[1]Supriya S. Kamble

[2]Sanjay A. Pardeshi

A Lightweight Secure User Authentication Approach for Unmanned Aerial Vehicle Networks

Abstract: - The utilization of Unmanned Aerial Vehicles (UAVs) is expanding across multiple industries, here requiring strong cryptographic techniques to guarantee secure connection and data integrity. In resource-constrained situations like UAV networks, this research article provides a lightweight cryptographic framework for secure message exchange and key agreement. In order to improve security in UAV operations, this research examines modern cryptographic algorithms, with a focus on Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard with Galois/Counter Mode (AES/GCM). ECC's strong security and cheap computing cost are utilized to create shared keys for numerous parties. Then, AES-GCM encryption is performed using the derived shared key, guaranteeing the integrity and secrecy of the data. A number of factors are taken into consideration while evaluating performance, such as computing cost and communication overhead. Findings show that the proposed approach greatly cut down on communication overhead while upholding strict security guidelines, which makes them appropriate for UAV systems with limited resources. According to the results, a scalable and effective framework for safe UAV operations is offered by ECC and AES/GCM. The future research directions include exploring adaptive cryptography systems that are suited to dynamic UAV situations and integrating post-quantum cryptography techniques to address growing threats.

Keywords: Unmanned Aerial Vehicles, UAVs, ECC, AES/GCM, User Authentication

I. INTRODUCTION

The rapid advancement and deployment of UAV networks have revolutionized various sectors, including agriculture, surveillance, transportation, and disaster management. However, the unique characteristics of these networks necessitate robust authentication mechanisms for several reasons: UAV networks are vulnerable to various cyber threats, including unauthorized access and control hijacking. Effective authentication ensures that only authorized users and devices can operate or interact with UAVs, safeguarding them from malicious attacks. UAVs often collect sensitive data, such as real-time surveillance footage or environmental monitoring information. Authentication helps ensure that the data transmitted from UAVs is secure and has not been tampered with, preserving its integrity and confidentiality. In critical applications, such as search and rescue or infrastructure inspection, the authenticity of the controlling entities is vital. Robust authentication mechanisms instill trust in the system, ensuring that only verified operators can influence UAV operations, which is crucial for safety and reliability. As UAVs often operate in resource-constrained environments, particularly within the Internet of Things (IoT) ecosystems, traditional cryptographic approaches may fall short due to their computational and bandwidth demands. This research paper presents a lightweight cryptographic framework designed specifically for secure message exchange and key agreement in UAV networks, utilizing advanced techniques such as “Elliptic Curve Cryptography (ECC)” and the “Advanced Encryption Standard with Galois/Counter Mode (AES/GCM)”.

ECC has emerged as a preferred solution due to its strong security profile and lower computational requirements compared to conventional public-key cryptosystems. This makes ECC particularly suitable for environments with limited processing power, such as those encountered by UAVs. Following key generation through ECC, AES-GCM is employed for encryption, ensuring both the confidentiality and integrity of the transmitted data. The proposed framework is evaluated based on several performance metrics, including computational cost and communication overhead, demonstrating significant improvements in efficiency while maintaining stringent security standards.

Our findings suggest that the integration of ECC and AES/GCM provides a scalable and effective security solution for UAV operations in resource-constrained scenarios. Future research will explore adaptive cryptographic systems tailored for dynamic UAV environments, as well as the incorporation of post-quantum cryptographic techniques to address emerging security challenges.

[1] *Corresponding author: Supriya S. Kamble 1 Department of Technology, Shivaji University, Kolhapur, Maharashtra, India

[2] Sanjay A. Pardeshi 2 Government Residence Women Polytechnic, Tasgaon, Maharashtra, India

