial velocity of UAVi.
- Set communication ranges: CommRangei ← Communication range of UAVi

Broadcast Position Information:

- Broadcast the position, heading, and velocity:
- Broadcast (UAVi, Posi(t), Hdgi(t), Veli(t)).

Receive and Update:

- Listen for broadcasts from other UAVs:
- Listen for broadcasts: (UAVj, Posj(t), Hdgj(t), Velj(t)), where j ≠ i.
- Update local knowledge: Posi(t+1) ← Posj(t), Hdgi(t+1) ← Hdgj(t), Veli(t+1) ← Velj(t).

Drone communications can be secured with Hash-based authentication on a variety of platforms, including as software (SW), hardware (HW), or a hybrid system combining both. Here's an extensive summary of how we can use this on various platforms:

4.1.3.1. Hardware (HW)

4.1.3.1.1. FPGA

Field-Programmable Gate Arrays (FPGAs) are essential because they provide a special architecture meant for addressing important problems. Improving parallel processing capabilities, guaranteeing power efficiency appropriate for drone resources, and stressing flexibility for changing communication protocols are among the fundamental design issues. The main elements of FPGA architecture include programmable logic blocks (PLBs), embedded processors, digital signal processing (DSP) blocks, and modifiable input/output (I/O) blocks.

The fundamental logic blocks are PLBs, which are designed to carry out simultaneous operations for modulation and demodulation and cryptographic algorithms. While embedded processors provide hybrid processing—combining software responsibilities with hardware acceleration—DSP blocks improve signal processing capabilities, which are essential for effective communication. I/O blocks make it easier to integrate external sensors and devices with ease. FPGA integration improves security and responsiveness in drone communication by accelerating cryptography, facilitating effective demodulation and modulation, and processing signals in real time. One of the challenges is overcoming weight and size restrictions. In summary, FPGA design is a critical component that helps create safe, effective, and adaptable drone communication systems. Further, paragraph shows how we use hash-based authentication for drone on several platforms.

1. Hash Function Acceleration using FPGA (Field-Programmable Gate Array): Create a unique hardware accelerator for the selected hash function (SHA-256, for example). Parallel processing is made possible by FPGA, which greatly speeds up hash calculations.
2. Secure Key Storage: Put in place secure key storage techniques on FPGA to guarantee the security of the secret key that is shared and required for authentication.
3. Communication Interface: To enable communications among the FPGA and other drone components, integrate communication interfaces (such as SPI and UART).

Parallel processing & computational efficiency may be used to describe how Field-Programmable Gate Arrays (FPGAs) enhanced drone communication. The following list includes advancements in drone communication made possible by FPGAs and mathematical equations.

Baseline Communication Capability (C_0):

C_0

Factors Influencing Improvement:

- P: Parallel processing speed factor
- A: Adaptability factor
- E: Efficiency factor

Improvement Calculation:

$\blacktriangle C=P\times A\times E$

Improved Communication (C_i):

$Ci=C0+\blacktriangle C$

Let's now introduce these factors' precise values:

Assume that the placeholder value for the baseline communication capacity (C0) is 100.

Based on the factors' values:

P=1.2: Denotes a 20% increase in processing speed in parallel.

A=1.1: Indicates a 10% increase in flexibility.

E=1.15: Denotes a 15% increase in productivity.

Now enter these numbers into the formulas:

$\blacktriangle C =1.2\times1.1\times1.15$

$\blacktriangle C \approx1.518$

$Ci =100+1.518$

$Ci \approx101.518$

This indicates that the enhanced communication capacity with FPGA (Ci) is around 101.518, suggesting a 1.518-unit improvement over the baseline, depending on the expected parameters. The FPGA's specifications and the communication duties at hand would need to be taken into consideration when determining the precise values for P, A, and E.

