RESEARCH ARTICLE

Advanced Hyperelliptic Curve-Based Authentication Protocols for Secure Internet of Drones Communication

Zeeshan Ali Haider[1,*], **Muhammad Fayaz**[2], **Yue Zhang**[2] and **Ahmad Ali**[3]

[1] Department of Computer Science, Qurtuba University of Science and Information Technology, Peshawar 25000, Pakistan
[2] Department of Computer Science and Engineering, Sejong University, Seoul 05006, Republic of Korea
[3] College of Mechatronics and Control Engineering, Shenzhen University, Shenzhen 518060, China

Abstract

The concept of an Internet of Drones (IoD) is becoming increasingly important in various domains, including surveillance and logistics. Effective communication between the interconnected systems is the essence of the Internet of Drones, however, due to the resource constraints of drones and the dynamic nature of the operating environment, security of communication within IoD networks is indeed the top priority. Considering these challenges on the part of IoD communication, a novel Hyperelliptic Curve Cryptography (HECC)-based authentication protocol is proposed in this paper to secure the data exchange between drones and their control servers and to ensure efficient communication. The proposed HECC protocol is compared with three existing protocols, Elliptic curve cryptography-based protocol with public secure authentication scheme (ECCCPSAS), Non-linear wireless unmanned aerial systems authentication scheme (NLWUAS), and the Multi-Agent System (MAS). The comparison is made among average performance metrics such as communication overhead, packet delivery ratio, throughput, and end-to-end delay. The experimental outcome assures that the HECC protocol outperforms the other protocols in terms of all metrics. The HECC-based authentication protocol reduces communication overhead by up to 30% and end-to-end delay to 75 ms while achieving a 95% packet delivery ratio and 8 Mbps throughput, outperforming ECCCPSAS, NLWUAS, and MAS across all evaluated metrics. These results confirm that HECC is a viable cryptographic solution for resource-constrained IoD deployments. Future work will focus on real-world protocol deployment and integration with quantum-resistant algorithms.

Keywords: hyperelliptic curve cryptography, internet of drones (IoD), authentication protocol, cryptographic protocols, drone communication networks, security in IoD.

1 Introduction

The rapid advancement of unmanned aerial vehicles (UAVs), more commonly referred to as drones, has substantially increased in multiple sectors such as surveillance, disaster management, agriculture, geographic mapping, aerial photography, as well as

Submitted: 13 March 2025
Revised: 21 May 2025
Accepted: 02 June 2025
Published: 08 July 2025

Vol. 1, **No.** 3, 2025.
10.62762/TACS.2025.926789

***Corresponding author:**
✉ Zeeshan Ali Haider
Zeeshan.ali9049@gmail.com

Citation
Haider, Z. A., Fayaz, M., Zhang, Y., & Ali, A. (2025). Advanced Hyperelliptic Curve-Based Authentication Protocols for Secure Internet of Drones Communication. *ICCK Transactions on Advanced Computing and Systems*, 1(3), 138–153.

© 2025 by the Authors. Published by Institute of Central Computation and Knowledge. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

logistics, as illustrated in Figure 1. The Internet of Drones (IoD), where unmanned aerial vehicles (UAVs) communicate with each other and share important data across wireless networks, has emerged, necessitating lightweight and privacy-preserving authentication mechanisms specifically designed for drone environments [1]. The intersection of IoD with 5G networks and cloud computing has the potential for greater connection and real-time processing of data, facilitating more nuanced and self-directed operations [2]. Traditional cryptographic approaches, particularly Elliptic Curve Cryptography (ECC), have been widely studied for securing resource-constrained IoT networks, highlighting both their potential and their scalability limitations when applied to dynamic aerial environments [3]. UAVs are subject to a large number of cybersecurity attacks, such as eavesdropping, data alteration, and unauthorized access [6]. Verifying the authenticity of internal and external communications (e.g., between drones and their servers) is vitally important to ensuring the integrity of ongoing operations, especially in critical use cases [4].

Elliptic Curve Cryptography (ECC) and RSA are frequently used to provide communication security in drone networks but have limits, particularly in resource-constrained environments. While ECC incurs non-trivial computational overhead and RSA requires large key sizes unsuitable for drones with limited processing power, existing authentication frameworks for IoD still face efficiency and anonymity challenges [5]. These challenges can be addressed by Hyperelliptic Curve Cryptography (HECC), which has a smaller key size, lower computational complexity, and better scalability, which makes it a candidate for IoD applications. An alternative approach for enhancing IoD security is to leverage blockchain technology, which has been explored alongside HECC owing to its properties of decentralization, immutability, and transparency. In comparison, blockchain adds substantial computational overhead, particularly arising from its consensus protocol and data replication, introducing additional security and privacy burdens that are especially pronounced in resource-constrained UAV environments [6]. Through the comparison of HECC and blockchain, the performance, scalability, and security will be dissected in the later sections for a better understanding of the strengths and limitations of each approach for securing drone communication [7].

Traditional cryptographic techniques, including Elliptic Curve Cryptography (ECC), have gained immense attention for securing communication for IoT and UAV networks [8]. The rapid expansion of UAV deployments has created complex security challenges that go beyond what existing cryptographic techniques alone can address, motivating the exploration of complementary approaches such as blockchain-assisted authentication for drone networks [9]. In order to overcome these limitations, this paper advocates the use of Hyperelliptic Curve Cryptography (HECC) to provide stronger and improved security in drone communication.

HECC represents a cryptographic technique that generalizes the principles of ECC (Elliptic Curve Cryptography) to hyperelliptic curves and has some advantages, such as higher security, smaller keys, and better performance in environments with limited resources. In particular, this paper focuses on HECC application in IoD, suggesting sophisticated authentication schemes aimed at strengthening the security and efficiency of information exchange of flying robots. The results of the comparative analysis show a significant reduction in overhead, an increase in packet delivery ratio, and a decrease in delay of the IoD system due to the strength of HECC over the existing cryptographic approaches. The primary contributions of this paper are:

- This paper presents a new approach to secure communications in the Internet of Drones (IoD) networks using HECC-based authentication protocols.
- We develop a new HECC-based authentication protocol for mutual authentication between the drone and control servers, which verifies the data exchanged in both directions, ensuring the authenticity and integrity of the information being transmitted.
- The proposed HECC-based authentication protocol demonstrates considerable improvements in packet delivery ratio, computational cost, and communication delay compared to state-of-the-art techniques such as Elliptic Curve Cryptography (ECC).
- The study highlights how HECC can address common IoD security challenges, including eavesdropping, unauthorized access, and data manipulation, by providing a more robust and efficient cryptographic solution for UAV communications.

