Asia-Pacific Journal of Information Technology and Multimedia 15(1) 2026: 379 – 409
https://doi.org/10.17576/apjitm-2026-1501-24

Lightweight Authentication Protocol for Unmanned Aerial Vehicles (LA-UAV) for Future Cellular Networks

Protokol Pengesahan Ringan Untuk Kenderaan Udara Tanpa Pemandu (LA-UAV) Bagi Rangkaian Selular Masa Hadapan

*Muhammad Ali Sattar[1], Adnan Shahid Khan[1], Faizan Qamar[*2], Sajid Ullah Khan[3], Sarra Ayouni[4], Mohamed Maddeh[5], Kashif Nisar[6]*

[1]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia
[2]Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), 43600 UKM Bangi, Selangor, Malaysia
[3] Department of Information Systems, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj, Saudi Arabia
[4] Department of Information Systems, College of Computer and Information sciences Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia
[5] College of Applied Computer Science, King Saud University Riyadh, Saudi Arabia
[6] School of Arts and Sciences, The University of Notre Dame Australia, Sydney 128-140, Australia

[*]Corresponding author: faizanqamar@ukm.edu.my

Received 17 November 2025
Accepted 11 February 2026, Available online 30 June 2026

ABSTRACT

When we draw picture of future world, we would be able to perceive numerous unmanned aerial vehicles and their applications in almost each and every field or domain globally. Unmanned Aerial Vehicle (UAV) networks are highly susceptible to security threats such as forgery attacks, Adversary-in-the-middle attacks (AiTM), impersonation and replay assaults due to their limited computational capacity and complex external operating environments. They tend to operate in highly dynamic environments for execution of their role and tasks in domains including; civil applications, agriculture, media, logistics and defense etc. Ensuring identity, authentication is paramount for secure communication among drones, with the top priority being the verification of legitimate drones within the network. Traditional authentication mechanisms, such as those relying on username/password or dynamic keys, offer inadequate security levels for UAV networks. This research proposes a Lightweight Multi-factor Authentication system for UAVs (LA-UAV), designed to address the scalability, fault-tolerance, and security requirements of UAV networks. The proposed LA-UAV system minimizes computational and

communication overhead while enhancing security. The architecture's effectiveness is validated through a comprehensive analysis of various threats and attacks, demonstrating its robustness in safeguarding UAV networks. Additionally, the LA-UAV protocol enhances security through the integration of features such as time-stamping, 3D location, a one-way hash function, and the Blind-Fold Challenge scheme. To maintain the protocol's lightweight nature, an ECC-based Diffie-Hellman (ECDH) key agreement technique is employed for secure secret sharing. These lightweight characteristics also improve the scheme's reliability in multi-hop communication scenarios within 5G and beyond cellular environments. Analytical results demonstrate that LA-UAV offers superior security compared to existing mechanisms, effectively mitigating threats such as man-in-the-middle (MITM) attacks, impersonation attacks, and other common vulnerabilities.

Keywords**:** 6G, Authentication, UAVs, Drones, Lightweight Multifactor, Impersonation attack.

ABSTRAK

Apabila kita membayangkan gambaran dunia pada masa hadapan, kita dapat melihat kehadiran pelbagai kenderaan udara tanpa pemandu serta aplikasinya dalam hampir setiap bidang atau domain di seluruh dunia. Rangkaian Kenderaan Udara Tanpa Pemandu (Unmanned Aerial Vehicle, UAV) amat terdedah kepada ancaman keselamatan seperti serangan pemalsuan, serangan penyerang-di-tengah (Adversary-in-the-Middle, AiTM), penyamaran dan serangan ulangan (replay) disebabkan oleh kapasiti pengiraan yang terhad serta persekitaran operasi luaran yang kompleks. UAV lazimnya beroperasi dalam persekitaran yang sangat dinamik bagi melaksanakan peranan dan tugasan mereka dalam pelbagai domain termasuk aplikasi awam, pertanian, media, logistik dan pertahanan. Menjamin identiti dan pengesahan adalah amat penting bagi memastikan komunikasi yang selamat antara dron, dengan keutamaan utama adalah pengesahan dron yang sah dalam rangkaian. Mekanisme pengesahan tradisional, seperti yang bergantung kepada nama pengguna/kata laluan atau kunci dinamik, menawarkan tahap keselamatan yang tidak mencukupi untuk rangkaian UAV. Kajian ini mencadangkan satu sistem Pengesahan Pelbagai Faktor Ringan untuk UAV (LA-UAV) yang direka bagi menangani keperluan kebolehskalaan, toleransi ralat dan keselamatan rangkaian UAV. Sistem LA-UAV yang dicadangkan meminimumkan beban pengiraan dan komunikasi di samping meningkatkan tahap keselamatan. Keberkesanan seni bina ini disahkan melalui analisis menyeluruh terhadap pelbagai ancaman dan serangan, sekali gus menunjukkan keteguhannya dalam melindungi rangkaian UAV. Selain itu, protokol LA-UAV meningkatkan keselamatan melalui integrasi ciri-ciri seperti penandaan masa, lokasi 3D, fungsi cincang sehala, dan skim Cabaran Blind-Fold. Bagi mengekalkan sifat ringan protokol ini, teknik perjanjian kunci Diffie-Hellman berasaskan ECC (ECDH) digunakan untuk perkongsian rahsia yang selamat. Ciri-ciri ringan ini turut meningkatkan kebolehpercayaan skim tersebut dalam senario komunikasi berbilang hop dalam persekitaran selular 5G dan seterusnya. Keputusan analisis menunjukkan bahawa LA-UAV menawarkan keselamatan yang lebih unggul berbanding mekanisme sedia ada, dengan berkesan mengurangkan ancaman seperti serangan penyerang-di-tengah (MITM), serangan penyamaran, dan kelemahan umum yang lain.

Kata kunci: 6G, Pengesahan, UAV, Dron, Pelbagai Faktor Ringan, Serangan Penyamaran.

INTRODUCTION

The rapid advancement and evolution of wireless communication technologies have driven the development and introduction of fifth-generation (5G) wireless networks. The primary objectives of 5G are to address contemporary demands, including the increasing number of users, enhanced Quality of Service (QoS), the rising volume of content requests, and the growing complexity of communication processing requirements. The integration of 5G with diverse technological infrastructures, including MEC (Mobile Edge Computing), SDN (Software-Defined Networking), Software-Defined WAN/long-haul networks, Fog Computing, smart network load balancing, IoT (Internet of Things), Blockchain, enhances its capabilities in data processing, speed, capacity, and cost efficiency. (Wang et al., 2019). While fifth-generation (5G) and emerging sixth-generation (6G) cellular networks enable ultra-low latency, high reliability, and massive connectivity, their integration with Unmanned Aerial Vehicle (UAV) networks introduces critical security challenges. Unlike terrestrial user equipment, UAVs operate in open, highly dynamic environments, experience frequent handovers, and possess limited onboard computational and energy resources. These characteristics expose UAV communications to a wide range of threats, including impersonation, replay, adversary-in-the-middle, and rogue-device attacks. Existing cellular authentication mechanisms are not optimized for such conditions, motivating the need for lightweight, multi-factor authentication schemes specifically tailored for UAV and Internet of Drones (IoD) environments.

Regardless of the extensive applications, reliability, and services offered by 6G-enabled network technology, security challenges remain a critical concern. The expansive network parameters introduced by 6G, particularly those enabling advanced "artificial intelligence-driven" capabilities, present significant vulnerabilities. These include potential threats such as malicious behavior, failures in the authentication process, weaknesses in access control mechanisms, vulnerabilities in the encryption process, and issues pertaining to communication integrity. Addressing these security and privacy challenges is essential to ensure the robustness and trustworthiness of cellular networks, which are poised to handle increasingly intricate and sensitive information environments.

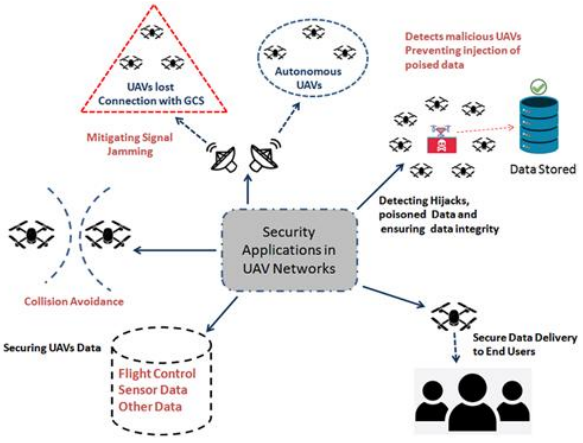

FIGURE 1. UAVs Communication & Operations Environment

Small cells enhance communication capacity for users by supporting higher data rates and offering increased bandwidth. This technology plays a crucial role in meeting the growing demands for high-speed, reliable connectivity in modern wireless communication. Furthermore, the reduced distance between users and access points

(APs), in small cell networks results in lower transmission power requirements and minimized path loss; thereby, it enhances signal quality and overall energy efficiency. However, deploying small cell systems presents several challenges. One notable issue is the high number of end-clients handled by each access point (AP), which leads to frequent handovers (Zhou et al., 2024). This can result in increased signaling overhead and potential disruptions to service continuity that tend to happen whenever an end-client transfers from one coverage-cell periphery to another cell (Yang et al., 2024). This happens because of the coverage sphere of a single cell is quite small. Consequently, this issue gives rise to inter-cell interference, which can degrade network performance and may also expose the system to malicious behavior. Additionally, it introduces security vulnerabilities, such as pollution attacks during packet encoding, which can compromise data integrity and disrupt network operations. These pertinent concerns eventually lead to issues with packet integrity, information privacy and possible data loss(Pimenta Rodrigues et al., 2024).

In recent years, drones and UAVs have gained significant acknowledgement in multiple domains as-well-as across various fields because of their unique attributes such as speed, long range reach, capabilities relating to exploration, flexibility, safety in challenging roles, tasks, and missions, and broad coverage (Huang et al., 2024) . With advancements in these domains, public demand for drones has surged, particularly for consumer-grade UAVs, as their applications continue to expand globally. UAVs are now widely employed in diverse fields, including security operations, film production, agriculture, and aerial photography. This growing adoption has fueled rapid market growth, with the UAV industry projected to expand at an annual rate of approximately 30 percent over the coming years. By the end of the next three years, the industry's market volume is expected to reach around USD 4.9 billion (Lei et al., 2021).

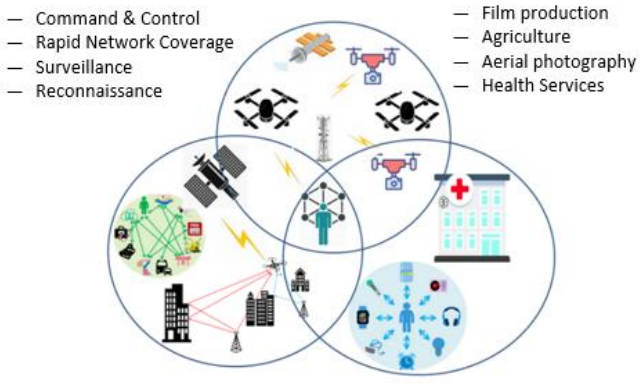

FIGURE 2. Employment of UAVs in Diverse Roles in Future Cellular Networks

The integration of UAVs into 5G and emerging 6G networks offers enhanced connectivity, ultra-low latency, and massive device support, making them ideal for real-time aerial operations and applications. These advanced networks enable seamless UAV communication, precise navigation, and efficient data transmission across diverse environments. However, the dynamic and open nature of UAV communication within 5G and 6G networks also introduces significant security challenges. The proposed lightweight authentication protocol ensures secure, fast, and resource-efficient verification of UAVs without overburdening their limited onboard processing power. This makes it highly relevant for secure UAV operations in future cellular infrastructures.

