A LIGHTWEIGHT AUTHENTICATION PROTOCOL LAPHECC FOR DRONE USING HECC SCHEME

K.Deepa[1] and Dr.M.Gobi[2]

[1]Research Scholar, Department of Computer Science, Chikkanna Government Arts College, Tirupur - 641602, Tamilnadu, India.
[2]Associate Professor, Department of Computer Science, Chikkanna Government Arts College, Tirupur - 641602, Tamilnadu, India.

ABSTRACT

With the growing use of unmanned aerial vehicles (UAVs) or drones, ensuring secure communication in open-access environments has become essential. While authentication systems based on Elliptic Curve Cryptography (ECC) are widely adopted due to their efficiency and reduced key sizes, further improvements are needed to enhance communication security and computational performance. To address this, we introduce LAPHECC, a lightweight authentication protocol that replaces ECC with Hyperelliptic Curve Cryptography (HECC). HECC is particularly well-suited for resource-limited devices, as it provides stronger security per bit and requires even smaller key sizes than ECC. The protocol incorporates a pre-registration stage and employs a Schnorr-based zero-knowledge session key update mechanism to guarantee both forward and backward secrecy. Security evaluations show that LAPHECC delivers minimal computational and communication overhead while ensuring core security properties such as confidentiality, mutual authentication, and resistance to replay and impersonation attacks.

KEYWORDS

Security, Handshake, Ground Station, Encryption, Networks.

1. INTRODUCTION

Unmanned Aerial Vehicles (UAVs) face significant communication security vulnerabilities such as spoofing and data interception. To enhance UAV network security, lightweight authentication is required. While Elliptic Curve Cryptography (ECC) is commonly used, it has limitations regarding backward security and scalability. Hyperelliptic Curve Cryptography (HECC) offers a more secure and lightweight alternative due to its use of algebraic curves of genus. This study introduces LAPHECC, a lightweight authentication protocol for UAV networks based on HECC, which maintains a three-phase structure and employs Schnorr-style proofs over hyperelliptic curve Jacobians for backward security in session key updates. Following is a communal set up for drone.

 DOI:10.5121/ijci.2026.150108

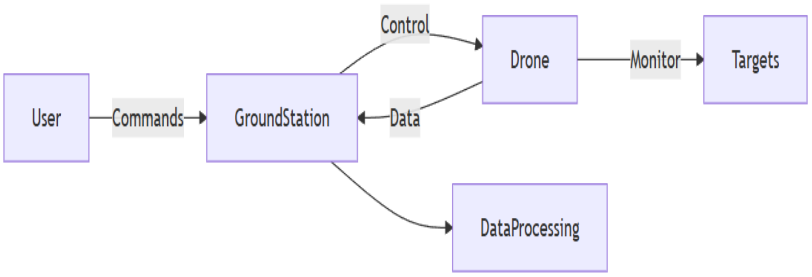

Figure 1. A Communal Drone Set-up

2. BACKGROUND STUDY

Scholars have proposed RFID technology as a method to address authentication challenges for Drones in civilian and defence applications, leveraging its versatility for tracking and identification. Drones can be embedded with RFID tags scanned and verified by a trusted server to determine security status. While RFID methods are efficient and easy to deploy, the limited processing power of RFID tags poses a security challenge. PUF technology is suggested to enhance RFID substantiation, offering improved hardware security. However, the effectiveness of PUF-based RFID solutions is limited within dynamic and broad-based substantiation systems.

2.1 Hyper Elliptical Curve Cryptography

Hyper-Elliptic Curve Cryptography (HECC) enhances Elliptic Curve Cryptography (ECC) by utilizing hyperelliptic curves (genus ≥ 2). This allows for 80-bit security with 160-bit keys, compared to ECC's 256-bit keys for similar security. HECC offers improved efficiency through divisor-based arithmetic, reducing point multiplication overhead and saving approximately 30% energy for drones. Its constant-time divisor operations also provide resilience against side-channel attacks. The HECC secure communication process involves key generation, authentication, key agreement, and zero-knowledge proof, where a drone signs a ground station nonce for verification and establishes a session key. Benefits include enhanced battery efficiency, forward secrecy, and potential quantum resistance with post-quantum variants, leading to prolonged drone flight duration and secure communication.The characteristics of ECC and HECC are illustrated in the table below.