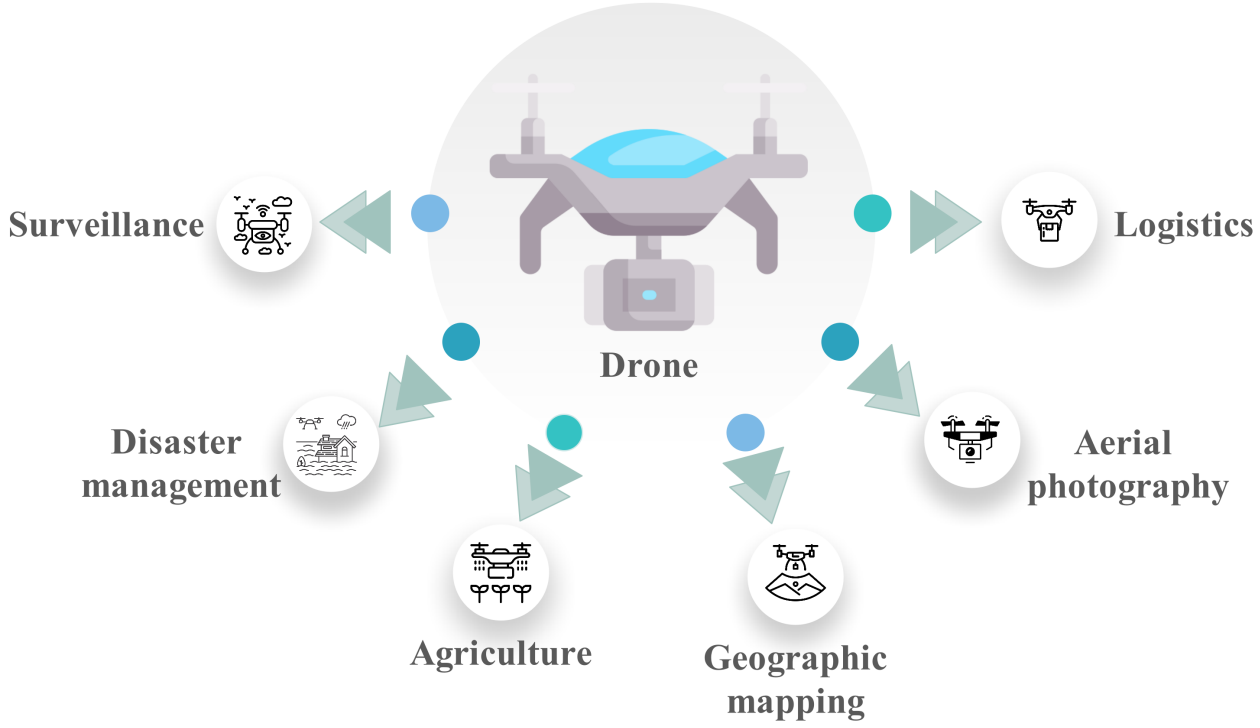

Figure 1. Applications areas of IoD.

- The proposed HECC protocol is more effectively served in IoD scenarios with limited computational resources because of its smaller key size and lower computational cost as compared with traditional cryptographic algorithms.

The rest of this paper is organized as follows: We discuss the security threats in the IoD ecosystem in Section 2. Section 3 discusses related works and addresses the limitations of current solutions. Section 4 introduces the HECC-based authentication protocol. Section 5 provides results and performance comparisons against classical methods. In the final Section, 6 concludes this paper and gives future work.

2 Security threats based on IoD

Due to the growing incorporation of the Internet of Drones (IoD) in most real-time applications, the security of the communication interface between UAVs and their controller is of the utmost necessity [10]. As drone usage becomes more prevalent, the IoD ecosystem is susceptible to different types of cyberattacks that threaten the confidentiality, integrity, and availability of data communicated within drone networks [11]. Drones communicate wirelessly over open channels that are vulnerable to a wide range of security threats, necessitating robust access authentication mechanisms to protect both the UAV and its serving network [12]. Figure 2 depicts some of the most important security threats emerging in the IoD.

2.1 Eavesdropping and Data Interception

Drones send and receive data packets over a wireless medium, which are subject to unauthorized interception and exploitation through eavesdropping attacks [13]. Attackers can intercept and eavesdrop on unsecured communication, thus exposing sensitive data such as location data, control commands, and mission data [14]. This data can be exploited to change the behavior of drone operations or to access uncoupled networks. Data loss would have tragic implications for any business, so using cryptographic measures, e.g., HECC-based device authentication and key agreement, to protect the communication channels prevents eavesdropping and guarantees the confidentiality of data being communicated in resource-constrained network environments, a principle demonstrated across multiple IoT deployment contexts [15].

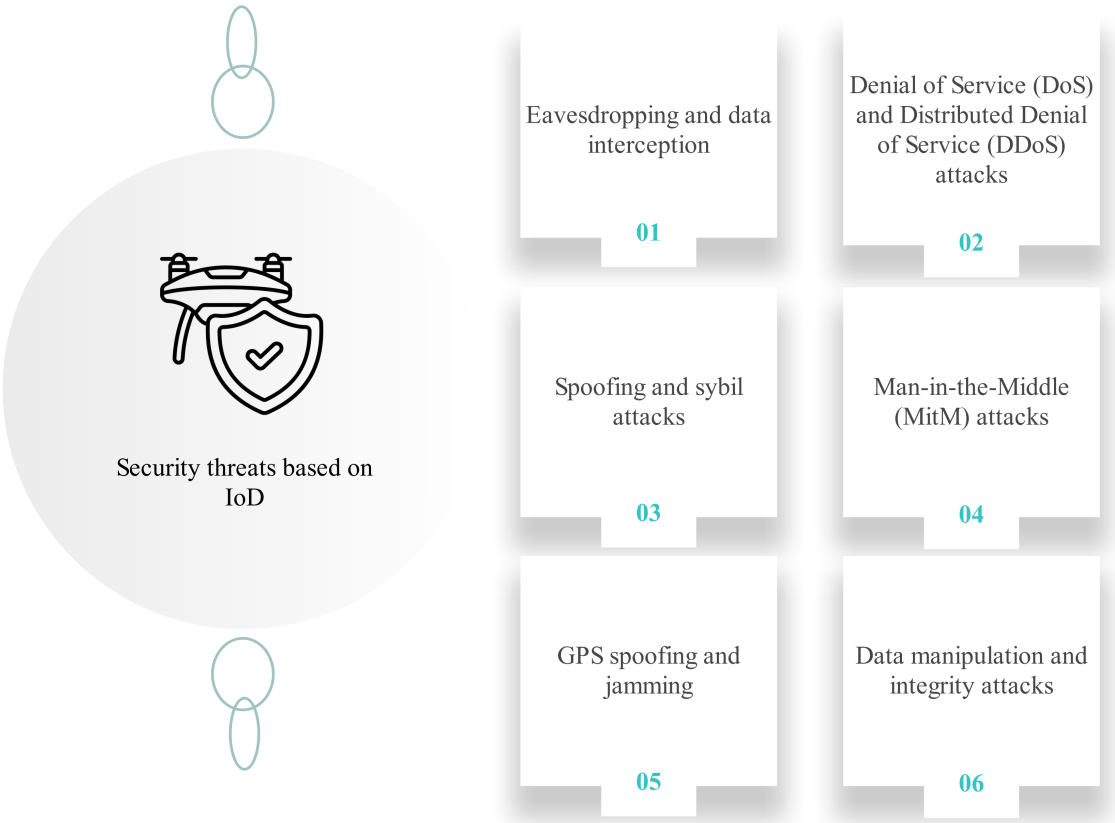

Figure 2. Security threats based on IoD.

2.2 Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are threats that flood the drone network with excess traffic and make the entire system unusable, and their growing prevalence in IoD environments has been documented through empirical detection studies [16]. As communication in IoD is critical for coordinated flight and navigation, DoS and DDoS attacks can greatly impact the normal operation of drones and cause missions or loss of communications [17]. These attacks are focused on the network infrastructure, including UAVs or servers that may block real traffic from reaching its destination [18]. By using HECC for authentication and communication, it is possible to prevent such attacks, as only authenticated and verified devices will be able to enter the network and communicate with others.

2.3 Spoofing and Sybil Attacks

Spoofing attacks in UAV networks encompass both identity-based impersonation and signal-level deception, where malicious entities either masquerade as authorized drones or inject false signals to mislead navigation and communication systems, both of which can be detected through lightweight intrusion detection mechanisms [19]. In a Sybil attack, a single malicious node generates multiple fake identities, allowing the malicious node to seize control of numerous drones and cause disruption in the communication between drones on the network [20]. The malicious actors attempt to impact the communication and data sharing, causing false data transmission, improper communication, and unauthorized command execution, compromising the overall IoD ecosystem [21]. These advanced authentication protocols, like the HECC-based methods discussed in this study, can combat both impersonation and Sybil attacks by confirming the identity of each drone and server in the network.

2.4 Man-in-the-Middle (MitM) Attacks

Man-in-the-Middle (MitM) Attack is when an attacker intercepts and modifies the communication between two drones or between a drone and the server. The attacker is capable of modifying the data that is being transmitted and thus will result in bad

decision-making or malicious behavior [22]. For example, an attacker could alter the drone's navigation commands or inject false data to trick operators. The adoption of cryptographic authentication methods like HECC can also include measures that help defend against MitM attacks by verifying the source and integrity of the messages in transit between parties.