II. RELATED WORK

The authentication strategy aims to secure UAVs on the Internet of Drones (IoD) using ECC. It establishes safe communication channels between UAVs and IoD network entities, protecting against security risks. Operating in dynamic and often hostile environments, UAVs face unique vulnerabilities that demand specialized security solutions [1] .Saeed Ullah Jan [2] suggested a lightweight, effective authentication approach for the IoD. This method secures IoD networks while addressing the efficiency, security, and resource constraints typical IoT environments. Within the Internet of Drones (IoD) ecosystem, the authentication protocol ensures scalable, secure, and efficient authentication for military UAVs. Using aggregate signatures and identity-based cryptography, it guarantees safe communication and authentication between UAVs and other IoD network devices [3]. An anonymous and secure authentication approach created especially for Internet of Things (IoT) applications which is suitable for devices with miniature resources, provides strong security, and protects user privacy through the use of a three-factor authentication approach [4]. It would also be beneficial to evaluate the approaches resistance to novel security threats and attack approaches in real-world Internet of Things scenarios. Yeongjae Cho [5] described a novel authentication approach for IoT-enabled smart homes, integrating PUFs into protocols to ensure user security and anonymity. This plan builds on earlier studies, emphasizing the importance of PUF-based authentication to counteract the prevalent security risks in smart home environments. The authentication system aims to provide IoT environments with reliable and fast device authentication. By combining cryptographic methods with authentication protocols, it ensures the security and efficiency of IoT devices across various settings, addressing the unique challenges of the IoT ecosystem [6]. Basudeb Bera [7] authentication approach uses blockchain technology to provide an open and secure access management system for Internet of Drones (IoD) deployments that are enabled by the Internet of Things. The solution leverages the decentralized and immutable characteristics of blockchain to ensure secure and unbreakable access control for UAVs operating within the Internet of Things network. The approach would likely address the challenges of securing communications and data exchange within IoT networks, which often consist of numerous interconnected devices with limited resources. By leveraging signature-based authentication, the approach aims to make sure the authenticity and secrecy of communication between IoT devices. Additionally, the key establishment aspect of the approach would focus on securely generating and distributing cryptographic keys to enable encrypted communication channels, thus safeguarding sensitive data transmitted within the IoT ecosystem [8]. The methodology involves designing a robust system architecture, defining a threat model, and creating an authentication scheme that emphasizes user privacy and security. The scheme uses advanced cryptographic techniques to ensure anonymity and secure communication, followed by a thorough analysis of its security and performance. Prototype implementation and testing further validate the practicality of the proposed scheme in real-world Digital Twin environments [9].

TABLE I Summary of the Related Work

Approaches	**Limitations**
S. Hussain [1]	It is not considered distinct vulnerabilities and specialized security solutions.
H. Lee [4]	It is not focused on common attacks alike Replay attacks, Man-in-the-Middle attacks, or insider threats.
Y. Cho [5]	It is not considered robustness against newly discovered attack vectors and flexibility to changing security requirements in IoT contexts.
B. Bera [7]	Both computation and vulnerabile to user anonymity attacks are present.
S. Challa [8]	There is no formal security evaluation and a very high computational cost.

III. RESEARCH CONTRIBUTION

A. Proposed Approach

This research combines real-time performance assessment and sophisticated cryptography approaches to secure communications in remote situations like UAV networks. The approach is centered on symmetric encryption with "Advanced Encryption Standard with Galois/Counter Mode (AES-GCM)" and "Elliptic curve cryptography (ECC)" for key exchange. Throughput and end-to-end latency metrics are used to gauge system performance. The researcher employ a 512-bit elliptic curve for this research because it is well-known for its excellent security and computational efficiency, which satisfies the needs of environments with limited resources. Scalar multiplication of the private keys with the elliptic curve's generator point yields the public keys. Secure computation is facilitated by the generator point, which is a predetermined standard point. The shared key has been produced with help of the elliptic curve point using ECC. This is an important step because it converts the points on the elliptic curve into a symmetric key that may be used for further encryption. The communication is then secured using AES-GCM encryption.

B. Algorithm of Proposed Approach

- **Input:** Each participant inputs a rank, ID, and UAV ID, representing a simplified use case for encrypted communications.
- **Key Generation:** ECC-based key exchange generates shared keys among the participants.
- **Encryption:** The user's ID is encrypted using AES-GCM with the symmetric key derived from the ECC-based shared key.
- **Decryption:** Encrypted messages are decrypted to validate both confidentiality and integrity.
- **Performance Metrics:** The system evaluates throughput and end-to-end delay to gauge real-time processing efficiency.

C. Performance Measurement

- **Throughput Calculation:** The system measures throughput by tracking the number of messages processed per second. This is calculated as the ratio of total messages to the elapsed time, providing insights into the system's processing capability under varying loads.
- **End-to-End Delay Measurement:** It is a critical performance metric for real-time communication systems. This delay, including encryption, transmission, and decryption times, is measured using timestamps. A running average of the delays is maintained using a `deque` to simulate real-world conditions.

IV. SYSTEM PARADIGM

This section is further divides into two parts: the Network Paradigm and the Threat Paradigm.