The primary contribution of this study is the design and development of a lightweight cryptographic multi-factor authentication system for a UAV based environment aimed at securing cell-free communication over open and untrusted channels (Mobini et al., 2024). This innovative crypto-system employs Elliptic Curve Cryptography (ECC) and the Diffie-Hellman protocol to ensure confidentiality, integrity, and non-repudiation. The adoption of Diffie-Hellman, with its smaller key size, not only reduces operational and communication costs but also ensures compatibility with resource-constrained devices like UAVs or IoD. Additionally, Diffie-Hellman facilitates key agreement, a critical requirement in high-mobility environments (El-Dalahmeh et al., 2024). To enhance security further, the scheme incorporates digital signatures for authentication, while a combination of one-way hashing using SHAv3 (DAVID, 2025), timestamps (Tzinas et al., 2024), 3D position data(Shuwandy et al., 2025), and a blindfold challenge mechanism enables robust security in multiple proportions, ensuring integrity, mutual authentication and message freshness.

The integration of one-way hash-function along with multi-factor authentication is crucial as it ensures data integrity, mutual authentication, and message newness (Mazor & Zhang, 2024). The embedded multi-factors for authentication in this scheme contain timestamps, the 3D location of participating UAVs or IoDs, and a challenge mechanism, collectively mitigating several major security threats in wireless communication. Furthermore, this scheme effectively reduces authentication overhead, as well as communication and computation costs, by leveraging a merged challenge-response mechanism, thereby enhancing the overall efficiency and security of the system. The lightweight nature particularly caters to the inherent limitations of UAV devices. The significance of this work is also provided in the following sub-sections.

MOTIVATION

As 5G technology approaches full commercial deployment, the integration of UAV- or drone-based systems into the envisioned 6G communication framework is emerging as a critical focus of contemporary research efforts in the field. Several studies highlight key applications and services of UAV systems within the context of 6G, including large-scale connected autonomous systems and many more applications. These applications often operate in combination under the broader umbrella of 5G-6G enabled UAV communication systems. Notably, they demand exceptionally high data rates, a high level of reliability and the lowest possible latency, with the type of sensitive data being collected becoming increasingly critical (Yu et al., 2024). In the case of UAVs, the communication environment is highly dynamic due to the mobility of such elements in the air, along with their inherent limitations such as onboard processing power and battery capacity. The present cellular network, there is only only a single base station that can serve multiple UEs (IoTs, IoDs, etc.). The existing 5G security mechanisms are not well-suited for such network environments, primarily due to unstable signal gain and high user mobility. Implementing 5G authentication mechanisms in this context could result in a significant increase in security vulnerabilities, as well as higher authentication, communication, and computational costs. Moreover, it has been demonstrated that the authentication phase requires a substantial amount of computational resources, which can lead to significant system strain and reduced network efficiency. This could increase the likelihood of attackers exploiting vulnerabilities, potentially compromising the authentication process and disrupting network security.

To tackle the challenges mentioned, a Lightweight Multifactor Authentication framework is proposed for Cell-Free networks within ultra-dense small cell-based 5G and beyond cellular

networks. This solution is designed to improve security while reducing computational and communication burdens in future communication environments. The proposed scheme utilizes an ECC-based Diffie-Hellman cryptosystem to mitigate the aforementioned communication attacks, while also reducing communication costs, authentication overhead, and computational expenses. The key challenges are associated with integrating future cellular networks and IoT or IoD (Internet of drones) technologies to achieve advanced solutions. The aim is to address the limitations present in both IoD and authentication protocols. In the latest authentication protocols applied to IoD, there is a notable oversight in accounting for computational loads, delays, and bandwidth overhead. This deficiency has given rise to a new set of challenges.

RELATED WORKS

UAVs offer unprecedented applications, particularly in situations where human lives might otherwise be endangered. SDN offers a viable approach to achieving flexible deployment and efficient management of future applications. SDN facilitates centralized management by decoupling the control plane from the data plane, dynamic network adaptability and improved scalability, making it an ideal solution for handling the complexities of next-generation network architectures and applications (Li et al., 2024). Additionally, this technology has the potential to enhance network availability and security while also contributing to cost reduction (Shaikh et al., 2022). Furthermore, the fundamental characteristics of UAV networks, such as flexibility and extended reach, exceed the capabilities of traditional MANETs and VANETs. Future applications of UAV networks will require protocols specifically designed to address challenges such as high mobility, intermittent connectivity, power limitations, dynamic topology and link quality that are fluctuating (Gaydamaka et al., 2023). Drones or unmanned aerial vehicles can be deployed for various profiles and missions based on their size. UAVs with relatively small sizes are often employed in swarms for joint missions and collaborative tasks, while larger UAVs are typically employed in solo missions. UAV networks serve a wide range of roles and applications, offering significant potential across a wide range of civilian applications. In the study (Perz, 2024), it is stated that drones are poised to become invaluable assets in the operations of organizations with roles and tasks pertaining to security domain, including fire brigades and police departments. Furthermore, advancements in sensor and electronics technologies are expanding the potential applications of UAV networks, enabling broader and more sophisticated use cases (Mohsan et al., 2023). This expansion is expected to encompass roles such as traffic surveillance, damage assessment, reconnaissance and remote sensing, and various other surveillance tasks. A key application of drones in a network is their role as sky-based base stations for extending communication, providing reliable coverage over considerable areas (Rahim & Peng, 2023) . UAV networks have the potential to function as infrastructure-based systems, supporting applications that are distinct from those typically associated with VANET and MANET networks. In such cases, drones will communicate and exchange data with each other while simultaneously communicating with a designated control center(Tychola et al., 2024) .

In scenarios in which drones offer network coverage over relatively large areas and remain in a hovering state, the probability of disruptions is minimal (Ali et al., 2024). However, intermittency is more likely in roles or applications that necessitate high mobility of UAVs (Banafaa et al., 2024). Delays in data transmission often result from low network quality or interruptions in the communication path. Such delays can also occur when UAV nodes temporarily store data as a result of the absence of a continuous end-to-end connection. These factors collectively contribute to the overall performance and reliability of UAV networks. A prominent example of a mobile IoT system (Yu et al., 2022)is the Internet of Drones (IoD),

which extends IoT capabilities to aerial platforms, enabling efficient data collection and interaction with physical surroundings (Ashraf et al., 2023; Srivastava & Prakash, 2023).

Unmanned aerial vehicles (UAVs) have made significant advancements within the Internet of Things (IoT) ecosystem, presenting promising applications for future generations. However, a critical challenge that demands urgent attention is guaranteeing the security of communication in the IoD environment. For instance, in 2016, Mexican drug traffickers exploited navigation satellite signal spoofing to disrupt border patrol drones during an unlawful border breach. Similarly, in July 2016, IBM security expert Nils Rodday highlighted that drones lacking encryption are highly susceptible to hijacking, a concern he emphasized during a Security Summit in Asia. Further underscoring this issue, the Iranian military successfully hijacked a U.S (Jaffe). MQ-9 UAV in 2019, resulting in significant data loss. These incidents underscore the urgent need for robust communication security measures to safeguard UAVs in roles such as patrolling and surveillance (Laghari et al., 2024).

Although the inadequate computational power and limited capacity of drone systems makes conventional security-designs unworkable, necessitating the development of lightweight, specialized approaches for these systems (Laghari et al., 2024) . A novel remote-node authentication & key-management system is suggested by (Wang et al., 2024). This scheme, known as AKAEC, is an authentication and key agreement (AKA) protocol that utilizes a three-factor approach—smart card, biometrics, and password—along with a physically-unclonable-function (PUF) to protect UAV-assisted emergency communications. Specifically, AKAEC comprises two components: ECV-to-UAV(E2U) and UAV-to-UAV(U2U). The former ensures secure communication between Emergency Communication Vehicles (ECVs) and drones, while the latter secures communication between UAVs. The provision of formal security proof is within the Real-Or-Random (ROR) model, and the system undergoes formal security verification using AVISPA. In the stated research paper, a security-improved AKAEC is based on three factors (biometrics, password, and smart card) and PUF, to prevent rescue message deletion, tampering, forgery, eavesdropping, and privacy parameter leakage. More, AKAEC supports challenge-response pair update in E2U (Emergency Comm Vehicle-To-UAV) and U2U (UAV-To-UAV) to resist physical attacks (Hemmati & Zarei, 2024). Additionally, password and biometric update are utilized to enhance practicability. Finally, smart card revocation and biometrics extraction are respectively applied to protect against loss of smart cards and biometric data leakage (Kim, 2024). Algarni introduces a lightweight security mechanism aimed at enhancing the authentication of participants in the Internet of Devices (IoD) using a biometric-based approach. This mechanism employs the MD5 algorithm and a fuzzy extractor to ensure secure communication and has been validated using rigorous tools such as ProVerif and the Random-Oracle Model (ROM). It effectively balances security and performance, maintaining key secrecy, reachability, and confidentiality while keeping communication and computation costs low. Similarly, Unmanned aerial vehicles (UAVs) have introduced new challenges to security, particularly in authenticating communication and preventing sensitive information from being intercepted (Yusop et al., 2025). A commonly used method for authentication is ECC, valued for its strong security and efficiency. However, limitations in ECC, such as inflexibility and lack of backward security, have prompted the development of improved protocols. One notable advancement is the Lightweight Authentication Protocol over Elliptic Curve (LAPEC), which addresses these limitations(Zhang et al., 2023). LAPEC is a novel authentication protocol designed to overcome challenges in the existing EDHOC (Ephemeral Diffie–Hellman over COSE) protocol, including the absence of pre-registration and the inability to secure past session keys (backward security). By ensuring backward security and enhancing flexibility, LAPEC offers robust security for UAVs without significantly increasing computational demands.

Existing UAV authentication schemes demonstrate strong security properties but often incur high computational or communication overhead due to reliance on heavyweight cryptographic operations, multi-round exchanges, or additional hardware such as smart cards and PUFs. While ECC-based approaches improve efficiency, many lack comprehensive multi-factor validation or scalability in highly dynamic UAV environments. In contrast, the proposed LA-UAV protocol integrates lightweight cryptographic primitives with contextual authentication factors—such as time and 3D location—achieving stronger security guarantees with reduced overhead, particularly in multi-hop and dense UAV deployments.