2.5 GPS Spoofing and Jamming

One of the most common threats to UAVs that rely on GPS for navigation is GPS spoofing and jamming [23]. GPS spoofing involves attackers sending out phony GPS signals, tricking drones into flying along false routes out of navigation. GPS jamming sends signals over the GPS communication channels to interrupt GPS information, causing navigation errors and failure of the mission [24]. These attacks can be especially harmful to mission-critical applications such as disaster management or surveillance. Although threats related to GPS cannot be totally removed, which need strong authentication approaches such as HECC can mitigate the risk of attacks by ensuring that drones can function in safe and authorized situations.

2.6 Data Manipulation and Integrity Attacks

Data manipulation attacks are attempts to manipulate the data sent to UAVs or received by UAVs. It may result in erroneous decisions, system breakdowns, or leaks of sensitive information [25]. Attackers could modify control commands, sensor data, or software updates to negatively impact the performance and security of the drones. Secure cryptographic protocols, like HECC-based authentication, along with multi-layer access control mechanisms, ensure that data integrity is maintained and validate the authenticity and accuracy of the transmitted information sent across the network.

The HECC protocol secures IoD from general attacks like eavesdropping, denial of service, and Man-in-the-Middle (MitM) attacks. Moreover, it is resistant to hierarchical attack vectors such as jamming, where an adversary floods the medium with noise to disrupt the communication channel. Even during such attacks, cryptographic validation and authentication can serve as a complementary layer to mitigate the impact of jamming on data integrity, a challenge extensively documented in wireless network security research, with anti-jamming strategies remaining an open problem for UAV communication environments [26]. Although HECCs are jam-resistant with small key sets and fast operations, they are not immune to advanced attacks such as replay attacks and insider attacks. These are mitigated with session-specific key usage, timestamps, and multi-factor authentication. In upcoming simulations, we will analyze HECC performance on these advanced attack models to provide a more detailed security analysis.

However, HECC is more computationally expensive than ECC because it uses hyperelliptic curves, which results in more complex mathematical operations. Nevertheless, it has a low computational burden, which is highly desirable for resource-limited contexts like drones, as demonstrated by HECC-based authentication schemes specifically optimized for UAV networks [27]. HECC has some relatively novel applications to IoD networks, which require sensitive accommodations for potential vulnerabilities, such as advanced mathematical attacks on the properties of the curve. Its capability to provide smaller key sizes without compromising security makes it a very appealing alternative, particularly in circumstances where low latency and energy efficiency are vital.

The use of HECC in IoD networks also introduces issues related to regulation and ethics, most notably around data security and privacy. With drones increasingly being used for surveillance and as delivery devices, strong data protection measures are needed. HECC can assist in maintaining the integrity and confidentiality of transmitted data. Future work could involve exploring the ethical implications of drones and also helping make sure this HECC is complying with privacy laws via descriptive textual inputs.

3 Related works

With the rise of the Internet of Drones (IoD), various researchers have tried to achieve secure communication in drone networks. Numerous researchers have investigated the use of several cryptographic approaches to mitigate the security issues inherent to IoD environments [28]. In this section, we present a review of the state-of-the-art works with the most relevance in the design of secure authentication protocols for the IoD, discussing their pros and cons.

3.1 Elliptic Curve Cryptography (ECC) in UAV Networks

Elliptic Curve Cryptography (ECC) has gained significant popularity in UAV networks owing to its optimal key size and computational efficiency. In [29], the author proposed an ECC-based authentication and

key agreement protocol for communication security between UAVs and their servers. It provided secure data transfer with key lengths orders of magnitude smaller than existing public-key cryptosystems such as RSA. It is efficient to compute ECC, but it still has challenges in addressing these security issues of the IoD, especially the scalability and the computational overhead in the resource-constrained environment [30].

3.2 Blockchain-Based Authentication for IoD

The blockchain technology is widely used to secure the communication of IoD networks. For reference, [31] introduced a blockchain-enabled authentication scheme to facilitate transparent and non-repudiation communication between drones in their research. The scheme not only maintains the integrity of the data generated in the transmission by the IoD systems but also provides a decentralized authentication mechanism. Blockchain provides strong data security, but the computational and communication overhead of existing blockchain-based IoD authentication schemes motivates the development of more efficient alternatives [32].

3.3 Lightweight Authentication Schemes

However, the limited resources available to UAVs motivate the development of lightweight authentication protocols, which have been proposed to reduce computation costs but still ensure security. The work [33] proposed a lightweight authentication scheme for IoD using Chebyshev chaotic maps with privacy preservation. This protocol showed a huge decrease in computational complexity, but is still inspired by traditional cryptographic practices, which may not be as secure as more cutting-edge methods, such as HECC. However, because lightweight schemes provide less strict security guarantees than their heavyweight counterparts, they are more suited for IoD environments.

3.4 Hyperelliptic Curve Cryptography (HECC) in IoT and UAV Networks

With the rise of IoT and UAV networks, HECC has attracted considerable interest as a potential method of improving security. The authors in [34] introduced an HECC-based authentication method for the Internet of Vehicles (IoV), demonstrating that HECC's reduced key size and lower computational cost over conventional ECC are transferable advantages applicable to similarly resource-constrained mobile network environments, including IoD. Existing security solutions for IoD, such as blockchain-based intrusion detection systems combining neural network classifiers, have demonstrated improvements in data integrity and anomaly identification within drone networks [35]. However, these approaches rely on computational infrastructure that is ill-suited to resource-constrained drones and do not leverage the compact key-size and low-overhead advantage of hyperelliptic curve cryptography, leaving a clear gap in lightweight cryptographic authentication specific to IoD. HECC stands for hyperelliptic curve cryptography, which is much more efficient, having the properties of small-size keys, making them secure as well as performing efficiently in resource-based environments, which makes them suitable for securing communication in IoD networks.

3.5 Hybrid Cryptographic Approaches for IoD

To leverage the advantages of various cryptographic techniques, several hybrid approaches have also been proposed for IoD security [36]. The authors in [37] present a hybrid encryption and authentication scheme in which elliptic curve cryptography is used to combine symmetric encryption to facilitate communication across the UAV network. Using this hybrid model, it was demonstrated that security improved and computational overheads were reduced compared to just using ECC. In contrast, hybrid schemes induce additional complexity, and their applications in large-scale systems need further optimization.

3.6 Security Challenges in Flying Ad Hoc Networks (FANETs)

Flying Ad Hoc Networks (FANETs), which consist of UAVs communicating in a decentralized manner, present unique security challenges. Several studies have focused on securing FANETs by implementing lightweight cryptographic techniques, including ECC and HECC. In [38] author discussed the security challenges in FANETs, including routing vulnerabilities and the need for robust authentication mechanisms. They highlighted the potential of HECC to provide more efficient and secure solutions for FANET-based IoD systems, although this area remains underactive in terms of detailed implementation and analysis.

3.7 Comparative Analysis of Cryptographic Techniques for IoD Security

In [39], the authors proposed an IoD authentication scheme that integrates blockchain as a certificate authority with Hyperelliptic Curve Cryptography

(HECC), demonstrating that HECC's compact key size and reduced computational burden offer security advantages over conventional ECC-based approaches in resource-constrained drone environments. This work established a foundation for the application of HECC to IoD security, as it effectively summarizes its benefits in comparison to conventional techniques.

3.8 Comparison with Data-Driven Anomaly Detection Approaches

Recent studies in IoD security have explored data-driven anomaly detection approaches as a complement to cryptographic solutions; for instance, [40] proposed DroneSSL, a self-supervised multimodal framework that leverages TinyML and Graph Neural Networks to detect anomalies in Internet of Drone Things environments through spatial crowdsourcing. While such approaches advance runtime threat identification at the application layer, they operate at a fundamentally different level from cryptographic authentication protocols: rather than securing the communication channel itself, they detect anomalies post-hoc after data has already been transmitted. Our work addresses security at the protocol level through HECC-based authentication. Future work may explore integrating such anomaly detection frameworks with HECC-based protocols to form a more comprehensive and layered security architecture for IoD communication.

To conclude, earlier works have contributed greatly to providing secure communication for IoD-based networks, however, there remains a gap in applying Hyperelliptic Curve Cryptography (HECC) to this domain. To fill this gap, this paper aims to introduce the HECC-based authentication protocol that improves the existing solutions for IoD by providing a more robust and less computationally expensive alternative.