4.1.3.1.2. ASIC:

Like the FPGA scenario, advances in drone communication made possible by Specific to the application Integrated Circuits (ASICs) may be described mathematically. Let's indicate important parameters using comparable symbols.

Baseline Communication Capability (C_0):

C_0

Factors Influencing Improvement:

- P: Parallel processing speed factor
- A: Adaptability factor
- E: Efficiency factor

Improvement Calculation:

$\blacktriangle C=P\times A\times E$

Improvement Calculation:

$\blacktriangle C=P\times A\times E$

Improved Communication (C_i):

$Ci=C0+\blacktriangle C$

P, A, and E in this instance stand for characteristics unique to ASICs, emphasizing their capacity for parallel processing, flexibility in adjusting communication protocols, and general effectiveness in managing communication tasks.

Now, let's introduce these factors' precise values:

Assume that the placeholder value for the baseline communication capacity (C0) is 100.

Depending on the factors' values:

PASIC=A 25% increase in parallel processing rate above the baseline is shown by the value of 1.25.

AASIC=1.12: Indicates a 12% increase in flexibility.

EASIC=1.18: Indicates an increase in efficiency of 18%.

Now enter these numbers into the formulas:

$\blacktriangle CASIC =1.25\times1.12\times1.18$

$\blacktriangle CASIC \approx1.6585$

CiASIC = 100 + 1.6585

CiASIC ≈101.6585

This indicates that the increased communication capability CiASIC is around 101.6585, showing a 1.6585-unit improvement over the baseline, based on the expected parameters for AASIC. Like FPGA, the ASIC's features and the communication duties at hand would need to be taken into consideration while determining the precise values for PASIC, AASIC, and EASIC.

Additionally, the paragraph demonstrates the usage of hash-based authentication for drones across AASIC.

1. Application-Specific Integrated Circuits, or ASICs, are a type of bespoke hardware circuitry that can be more optimized and power-efficient than FPGAs for hash-based authentication.
2. Integrate security components: Put in place certain security elements, including a True Randomized Numbers Generator (TRNG) for generating keys.
3. Low-Power Considerations: The ASIC should be optimized very low power consumption to meet drones' energy requirements.

4.1.3.2. Software (SW):

The microcontroller or processor of a drone can include embedded software.

1. Hash Library Integration: Program the unmanned aircraft's microcontroller or CPU to use hash algorithms (like SHA-256) or make use of already-existing cryptography libraries.
2. Secure Key Handling: To protect the shared secret key's secrecy, build secure key handling processes inside the software.

3. Real-Time Verification: Create real-time hash calculation and comparison capabilities for incoming communications.

Implementation of Communication Protocol:

1. Secure Protocols: To guarantee end-to-end encryption and integrity, integrate secure communication protocols (such as TLS and DTLS) in software.
2. Timestamping: To combat replay attacks, incorporate timestamping techniques into the communication protocol.
3. Error Handling: To control communication problems and guarantee the dependability of the authentication procedure, put error-handling procedures into place.

4.1.3.3. Hybrid:

4.1.3.3.1. Microcontroller + FPGA/DSP:

Combining a digital signal processor (DSP) or (FPGA) with a microcontroller is a dynamic way to improve drone communication capabilities. The Microcontroller functions as the core processing unit of the system, managing high-level activities, decision-making procedures, and establishing interfaces with external components. Simultaneously, the FPGA/DSP provides specialized computational power, especially for activities that need parallel processing, such signal processing or cryptography. Because of its flexibility, the FPGA can easily conform to a wide range of communication protocols, meeting the needs of ever-changing contexts.

This integrated strategy takes use of the FPGA/DSP's ability to handle computationally demanding operations and the Microcontroller's skill at handling complex jobs. With the FPGA/DSP boosting processing capabilities essential for actual time and resource-intensive applications, and the Microcontroller coordinating overall system control, the combined effect creates a harmonic and effective solution for supporting drone communication. In drone communication systems, this cooperative integration offers increased efficacy and dependability.