Table 1. Comparison of ECC and HECC

Feature	ECC	HECC
Curve Genus	1	>=2
Key Size	256-bit	160 bit
Speed	Fast	Faster
Mathematical Complexity	Moderate	Higher

2.2 Scheme of Hedhoc

The HEDHOC protocol, an evolution of EDHOC for IoT, features a streamlined 2-message handshake, a reduction from EDHOC's 3 messages. This is achieved through post-quantum hybrid signatures combining CRYSTALS-Kyber and Ed25519. HEDHOC employs a sign-then-MAC authentication method with lightweight PUFs for device identification, contrasting with

EDHOC's MAC-then-Sign approach. It also enhances security with forward secrecy via X25519 and improved resistance to side-channel attacks, building upon EDHOC's reliance on ephemeral Diffie-Hellman. Furthermore, HEDHOC optimizes payload efficiency using CBOR-encoded headers, which are 20% smaller than EDHOC's COSE headers, making it more suitable for IoT applications.

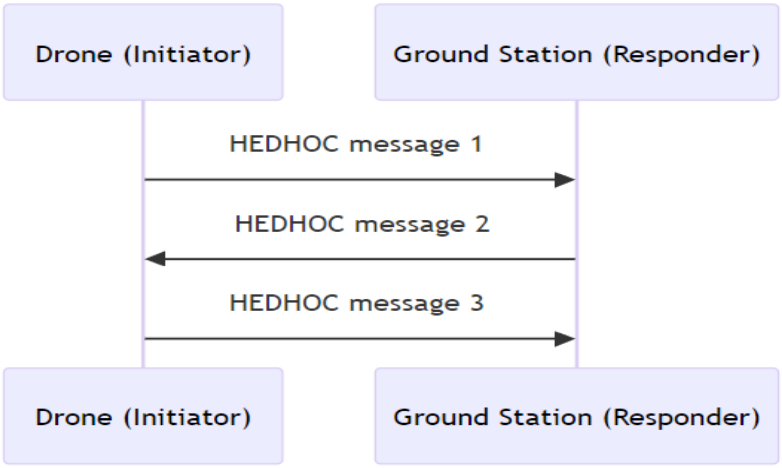

Figure 2. Flow of interactions in the scheme of HEDHOC

The image depicts a three-message HEDHOC protocol exchange between a drone (initiator) and a ground station (responder) for efficient, secure, and lightweight communication in distributed systems. The protocol facilitates identity authentication, secure channel establishment, and uninterrupted mobility. The drone initiates with a handshake/authentication request, the ground station responds with a challenge/parameter, and the drone finalizes with key confirmation/integrity check. HEDHOC's lightweight design is ideal for resource-constrained drones and mobile networks, ensuring data integrity, confidentiality, and continuity for missions like surveillance or delivery.

2.3 Analysis of Problem

Ephemeral Diffie-Hellman Over COSE (EDHOC) presents several limitations for drone communications, including vulnerability to hijacking due to static identity keys, unsuitability for dynamic networks because of its reliance on pre-shared public keys, and a lack of built-in mechanisms for frequent key updates and backward secrecy. The protocol's cryptographic operations, while more efficient than traditional Public Key Infrastructure (PKI), still impose significant computational overhead that can strain drone batteries and exceed the processing capabilities of smaller drones, suggesting a need for more lightweight and adaptable security solutions for resource-constrained or large-scale drone deployments.

3. PROPOSED FRAMEWORK

3.1 Design Strategies

The protocol for secure drone operations establishes a secure, authenticated air-to-ground communication link through several phases: pre-registration for identity exchange, authentication to verify drone and ground station identities, and session key update for encrypted communication. The LAPHEC protocol validates session setup with a three-way handshake,

while a zero-knowledge proof (ZKHP) phase verifies the drone's legitimacy without revealing secrets. This process results in a fully authenticated, encrypted channel. Key features include lightweight design, forward secrecy, attack resilience, and enhanced privacy via ZKHP, making it suitable for secure drone operations against potential adversaries.