4 Methodology

In this section, the authentication protocol based on the Hyperelliptic Curve Cryptography (HECC), which ensures secure communication for the Internet of Drones (IoD) network, is presented. Relying on the sophisticated cryptographic features of HECC, which support stronger security with less computational power than classical primitives, including ECC, especially in lightweight contexts common to applications such as drones. Table 1 provides different notations along with their descriptions. Hyperelliptic curve encryption provides much more protection with such a smaller byte size and only small computing costs. Figure 3 visually represents the key generation, encryption/decryption, and digital signature processes of the HECC-based authentication protocol. Figure 3 provides a step-by-step overview of how the protocol functions, from the initial key exchange between the drone and server to the signing and verification of messages. The proposed methodology involves three main cryptographic operations:

1. Key Generation
2. Encryption/Decryption
3. Digital Signature Generation and Verification Each of these operations is explained in detail below.

Table 1. Notation table.

Notation	Description
G	Generator point on the hyperelliptic curve used for key generation.
d	Private key, a randomly chosen integer from the set Z_q.
P	Public key, computed as $P = dG$, where d is the private key and G is the generator point.
q	Order of the curve, the size of the finite field F used in the cryptosystem.
P_A	Public key of entity A (e.g., a drone), computed as $P_A = d_A G$.
P_B	Public key of entity B (e.g., a server), computed as $P_B = d_B G$.
S_A	Shared secret computed by entity A, calculated as $S_A = d_A P_B$.
S_B	Shared secret computed by entity B, calculated as $S_B = d_B P_A$.
M	Message that is being transmitted between entities.
r	Random integer chosen by entity A for encryption.
C_1	First part of the ciphertext, computed as $C_1 = rG$, where r is a random integer.
C_2	Second part of the ciphertext, computed as $C_2 = M + rP_B$, where P_B is the public key of the receiver.
k	Random integer chosen by entity A for generating a digital signature.
Q	Point on the curve used in digital signature generation, computed as $Q = kG$.
σ	Digital signature for message M, computed as $\sigma = k^{-1}(H(M) + d_A \cdot Q) \bmod q$.
$H(M)$	Hash value of message M, used in digital signature computation.
v_1	First part of the signature verification computation, computed as $v_1 = H(M) \cdot G$.
v_2	Second part of the signature verification computation, computed as $v_2 = \sigma \cdot P_A + Q$.

4.1 Hyperelliptic Curve Cryptosystem

The proposed method is based on the principles of the HECC. HECC generalizes elliptic curves but is more complicated and can provide strong security. They are defined by the general equation:

$$y^2 + h(x)y = f(x) \tag{1}$$

where $h(x)$ and $f(x)$ are polynomials. The degree of $f(x)$ is $2n + 1$ (where n is a non-negative integer), and

the degree of $h(x)$ is at most n. In contrast to elliptic curves, which have a genus of 1, hyperelliptic curves have a genus $g \geq 2$, making them more secure for cryptographic applications.

The HECC protocol employs cryptographic operations that are selected for good trade-offs between security and computational efficiency. In particular, the work is based on the key generation process, which utilizes the properties of hyperelliptic curves to produce even smaller keys with higher security than ECC up to date. These are among the most computationally efficient steps performed for data confidentiality. Later, these operations were optimized even more for use in very resource-constrained environments such as drone networks, where processing power and memory are at a premium. The reason behind selecting these operations is that these operations can provide strong security guarantees and have very high operational efficiency, which is the most important thing for the success of the IoD system.

In the context of IoD, this algebraic structure enables stronger encryption and key agreement protocols crucial for securing communications between drones, especially in complex missions involving multiple drones.

4.2 Key Generation

HECC key generation generally follows the same process as conventional public-key cryptography. Whether it is a drone or a server, each generates a private-public key pair. The private key is private, while the public key is shared with others for authentication.

1. Private Key: A randomly chosen integer d is selected from the finite field Z_q where q is the order of the curve.

$$d \in Z_q \tag{2}$$

2. Public Key: The public key P is calculated by multiplying the private key d with the generator point G on the hyperelliptic curve. The result is the public key:

$$P = dG \tag{3}$$

Such a public key is known to the communicating parties, in this example drone and its same server with which authentication and secure communication is established.

Key generation in the HECC protocol follows standard public-key cryptography methods but utilizes hyperelliptic curves for increased security. The process begins with the selection of a private key d as a random integer from the set of elements in the finite field. This private key is then used to compute the corresponding public key $P = d \cdot G$, where G is the generator point on the hyperelliptic curve, and P is the point that is publicly shared. The encryption process relies on the shared secret between the drone and the server, derived using Diffie-Hellman key exchange adapted for HECC. The message is encrypted using elliptic curve encryption and the recipient's public key. This process is followed by digital signature generation to ensure the integrity and authenticity of the message. Each of these cryptographic steps is carefully optimized for IoD environments, ensuring that the protocol remains computationally efficient.

4.3 Authentication Protocol

The authentication protocol is implemented to identify the drones and the servers in the IoD network, solving the problems where both are communicating with each other. To be trusted, a protocol must include key agreement, encryption and decryption, and signing processes. All of these steps guarantee that the exchanged data between drones and servers is secured against eavesdropping, man-in-the-middle attacks, or data manipulation.

4.3.1 Key Agreement

In terms of the specific Key Agreement process, each side, the drone and the server, must be able to agree on a common secret without passing the secret itself directly. This is based on the Diffie-Hellman key exchange mechanism with an adaptation for HECC.

- **Step 1**: Initialization: Entity A (drone) and entity B (server) exchange their public keys P_A and P_B, where:

$$P_A = d_A G \quad and \quad P_B = d_B G \tag{4}$$

- **Step 2:** Private Key Selection: Each entity selects its private key d_A (for the drone) and d_B (for the server) from Z_q.
- **Step 3:** Shared Secret Computation: Both entities compute the shared secret S by performing the following:

$$S_A = d_A P_B \quad and \quad S_B = d_B P_A \tag{5}$$

Since $S_A = S_B = d_A d_B G$, both entities now share the same secret key S, which can be used for encrypting messages between them.

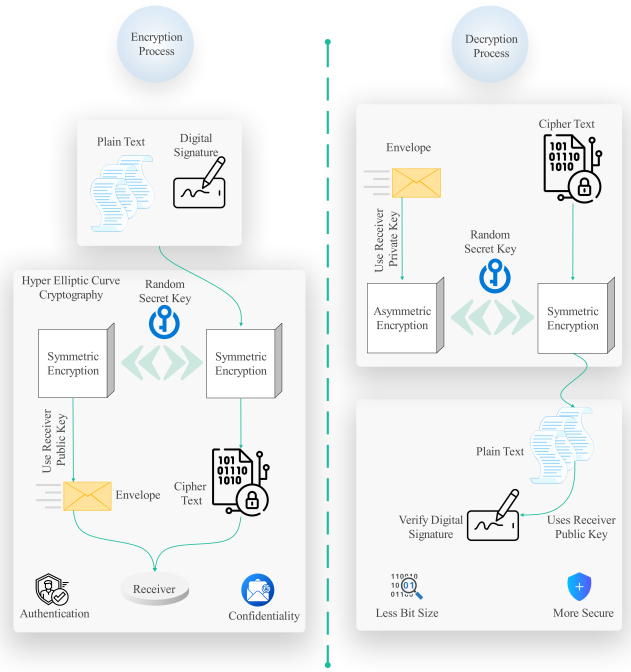

Figure 3. Encryption and decryption process for HECC.

4.3.2 *Encryption and Decryption*

The established shared secret is used for security between drones and servers. The recipient can read the encrypted messages using its private key, which corresponds to the shared secret that is derived from HECC.

- **Encryption:** To send a message M securely from the entity A (drone) to entity B (server), entity A performs the following steps:
  1. Select a random integer r.
  2. Calculate $C_1 = rG$ (a point on the curve).
  3. Calculate $C_2 = M + rP_B$, where P_B is the public key of an entity B.