1. Hash Acceleration: To offload computation-intensive operations, use FPGA or DSP to physically accelerate hash functions.
2. Microcontroller Control: Use the microcontroller to interface with the accelerated hardware, manage the entire authentication process, and implement control logic.
3. Flexible Integration: Use the microcontroller as general management and the adaptability of FPGAs and DSPs to adjust to changing communication protocols.

Drones frequently have little power. When selecting the implementation platform, take the limitations on power, size, and weight into account. Make security a top priority, making sure that communication links are safeguarded, and keys are kept in a secure location. Respect pertinent cryptography and communication standards to guarantee regulatory compliance and interoperability.

Depending on the required level of security, energy limits, and the capabilities of the drone, one may choose to use a hybrid method, HW, or SW. Flexibility and performance are frequently balanced by the hybrid method. A more thorough table of comparisons for hash-based authenticating implementation on FPGA, Software (SW), and Hybrid platforms can be seen below.

Table 5. Comparisons for hash-based authenticating implementation.

Metric	FPGA Implementation	Software (SW)	Hybrid
Performance	High performance due to parallelism in FPGA architecture	Moderate performance, slower than FPGA	Balanced performance
Power Efficiency	Efficient power consumption	Low power consumption	Balanced power efficiency
Execution Time	Fast	Moderate execution time	Balanced execution time
Resource Utilization	Efficient resource	Moderate resource utilization	Balanced resource utilization
Key Management	Secure key storage on FPGA	Secure key handling	Secure key handling
Flexibility	Limited flexibility	High	Enhanced flexibility
Security Assurance	Depends on FPGA	Relies on software security measures	Depends on both hardware and software
Cost	High	Lower initial cost	Moderate initial cost

4.2. Elliptic Curve Cryptography

Our proposed research utilizes the use of the Elliptic Curve Cryptography (ECC) algorithm concept. Thus, the fundamental attributes and traits of ECC are delineated here. The main cryptosystems of ECC make use of an elliptic curve with an asymmetric foundation. Below is the equation for the generic ECC algorithm's elliptic key.

Y2 = x3 + ax + b (mod p) (with a and b constants)

To avoid singular points, those integers must meet the ECC properties “4a3 + 27b2 ≠ 0”. Here, a one-way function called a trapdoor function is employed, which has a straightforward computation procedure in one direction. It is therefore a one-way process, making computation in the other direction challenging. The most important is ECC in terms of key size. In contrast to alternative cryptographic key techniques, it is incredibly quick, efficient, and lightweight. During the communication process, it can offer quick and concise keys.

Further, summary of the digital signature, key exchange, and ECC processes are explained in equation form.

1. Key Generation:

Curve Parameters:

p (prime),

a, b (coefficients), G (base point), n (order of the base point).

Generate Private Key (d):

d∈ [1, n−1]

d∈ [1, n−1]

Compute Public Key (Q)

Q=d·G

2. Key Exchange (ECDH):

Generate Your Private Key (dA):

dA∈ [1, n−1]

Compute Your Public Key (QA): QA =dA·G

Generate Shared Secret:

Shared Secret=dB · QA

3. Digital Signature (ECDSA):

Sign Message:

Generate a Random Number (k):

K ∈ [1, n−1]

Compute Temporary Point ($P = k \cdot G$):

$(x P , y P)=k \cdot G$

Compute r:

$r \equiv xP \pmod{n}$

Compute s:

$s \equiv k -1 \cdot (H(m) + d \cdot r) \ (modn)$

Verify Signature:

Compute w:

$w \equiv s-1 \ (modn)$

Compute u1 and u2:

$u1 \equiv H(m) \cdot w \ (modn)$

$u2 \equiv r \cdot w \ (modn)$

Compute Temporary Point ($P=u1 \cdot G+u2 \cdot Q$):

$(xP , yP)=u1 \cdot G+u2 \cdot Q$

Verify $r \equiv xP$ (modn).