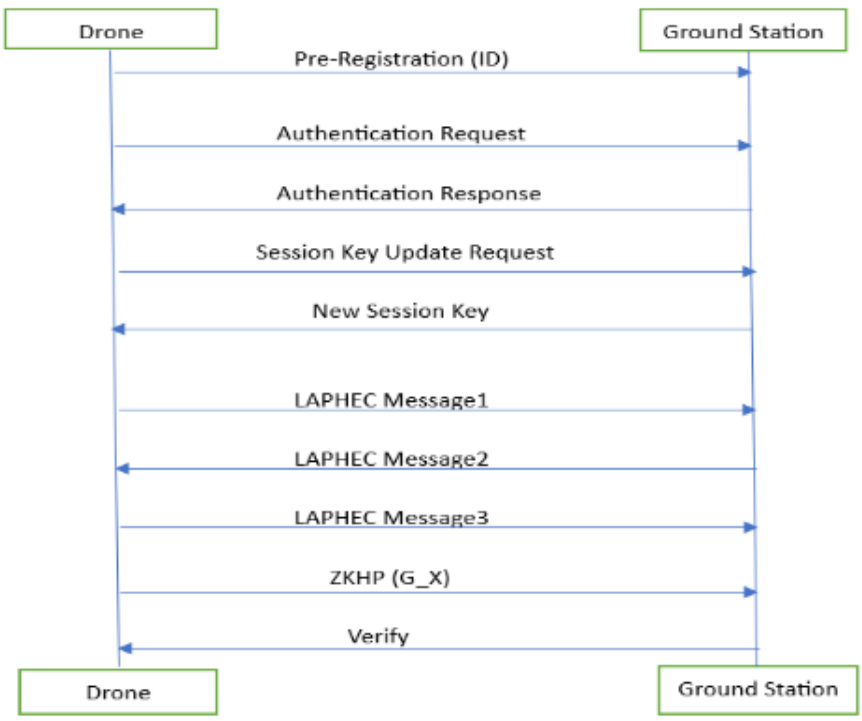

Figure 3. Interaction flow of LAPHEC message

The provided text describes a secure authentication and key establishment protocol, LAPHEC, used between a drone and a ground station. The protocol consists of several phases: pre-registration for initial trust and identity exchange, authentication using request-response mechanisms with signed challenges to prevent impersonation, session key update via methods like Diffie-Hellman for encrypted communication, LAPHEC protocol execution involving a 3-way handshake for session parameter finalization and replay attack protection, and Zero-Knowledge Proof (ZKHP) verification to prove knowledge of a secret without disclosure. Successful execution results in an authenticated and encrypted channel for secure drone-ground station communications.

3.2 Pre-Registration Phase

The drone and control station have their own public and private key pairs, and, respectively. In this case, D and G represent the private keys used by mutual revelries for authentication. The key pairs are generated as APK_D = DB and APK_G = GB, where B represents the base point of an elliptical curve acknowledged by mutual revelries.

3.3 Authentication Phase

The authentication process between an aerial node (drone) and a control station involves a multi-stage secure communication link establishment. The initial pre-registration phase requires the drone to transmit its credentials, including a unique device identifier and a public key or

certificate, to the ground station. The ground station then responds with a validation signal, potentially using a cryptographic nonce or signal strength checks, to confirm the drone's presence and facilitate mutual authentication.

During substantiation, the control station sends its credentials and an authentication token to the drone, which replies with proof of identity (e.g., a signature or zero-knowledge proof). The control station then verifies this proof. In the session key update phase, the drone confirms readiness, after which the control station securely delivers an encrypted session key (e.g., via AES-GCM and key wrapping). This protocol ensures mutual authentication, secure key exchange, and protection against eavesdropping, tampering, and replay attacks.