A. Network Paradigm

As shown in Fig. 1, the network paradigm consists of three components: Server, UAVs, and users. Various UAVs are deployed in different areas based on the network model. These Unmanned Aerial Vehicles (UAVs) transmit information to the server. However, if a user (Ua) needs real-time data from a UAV in a specific area, then the server's information is not up to date. A particular deployed UAVs real-time information can be accessed by Ua [10] . However, since this communication takes place via an open channel, there is a potential for various attacks. To prevent various attacks on UAVs, only authenticated users are allowed to access specific UAV.

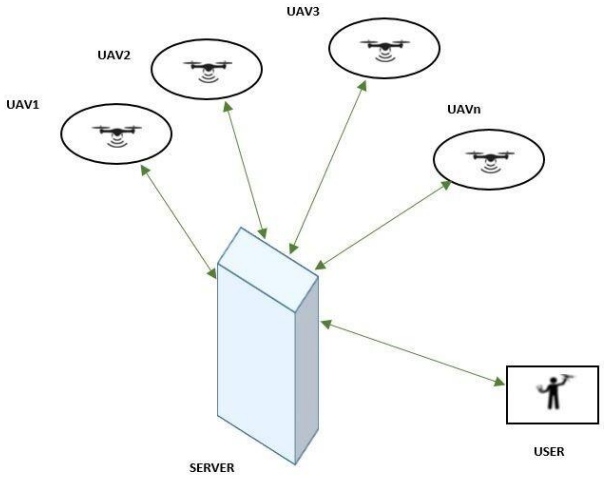

Fig. 1 System Model

TABLE II Abbreviations Used

Symbol	Description
Ua	User
S	Server
A	Opponent

B. Threat Paradigm

The proposed approach follows the widely used Dolev-Yao (DY) threat paradigm [11]. In this paradigm, any communication between two parties occurs over an open channel. Thus, an opponent (*A*) can intercept, remove or eavesdrop the information being transmitted. Furthermore, as mentioned in [12] , UAVs have the ability to function in hostile, unattended situations while gathering sensor data. They run the risk of being taken prisoner by opponent *A* as a result [13] . However, it is assumed that server S is a fully reliable entity and will not jeopardized by opponent *A* [10].

V. PERFORMANCE ANALYSIS

A. Analysis of Communication Overhead

Each private key generated using the proposed approach has is approximately 256 bits in length. ECC is employed to derive public keys from private keys, with each key exchange involving around 512 bits. Additionally, shared keys used in key exchanges consist of roughly 512 bits. The AES-GCM cipher, which typically uses a 256-bit key, defines the size of the symmetric encryption key, which is derived from the shared key. As a result, 256 bits of the symmetric encryption key are exchanged to encrypt data. In total, around 1536 bits are exchanged.

Table III and Fig. 2 compares the bits exchanged of the proposed approach with those in related approaches [1] , [7] , and [8]. The results indicate that the proposed approach incurs smaller communication overhead relative to the designs by S. Hussain [1] , B. Bera [7] , and Challa [8]. Additionally, it suggests that the proposed approach is more secure than the other approaches.

TABLE III Communication Cost Evaluation

Approaches	**S. Hussain** [1]	**B. Bera** [7]	**S. Challa** [8]	**Our**
Bits Exchanged	2208	1696	2528	1536