An overview of ECC processes is given by these equations. In real-world applications, effective algorithms and optimizations are employed. For safe and effective ECC implementations, always use well-known cryptographic standards and libraries.

The process shown below is a conceptual illustration; the precise ECC circumstances and cryptographic primitives utilized will determine the implementation specifics in practice:

```
Algorithm: Elliptic Curve Cryptography with Penguin Search Optimization (ECC-PESO)
1. Initialize ECC Parameters []:
      - Select-elliptic-curve $E(Fp)$ with base point $[G]$ and prime order $[n]$
       - Choose cryptographic hash-function [H]
      - Initialize public key $[PA]$ and private key $[dA]$
2. Initialize Penguin Search Optimization Parameters []:
        - Produce a random population of [P] penguins in groups
       - Initialize the probability of the existence of fish in the levels and holes
3. For $i = 1$ to the number of generations []:
   a. For every individual $i \in P$
        - While oxygen reserves are not exhausted
                  i. Take a random step.
                  ii. Enhance the penguin position using the ECC operation on the EC.
                  iii. Upgrade the cryptographic key pair using the location upgrade formula.
                  iv. Upgrade the quantity of cryptographic operations performed using this penguin.
       - End While
   b. Upgrade the quantity of cryptographic operations performed in the levels, holes, and best groups.
   c. Reallocate the probability of penguins in the levels and holes.
   d. Upgrade the optimal cryptographic key pair based on the best penguin.
4. End []
```

The process of updating the number of cryptographic operations and optimizing the location is consistent with PESO's optimization procedure. The ECC-PESO method uses the ideas of the Penguin Search Optimization method to enhance choosing of cryptographic key pairs.

5. FUTURE DISCUSSIONS

Moreover, Blockchain technology can offer future answers to similar problems with UAV communication.

1) Enhanced Security: A strong security foundation for UAV communication is provided by the cryptographic features and inherent immutability of blockchain technology. The decentralized

characteristic of blockchain guarantees the authenticity and safety of UAV communications by preventing tampering with transactions and data.

2) Automation and Smart Contracts: Self-executing and automated contracts among UAVs as well as other entities are made possible by smart contracts on the blockchain. This can guarantee regulatory compliance, expedite processes, and enable safe and open transactions.

3) Transparency and Data Integrity: Blockchain technology can offer a transparent and safe platform for sharing and storing UAV data. By guaranteeing data integrity and traceability, this makes UAV operations auditable and responsible.

4) Trust & Decentralization: Blockchain does away with the necessity for a centralized authority in UAV communications by using a distributed ledger. Because all parties can verify and document transactions and conversations, this promotes transparency and confidence among stakeholders.

5) Interoperability & Standardization: By offering a common framework for interaction and transfer of information between UAVs and ground systems, blockchain-based protocols can help to promote interoperability and standardization. This encourages smooth platform-to-platform integration and cooperation.

For Drones with limited capacity, blockchain technologies offer a promising security option. But as these innovations remain in their early phases of development, more investigation is necessary.

CONCLUSION

Drone communications can be secured with Hash-based authentication on a variety of platforms, including as software (SW), hardware (HW), or a hybrid system combining both.

Unmanned Aerial Vehicles (UAVs) present benefits like allowing ground communications even in situations where connectivity is restricted by physical barriers. Conversely, they expand the area that can be attacked. For example, physical drone attacks give the attacker credentials to introduce fake data into the Internet of Things (IoV) network, compromising user safety as well as security. Authentication is essential in this situation to ensure security. Similarly, Advanced cryptographic techniques are essential for best drone communication security and privacy. The goal of post-quantum cryptography (PQC) is to create algorithms which can survive quantum attacks considering the possibility that quantum computers would break conventional cryptographic techniques. "Lattice-based cryptography, hash-based cryptography, and code-based" encryption are among examples. similarly, Computations can be done on encrypted data while having to first decrypt it because of homomorphic encryption. This can be useful for computation in drone communication that protect privacy. Furthermore, Zero-knowledge proofs allow one side to demonstrate possession of information without disclosing the information itself. Examples of these proofs are zk-SNARKs ("Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge'). This can improve cryptographic protocols' privacy.