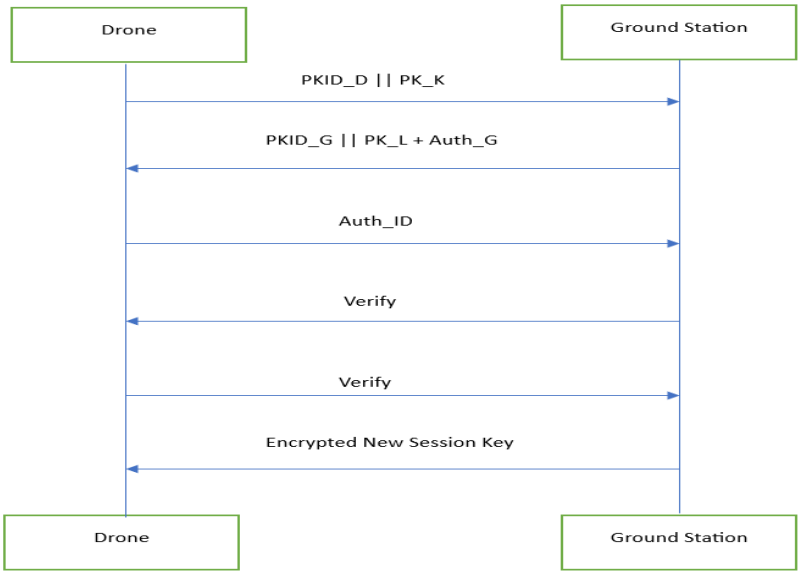

Figure 4. Authentication Phase process flow

3.4 Session Key Update Phase

The ground station transmits an encrypted message to the drone, including a session key (SK), a public key component (G_X), a proof (z), and a timestamp (tD). The drone then decrypts this message and performs three verification processes: retrieving the components through decryption, validating the timestamp to prevent replay attacks, and confirming the cryptographic proof by verifying a specific equation, $z \times B = G\_X + c \times pD$

The described communication protocol requires verification of messages using a base point B and a drone's public key pD, associated with a challenge c. Successful verification by both parties allows for the use of a derived session key (SK') for secure communication. If any verification step fails, such as incorrect decryption, an expired timestamp, or an invalid proof, the communication process is terminated to maintain the safety of the arrangement.The provided figure illustrates a secure communication protocol between an aerial node and a control station.

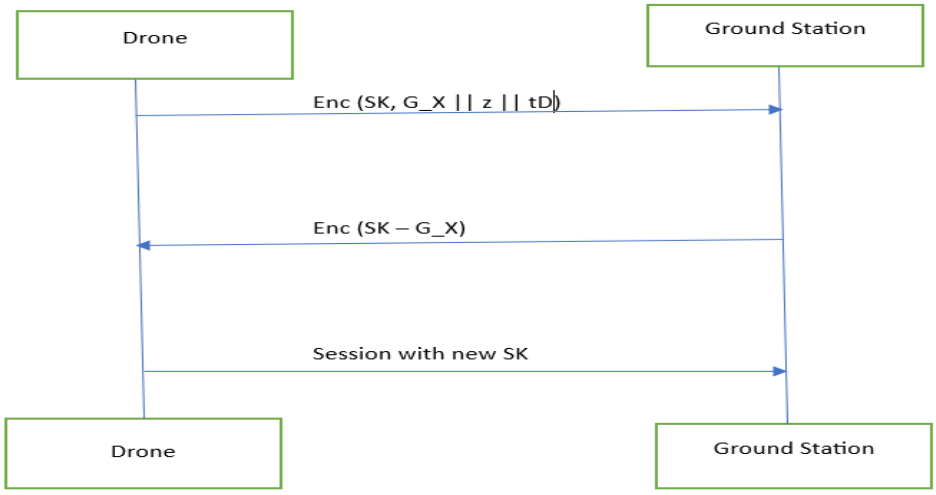

Figure 4. Updation of Session Key

4. SECURITY POSSESSIONS ANALYSIS

The LAPEC protocol incorporates five key security attributes: backward security (protecting past sessions from current key compromise), anti-replay attack (preventing message reuse), forward security (protecting future sessions from long-term key compromise), session key confidentiality (ensuring keys are not disclosed to unauthorized parties), and anti-masquerade attack (verifying participant authenticity). It also features minimized key size for user convenience. Following is the table for Security possessions of equettes.

Table 3. Security possessions of etiquettes.

Security Possessions	LAPHEC	HEDHOC
Backward Security	Yes	No
Anti-replay Attack	Yes	Yes
Forward Security	Yes	Yes
Session Key Confidentiality	Yes	Yes
Anti-masquerade attack	Yes	Yes
Key Size	Small	Big

The LAPEC protocol provides superior security compared to the HEDHOC protocol due to its supplementary backward security feature, offering a more comprehensive solution for secure communication, while HEDHOC's security remains robust for its intended applications.

5. CONCLUSION

The document presents LAPHECC, a lightweight authentication protocol for Unmanned Aerial Vehicles (UAVs) employing Hyperelliptic Curve Cryptography (HECC). Designed for resource-constrained drones, LAPHECC integrates zero-knowledge proofs (ZKHP) for a secure and efficient framework. The protocol operates in three phases: pre-registration, authentication, and session key update, culminating in a secure session establishment. By substituting Elliptic Curve Cryptography (ECC) with HECC, LAPHECC enhances security while reducing resource consumption, leading to improved battery efficiency and potential for quantum resistance. The protocol, exemplified by HEDHOC, ensures mutual authentication, session confidentiality,

integrity, key exchange, and key updates with backward secrecy, making it ideal for dynamic drone networks.