  The encrypted message consists of C_1 and C_2 which are sent to an entity B.
- Decryption: Upon receiving C_1 and C_2, entity B (server) decrypts the message M using its private key d_B:

$$M = C_2 - d_B C_1 \tag{6}$$

The decryption process recovers the original message by subtracting the value $d_B C_1$, which is computed as $d_B rG = rP_B$.

4.3.3 *Digital Signature Generation and Verification*

A digital signature is formed to verify the integrity and authenticity of the messages transmitted between drones and the servers. Digital signatures ensure the message remains unmodified in transit and was produced by the legitimate entity.

- **Signature Generation:** To sign a message M, entity A (drone) computes a random integer k and a point $Q = kG$. Then, the signature σ is computed as:

$$\sigma = k^{-1}(H(M) + d_A \cdot Q) \bmod q \tag{7}$$

  where $H(M)$ is the hash of the message M.
- **Signature Verification:** Upon receiving the signed message, the entity B (server) verifies the signature by performing the following operations:

$$v_1 = H(M) \cdot G, \quad v_2 = \sigma \cdot P_A + Q \tag{8}$$

  If $v_1 = v_2$, the signature is valid, confirming that the message M was sent by an entity A and has not been tampered with.

HECC-based authentication protocol provides security against the attack as it relies on the combination of multiple cryptographic operations to secure the communication in the Internet of Drones (IoD) ensuring confidentiality, integrity, and authenticity of the exchanged messages between drones and their respective servers. The key features of this methodology include:

1. Efficient key generation based on the hyperelliptic curve.
2. Secure key agreement using the Diffie-Hellman approach adapted for HECC.
3. Encrypted communication using the shared secret derived from HECC.
4. Digital signatures for verifying the authenticity of messages and preventing tampering.

By leveraging Hyperelliptic Curve Cryptography (HECC), the proposed protocol enhances both security and computational efficiency over existing cryptographic protocols, which is suitable in the dynamic and resource-limited context of drone networks.

Alongside performance metrics, a theoretical computational complexity analysis of the HECC protocol must also be carried out. HECC achieves equivalent security levels to ECC with substantially smaller key sizes—typically 80 bits for genus-2 HECC versus 160 bits for standard ECC—owing to the richer algebraic structure of hyperelliptic curves. This

reduction in key size directly lowers the number of arithmetic operations required per transaction, translating into reduced computational overhead and faster key generation and signature verification. Furthermore, HECC has fewer communication rounds than RSA-based schemes, which translates into lower overall overhead. This approach is useful in IoD networks since high-speed and low-latency communication is required.

4.4 Security Analysis

The HECC-based protocol is analyzed against the Dolev–Yao threat model [22], in which the adversary has full control over the communication channel. The security properties of the proposed protocol are summarized as follows:

- **Mutual Authentication:** Both the drone and server verify each other's identity through the shared secret $S = d_A d_B G$, which cannot be derived by an adversary without knowledge of either private key.
- **Forward Secrecy:** Each session uses an independent random integer r (for encryption) and k (for signing), ensuring that compromise of long-term keys does not expose past session data.
- **Replay Attack Resistance:** The random integers r and k are freshly generated per session, preventing replay of intercepted ciphertexts.
- **Man-in-the-Middle Resistance:** The digital signature scheme (Section 4.3.3) ensures that any modification to message M in transit is detectable, as $v_1 \neq v_2$ upon verification.
- **Eavesdropping Resistance:** Message confidentiality is guaranteed by the computational hardness of the Hyperelliptic Curve Discrete Logarithm Problem (HCDLP): recovering d_A from the public key $P_A = d_A G$ is computationally infeasible.

Formal verification using tools such as ProVerif or the Scyther tool is reserved for future work, where the protocol will be modeled in applied pi-calculus to provide machine-checked security guarantees, complementing the provable security approaches adopted in existing lightweight IoD authentication schemes [29].

5 Results and Discussion

This section provides a comprehensive comparative analysis of the performance of the proposed Hyperelliptic Curve Cryptography (HECC)-based authentication protocol with three previously proposed protocols, namely Elliptic Curve Cryptography-Based Protocol with Public Secure Authentication Scheme (ECCCPSAS), Non-Linear Wireless Unmanned Aerial Systems Authentication Scheme, (NLWUAS) and Multi-Agent System (MAS). The feedback is centered on metrics like communication overhead, packet delivery ratio, throughput, and end-to-end delay to evaluate these protocols. It illustrates the advantages of HECC being more secure, more efficient, and higher network performance overall.

Python and Google Colab were used in the experimental setup to evaluate the HECC protocol as they facilitate a flexible and scalable environment for simulating the conditions of the IoD network. The simulation was developed to evaluate different conditions such as the number of drones that can be deployed and the level of the drone network. The network was tested in the following environments. The network was evaluated under the following parameters:

- **Network Size:** The network included up to 50 drones for small-scale experiments and up to 100 drones for large-scale evaluations.
- **Drone Mobility Patterns:** Drone mobility was modeled using both random waypoint and predefined paths, simulating dynamic and semi-static drone fleets.
- **Environmental Factors:** Network conditions such as signal interference, bandwidth fluctuations, and latency were adjusted to represent typical urban and rural IoD deployments. These variations helped assess the protocol's performance under different network scenarios, providing valuable insights into its scalability and robustness.

The HECC protocol was implemented in Python within the Google Colab environment, alongside benchmark protocols for comparison. This setup allows for easy replication of the experiment and testing under similar conditions in future studies.

For performance evaluation of HECC over varied network topologies, we also performed simulations for multi-drone scenarios with different mobility patterns. Network topology was also changed with either static or dynamic drone fleets, in which some drones were highly mobile while others had fixed point operations.

To assess the scalability of the protocol, we also evaluated its performance in large-scale drone fleets (up to 100 drones). The results showed that HECC consistently outperformed its competitors in terms of all measured metrics even with an increase in network size and mobility patterns in operation. This demonstrates HECC's strength of scaling in a more advanced IoD scenario.

5.1 Communication Overhead

As an important performance metric in IoD networks, communication overhead can be a bottleneck metric for IoD networks where IoDs, such as drones are resource-critical. Communication overhead is the overhead of sending additional information that is used to secure communication, such as encrypted messages, authentication data, and cryptographic keys.

Compared to traditional systems like RSA, the communication overhead of public key generation in the ECCCPSAS protocol based on Elliptic Curve Cryptography (ECC) is lower. But when drones and network size increase, then overhead becomes significant. NLWUAS is based on a non-linear cryptographic approach that has a heavy communication overhead due to complex authentication steps, especially in high-traffic networks. Similar to other multi-agent system coordination, MAS-based approaches incur high communication overhead due to the complexity of agent communication and data routing to facilitate authentication.

In contrast, the HECC protocol we proposed significantly reduces communication overhead. HECC leverages smaller key sizes and a more efficient cryptographic structure allowing faster key exchanges and less authentication data transmission. The Proposed HECC generates the keys and authenticates them in a way that reduces the total communication overhead in the IoD space while providing the same level of security. HECC has a 5% increase in communication overhead compared to conventional systems, but ECCCPSAS has 15%, NLWUAS has 30%, and MAS has 35%. Figure 4 depicts the overhead in communication for the four mentioned protocols; specifically, the increase in a number of bytes to secure the communication. HECC demonstrates the lowest communication overhead, with only a 5% increase, making it highly efficient, especially compared to the 15% increase for ECCCPSAS, 30% for NLWUAS, and 35% for MAS.

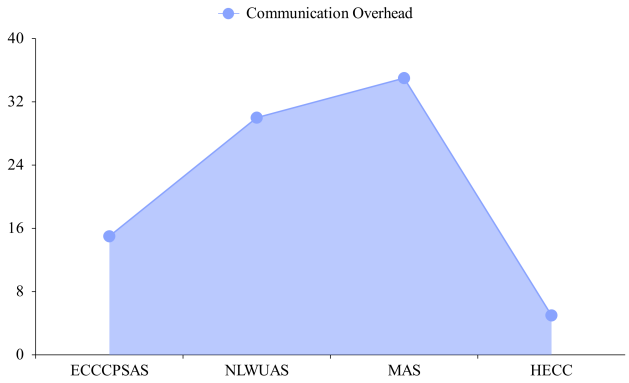

Figure 4. Communication overhead comparison of protocols.