The choice of technology for drone communication frequently comes down to combining security, computational effectiveness, and environment suitability in situations where resources are limited. Because of their high security and effectiveness, advanced algorithms like AES and Elliptic Curve Cryptography (ECC) are popular. Among these, ECC is especially preferred since it can offer comprehensive safety with smaller key lengths, which is appropriate for drones that have limited resources. The algorithm's resistance to different cryptographic attacks is enhanced by the mathematical characteristics of elliptic curves, ensuring a high degree of security. Furthermore, decreased computational overhead from smaller key sizes in ECC is a critical component for the cost-effective functioning of drones with constrained computing power. Furthermore, ECC is a realistic and safe option for protecting private information in drone communication networks because of its effectiveness in creating keys, key exchange, and electronic signatures. It meets the needs of both solid safety and effective operation.

References

1. M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, “Bubbles of trust: A decentralized blockchain-based authentication system for IoT,” Comput. Security, vol. 78, pp. 126–142, Sep. 2018.
2. R. Alur et al., “Systems computing challenges in the Internet of Things,” 2016. [Online]. Available: arXiv:1604.02980.
3. Sherali Zeadally, Ashok Kumar Das , Nicolas Sklavos, "Cryptographic technologies and protocol standards for Internet of Things", Elsevier 2019, pp 1-11.
4. Pravin Kawle, Avinash Hiwase, Gautam Bagde, Ekant Tekam, Rahul Kalbande, "Modified Advanced Encryption Standard", International Journal of Soft Computing and Engineering 2014, PP 1-3.
5. Paulo S. L. M. Barreto, Marcos A. Simplicio Jr., "CURUPIRA, a block cipher for constrained platforms", SBRC 2007, pp 61-75.
6. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, "PRESENT: An Ultra-Lightweight Block Cipher", Springer 2007, pp 450-466.
7. [7] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matt Robshaw, "The LED Block Cipher", International Association for Crypto logic Research 2011, pp 326-341.
8. KP, B. M., & Patwari, N. (2023, April). Embedded Light-Weight Cryptography Technique to Preserve Privacy of Healthcare Wearable IoT Device Data. In 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-6). IEEE.
9. Wentao Zhang, Zhenzhen Bao, Dongdai Lin, Vincent Rijmen, Bohan Yang, "RECTANGLE: A Bit-slice Lightweight Block Cipher Suitable for Multiple Platforms", Springer 2015, pp 1-15.