TABLE 1. Analysis of Related Works

Feature	**LA-UAV (Proposed)**	**Wang et al.**	**Zhang et al. (LAPEC)**	**Algarni et al.**
Cryptographic Basis	ECC + ECDH	ECC + PUF	ECC-based	Hash + Biometrics
Authentication Factors	Timestamp, 3D Location, Challenge	Password, Biometrics, PUF	Key-based	Biometrics
Forward Secrecy	✔ Yes	✘ Partial	✔ Yes	✘ No
Multi-Hop Support	✔ Yes	✘ Limited	✘ No	✘ No
Rogue Node Detection	✔ Yes	✘ No	✘ No	✘ No
Computational Complexity	(O(n))	(O(n^2))	(O(n))	(O(n))
Suitability for UAVs	High	Medium	Medium	Low

SYSTEM DESIGN

The proposed LA-UAV authentication framework follows a hierarchical yet lightweight architecture designed to support highly dynamic UAV environments. As illustrated in Figures 3 and 4, the system comprises three primary entities: User Equipment (UE), Cluster Heads (CLHs), and a Global Head (GH). UAVs act as UEs and are organized into clusters based on proximity and mobility patterns. Each cluster is managed by a CLH, which serves as a localized authentication gateway, while the GH functions as a trusted authority responsible for global verification and authorization. Authentication is performed in a multi-layer manner. First, the UE undergoes local verification with its respective CLH, followed by inter-cluster and global validation through the GH. This layered approach distributes authentication workload, reduces signaling overhead, and enhances scalability. The architecture integrates multi-factor authentication using timestamps, 3D positional information, challenge–response mechanisms, and cryptographic primitives to ensure mutual authentication, message freshness, and resistance to impersonation and replay attacks. By combining hierarchical trust with lightweight cryptographic operations, the LA-UAV architecture achieves a balance between strong security guarantees and resource efficiency.

PROTOCOL MODEL

In Figure 3, we propose a Lightweight Multi-Factor Authentication system for UAVs, named (LA-UAV), for the future UAV network that reduces computational and communication overhead. In this model, we showcase the effectiveness of our proposed scheme in ensuring security by evaluating various threats and attacks. The proposed LA-UAV scheme consists of two layers of security measures which is Multifactor

Authentication (MFA) Layer and Security Layers shown in the figure below. The authentication component of both layers is also explained in subsequent paragraphs.

The proposed scheme provides an amalgamation of MFA and ECC-based Diffie-Hellman to achieve a lightweight authentication scheme (Couteau et al., 2025), especially in scenarios where security, efficiency, and decentralization are essential. ECDH will be used for secure key exchange between two parties. Each party generates a public-private key pair based on elliptic curve cryptography. They then exchange their public keys securely, typically through an authenticated channel. When two parties need to authenticate each other, they can perform an ECDH key exchange to establish a shared secret key. Once the shared secret key is derived, it will be used to encrypt and decrypt authentication messages securely(Koppl et al., 2021). In the context of unmanned aerial vehicles (UAVs) organized into clusters (Figure 4), a security enhancement strategy named Lightweight Multi-Factor Authentication (LMA) has been proposed. This approach aims to fortify the security framework surrounding UAV clusters. In this setup, clusters are overseen by designated Cluster Heads (CLHs), with all CLHs interconnected via a central entity known as the Global Head (GH). When an individual UAV within a cluster initiates an authentication procedure, it communicates with its respective CLH. Acting as a localized authentication gateway, the CLH conducts a meticulous verification process as per the proposed design, leveraging the resources of the Global Head for additional security layers. Through this Multi-Factor Authentication (MFA) system, each UAV undergoes a comprehensive authentication phase, significantly bolstering the security posture of UAV clusters. The lightweight design of this solution is specifically tailored to minimize computational burdens and communication delays, thus enabling swift and secure authentication within the dynamic and resource-constrained environment inherent to the UAV domain. The proposed LA-UAV protocol employs an ECDH key exchange mechanism, in which both communicating entities generate fresh temporary key pairs for each authentication session. This approach ensures forward secrecy by preventing the disclosure of past session keys even if long-term credentials are compromised. As a result, the protocol provides stronger resistance against key compromise and related cryptographic attacks in dynamic UAV network environments.

The LA-UAV protocol verifies the 3D location of a UAV by computing the Euclidean distance between the reported position and the expected reference coordinates. Authentication is considered valid only if this distance lies within a predefined meter-level tolerance threshold, which accounts for GPS and sensor inaccuracies. This location-validation mechanism enhances security by effectively mitigating location spoofing and replay attacks.

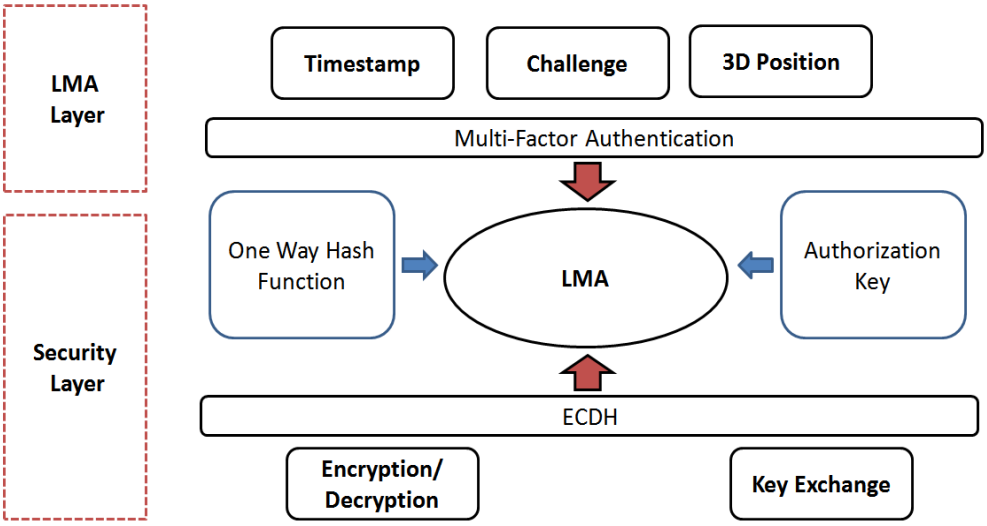

FIGURE 3. LA-UAV Model

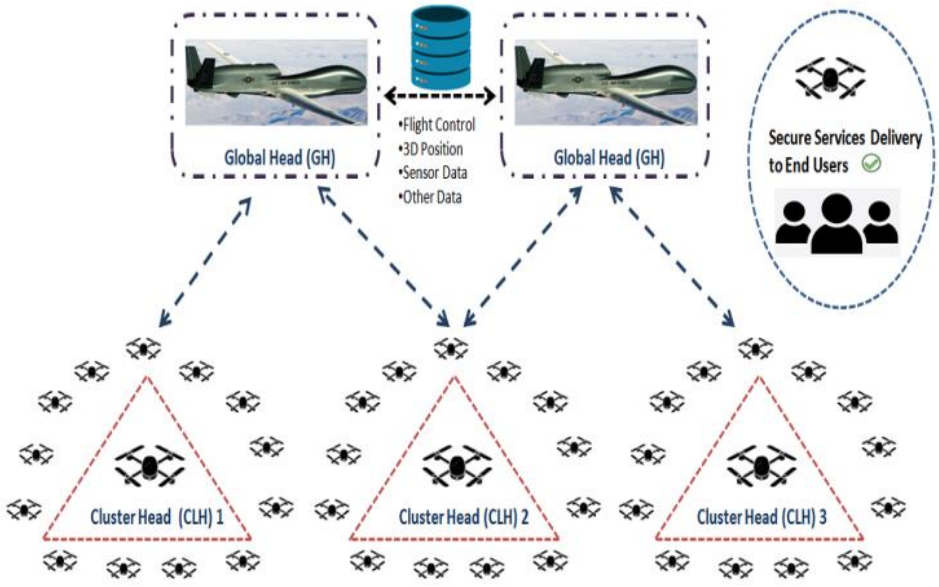

FIGURE 4. LA-UAV Implementation

The proposed algorithm of LA-UAV mechanisms is explained in detail as follows.

DEVELOPMENT OF LA-UAV SYSTEM

In this framework, the LA-UAV protocol scheme is described, demonstrating that the communication process ensures secure mutual authentication. In this protocol, User Equipment (UE) represents UAVs seeking to communicate via a Cluster Head (CLH). The CLH serves as a relay agent, forwarding requests and responses between devices. A challenge value, denoted as Ch, is incorporated into each message to validate the communicating device. A cryptographic hash function, represented as H, is employed in all request and response messages for security. Devices utilize an Authorization Key (AK) to

gain authorization, and a Pseudo Identity (PID) is used to obfuscate the real identity of devices during communication. The combination of the PID with a 3D location is represented as PID||3D to enhance privacy. In this framework, a public key Kn is utilized to encrypt messages intended for the receiver, while a private key Kn is employed to digitally sign outgoing messages. The communication process begins with the UE sending a communication request to the CLH. The CLH sends an Auth-Req message to the Global Head (GH) to authenticate both the CLH and the GH. Upon receiving the request, the CLH validates its legitimacy with the GH and responds to the UE with an Auth-Res message.

The detailed pseudo-code corresponding to each communication step is outlined in the subsequent sections. Algorithm 1.1 illustrates a sample request message from the UE. The message intended for authentication and services from the Global Head (GH) is first sent to the Cluster Head (CLH). This message includes the pseudo-identity (PID) of the sender, a timestamp, a challenge value, and a hash of the timestamp. The hash value is securely signed using the private key of the User Equipment (UE) to ensure message integrity and authenticity. Finally, the entire message is encrypted with the public key of the CLH, ensuring confidentiality during transmission.

Figure-5 shows the timing diagram represents the complete message flow of during the authentication process between UE, CLHs and GH. The detail explanation of the messages is reflected in Figure-5. In the proposed LA-UAV protocol, message integrity and authenticity are ensured by computing a cryptographic hash of the message and signing it with the sender's private key. Under the assumed public-key trust model, this hash-based digital signature provides security guarantees equivalent to a message authentication code (MAC), as only a legitimate entity possessing the private key can generate a valid signature. This approach eliminates the need for additional symmetric-key management, thereby maintaining the lightweight design of the protocol while effectively protecting against message modification and impersonation attacks.

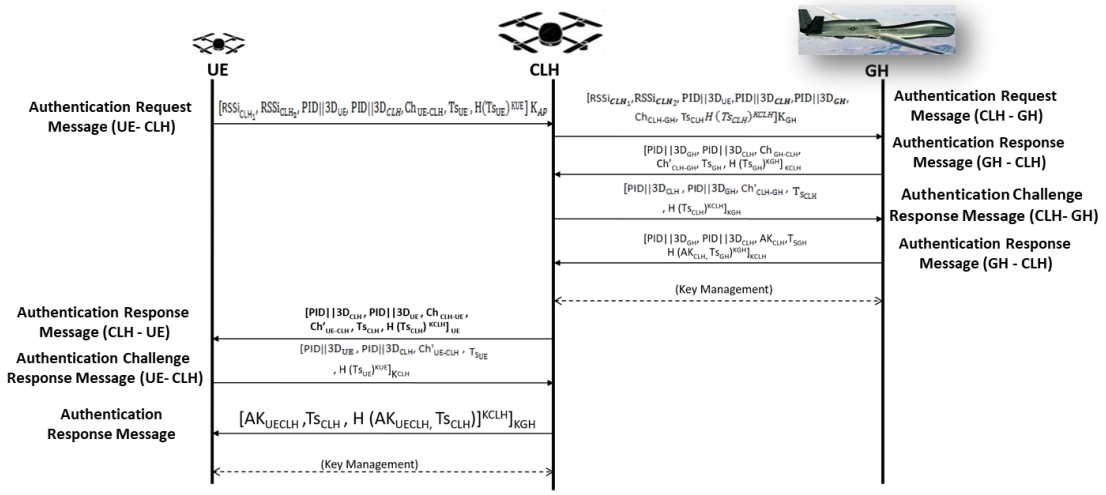

FIGURE 5. The proposed LA-UAV protocol messages timing diagram

To ensure clarity and consistency, the primary notations used in the LA-UAV protocol are defined as follows. Let **PID** denote a pseudo-identity assigned to a UAV to conceal its real identity during communication. The notation **PID||3D** represents the concatenation of the

pseudo-identity with the UAV's three-dimensional location coordinates. The 3D location is expressed as an ordered tuple *(x, y, z)* corresponding to latitude, longitude, and altitude, respectively. Each coordinate is quantized and represented using fixed-length binary encoding, resulting in a compact representation suitable for lightweight authentication.