5.2 Packet Delivery Ratio

The packet delivery ratio (PDR) is a key metric assessing the ratio between the packets successfully received and those sent throughout the network. More specifically, the PDR is an essential metric since a higher PDR represents more efficient and less packet-loss-prone communication protocols, which is critical in mobile and often lossy environments like the IoD.

ECCCPSAS had a moderately high packet delivery ratio of 85% and its performance was satisfactory. However, the overhead computation cost comes with a slightly lower PDR as networks grow in scale, especially for larger systems. NLWUAS has a PDR of 70% lower due to the complexity of cryptographic operations and more communication overhead. MAS further reduces the PDR even further to 60%, which is explained by the latency and packet loss that comes with high-stake multi-agent coordination. Thanks to optimized key generation and smaller key sizes, HECC gives us, with a detail of the aggressiveness and less expensive cryptographic operations, a very high packet delivery ratio of 95% with very low delay and packet loss rates. The packet delivery ratio for the four protocols is shown in Figure 5. The best PDR is that of HECC at a rate of 95%, meaning it is more effective to keep up communication with the lowest losses of packets. However, ECCCPSAS achieves a PDR of 85%, NLWUAS reaches 70%, and MAS yields a minimum PDR of only 60%.

5.3 Throughput

Throughput is the amount of data that is successfully transported across the network in a given interval of time, usually specified in bits per second (bps). One

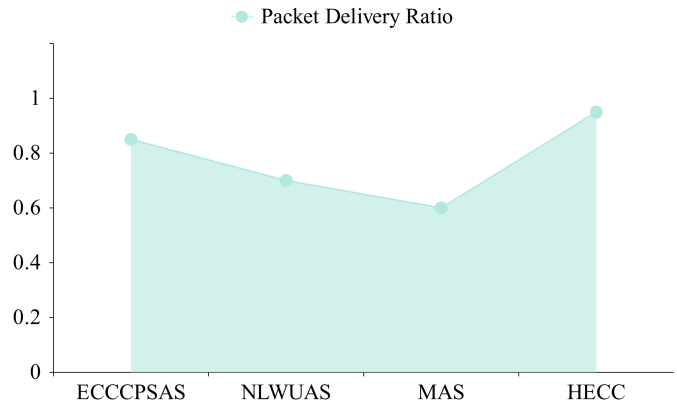

Figure 5. Packet Delivery Ratio comparison of protocols.

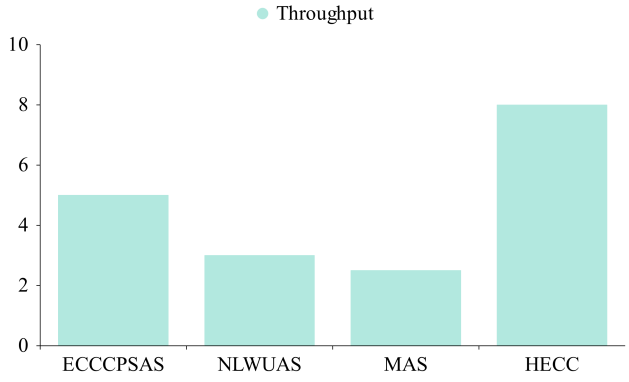

Figure 6. Throughput comparison of protocols.

of the critical requirements in IoD networks is the high throughput needed for the rapid communication and exchange of data, particularly when large volumes of data are involved, e.g., sensor data or video flows coming out of drones.

ECCCPSAS has a moderate throughput of 5 Mbps, although this can be curtailed depending on the computational burden of ECC encryption and decryption. Throughput often decreases as the system replicates due to the more complex cryptographic operations. However, due to the more expensive nature of the cryptography used in NLWUAS and the additional round trips to perform the authentication, NLWUAS achieves a lower throughput of 3 Mbps. Overall, MAS performs far worse too with a throughput of only 2.5 Mbps this is because high overhead exists to allow communication across the multi-agent system. However, due to efficient encryption, authentication processes, and reduced computational burden HECC gives the maximum throughput of 8 Mbps. Throughput values for each of the protocols are shown in Figure 6. At 8 Mbps, HECC has the highest throughput obtained, showing its ability to manage high data transmission rates. The Native NLWUAS gets a throughput of 3 Mbps, while the MAS provides the least throughput at 2.5 Mbps. The 5 Mbps throughput is achieved by the ECCCPSAS.

5.4 End-to-End Delay

End-to-end delay refers to the time it takes for a packet to reach its destination, including delays due to encryption, decryption, authentication, and routing. Timely response is crucial in real-time systems, such as drone communication networks, where minimizing the delay as much as possible is vital for mission accomplishment.

ECCCPSAS introduces a moderate end-to-end delay of 150 ms with a known maximum delay. While ECC is efficient in smaller networks. Due to extra computation complexity for cryptographic operations and coordination overhead, NLWUAS suffers an extra 250 ms delay compared to ECCCPSAS. Because of its multi-agent system, MAS has a maximal delay of 300 ms since the overhead of agent-to-agent communication and the authentication steps increase the processing time. By reducing the time-consuming tasks for HECC, the end-to-end delay of the final time for the encryption and key generation is minimized to 75 ms. In Figure 7, we observe the visualization of the end-to-end delay by the protocols and the values in milliseconds, where we can see that HECC achieves a low delay of 75 ms, demonstrating its capability for fast communication, which is essential for real-time applications. ECCCPSAS has a delay of 150 ms, followed by NLWUAS with 250 ms, while MAS exhibits the entire highest delay with 300 ms.

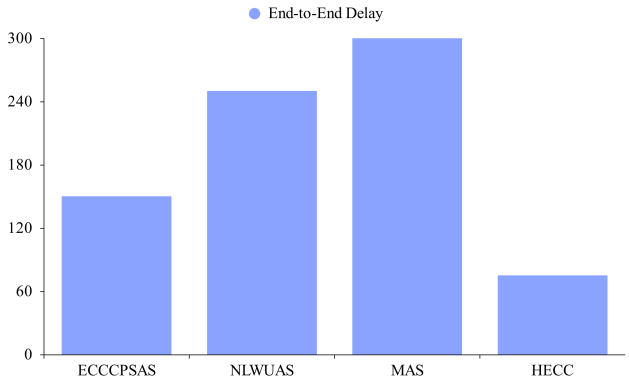

Figure 7. End-to-End Delay comparison of protocols.

Table 2. Compares the performance communication protocols.

Protocol	Communication Overhead	Packet Delivery Ratio	Throughput	End-to-End Delay
ECCCPSAS	15% increase	85%	5 Mbps	150 ms
NLWUAS	30% increase	70%	3 Mbps	250 ms
MAS	35% increase	60%	2.5 Mbps	300 ms
HECC	**5% increase**	**95%**	**8 Mbps**	**75 ms**

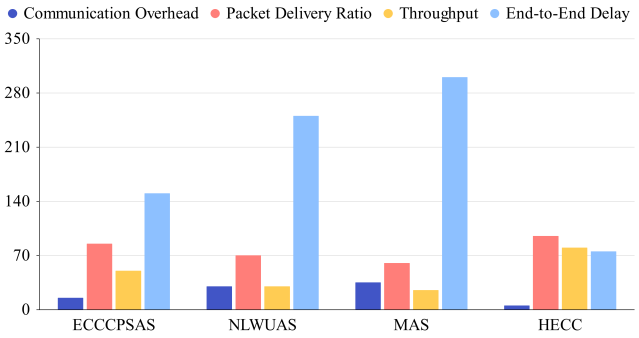

Figure 8. Performance comparison of protocols.

5.5 Overall Performance Comparison

The analysis results show a great performance of HECC over the four protocols in terms of communication overhead, Packet Delivery Ratio, Throughput, and End-to-End Delay. Hence, HECC is the most suitable type for secure communication in IoD networks in required settings like drone-based networks as it limits communication overhead, optimizes packet delivery ratio, enhances the throughput, and reduces end-to-end delay.