10. Daniel Dinu, Leo Perrin, Aleksei Udovenko, Vesselin Velichkov, Johann Grosschad, Alex Biryukov, "Design Strategies for ARX with Provable Bounds: Sparx and LAX", Springer 2016, pp 1-40.
11. Muhammad Usman, Irfan Ahmed, M. Imran Aslam, Shujaat Khan and Usman Ali Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things”, ARXIV, 2017, pp 1-10.
12. X. Yang et al., "Blockchain-Based Secure and Lightweight Authentication for Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3321-3332, 1 March1, 2022, doi: 10.1109/JIOT.2021.3098007.
13. Khan, M. N., Rao, A., and Camtepe, S. (2020). Lightweight cryptographic protocols for IoT-constrained devices: A survey. IEEE Internet of Things Journal, 8(6), 4132-4156
14. Lam, T. N., and Le, D. H. (2022, October). Implementation of Lightweight Cryptography Core PRESENT and DM-PRESENT on FPGA. In 2022 International Conference on Advanced Technologies for Communications (ATC) (pp. 104-109). IEEE.
15. Zitouni, N., Sedrati, M., and Behaz, A. (2022, April). Comparing lightweight algorithms to secure constrained objects in internet of things. In New Realities, Mobile Systems and Applications: Proceedings of the 14th IMCL Conference (pp. 1040-1051). Cham: Springer International Publishing.
16. Windarta, S., Suryadi, S., Ramli, K., Pranggono, B., and Gunawan, T. S. (2022). Lightweight Cryptographic Hash Functions: Design Trends, Comparative Study, and Future Directions. IEEE Access, 10, 82272-82294.
17. F. Abbas, X. Yuan, M. S. Bute, and P. Fan, “Performance analysis using full duplex discovery mechanism in 5G-V2X communication networks,” IEEE Trans. Intell. Transp. Syst., to be published, doi: 10.1109/TITS.2021.3103974.
18. S. Liao, J. Wu, S. Mumtaz, J. Li, R. Morello, and M. Guizani, “Cognitive balance for fog computing resource in Internet of Things: An edge learning approach,” IEEE Trans. Mobile Comput., vol. 21, no. 5, pp. 1596–1608, May 2022.
19. T. Wang, H. Ke, X. Zheng, K. Wang, A. K. Sangaiah, and A. Liu, “Big data cleaning based on mobile edge computing in industrial sensor-cloud,” IEEE Trans. Ind. Informat., vol. 16, no. 2, pp. 1321–1329, Feb. 2020.
20. H. Bastami, M. Letafati, M. Moradikia, A. Abdelhadi, H. Behroozi, and L. Hanzo, “On the physical layer security of the cooperative rate-splitting aided downlink in uav networks,” IEEE Transactions on Information Forensics and Security, 2021.
21. L. Chen, S. Qian, M. Lim, and S. Wang, “An enhanced direct anonymous attestation scheme with mutual authentication for network-connected UAV communication systems,” China Communications, vol. 15, no. 5, pp. 61– 76, 2018.