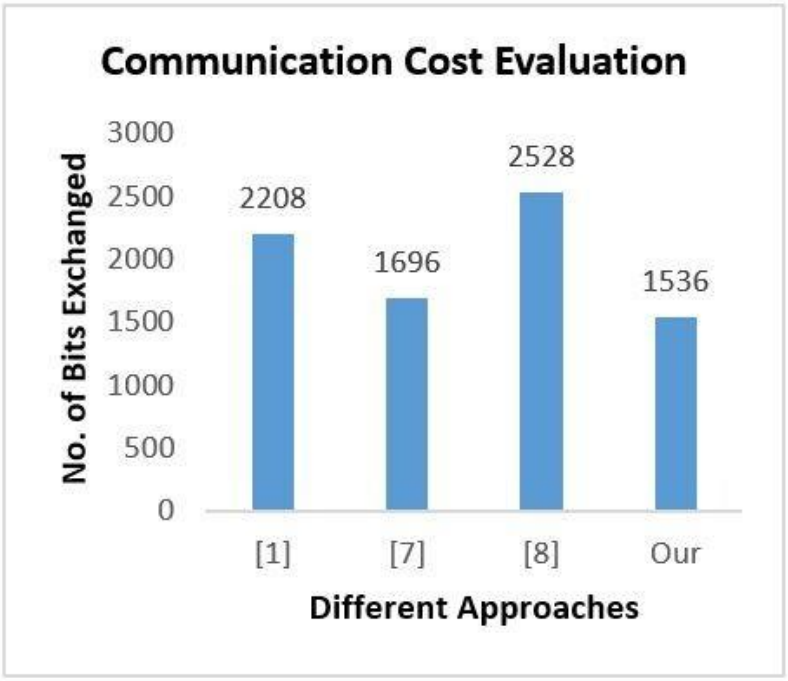

Fig. 2 Communication Cost Evaluation

VI. CONCLUSION AND FUTURE SCOPE

This research presents a lightweight cryptographic framework designed for secure communication in resource-constrained environment especially for UAV networks. With the use of AES-GCM for symmetric encryption and ECC for key exchange, the proposed framework effectively addresses the challenges of securing data transmission in UAV operations. ECC is well – suited for limited resource systems, as it allows secure key exchange with minimal computational overhead. Meanwhile, AES-GCM ensures a high level of security by maintaining the confidentiality, integrity, and authentication of transmitted data. Evaluating performance measures such as communication overhead and computation cost helps identify and mitigate potential bottlenecks. The results indicate that the proposed framework is highly suitable for UAV applications, significantly reducing communication overhead while maintaining robust security guarantees. By integrating AES-GCM and ECC, UAV operations can be secured in a scalable and efficient manner.

The future research directions include investigating adaptive cryptography systems tailored to dynamic UAV environment and incorporating post-quantum cryptography techniques to address emerging threats.

REFERENCES

[1] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones," IEEE Syst J, 2021, doi: 10.1109/JSYST.2021.3057047.

[2] 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, 2021, doi: 10.1109/ACCESS.2021.3076692.

[3] S. U. Jan and H. U. Khan, "Identity and Aggregate Signature-Based Authentication Protocol for IoD Deployment Military Drone," IEEE Access, vol. 9, pp. 130247–130263, 2021, doi: 10.1109/ACCESS.2021.3110804.

[4] H. Lee, D. Kang, J. Ryu, D. Won, H. Kim, and Y. Lee, "A three-factor anonymous user authentication scheme for Internet of Things environments," Journal of Information Security and Applications, vol. 52, Jun. 2020, doi: 10.1016/j.jisa.2020.102494.

[5] Y. Cho, J. Oh, D. Kwon, S. Son, J. Lee, and Y. Park, "A Secure and Anonymous User Authentication Scheme for IoT-Enabled Smart Home Environments Using PUF," IEEE Access, vol. 10, pp. 101330–101346, 2022, doi: 10.1109/ACCESS.2022.3208347.

[6] A. Thakare and Y. G. Kim, “Secure and efficient authentication scheme in iot environments,” Applied Sciences (Switzerland), vol. 11, no. 3, pp. 1–27, Feb. 2021, doi: 10.3390/app11031260.

[7] B. Bera, D. Chattaraj, and A. K. Das, “Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment,” Comput Commun, vol. 153, pp. 229–249, Mar. 2020, doi: 10.1016/j.comcom.2020.02.011.

[8] S. Challa, M. Wazid, A.K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, K.-Y. Yoo, “Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications,” IEEE. Translations and, vol. 2016, no. 2016, pp. 1–16, 2017, doi: 10.1109/ACCESS.2017.2676119.

[9] C. Patel, A. Pasikhani, P. Gope, and J. Clark, “User-empowered secure privacy-preserving authentication scheme for Digital Twin,” Comput Secur, vol. 140, May 2024, doi: 10.1016/j.cose.2024.103793.

[10] J. Won and E. Bertino, “A Secure Communication Protocol for Drones and Smart Objects,” in ASIA CCS’15, 2015. doi: 10.1145/2714576.2714616.

[11] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, “Examining Smart-Card Security under the Threat of Power Analysis Attacks.”

[12] W. Mohammad, D. A. Kumar, K. Neeraj, and V. A. V, “Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment,” IEEE Internet Things J, 2018, doi: 10.1109/JIOT.2018.2888821.

[13] “AVISPA, ‘Automated Validation of Internet Security Protocols and Applications,’ http://www.avispa-project.org/.”