The HECC-based authentication scheme is superior in all aspects to the ECCCPSAS, NLWUAS, and MAS protocols, facilitating a secure and efficient method to access drone communications in inter-disciplines. This protocol proves to be an efficient mechanism to decrease communication overhead, enhance packet delivery, augment throughput, and reduce delay, ranking it the most applicable option amongst its peer protocols, particularly for IoD applications needing real-time communication and high data throughput. The comparison of four communication protocols ECCCPSAS, NLWUAS, MAS, and HECC for each of the metrics is shown in Table 2. HECC outperforms the others. The performance of these protocols is shown in Figure 8 as well.

HECC protocol outperforms in significant energy efficiency and scalability for IoD networks. The HECC protocol demonstrated lower energy consumption per transaction compared to ECC and RSA, due to reduced key sizes and fewer arithmetic operations required, making it suitable for long-endurance drone operations, especially beyond the line of sight (BLOS), where no constant power source is available and all systems, including communication, are entirely dependent on battery energy. Furthermore, in terms of performance, the protocol continued performing well as the network size increased, with low communication overhead and stable performance metrics, with networks of up to 100 machines. As the network expands, though, further optimization is needed to avoid future congest points. From a computational perspective, HECC provided competitive key generation and signature verification times, enabling its application to real-time systems with stringent latency constraints. In our future work, we will further investigate HECC performance in single case studies of thousands of drones and dynamic topologies, to really unveil its scalability in larger-scale IoD systems.

5.6 Limitations and Future Work

However, similar to all other protocols, it needs to be further tested when implemented in physical experiments. The future work will focus on the following areas:

- Hybrid Approaches: The ties between HECC and advancements in other cryptographic systems, such as symmetric encryption, may yield additional methods for refining the balance between security and computer efficiency.
- Real-World Testing: Real-world experiments are important to be able to test the protocol on a practical basis and see how it performs under the effects of real network issues, such as interference and mobility.
- Quantum-Resistant Cryptography: As quantum computing advances, the combination of quantum-resistant algorithms with HECC will also need to be considered to guarantee the long-term security of communication in IoD. Post-quantum cryptographic approaches, such as

lattice-based cryptography, represent a promising direction for integration with HECC to enable the long-term deployment of IoD systems.

- AI and ML integration will be investigated to improve the speed and security of the HECC protocol. For example, AI anomaly detection could aid in real-time identification of network threats, while ML algorithms could dynamically make adjustments to encryption layers depending on network parameters to improve performance and enhance IoD security.

6 Conclusion

We proposed a HECC-based authentication protocol in this study, which is used for securing the communication between IoD networks and analyzed against other three existing approaches ECCCPSAS, NLWUAS and MAS. The performance metrics include communication overhead, packet delivery ratio, throughput, and end-to-end delay, and the assessment showed that HECC is superior to all other methods in these parameters. It had the minimum communication overhead, the maximum packet delivery ratio, the maximum throughput, and the minimum end-to-end delay, along with being a perfect fit for implementation in IoD networks with limited resources, where low latency and high throughput are critical.

The HECC protocol's outstanding performance relies on its use of high-overhead security together with the efficient cryptographic operation to yield drones that are able to operate compactly with various transmission capabilities. Due to smaller key sizes, HECC supports fast key generation and authentication, which is essential for reliable communication in dynamic scenarios such as multi-drone surveillance operations and autonomous delivery fleets. These efficiencies position HECC as an ideal solution for the expansion of IoD deployments, especially in mobile and real-time stretches where seamless and rapid communication is paramount.

Future research efforts will validate the HECC protocol in real IoD systems with pilot projects using fleets of autonomous drones to investigate its performance under operational conditions, including real-time communication capabilities, security resilience, and energy efficiency in practice. The paper will also touch upon the potential of leveraging HECC with novel technologies, including quantum-safe methods and AI-based detection systems, to further boost HECC's efficiency and resistance. Offering HECC wider support of larger-scale networks and exploring its use across diverse industries, such as automated delivery, surveillance, and disaster management, will be vital in optimizing its utility within an IoD context.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Berini, A. D. E., Ferrag, M. A., Farou, B., & Seridi, H. (2023). HCALA: Hyperelliptic curve-based anonymous lightweight authentication scheme for Internet of Drones. *Pervasive and Mobile Computing, 92*, 101798. [CrossRef]

[2] Bera, B., Saha, S., Das, A. K., Kumar, N., Lorenz, P., & Alazab, M. (2020). Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment. *IEEE Transactions on Vehicular Technology, 69*(8), 9097-9111. [CrossRef]

[3] Adeniyi, A. E., Jimoh, R. G., & Awotunde, J. B. (2024). A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security. *Computers and Electrical Engineering, 118*, 109330. [CrossRef]

[4] Hussain, S., Chaudhry, S. A., Alomari, O. A., Alsharif, M. H., Khan, M. K., & Kumar, N. (2021). Amassing the security: An ECC-based authentication scheme for Internet of Drones. *IEEE Systems Journal, 15*(3), 4431-4438. [CrossRef]

[5] Tanveer, M., Alasmary, H., Kumar, N., & Nayak, A. (2023). SAAF-IoD: Secure and anonymous authentication framework for the Internet of Drones. *IEEE Transactions on Vehicular Technology, 73*(1), 232-244. [CrossRef]

[6] 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. [CrossRef]

[7] Tan, Y., Wang, J., Liu, J., & Kato, N. (2022). Blockchain-assisted distributed and lightweight

authentication service for industrial unmanned aerial vehicles. *IEEE Internet of Things Journal, 9*(18), 16928-16940. [CrossRef]

[8] Sharma, J., & Mehra, P. S. (2023). Secure communication in IOT-based UAV networks: A systematic survey. *Internet of Things, 23*, 100883. [CrossRef]

[9] Hawashin, D., Nemer, M., Gebreab, S. A., Salah, K., Jayaraman, R., Khan, M. K., & Damiani, E. (2024). Blockchain applications in UAV industry: Review, opportunities, and challenges. *Journal of Network and Computer Applications, 230*, 103932. [CrossRef]

[10] Yahuza, M., Idris, M. Y. I., Ahmedy, I. B., Wahab, A. W. A., Nandy, T., Noor, N. M., & Bala, A. (2021). Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access, 9*, 57243-57270. [CrossRef]

[11] Abdelmaboud, A. (2021). The internet of drones: Requirements, taxonomy, recent advances, and challenges of research trends. *Sensors, 21*(17), 5718. [CrossRef]

[12] Ma, R., Cao, J., He, S., Zhang, Y., Niu, B., & Li, H. (2023). A UAV-assisted UE access authentication scheme for 5G/6G network. *IEEE Transactions on Network and Service Management, 21*(2), 2426-2444. [CrossRef]

[13] Shen, A., Luo, J., Ning, J., Li, Y., Wang, Z., & Duo, B. (2023). Safeguarding UAV networks against active eavesdropping: An elevation angle-distance trade-off for secrecy enhancement. *Drones, 7*(2), 109. [CrossRef]

[14] Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad hoc networks, 133*, 102894. [CrossRef]

[15] Pirayesh, J., Giaretta, A., Conti, M., & Keshavarzi, P. (2022). A PLS-HECC-based device authentication and key agreement scheme for smart home networks. *Computer Networks, 216*, 109077. [CrossRef]

[16] Alsumayt, A., Nagy, N., Alsharyofi, S., Al Ibrahim, N., Al-Rabie, R., Alahmadi, R., ... & Alahmadi, A. A. (2024). Detecting denial of service attacks (DoS) over the Internet of Drones (IoD) based on machine learning. *Sci, 6*(3), 56. [CrossRef]

[17] Hadi, H. J., Cao, Y., Nisa, K. U., Jamil, A. M., & Ni, Q. (2023). A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. *Journal of Network and Computer Applications, 213*, 103607. [CrossRef]

[18] Wang, Z., Li, Y., Wu, S., Zhou, Y., Yang, L., Xu, Y., ... & Pan, Q. (2023). A survey on cybersecurity attacks and defenses for unmanned aerial systems. *Journal of Systems Architecture, 138*, 102870. [CrossRef]