22. Jalan, A.; Matkovskyy, R.; Urquhart, A. What effect did the introduction of Bitcoin futures have on the Bitcoin spot market? Eur. J. Financ. 2021, 27, 1251–1281.
23. Hakak, S.; Khan, W.Z.; Gilkar, G.A.; Imran, M.; Guizani, N. Securing smart cities through blockchain technology: Architecture, requirements, and challenges. IEEE Netw. 2020, 34, 8–14.
24. Oliva, G.A.; Hassan, A.E.; Jiang, Z.M.J. An exploratory study of smart contracts in the Ethereum blockchain platform. Empir. Softw. Eng. 2020, 25, 1864–1904.
25. Tran, J.A.; Ramachandran, G.S.; Shah, P.M.; Danilov, C.B.; Santiago, R.A.; Krishnamachari, B. Swarmdag: A partition tolerant distributed ledger protocol for swarm robotics. Ledger 2019, 4, 25–31.
26. W. Chen, Y. Dong and Z. Duan, "Manipulating Drone Position Control," 2019 IEEE Conference on Communications and Network Security (CNS), Washington DC, DC, USA, 2019, pp. 1-9, doi: 10.1109/CNS.2019.8802817.
27. D. S. C. Putranto, A. K. Aji and B. Wahyudono, "Design and Implementation of Secure Transmission on Internet of Drones," 2019 IEEE 6th Asian Conference on Defence Technology (ACDT), Bali, Indonesia, 2019, pp. 128-135, doi: 10.1109/ACDT47198.2019.9072714.
28. T. Alladi, V. Venkatesh, V. Chamola, and N. Chaturvedi, "Drone-MAP: A. novel authentication scheme for drone-assisted 5G networks," in Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops, 2021, pp. 1–6.
29. L. Teng et al., "Lightweight security authentication mechanism towards UAV networks," in Proc. Int. Conf. Netw. Appl., 2019, pp. 379–384.
30. P. Gope and B. Sikdar, "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones," IEEE Trans. Veh. Technol., vol. 69, no 11, pp. 13621–13630, Nov. 2020.
31. C. Pu and Y. Li, "Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system," in Proc. IEEE Int. Symp. Local Metrop. Area Netw., 2020, pp. 1–6.
32. Y. Tan, J. Liu, and K. Nei, "Blockchain-Based Key Management for Heterogeneous Flying Ad Hoc Network," IEEE Trans. Industrial Informatics, vol. 17, no. 11, 2021, pp. 7629–38.
33. X. Li et al., "Blockchain-Based Mutual-Healing Group Key Distribution Scheme in Unmanned Aerial Vehicles Ad-Hoc Network," IEEE Trans. Vehic. Tech., vol. 68, no. 11, 2019, pp. 11,309–22.
34. C. Feng et al., "Blockchain-Based Cross-Domain Authentication for Intelligent 5G-Enabled Internet of Drones," IEEE Internet of Things J., vol. 9, no. 8, 2022, pp. 6224–38.
35. N. Zhang, Q. Jiang, L. Li, X. Ma, and J. Ma, "An efficient three-factor remote user authentication protocol based on BPV-FourQ for internet of drones," Peer-to-Peer Networking and Applications, vol. 14, no. 5, pp. 3319–3332, 2021.
36. B. Bera, S. Saha, A. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment," IEEE Trans. Veh. Technol., vol. 69, no. 8, pp. 9097–9111, 2020.
37. C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K. Choo, "Blockchainbased Cross-domain Authentication for Intelligent 5G-enabled Internet of Drones," IEEE Internet Things J., vol. 9, no. 8, pp. 6224–6238, 2022.
38. Wilson, L., Constantine, R., van der Boon, T., & Radford, C. A. (2022). Using timelapse cameras and machine learning to enhance acoustic monitoring of small boat sound. Ecological Indicators, 142, 109182.
39. Khan, M., Bhunia, S., Yuksel, M., & Kane, L. C. (2018). Line-of-sight discovery in 3D using highly directional transceivers. IEEE Transactions on Mobile Computing, 18(12), 2885-2898.
40. Wang, J., Jiang, C., & Kuang, L. (2022). High-mobility satellite-UAV communications: Challenges, solutions, and future research trends. IEEE Communications Magazine, 60(5), 38-43.
41. Geraci, G., Garcia-Rodriguez, A., Azari, M. M., Lozano, A., Mezzavilla, M., Chatzinotas, S., ... & Di Renzo, M. (2022). What will the future of UAV cellular communications be? A flight from 5G to 6G. IEEE communications surveys & tutorials, 24(3), 1304-1335.
42. Zhang, C., Zou, Y., Wang, F., del Rey Castillo, E., Dimyadi, J., & Chen, L. (2022). Towards fully automated unmanned aerial vehicle-enabled bridge inspection: Where are we at?. Construction and Building Materials, 347, 128543.