Timestamps (**Ts**) are used to ensure message freshness and prevent replay attacks. Hash values (**H(·)**) are generated using a secure one-way hash function. Public and private keys are denoted as $\mathbf{K_n}$ and $\mathbf{K_n}$, respectively, while **AK** represents an authorization key issued upon successful mutual authentication. Challenge values (**Ch**) and their corresponding solutions (**Ch′**) are used to validate liveness and legitimacy of communicating entities.

Algorithm-1.1 –Authentication-Request-Message UE-CLH

Step-1:-Obtain participant IDs via neighbour-discovery
Step-2:-Obtain Public-key of
CLH=K_{CLH} ;GH=K_{GH} ;UAV= K_{UE}
Step-3:- Obtain Private-key of UE=K^{UE}
Step-4:-Create a challenge using the Blind-Fold-Challenge scheme for
$Ch_{UE\text{-}CLH}$
Step-5:-Resolve the challenge for
$Ch_{UE\text{-}CLH} = Ch_{UE\text{-}CLH}'$
Step-6:-Creat timestamps and location T_{SUE}
Step-7:- Compute
$RSSi_{CLH_1}, PID||3D_{UE},, PID||3D_{CLH}, Ch_{UE-CLH}, Ts_{UE}$= M
Hash of timestamps = H(Ts_{UE})
Step-8:- Encrypt (UE-CLH)//Encryption for CLH
$[H\ (Ts_{UE})]^{KUE}$
$[M, H\ (Ts_{UE})]^{KUE}]_{KCLH}$
Step-9:- AUTH-REQ: [Encrypt (UE-CLH)]
Step-10:-Transmit AUTH-REQ to CLH

In Algorithm 1.2, the request message received by the Cluster Head (CLH) is decrypted using its corresponding public key. The CLH validates the integrity and freshness of the message by comparing it with its computed hash value. If the hash value matches the received message, the message is deemed valid and fresh; otherwise, it is discarded. Upon successful validation, the CLH initiates the next step by sending an authentication request message to the Global Head (GH).

Algorithm-1.2- Authentication-Request-Message CLH-GH

Step-1:-Obtain participant's IDs via neighbour-discovery
Step-2:-Obtain Public-key of
CLH=K_{CLH} ;GH=K_{GH} ; UE= K_{UE}
Step-3:-Obtain Private-key of CLH=K^{CLH}
Step-4:-Create challenge utilizing Blind-fold-challenge scheme for
$Ch_{CLH\text{-}GH}$
Step-5:-Resolve challenge for
$Ch_{CLH\text{-}GH} = Ch_{CLH\text{-}GH}$'
Step-6:-Creat time-stamps Ts_{CLH}
Step-7:-Compute
$RSSi_{\mathrm{CLH}_1}, PID||3D_{UE}, PID||3D_{\mathrm{CLH}}, PID||3D_{\mathrm{GH}}, Ch_{CLH-GH}, Ts_{CLH}$= M
Hash of timestamps = H(Ts_{CLH})
Step8: Encrypt (CLH-GH)//Encryption for GH
[H (Ts_{CLH})]^{KCLH}
[M, [H (Ts_{CLH})]^{KCLH}]$_{KGH}$
Step-9:-AUTH-REQ: [Encrypt (CLH-GH)]
Step-10:-Transmit AUTH REQ to GH

In Algorithm 1.3, the Global Head (GH) receives an encrypted request message from the Cluster Head (CLH). The GH decrypts the message using its private key and verifies its validity by comparing the actual timestamp with the hash of the timestamp. If the values match, the message is deemed valid and fresh; otherwise, it is discarded. To confirm the legitimacy of the CLH, the GH responds by generating a new challenge. The response message includes the pseudo-ID, challenge, timestamp, and the solution to the challenge. This message is encrypted using the GH's private key and the CLH's public key before being sent back to the CLH.

Algorithm-1.3–Authentication Challenge-Response-Message at GH

Decryption:
Step-1:-Obtain Public-key of
AP=K_{CLH} ;GH=$K_{GH;}$ UE= K_{UE}
Step-2:-Obtain Private-key of GH =K^{GH}
Step-3:-Obtain AUTH-REQ (CLH- GH):
[Encrypt(CLH- GH)] = [M, [H (Ts_{CLH})]^{KCLH}]$_{KGH}$
Step-4:-Compute utilizing private-key of GH (K^{GH})
M, [H(Ts_{CLH})]^{KCLH}
Step 5: Compute using public key of CLH (K_{CLH})
M, H (Ts_{CLH})
Step 6: Compute H(Ts_{CLH}) & Compare with Ts_{CLH}
Proceed if the condition is satisfied (i.e., both values match); otherwise, discard the message.
Encryption:-
Step-1:-Create challenge utilizing Blind-fold-challenge scheme for
$Ch_{GH\text{-}CLH}$
Step-2:-Solve the Challenge for
$CH_{GH\text{-}CLH} = CH_{GH\text{-}CLH}$'
Step-3:-Create time-stamps Ts_{GH}
Step -4:-Compute

$PID||3D_{GH}$, $PID||3D_{CLH}$, $Ch_{GH\text{-}CLH}$, $Ch'_{CLH\text{-}GH}$, Ts_{GH}= M
Hash value of Ts_{GH}= H (Ts_{GH})
Step-5:-Encrypt (GH-CLH)
$[H\ (Ts_{GH})]^{KGH}$
$[M, [H\ (Ts_{GH})]^{KGH}]_{KCLH}$
Step-6:-AUTH-CHALLENGE-REQ:[Encrypt(GH-CLH)]
Step-7:-Send AUTH-CHALLENGE-REQ to CLH

In Algorithm 1.4, the CLH receives a response message from the GH to address the challenge previously given. CLH first decrypts the message with its private key, solves the challenge, checks the timestamp, and matches it with hashed timestamp. If the timestamp and its hash are the same, it considers the message valid and fresh, confirming that there is no replay attack. CLH sends the challenge response to the GH along with the hash value of timestamp. CLH encrypts the message with its private key and the public key of the GH.

Algorithm-1.4 –Auth-Challenge-ResponseMessage at CLH

Decryption:-
Step-1:-Obtain AUTH-CHALLENGE-REQ
$[Encrypt(GH\text{-}CLH)] = [M, [H\ (Ts_{GH})]^{KGH}]_{KCLH}$
Step-2:- Compute utilizing private-key of CLH (K_{CLH})
$M, [H\ (Ts_{GH})]^{KGH}$
Step-3:-Compute utilizing public-key of GH
$M, H\ (Ts_{GH})$
Step-4-Compute $H(Ts_{GH})$ and Compare with Ts_{GH}
Proceed if the condition is satisfied (i.e., both values match); otherwise, discard the message
Encryption:-
Step-5-Create challenge utilizing Blind-fold-challenge scheme for
$Ch_{CLH\text{-}GH}$
Step6: Solve the Challenge for
$Ch_{CLH\text{-}GH} = Ch'_{CLH\text{-}GH}$
Step7: Generate timestamps Ts_{CLH}
Step8: Compute
$PID||3D_{CLH}, PID||3D_{GH}, Ch'_{CLH-GH}, T_{S_{CLH}}$= X
Hash value of Ts_{CLH}= H(Ts_{CLH})
Step 9: Encrypt (CLH-GH)
$[H\ (Ts_{CLH})]^{KCLH}$
$[M, [H\ (Ts_{CLH})]^{KCLH}]_{KGH}$
Step-10:-Authentication Challenge Resp: [Encrypt (CLH-GH)]
Step-11:-Transmit AUTH-CHALLENGE-RESP to GH

In Algorithm-1.5, the response-message from the Cluster Head (CLH) is received by the Global Head (GH). The GH decrypts the entire message using its private key. Subsequently, the GH decrypts the timestamp using the public key of the CLH. The GH then verifies the challenge solution and compares the hashed timestamp with the actual timestamp. If both values match, the process continues; otherwise, the message is discarded. Following successful decryption, the GH generates an authorization key to finalize mutual

authentication with the CLH. The authorization key, along with the timestamp, is then hashed, signed with the GH's private key, and sent back to the CLH.

Algorithm-1.5:-Auth-Response-Message at GH

Decryption:
Step-1:-Obtain AUTH-CHALLENGE RESP
[Encrypt (CLH-GH)] = [M, [H (Ts_{CLH})]^{KCLH}]$_{KGH}$
Step-2:-Compute using private key of GH (K_{GH})
M, [H (Ts_{CLH})]^{KCLH}
Step-3:-Solve utilizing public-key of CLH
M, H (Ts_{CLH})
Step-4:-Solve H(Ts_{CLH}) andcarry out comparison with Ts_{CLH}
Proceed if the condition is satisfied (i.e., both values match); otherwise, discard the message
Encryption:
Step-5:-Generate Authorization Key for CLH
AK_{CLH}
Step 6: Generate timestamps Ts_{GH}
Step 7: Compute
PID||$3D_{GH}$, PID||$3D_{CLH}$, AK_{CLH},T_{SGH} = M
Hash value of AK_{CLH} and Ts_{GH}= H ($AK_{CLH,}$ Ts_{GH})
Step 8: Encrypt (GH-CLH)
[H ($AK_{CLH,}$ Ts_{GH})]^{KGH}
[M, H ($AK_{CLH,}$ Ts_{GH})]^{KGH}]$_{KCLH}$
Step 9: AUTH-RES: [Encrypt (GH-CLH)]
Step 10: Send AUTH-RES (GH- CLH) to CLH

In Algorithm-1.6, the Cluster Head (CLH) decrypts the message received from the Global Head (GH) using its private key, extracts the authorization key, and checks the timestamp. The CLH then compares this timestamp with the hash of the message, which is encrypted using the private key of the GH. To verify the integrity of the message, the CLH decrypts it using the public key of the GH. If both the decrypted message and the hash match, the message is considered valid, and the system confirms that no replay attack has occurred. Following this validation, the CLH is mutually authenticated with the GH. It then proceeds with the authentication process for the User Equipment (UE), addresses the challenge provided, and sends a new challenge for the UE to resolve.

In Algorithm 1.7, the User Equipment (UE) decrypts the message received from the Cluster Head (CLH) using its private key, solves the challenge, and checks the timestamp. The UE then compares this timestamp with the hash of the timestamp, which has been encrypted with the private key of the CLH. To verify the integrity of the message, the UE decrypts it using the public key of the CLH. If the decrypted timestamp matches the hashed timestamp, the UE considers the message valid and confirms that no replay attack has occurred. Subsequently, the UE responds with the solution to the challenge provided by the CLH, enabling the CLH to generate an authorization key that grants the UE access to services from both the CLH and the Global Head (GH).