REFERENCES

[1] M. Gobi, S. Selvi, "Improving Cloud Data Security using Hyper Elliptical Curve Cryptograph and Steganography", *International Journal for Scientific Research and Development* 2017.

[2] M. Gobi, G. Kishore Kumar, "Current Trend in Cloud Computing Security & Future Research Challenges", *International Journal for Research & Development in Technology (IJRDT)* 2017.

[3] M. Gobi, S. Selvi, "Hyper elliptic curve based homomorphic encryption scheme for cloud data security" *International Conference on Intelligent Data Communication Technologies* 2019.

[4] B. Blanchet, B. Smyth, V. Cheval, M. Sylvestre, ''ProVerif2.00:Auto-matic cryptographic protocol verifier, user manual and tutorial,'' *Version*,2018, pp 5–16.

[5] L. Wu, J. Wang, K. K. R Choo, D. He, ''Secure key agreement andkey protection for mobile device user authentication,'' *IEEE Trans. Inf.Forensics Security*, vol. 14, no. 2, 2019, pp 319–330.

[6] G. Cho, J. Cho, S. Hyun, H. Kim, ''SENTINEL: A secure and efficient authentication framework for unmanned aerial vehicles,'' *Appl. Sci.*,vol. 10, no. 9, 2020, pp 3149.

[7] S. Selvi, Aggarwal, Kapil, Pandurangan, Raji, Vijayan, P. Vinodh, Ali, Anooja, K. Anuradha, "Enhancing the accuracy of target detection in remote video surveillance analytics through federated learning Optical and Quantum Electronics" *Springer US* 2023.

[8] S. Selvi, D. Mohanapriya, T. Hariharan, "Intrusion Identification Frameworks to detect attacks in Networks using Gaussian Naïve Bays", *International journal of research and analytical reviews (IJRAR)* 2023.

[9] K. Deepa, M. Gobi "Design and Analysis of an Authentication Protocol for Securing IoD using MD5", *Indian Journal of Natural Sciences vol 15, Issue 87,* 2024 pp.*85678 - 85682 Open Access ISSN: 0976 – 0997*.

[10] D. Mohanapriya, S. Selvi, S. Rekha, C. V. Banupriya, M. Gobi "Enhanced Quantifying Assessment Model for Monetary Implication and Security in Cloud Computing" 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), *IEEE* 2024.

[11] X. Xu, P. Zhu, Q.Wen, Z. Jin, H. Zhang, L. He "AsecureandefficientauthenticationandkeyagreementschemebasedonECC for telecare medicine information systems" *J. Med. Syst.*, *38*, 2014, pp 1–7.

[12] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, S. Kumari, "A robust ECC-based provable secure authentication protocol withprivacypreservingforindustrialInternetofThings" *IEEETrans.Industry.Inform.14*, 2018, pp 3599–3609.

[13] B. D. Deebak, F. Al-Turjman, " AsmartlightweightprivacypreservationschemeforIoT-basedUAVcommunicationsystems", *Comput, Commun, 162*, 2020, pp 102–117.

[14] J. Y. Sung, K. D. Ashok, P. Youngho,L Pascal, "S L A P - IoD Secureandlightweightauthenticationprotocolusingphysical unclonable functions for internet of drones in smart city environments" IEEE *Trans. Veh. Technol.71*, 2022, pp 10374–10388.

[15] G. Bansal, B. S. Sikdar, "MAPS - ScalableMutualAuthenticationProtocolforDynamicUAVSwarms"*IEEETrans.Veh.Technol* 70, 2021, pp 12088–12100.

[16] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos,Rodrigues, " J JDesignandanalysisofsecurelightweightremoteuserauthenticationandkeyagreementschemeininterneto fdronesdeployment" IEEE*InternetThingsJ.6*, 2018, pp 3572–3584.

AUTHORS

K. Deepa is a Ph.D. Research Scholar in Full-Time at PG & Research Department of Computer Science, Chikkanna Government Arts College, Tiruppur, Affiliated to Bharathiar University, Coimbatore. Her research focuses on Network Security. Shehas published papers in International Journals and presented at conferences. She is passionate about teaching.

Dr. M. Gobi serves as the Associate Professor, Chikkanna Government Arts College, Tirupur. He holds MCA., M.Phil., and Ph.D., degrees, all completed at Bharathiar University. With over 29years ofteachingexperience. He has published papers in International Journals and acted as reviewer for computer science Journals. He presented and attended many conferences. Acts as resource person in various institutions.