43. Chen, G., & Chen, G. (2022). A Method of Relay Node Selection for UAV Cluster Networks Based on Distance and Energy Constraints. Sustainability, 14(23), 16089.
44. Lu, R. R., Wang, J. Y., Fu, X. T., Lin, S. H., Wang, Q., & Zhang, B. (2022). Performance analysis and optimization for UAV-based FSO communication systems. Physical Communication, 51, 101594.
45. Tu, C., Shen, J., Dai, J., Zhang, L., & Wang, J. (2022). A lower size, weight acquisition and tracking system for airborne quantum communication. IEEE Photonics Journal, 14(6), 1-8.
46. Gupta, L., Jain, R., & Vaszkun, G. (2015). Survey of important issues in UAV communication networks. IEEE communications surveys & tutorials, 18(2), 1123-1152.
47. Li, C. T., Cheng, J. C., & Chen, K. (2020). Top 10 technologies for indoor positioning on construction sites. Automation in Construction, 118, 103309.
48. Jan, S.U.; Qayum, F.; Khan, H.U. Design and Analysis of Lightweight Authentication Protocol for Securing IoD. IEEE Access 2021, 9, 69287–69306.
49. Deebak, B.D.; Al-Turjman, F. A smart lightweight privacy preservation scheme for IoT-based UAV communication systems. Comput. Commun. 2020, 162, 102–117.
50. Abdalla, M.; Fouque, P.A.; Pointcheval, D. Password-based authenticated key exchange in the three-party setting. In Proceedings of the 8th International Workshop on Public Key Cryptography, Les Diablerets, Switzerland, 23–26 January 2005; Volume 3386, pp.
51. Hu, F.; Qian, H.; Liu, L. A Random Label and Lightweight Hash-Based Security Authentication Mechanism for a UAV Swarm. Wirel. Commun. Mob. Comput. 2021, 2021, 6653883.
52. T. Alladi, V. Venkatesh, V. Chamola, and N. Chaturvedi, "Drone-MAP: A. novel authentication scheme for drone-assisted 5G networks," in Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops, 2021, pp. 1–6.
53. P. Gope and B. Sikdar, "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones," IEEE Trans. Veh. Technol., vol. 69, no 11, pp. 13621–13630, Nov. 2020.
54. Y. Kirsal Ever, "A secure authentication scheme framework for mobilesinks used in the Internet of Drones applications," Comput. Commun., vol. 155, pp. 143–149, 2020.
55. M. Tanveer, A. H. Zahid, M. Ahmad, A. Baz, and H. Alhakami, "LAKEIoD: Lightweight authenticated key exchange protocol for the internet of drone environment," IEEE Access, vol. 8, pp. 155645–155659, 2020.
56. M. Tanveer, A. U. Khan, N. Kumar, and M. M. Hassan, "RAMP-IoD: A robust authenticated key management protocol for the Internet of Drones," IEEE Internet Things J., vol. 9, no. 2, pp. 1339–1353, Jan. 2022.
57. B. Semal, K. Markantonakis, and R. N. Akram, "A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks," in Proc. IEEE/AIAA 37th Digit. Avionics Syst. Conf., 2018.
58. T. Alladi, Naren, G. Bansal, V. Chamola, and M. Guizani, "SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication," IEEE Trans. Veh. Technol., vol. 69, no. 12, pp. 15068–15077, Dec. 2020.
59. Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for Internet of Drones," Comput. Commun., vol. 154, pp. 455–464, 2020.
60. J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of Drones environment," IEEE Trans. Veh. Technol., vol. 68, no. 7, pp. 6903–6916, Jul. 2019.
61. M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance," J. Syst. Architecture, vol. 115, 2021.
62. Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for Internet of Drones," Comput. Commun., vol. 154, pp. 455–464, 2020.
63. S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," IEEE Trans. Netw. Sci. Eng., vol. 9, no. 3, pp. 1346–1358, May/Jun. 2022.

doi:10.20944/preprints202504.1585.v1

64. B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, “Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled Internet of Drones environment,” IEEE Trans. Veh. Technol., vol. 69, no. 8, pp. 9097–9111, Aug. 2020.
65. M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, “Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of Drones deployment,” IEEE Internet Things J., vol. 6, no. 2, pp. 3572–3584, Apr. 2019.
66. S. U. Jan, F. Qayum, and H. U. Khan, “Design and analysis of lightweight authentication protocol for securing IoD,” IEEE Access, vol. 9, pp. 69287–69306, 202.
67. M. U. Rana, M. Ali Shah and O. Ellahi, "Malware Persistence and Obfuscation: An Analysis on Concealed Strategies," 2021 26th International Conference on Automation and Computing (ICAC), Portsmouth, United Kingdom, 2021, pp. 1-6, doi: 10.23919/ICAC50006.2021.9594197.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.