Algorithm-1.6–Auth-Challenge-Response Message at CLH

Decryption:-
Step-1:-Obtain Public-key of AP=K_{CLH} ;GH=$K_{GH;}$ UE= K_{UE}
Step-2:-Obtain Private-key of CLH =K_{CLH}
Step-3:-Obtain AUTH-RES (GH-CLH):
[Encrypt-(GH-CLH)]= [M, H ($AK_{CLH,}$ Ts_{GH})]^{KGH}]$_{KCLH}$
Step-4:-Solve utilizing CLH's private-key
M, [H($AK_{CLH,}Ts_{GH}$)]^{KGH}
Step-5:-Solve utilizing GH's public-key
M, H ($AK_{CLH,}Ts_{GH}$)
Step-6:-Solve H($AK_{CLH,}Ts_{CLH}$) and Compare with AK_{CLH}&Ts_{CLH} Proceed if the condition is satisfied (i.e., both values match); otherwise, discard the message
Encryption:-
Step-1:-Create challenge utilizing Blind-fold-challenge scheme for
Ch_{CLH-UE}
Step-2:-Solve the Challenge for
Ch_{CLH-UE} = Ch_{CLH-UE}'
Step-3:- Generate time-stamps Ts_{CLH}
Step-4:-Compute
PID||3D_{CLH}, PID||3D_{UE}, Ch_{CLH-UE}, Ch'$_{UE-CLH}$, Ts_{CLH}= M
Hash value of Ts_{CLH}= H (Ts_{CLH})
Encryption for UE:
Step-5:-Encrypt (CLH-UE)
[H (Ts_{CLH})]^{KCLH}
[M, [H (Ts_{CLH})]^{KCLH}]$_{KUE}$
Step-6:-AUTH-CHALLENGE-RES: [Encrypt (CLH-UE)]
Step-7:-Transmit AUTH-CHALLENGE-REStoto UE

Algorithm 1.7 – Authentication Challenge Response Message at UE
Decryption:
Step-1:-Get AUTH CHALLENGE RES
Encrypt(CLH-UE) = [M, [H (Ts_{CLH})]^{KCLH}]$_{KUE}$
Step-2:-Solveutilizing private-key of UE
M, [H (Ts_{CLH})]^{KCLH}
Step 3: Solve utilizing public-key of CLH
M, H (Ts_{CLH})
Step-4:-Compute H(Ts_{CLH}) and Compare with Ts_{CLH}

Proceed if the condition is satisfied (i.e., both values match); otherwise, discard the message

Encryption
Step5: Generate challenge using Blind fold challenge scheme for
Ch_{UE-CLH}
Step6: Solve the Challenge for
Ch_{UE-CLH} = Ch'$_{UE-CLH}$
Step7: Generate timestamps Ts_{UE}

Step 8: Compute
$PID||3D_{UE}, PID||3D_{CLH}, Ch'_{CLH-UE}, T_{S_{UE}}$ = M
Hash value of Ts_{UE}= H(Ts_{UE})
Step 9: Encrypt (UE-CLH)
$[H\ (Ts_{UE})]^{KUE}$
$[M, [H\ (Ts_{UE})]^{KUE}]_{KCLH}$
Step-10:- AUTHENTICATION CHA RES: [Encrypt (UE-CLH)]
Step-11:- Transmit AUTHENTICATION CHA RES to CLH

In Algorithm-1.8, the response message from the User Equipment (UE) is received by the Cluster Head (CLH). The CLH decrypts the entire message using its private key and subsequently verifies the timestamp by decrypting it with the public key of the UE. The CLH then verifies the challenge solution and compares the hashed timestamp with the actual timestamp. If both values match, the process continues; otherwise, the message is discarded. After successful decryption, the CLH generates an authorization key to complete mutual authentication with the UE. The authorization key, along with the timestamp, is hashed, signed with the CLH's private key, and sent to the UE.

Algorithm-1.8– Auth-Resp-Message at CLH

Decryption:
Step-1:-Obtain AUTH-CHA-RES
$[Encrypt(CLH\text{-}UE)] = [M, [H\ (Ts_{UE})]^{KUE}]_{KCLH}$
Step-2:-Solve utilizing private-key of CLH
$M, [H\ (Ts_{UE})]^{KUE}$
Step-3:-Compute utilizing public-key of UE
$M, H\ (Ts_{UE})$
Step-4:-Compute $H(Ts_{UE})$ and Compare with Ts_{UE}
Proceed if the condition is satisfied (i.e., both values match); otherwise, discard the message
Encryption:
Step-5:-Generate Auth-Key for UE
AK_{UE}
Step 7: Generate timestamps Ts_{CLH}
Step 10: Compute
AK_{UE}, Ts_{CLH} = M
Hash value of AK_{UE} and Ts_{CLH}= H ($AK_{UE,}$ Ts_{CLH})
Step 11: Encrypt (CLH-UE)
$[H\ (AK_{UE,}\ Ts_{CLH})]^{KCLH}$
$[M, H\ (AK_{UE,}\ Ts_{CLH})]^{KCLH}]_{KUE}$
Step 12: AUTH-RES: [Encrypt (CLH-UE)]
Step 13: Send AUTH-RES (CLH-UE) to UE

MATHEMATICAL ANALYSIS

The evaluation of the proposed LA-UAV and benchmarks protocol will be based on Mathematical Analysis, by performing the calculation of Communication Cost to find out if

the proposed LA-UAV is much more lightweight compared to the other benchmark, Computational Cost to obtain the total number of computation to be made and Authentication Overheads to find the overhead of the authentication messages before the actual communication occur. To find total communication of the proposed algorithm, Capkun cost equation is employed. The communication-cost is computed for LA-UAV and the other three benchmark algorithms. From a computational complexity perspective, the proposed LA-UAV protocol is lightweight and scalable. Let n denote the number of authentication hops and m the number of participating UAVs. Each authentication session involves a constant number of elliptic curve point multiplications, hash computations, and encryption/decryption operations. So the complexity of the propose scheme is O(n).

COMMUNICATON COST

In the proposed algorithm, the User Equipment (UE) aims to communicate with both the Cluster Head (CLH) and the Global Head (GH). The CLH acts as an access point, forwarding authorization requests from the GH to the UAV. Several messages are exchanged between the UE, CLH, and GH. To calculate the total cost, this research considers all operations involved in ensuring secure communication. Specifically, in the LA-UAV algorithm, five operations are integral to secure communication. The messages sent in the LA-UAV protocol consist of pseudo-ID, challenge, challenge solution, hash, and timestamp, which are denoted by $PC_{PID||3DL}$, PC_{Ch}, $PC_{Ch'}$, PC_{H}, and $PC_{Ts,}$ respectively. The communication cost for each message is calculated as follows. The initial message is sent from the UE to the CLH and contains a request from the UE for communication with the CLH. The message sent includes pseudo-IDs, challenge, timestamp, and hash. Thus, the total size of the message will be the sum of pseudo-IDs, challenge, timestamp, and hash, which is the sum of$\{PC_{PID||3DL}, PC_{CH}, PC_{TS}, PC_{DH}\}$. Therefore, the size of the authentication message can be calculated using Equation-1.

$$m_{C1} = \ \rangle \ \{Pc_{PID||3DL} + Pc_{Ch} + \ Pc_{TS} + \ Pc_{H}\} \tag{1}$$

The second message is sent from the Cluster Head (CLH) to the Global Head (GH) after being triggered by the request message from the User Equipment (UE). The communication cost for this second message is represented by Equation-2.

$$m_{C2} = \sum \{Pc_{PID||3DL} + \ Pc_{Ch} + Pc_{TS} + \ Pc_{H}\} \tag{2}$$

The third message is a response from the Global Head (GH) to the Cluster Head (CLH), aimed at verifying the CLH with a new challenge. The communication cost for this third message is calculated and presented by Equation-3.

$$m_{C3} = \sum \{Pc_{PID||3DL} + Pc_{Ch} + \ Pc'_{Ch} + Pc_{TS} + \ Pc_{H}\} \tag{3}$$

The fourth message is sent from the Cluster Head (CLH) to the Global Head (GH), in which the CLH addresses the challenge provided by the GH. The communication cost for this fourth message is presented by Equation-4.

$$m_{C4} = \sum \{Pc_{PID||3DL} + Pc_{Ch} + \ Pc'_{Ch} + Pc_{TS} + \ Pc_{H}\} \tag{4}$$

Message five is a response from the Global Head (GH) to the Cluster Head (CLH), in which the GH transmits the authorization key (AK) to the CLH. The communication cost for this fifth message is represented by Equation-5.

$$m_{C5} = \sum_{Au=1}^{k=1} \{Pc_{PID||3DL} + Pc_{AK} + Pc_{TS} + Pc_H\} \quad (5)$$

Message-number-six is from CLH to UE as a response message where CLH caters challenge from UE. The communication-cost for message number 6 is shown by Equation-6.

$$m_{C6} = \rangle \{Pc_{PID||3DL} + Pc_{Ch} + Pc'_{Ch} + Pc_{TS} + Pc_H\} \quad (6)$$

Message number seven is response message from CH to UE where UE address the challenge from CLH. The communication cost for message number 7 is shown by Equation-7.

$$m_{C7} = \rangle \{Pc_{PID||3DL} + Pc_{Ch} + Pc'_{Ch} + Pc_{TS} + Pc_H\} \quad (7)$$

CLH sends an authorization key AK to UE in message number eight, Communication-cost for message 8 is shown by Equation-8.

$$m_{C8} = \rangle \{Pc_{AK} + Pc_{TS} + Pc_H\} \quad (8)$$

After looking into above Equations 1 to 8 and for Message 1 to message 8, cumulative computation of communication cost has been calculated as follows.

$$\begin{aligned} AuthM_C = {} & a * \sum_{k=8}^{k=4} \{Pc_{PID||3DL}\} + b * \sum_{k=2}^{Au=1} \{Pc_{Ch}\} + c \\ & * \sum_{Au=1}^{Au=1} \{Pc'_{Ch}\} + d \\ & * \sum_{Au=1}^{Au=1} \{Pc_{Ts} + Pc_H\} + e * \sum_{Au=1}^{Au=1} \{Pc_{AK}\} \end{aligned} \quad (9)$$

Where a, b, c, d, e are constants and can be simply stated as

$$Auth\ M_C = \alpha * \sum_{Au=1}^{} \{Pc_{PID||3DL} + Pc_{Ch} + Pc'_{Ch} + Pc_{TS} + Pc_{AK}\} \quad (10)$$

Equation-10 shows the message for one hop communication where α shows the number of individual messages and β represents the number of messages transmitted. As shown, that LA-UAV can handle two-hop communication, as shown in Equation-11.

$$AuthM_C(2) = 2h \left(\alpha * \sum_{Au=1}^{k=\beta} \{Pc_{PID||3DL} + Pc_{Ch} + Pc'_{Ch} + Pc_{TS} + Pc_H + Pc_{AK}\} \right) \quad (11)$$

Where h is number of hops.