[19] Arthur, M. P. (2019, August). Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS. In *2019 international conference on computer, information and telecommunication systems (CITS)* (pp. 1-5). IEEE. [CrossRef]

[20] Rugo, A., Ardagna, C. A., & Ioini, N. E. (2022). A security review in the UAVNet era: Threats, countermeasures, and gap analysis. *ACM Computing Surveys (CSUR), 55*(1), 1-35. [CrossRef]

[21] Kharchenko, V., & Torianyk, V. (2018, May). Cybersecurity of the internet of drones: Vulnerabilities analysis and imeca based assessment. In *2018 IEEE 9th international conference on dependable systems, services and technologies (DESSERT)* (pp. 364-369). IEEE. [CrossRef]

[22] Ko, Y., Kim, J., Duguma, D. G., Astillo, P. V., You, I., & Pau, G. (2021). Drone secure communication protocol for future sensitive applications in military zone. *Sensors, 21*(6), 2057. [CrossRef]

[23] Derhab, A., Cheikhrouhou, O., Allouch, A., Koubaa, A., Qureshi, B., Ferrag, M. A., ... & Khan, F. A. (2023). Internet of drones security: Taxonomies, open issues, and future directions. *Vehicular Communications, 39*, 100552. [CrossRef]

[24] Eldosouky, A., Ferdowsi, A., & Saad, W. (2019). Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing. *IEEE Internet of Things Journal, 7*(4), 2840-2854. [CrossRef]

[25] Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things, 11*, 100218. [CrossRef]

[26] Pirayesh, H., & Zeng, H. (2022). Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE communications surveys & tutorials, 24*(2), 767-809. [CrossRef]

[27] Sharma, J., & Mehra, P. S. (2024). HCFAIUN: A novel hyperelliptic curve and fuzzy extractor-based authentication for secure data transmission in IoT-based UAV networks. *Vehicular Communications, 49*, 100834. [CrossRef]

[28] Hussain, S., Farooq, M., Alzahrani, B. A., Albeshri, A., Alsubhi, K., & Chaudhry, S. A. (2023). An efficient and reliable user access protocol for Internet of Drones. *IEEE Access, 11*, 59688-59700. [CrossRef]

[29] Nikooghadam, M., Amintoosi, H., Islam, S. H., & Moghadam, M. F. (2021). A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance. *Journal of Systems Architecture, 115*, 101955. [CrossRef]

[30] Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2018). Elliptic curve lightweight cryptography: A survey. *Ieee Access, 6*, 72514-72550. [CrossRef]

[31] Subramani, J., Maria, A., Rajasekaran, A. S., & Lloret, J. (2024). Physically secure and privacy-preserving blockchain enabled authentication scheme for internet of drones. *Security and Privacy, 7*(3), e364. [CrossRef]

[32] Tanveer, M., Aldosary, A., Kumar, N., & Aldossari, S. A. (2024). SEAF-IoD: Secure and efficient user

authentication framework for the Internet of Drones. *Computer Networks, 247*, 110449. [CrossRef]

[33] Nair, A. S., & Thampi, S. M. (2023). A location-aware physical unclonable function and Chebyshev map-based mutual authentication mechanism for internet of surveillance drones. *Concurrency and Computation: Practice and Experience, 35*(19), e7564. [CrossRef]

[34] Shah, T. A., Algarni, F., Ullah, I., Abdullah, A. M., Noor, F., & Asghar Khan, M. (2022). Cost-Efficient Privacy-Preserving Authentication and Key Management Scheme for Internet of Vehicle Ecosystem. *Complexity, 2022*(1), 8406649. [CrossRef]

[35] Heidari, A., Navimipour, N. J., & Unal, M. (2023). A secure intrusion detection platform using blockchain and radial basis function neural networks for internet of drones. *IEEE Internet of Things Journal, 10*(10), 8445-8454. [CrossRef]

[36] Yang, W., Wang, S., Yin, X., Wang, X., & Hu, J. (2022). A review on security issues and solutions of the internet of drones. *IEEE Open Journal of the Computer Society, 3*, 96-110. [CrossRef]

[37] Zhang, S., Liu, Y., Han, Z., & Yang, Z. (2023). A lightweight authentication protocol for UAVs based on ECC scheme. *Drones, 7*(5), 315. [CrossRef]

[38] Jan, S. U., Abbasi, I. A., Algarni, F., & Khan, A. S. (2022). A verifiably secure ECC based authentication scheme for securing IoD using FANET. *IEEE Access, 10*, 95321-95343. [CrossRef]

[39] Javed, S., Khan, M. A., Abdullah, A. M., Alsirhani, A., Alomari, A., Noor, F., & Ullah, I. (2022). An efficient authentication scheme using blockchain as a certificate authority for the internet of drones. *Drones, 6*(10), 264. [CrossRef]

[40] Akram, J., Anaissi, A., Othman, W., Alabdulatif, A., & Akram, A. (2024). Dronessl: Self-supervised multimodal anomaly detection in internet of drone things. *IEEE Transactions on Consumer Electronics*, 70(1), 4287-4298. [CrossRef]



Zeeshan Ali Haider is currently pursuing a Ph.D in computer science at Qurtuba University of Science and Information Technology, Peshawar, Pakistan. He holds an MS in Computer Science from Abasyn University, Peshawar, Pakistan, where he was awarded distinction, and a BS in Computer Science from Islamia College, Peshawar, Pakistan. He has also published a book chapter in a top-tier journal. His research interests encompass a wide range of fields, including the Internet of Vehicles (IoV), Cybersecurity, Cryptography, Blockchain, Machine Learning, Deep Learning, the Internet of Things (IoT), and Data Mining. (Email: Zeeshan.ali9049@gmail.com)



Muhammad Fayaz completed his bachelor's degree from Islamia College University Peshawar and earned a master's degree in Computer Engineering, specializing in computer vision, deep learning, and machine learning, from the Department of Computer Engineering at Cyprus International University, Turkish Republic of Northern Cyprus. He is currently a research assistant at the Computer Vision and Pattern Recognition (CVPR) Laboratory at Sejong University. His research interests span computer vision, deep learning, and machine learning, with a particular focus on both medical image analysis and land cover classification. In the realm of medical image analysis, he is contributing to the development of advanced techniques for image classification and segmentation, aimed at improving diagnostic accuracy and medical decision-making. His work in land cover classification focuses on leveraging deep learning to analyze satellite and aerial imagery, enabling more effective monitoring of environmental changes, and land cover shifts, and supporting sustainable development. Through his interdisciplinary approach, Muhammad is making significant contributions to both fields, using state-of-the-art computational methods to solve complex challenges in medical imaging and environmental monitoring. (Email: muhammadfayaz@sju.ac.kr)



Yue Zhang holds a bachelor's degree in Electronic Information and Communication Engineering from Yanbian University in China, along with a graduate degree in Computer Science from Sejong University in South Korea. Her research interests are focused on computer vision, deep learning, and machine learning, and she is actively contributing to advancements in these areas. (Email: zhyuebbb@gmail.com)



Dr. Ahmad Ali , obtained his Master and Ph.D. degrees from Shanghai Jiao Tong University, China, where he built a strong foundation in computer science and engineering. Currently, he is a Postdoctoral Researcher in the College of Computer Science and Software Engineering at Shenzhen University, China. His research interests span deep learning, big data analytics, data mining, urban computing, cloud computing, and fog computing. Beyond his research contributions, Dr. Ahmad Ali has played an active role in peer review and scholarly evaluation, having reviewed over 1,200 research articles for prestigious academic journals, including Information Sciences, Information Fusion, Neural Networks, Applied Intelligence, IEEE Transaction on Industrial Informatics, IEEE Internet of Things, Neural Computing and Applications, Multimedia Tools and Applications, Wireless Networks, and IEEE Access. In addition, he has been involved in several cutting-edge research projects, leading to numerous publications in top-tier journals and conferences, further demonstrating his expertise and contributions to the field. Passionate about leveraging advanced computing technologies to address real-world challenges, particularly in urban environments, his work focuses on efficient data processing and intelligent decision-making to enhance modern computing applications. (Email: ahmadali@szu.edu.cn)