Similarly, for three hops the Equation-11 will be as below

$$AuthM_C(3) = 3h \left(\alpha * \sum_{Au=1}^{k=\beta} \{Pc_{PID||3DL} + Pc_{Ch} + Pc'_{Ch} + Pc_{TS} + Pc_H + Pc_{AK}\} \right) - \mathrm{L} \quad (12)$$

Thus, for multi-hop scenario, the Equation-12 will be hop times the equation.

$$AuthM_C(h) = h\left(\alpha * \sum_{k=\beta}^{} \{Pc_{PID|3DL} + Pc_{Ch} + Pc'_{Ch} + Pc_{TS} + Pc_H + Pc_{AK}\}\right) \quad (13)$$

For more than one hops, the number of messages transmitted is multiple of number of hops. In multi-hop scenario, total authentication cost is equal to number of hops multiplied by number of messages in single hop plus number of messages in forwarding request as shown in Equation-14.

$$AutM_{MH}(h) = number\ of\ hops * (Single\ hop\ message + forwarding\ request) \quad (14)$$

EMPIRICAL ANALYSIS

To compute the total communication cost, all credentials are standardized to a 16-byte (128-bit) length to maintain uniformity across benchmarks and ensure consistency with the proposed LA-UAV scheme. Based on Equation-10, which addresses single-hop communication within the LA-UAV framework, the total communication cost for the scheme amounts to 4672 bits. In the case of multi-hop scenarios, the total communication cost for the respective scheme is expressed as 4480n, 8832n, 11648n, and 4096n bits, where n denotes the number of hops. Table-1 provides a detailed breakdown of the total communication costs in multi-hop scenarios.

In the empirical analysis, all cryptographic credentials and protocol parameters are standardized to a 16-byte (128-bit) length. This selection aligns with widely accepted cryptographic security recommendations, providing sufficient resistance against brute-force and collision attacks while maintaining computational efficiency. The 128-bit size offers a balanced trade-off between security strength and resource consumption, making it well-suited for UAVs with constrained processing power and energy reserves. Standardizing parameter sizes across LA-UAV and benchmark schemes also ensures a fair and consistent comparative evaluation. Hash outputs, pseudo-identities, timestamps, and authorization keys are uniformly represented, eliminating bias that could arise from differing parameter lengths. This design choice reinforces the lightweight nature of the proposed protocol while preserving robust security guarantees.

Furthermore, for each hop within the symmetric key cryptosystem, the scheme necessitates a key refresh to reinitialize secure communication. In the LA-UAV protocol, the hash function is operated 10 times for the whole authentication process. The hash function is required to maintain the integrity of certain credentials or messages during the authentication process. Based on Algorithm1.1, for the first authentication request message from UE to CLH, the timestamp of the message is hashed one time before the message is send to CLH. This is also applied to messages in the above algorithms, where each timestamp of the messages needs to be hashed before it is sent to the desired receiver. However, to complete the mutual authentication process, an authorization key is generated by the GH and needs to be sent to the UE via the CLH securely. Hence, to keep the integrity of the authorization key, it also needs to be hashed along with the timestamp. Consequently, the hash operation in both messages is performed two times each where the authorization key and timestamp are both hashed. In the proposed LA-UAV scheme, asymmetric cryptography is employed to perform encryption and decryption operations. By leveraging the private key (\(K_n\)) and public key (\(K_n\)) of participants within the network, the scheme effectively mitigates threats such as

Man-in-the-Middle (MITM) attacks, impersonation attacks, and masquerading attacks. Each timestamp's hash value within a message is encrypted (digitally signed) using the sender's private key. Hashing ensures data integrity by preventing unauthorized modifications, while encryption ensures that the message originates from a legitimate device or entity. Additionally, the entire message is encrypted using the receiver's public key to preserve its confidentiality, further mitigating masquerading attacks.

Overall, the proposed scheme requires eight encryption and eight decryption computations to achieve the desired level of security. Table I also shows the total computation involved in the generation and validation of parameters or credentials in our proposed scheme and all three benchmarks. These generation (Compute) and validation (Check) processes are required for generating some credentials and parameters as rules and conditions during the authentication process. In our proposed scheme, there are a total of 17 computations for generation and one validation process of parameters and credentials at the UE's end. Meanwhile, there are a total of 36 generations and three validations at AP and a total of 19 generations and two validation processes at GH. Overall, our proposed scheme requires a total of 72 generations and six validation processes to complete the authentication process.

TABLE 2. Empirical Analysis of LA-UAV

Analsyis	Performance						
Number ofhops	2	3	4	5	6	7	8
Authentication Overhead as number of messages	16	24	32	40	48	56	64
Communication Cost as number of bits	9384	14066	18738	23410	28082	32754	37426
Total Computation 104	H (10) + XOR (None) + Enc (8) + Dec(8) +Generation Process (72) + Validation Process (6)						

THREAT MODELING AND ATTACKS MITIGATION

The proposed LA-UAV protocol is analyzed under a realistic and widely accepted adversarial model for UAV and IoD environments. We assume that the communication channel between UAVs, Cluster Heads (CLHs), and the Global Head (GH) is open and insecure, allowing adversaries to eavesdrop, intercept, replay, modify, and inject messages.

The attacker is assumed to possess moderate computational resources, consistent with practical adversaries, but is unable to break standard cryptographic primitives such as ECC, secure hash functions, or digital signatures within polynomial time. Both passive attackers (eavesdropping and traffic analysis) and active attackers (replay, impersonation, rogue relay deployment, and message modification) are considered.

The adversary may compromise or deploy rogue UAVs or relay nodes but cannot simultaneously compromise the Global Head and multiple legitimate Cluster Heads.

Physical capture of UAVs is assumed possible; however, extraction of long-term cryptographic secrets is mitigated through ephemeral key usage and challenge-response validation. This threat model reflects realistic operational conditions in future cellular-enabled UAV networks.

The CIA triad is a fundamental security evaluation model that serves as a conceptual framework for evaluating and designing secure systems, protocols, and architectures. A detail summary is presented in Table II.

TABLE 3. Notations and Description

Notation	Purpose	Attack Mitigation
Ch	In proposed LA-UAV design, The Challenge (Ch) is utilized to achieve mutual authentication.	Challenge (Ch) mechanism is employed to mitigate malware-attacks by allowing only legitimate UAVs.
UAV 3D position	The notion that only one UAV can take a 3D location at a given time.	Provides security against forgery and non-repudiation. Injection attacks and message forgery as only one UAV can be at a certain 3D location at a certain Timestamp.
T_S	Time stamping is employed to ensure message freshness.	Ensuring Mitigation of replay-attack.
Ch′	Challenge Solution is transmitted to confirm genuinely of receiver UAV.	Mutual-Authentication.
H	Hashing is performed to ensure : • Message-Integrity • Confusion &diffusion	To mitigate Pre image attacks, weak collision-attacks, , and data-modification attacks, ensuring the integrity and authenticity of the transmitted data
K^n	The private-key is employed in order to digitally sign data also contributing to confidentiality	Mitigating Man-in-the-Middle & impersonation attacks etc.
K_n	Employment of Public-key is carried out to encrypt data	The issuance of the public key helps prevent masquerading attacks
AK_{UE}	The device is authorized and services are provided only to legitimate devices, ensuring validation at two levels for enhanced security.	Mitigation of attacks such as rouge-device attack
AK_{CLH}	The device is authorized, and services are granted exclusively to legitimate devices, with validation occurring at two levels to ensure robust security.	Mitigation of attacks such as rouge-device-attack and several well known relevant attack types.

It is widely used in cyber security risk assessments, protocol design, and compliance audits. In the context of the CIA triad model, attackers targeting UAVs may attempt to breach confidentiality by eavesdropping on wireless communications to extract sensitive data. To

compromise integrity, they could inject, modify, or replay messages, potentially leading to false commands or misinformation. Attacks on availability may involve jamming signals or launching denial-of-service (DoS) attacks to disrupt UAV operations. Given the open and dynamic environment of flying drones, attackers may have moderate computational power, mobility, and access to communication channels, enabling both passive and active attacks. Therefore, the proposed lightweight authentication protocol must defend against such adversaries while remaining efficient for UAV resource constraints. The proposed protocol LA-UAV is highly resilient to threats in a wireless environment populated with drones / UAVs executing diverse roles and missions in future applications. Following discussion / security proofs provide a rigorous foundation and enhance the credibility of the proposed protocol's effectiveness against attacks.

SECURITY VERIFICATION AND FORMAL PROOF

The proposed lightweight authentication protocol for UAVs aligns with the CIA triad by ensuring confidentiality, integrity, and availability. Confidentiality is maintained through secure key exchange and encrypted communication, preventing unauthorized access to UAV data. The protocol incorporates traditional ECC-based cryptographic methods to ensure that the data transmitted between UAVs and the network is encrypted. By leveraging multi-factor authentication, which includes timestamps, and 3D positional data, the protocol ensures that only authenticated and authorized UAVs can access the network. Integrity is ensured by incorporating message authentication codes and hash functions to detect any tampering during data transmission. The use of cryptographic methods includes hash functions, which help in maintaining data integrity. The integration of 3D positional data acts as a unique identifier, which can be cross-verified to detect any tampering or spoofing attempts. The protocol also supports availability by minimizing computational and communication overhead, thus enabling real-time authentication even in resource-constrained environments. The protocol is designed to be lightweight, reducing computational overhead and authentication time. This efficiency ensures that UAVs can maintain continuous communication without significant delays, enhancing availability. Together, these features demonstrate the protocol’s compliance with the foundational principles of secure communication.

SIMULATION ANALYSIS AND COMPARISON

The proposed scheme is evaluated in comparison with benchmark protocols by performing simulation analysis by taking into consideration and calculation of Packet Delivery Ratio, Packet Overhead, Processing Time and Effect of Rogue Relay Station. In the simulation, the attacker’s actions vary across concepts, degrading the network performance in specific ways. For Packet Delivery Ratio (PDR), the attacker introduces replay attacks or packet drops by refusing to forward packets or delaying their delivery, reducing the overall PDR. For Packet Overhead, the attacker activities include, sending re-authentication requests or introducing fake packets causing impersonation attacks, which increase the computational and communication overhead required to mitigate their actions. In Processing Time, the attacker escalates delays by injecting malicious traffic or triggering unnecessary encryption and signature validation processes, thus increasing the time taken to process legitimate packets. Finally, for Rogue Relay Impact, the attacker sets up compromised relay stations that obstruct or reroute network traffic, causing a significant decline in legitimate traffic transmission and potentially leading to near-DoS (Denial of Service) conditions as rogue relays outnumber legitimate ones. Each of these actions directly undermines the efficiency and reliability of the network under the simulated scenarios.

PACKET DELIVERY RATIO

Figure 6 illustrates the impact of packet delivery ratio (PDR) in the absence of attackers within the network. The graph presents the PDR against the number of nodes for four different approaches. The LA-UAV without attacker consistently achieves the highest PDR, remaining close to 1.0, indicating reliable communication as the network scales. In contrast, Benchmark 3 (Algarni & Jan, 2024) performs the worst, with a significant drop in PDR as node count increases, while Benchmark 1 (Wang et al., 2024) and Benchmark 2 (Zhang et al., 2023) show intermediate but relatively stable performance. The results demonstrate that the proposed LA-UAV protocol achieves the highest PDR as the number of transmitted packets increases. PDR is quantified in terms of million bits per second. In the LA-UAV protocol, packets transmitted per message are smaller in size and require lower computational overhead, contributing to its high efficiency. However, as the number of nodes increases, a slight drop in PDR—approximately 0.019%—is observed. This reduction is attributed to the increased overhead caused by device and node verification times.

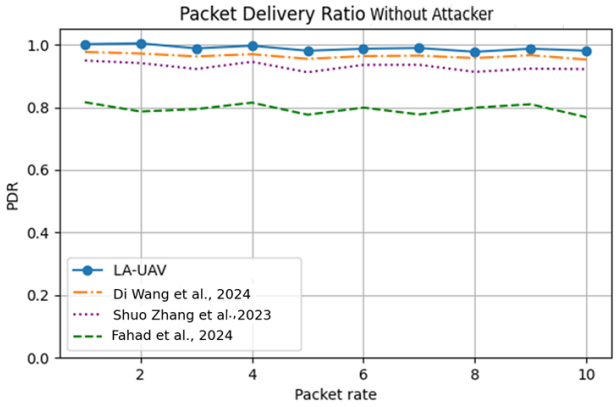

FIGURE 6. PDR performance of LA-UAV without attacker

This variation primarily results from design modifications in the LA-UAV protocol, including the embedding of acknowledgments within regular messages and the implementation of multi-factor verification processes. The observed difference becomes more pronounced as additional nodes join the network, leading to an increase in communication requests and packet rates. Figure 7 illustrates the impact of packet delivery ratio (PDR) in the presence of attackers within the network. When an attacker infiltrates the network, the performance of the proposed LA-UAV protocol remains superior to other benchmark protocols. This resilience is primarily attributed to its ability to prevent replay attacks, thereby maintaining higher throughput.

Although the packet rate under attack conditions is slightly lower than the packet delivery ratio observed in the absence of attacks, the LA-UAV protocol continues to demonstrate robust performance as shown in Figure 7 PDR performance of LA-UAV with attacker. In this scenario, attackers are modeled as rogue devices or nodes that disrupt communication by refusing to forward messages, generating repeated re-authentication requests, or failing to acknowledge packet receipt. Despite these adversarial behaviors, the LA-UAV protocol effectively mitigates such threats, ensuring reliable communication and sustained network performance. The LA-UAV with attacker maintains the highest PDR across all node counts, consistently outperforming Benchmark 1, 2, and 3, which all show lower and more fluctuating performance. Benchmark 3 performs the worst, with PDR values

steadily below 0.7, indicating that LA-UAV remains the most resilient and reliable even under adversarial conditions.

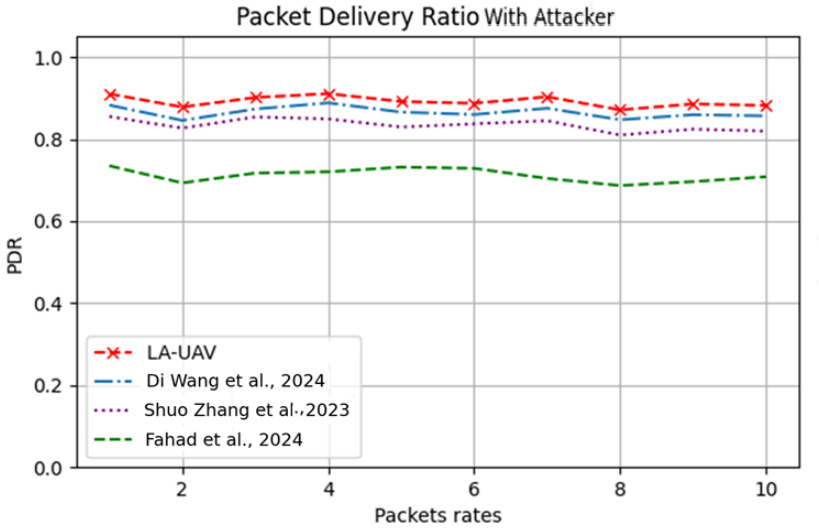

FIGURE 7. PDR performance of LA-UAV with attacker

PACKET-OVERHEAD EFFECT

Packet overhead refers to the total time required for transmitting packets across the network, encompassing the duration from the source to the destination. As illustrated in Figure 8, simulation results indicate that the proposed LA-UAV protocol performs well for packet overhead in the absence of an attacker. In the LA-UAV protocol, initial transmissions consist of smaller 'hello' packets, which facilitate faster and more efficient communication. The sharp drop observed in the packet overhead corresponds to the initiation of multiple authentication messages, which are designed to validate authentication processes swiftly. The LA-UAV protocol maintains lower packet overhead by optimizing packet size while simultaneously enhancing security and mitigating various attacks in comparison with benchmarks.

In the presence of an attacker, the LA-UAV protocol continues to exhibit reduced packet overhead due to its multi-factor authentication mechanism. This approach enables the protocol to bypass unnecessary packet exchanges, thereby enhancing efficiency. If an attacker successfully infiltrates the network, the malicious node is promptly identified and blocked. The results, as shown in Figure 9, reveal that when an attacker is introduced, all protocols utilize hash functions and timestamps to counter the attack. However, packet drops caused by the attack result in additional packet transmissions, leading to increased packet overhead. Specifically, the LA-UAV protocol experiences a rise in packet overhead compared to its performance without an attacker. Despite this increase, LA-UAV maintains superior performance through trust validation, multi-factor authentication, and hash mechanisms, and achieves a slight performance improvement over existing schemes and benchmarks. While other protocols provide comparable levels of security, they suffer from larger packet sizes, resulting in lower packet delivery ratios (PDR) and higher computational costs.

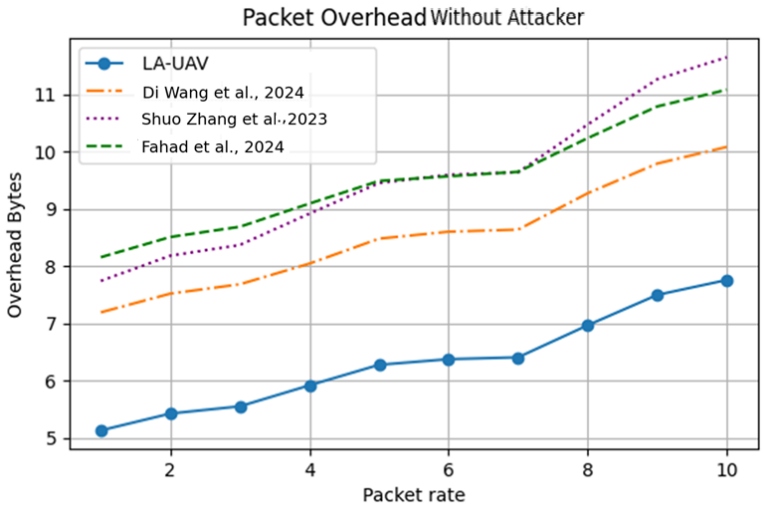

FIGURE 8. Packet Overhead performance of LA-UAV without attacker in Bytes

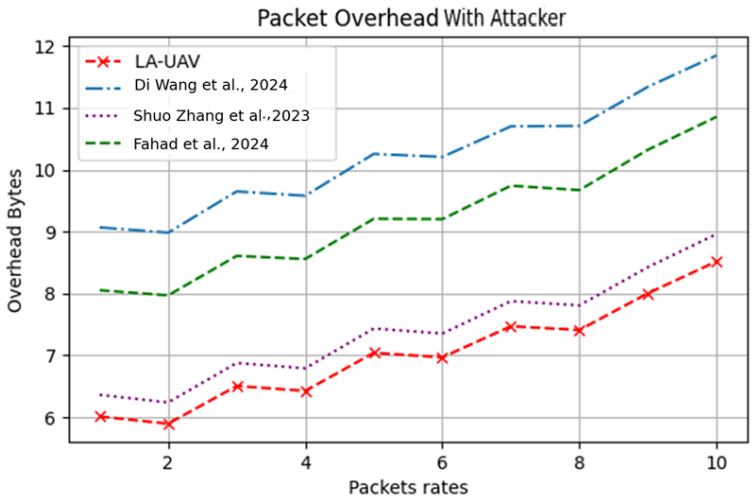

FIGURE 9. Packet Overhead performance of LA-UAV with attacker in Bytes

PROCESSING-TIME

Figure 10 illustrates the processing time associated with the protocol. This metric is crucial, as it directly impacts the delivery rate or ratio. Higher processing times can lead to increased processing costs and pose challenges for adaptation in small-scale devices. From the simulation analysis, it is evident that the processing time of the proposed LA-UAV protocol is significantly lower compared to other benchmark schemes. Notably, the processing time for LA-UAV remains consistently low even as the number of packets increases. The processing cost is primarily influenced by computational operations, including encryption, decryption, and signature computation. The higher processing times observed in other schemes are a result of larger data sizes, the separate handling of hash values, timestamps, and key exchanges, all of which contribute to increased computational overhead. Effect of increasing rogue relay station

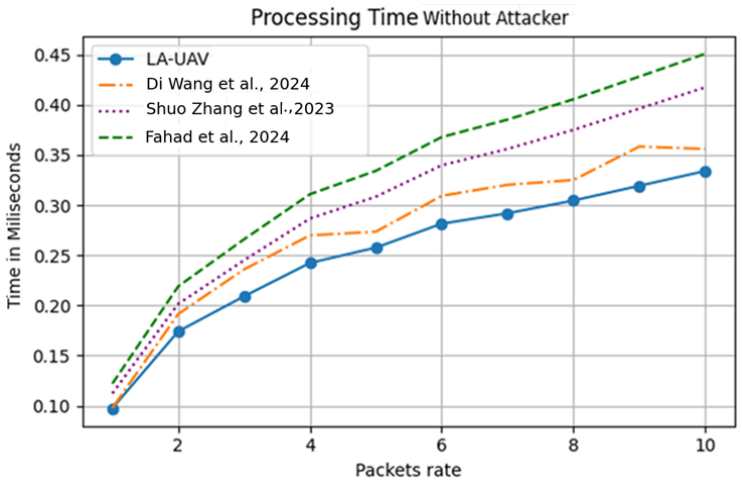

FIGURE 10. Processing Time (ms) performance without attacker

Similarly, Figure 11 illustrates the Processing Time performance of LA-UAV with attacker. As the number of packets increases, all schemes exhibit a gradual rise in processing time, reflecting increased computational overhead. Among the methods, LA-UAV with attacker consistently demonstrates the lowest processing time, making it the most efficient in terms of computation. Benchmark 1 performs slightly worse but remains competitive. In contrast, Benchmark 2 and Benchmark 3 show significantly higher processing times, with Benchmark 3 being the least efficient overall. This suggests that the LA-UAV approach is better optimized for handling larger data loads with minimal processing delay, even in the presence of attackers.

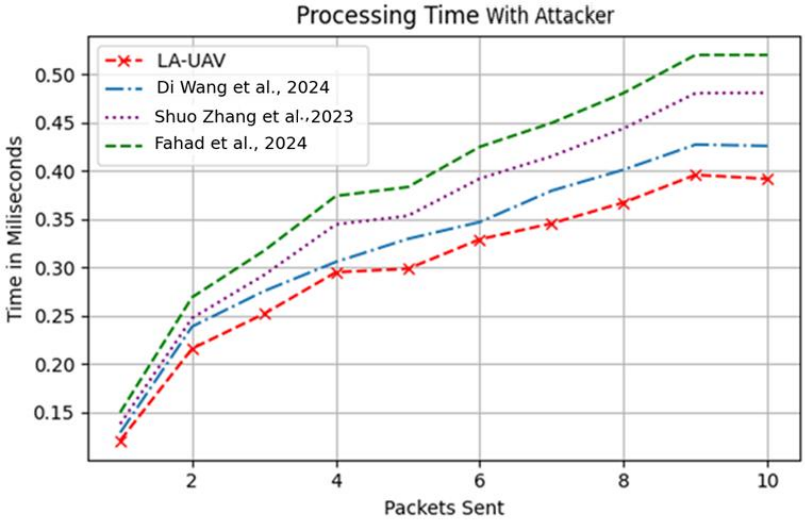

FIGURE 11. Processing Time (ms) performance with attacker

EFFECT OF INCREASING ROGUE RELAY STATION

As illustrated in Figure 12, an increase in the number of rogue relays leads to a rise in attacks. When the number of rogue relays exceeds that of legitimate relays, traffic transmission can

be obstructed, potentially resulting in a Denial of Service (DoS) attack. Despite this, the LA-UAV protocol ensures that no illegitimate traffic can pass through the network due to its robust prior registration and mutual authentication processes.

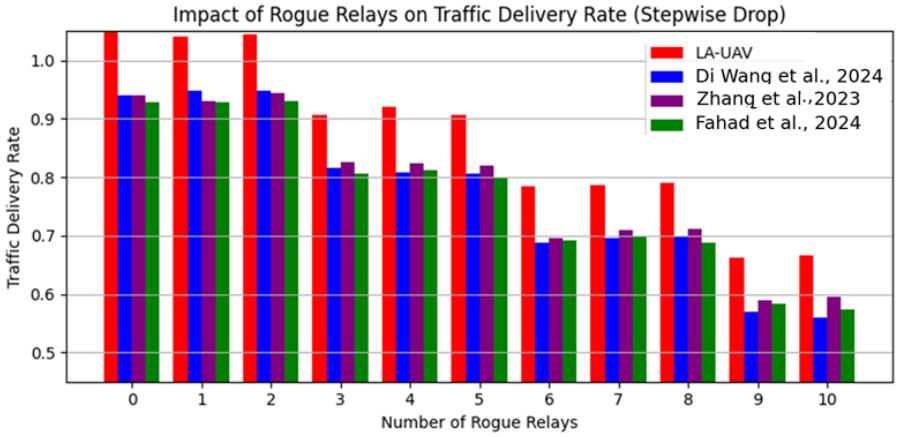

FIGURE 12. Comparison of the rogue relay effects

When the number of rogue relays exceeds that of legitimate relays, traffic transmission can be obstructed, potentially resulting in a Denial of Service (DoS) attack. Despite this, the LA-UAV protocol ensures to prevent illegitimate traffic from passing through the network due to its robust prior registration and mutual authentication processes. The delay observed in the LA-UAV scheme results from node re-verification and subsequent verification message transmission of verification messages.

ENERGY EFFICIENCY COMPARISONS

The endurance and overall performance of UAV devices may be adversely impacted if they are subjected to overly frequent or computationally intensive authentication schemes (Hussain et al., 2024). The proposed LA-UAV protocol demonstrates superior energy performance by significantly reducing message overhead and computational complexity. Unlike conventional schemes that involve multiple message exchanges and heavy cryptographic operations, LA-UAV streamlines the authentication process with minimal communication steps and its lightweight design. This efficiency leads to lower energy consumption, which is critical for resource-constrained UAVs as the empirical analysis shown in Table III. As a result, it enhances UAV flight endurance and operational sustainability in real-world deployments keeping intact security needs of these devices.

TABLE 4. Empirical Analysis of LA-UAV

Scheme	**Number of Messages/hops**						
	2	3	4	5	6	7	8
LA-UAV	16	24	32	40	48	56	64
Di Wang et al	18	27	36	45	54	63	70
Zhang et al	22	33	44	55	66	77	88
Fahad et al	24	36	48	60	72	84	96

CONCLUSION

This study proposes a novel security algorithm designed to strengthen protection mechanisms while minimizing communication, computational, and authentication overhead, attributed to its lightweight architecture. Although considerable research has been devoted to security algorithms for single-hop Cell-Free systems, investigations into their applicability within multi-hop Cell-Free networks are still in the early stages of development. This study investigates both multi-hop and direct Cell-Free communication paradigms. The proposed algorithm employs multi-factor authentication to ensure secure communication among User Equipment (UEs), Cluster Heads (CLHs), and the Global Head (GH) within a drone network environment. The inclusion of an explicit threat model, formal complexity analysis, and comparative evaluation further strengthens the validity and applicability of the proposed LA-UAV protocol for real-world UAV deployments.

The proposed authentication protocol presents an innovative solution tailored specifically to the unique demands of future Internet of Drones (IoD) and UAV networks. By addressing the inherent limitations of UAVs, such as constrained onboard power and limited processing capabilities, the protocol ensures efficient and secure identity verification. As the role of UAVs expands across diverse domains, including agriculture, media, logistics, civil infrastructure, and defense, the need for robust authentication mechanisms becomes increasingly critical. Given their vulnerability to a wide range of security threats such as forgery, impersonation, replay, and adversary-in-the-middle attacks, establishing trusted communication between UAVs is essential. This protocol represents a significant step forward in enhancing the overall security posture of drone networks in an increasingly connected and automated world. The LA-UAV scheme offers several key contributions, including enhanced security and privacy, coupled with low communication and computational overhead. Its robust device validation mechanisms and multi-factor authentication features effectively prevent adversaries from compromising devices through malicious activities.

REFERENCES

Algarni, F., & Jan, S. U. (2024). PSLAPS-IoD: A Provable Secure and Lightweight Authentication Protocol for Securing Internet-of-Drones (IoD) Environment. *IEEE Access*.

Ali, S., Abu-Samah, A., Abdullah, N. F., & Mohd Kamal, N. L. (2024). Propagation modeling of unmanned aerial vehicle (UAV) 5G wireless networks in rural mountainous regions using ray tracing. *Drones*, *8*(7), 334.

Ashraf, S. N., Manickam, S., Zia, S. S., Abro, A. A., Obaidat, M., Uddin, M., Abdelhaq, M., & Alsaqour, R. (2023). IoT empowered smart cybersecurity framework for intrusion detection in internet of drones. *Scientific Reports*, *13*(1), 18422.

Banafaa, M. K., Pepeoğlu, Ö., Shayea, I., Alhammadi, A., Shamsan, Z. A., Razaz, M. A., Alsagabi, M., & Al-Sowayan, S. (2024). A comprehensive survey on 5G-and-beyond networks with UAVs: Applications, emerging technologies, regulatory aspects, research trends and challenges. *IEEE Access*, *12*, 7786-7826.

Couteau, G., Devadas, L., Hegde, A., Jain, A., & Servan-Schreiber, S. (2025). Multi-key homomorphic secret sharing. Annual International Conference on the Theory and Applications of Cryptographic Techniques,

DAVID, S. (2025). Comparative Analysis of Modern Hashing Algorithms: SHA-2, SHA-3 vs Legacy Algorithms (MD2, MD5, SHA-1) for Intrusion Detection Systems.

El-Dalahmeh, A., El-Dalahmeh, M., Razzaque, M. A., & Li, J. (2024). Cryptographic methods for secured communication in SDN-based VANETs: A performance analysis. *Security and Privacy*, *7*(6), e446.

Gaydamaka, A., Samuylov, A., Moltchanov, D., Ashraf, M., Tan, B., & Koucheryavy, Y. (2023). Dynamic topology organization and maintenance algorithms for autonomous UAV swarms. *IEEE Transactions on Mobile Computing*, *23*(5), 4423-4439.

Hemmati, A., & Zarei, M. (2024). UFC3: UAV-aided fog computing based congestion control strategy for emergency message dissemination in 5G internet of vehicles. *Automotive Innovation*, *7*(3), 456-472.

Huang, G., Hu, M., Yang, X., Lin, P., & Wang, Y. (2024). Addressing Constraint Coupling and Autonomous Decision-Making Challenges: An Analysis of Large-Scale UAV Trajectory-Planning Techniques. *Drones*, *8*(10), 530.

Hussain, A., Li, S., Hussain, T., Lin, X., Ali, F., & AlZubi, A. A. (2024). Computing Challenges of UAV Networks: A Comprehensive Survey. *Computers, Materials & Continua*, *81*(2).

Jaffe, E. pIckIng sIdes AFter plAyIng: why reAgAn's grAduAl IrAn-IrAq wAr tIlt wAs rAtIonAl. *An Undergraduate Journal of International Affairs at Dartmouth College*, 42.

Kim, H. (2024). Security Enhancement of biometric-based authentication systems using smart card. *IEEE Access*.

Koppl, M., Siroshtan, D., Orgon, M., Pocarovsky, S., Bohacik, A., Kuchar, K., & Holasova, E. (2021). Performance Comparison of ECDH and ECDSA. 2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT),

Laghari, A. A., Jumani, A. K., Laghari, R. A., Li, H., Karim, S., & Khan, A. A. (2024). Unmanned aerial vehicles advances in object detection and communication security review. *Cognitive Robotics*, *4*, 128-141.

Lei, Y., Zeng, L., Li, Y.-X., Wang, M.-X., & Qin, H. (2021). A lightweight authentication protocol for UAV networks based on security and computational resource optimization. *IEEE Access*, *9*, 53769-53785.

Li, T., Yang, C., Song, Y., Cai, L., Zheng, R., Liu, X., Ji, Z., & Liu, S. (2024). Architecting Autonomous Network Management and Control via Intent-Driven Decoupled Network. *IEEE Network*, *38*(6), 361-369.

Mazor, N., & Zhang, J. (2024). Simple constructions from (almost) regular one-way functions. *Journal of Cryptology*, *37*(3), 25.

Mobini, Z., Ngo, H. Q., Matthaiou, M., & Hanzo, L. (2024). Cell-free massive MIMO surveillance of multiple untrusted communication links. *IEEE internet of things journal*, *11*(20), 33010-33026.

Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., & Khan, M. A. (2023). Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. *Intelligent service robotics*, *16*(1), 109-137.

Perz, R. (2024). The multidimensional threats of un-manned aerial systems: exploring biomechanical, technical, operational, and legal solutions for ensuring safety and security. *Archives of Transport*, *69*(1), 91-111.

Pimenta Rodrigues, G. A., Marques Serrano, A. L., Lopes Espiñeira Lemos, A. N., Canedo, E. D., Mendonça, F. L. L. d., de Oliveira Albuquerque, R., Sandoval Orozco, A. L., & García Villalba, L. J. (2024). Understanding data breach from a global perspective: Incident visualization and data protection law review. *Data*, *9*(2), 27.

Rahim, S., & Peng, L. (2023). Intelligent space-air-ground collaborative computing networks. *IEEE Internet of Things Magazine*, *6*(2), 76-80.

Shaikh, M. R., Khuhawar, F. Y., Nisar, K., Memon, A. A., & Khan, A. S. (2022). Vulnerability Assessment & Analysis of Software-Defined Networking using a Virtual Testbed. 2022 Global Conference on Wireless and Optical Technologies (GCWOT),

Shuwandy, M. L., Alsharida, R. A. F., & Hammood, M. M. (2025). Smartphone Authentication Based on 3D Touch Sensor and Finger Locations on Touchscreens via Decision-Making Techniques. *Mesopotamian Journal of CyberSecurity*, *5*(1), 165-177.

Srivastava, A., & Prakash, J. (2023). Internet of Low-Altitude UAVs (IoLoUA): a methodical modeling on integration of Internet of "Things" with "UAV" possibilities and tests. *Artificial Intelligence Review*, *56*(3), 2279-2324.

Tychola, K. A., Voulgaridis, K., & Lagkas, T. (2024). Beyond flight: Enhancing the Internet of Drones with blockchain technologies. *Drones*, *8*(6), 219.

Tzinas, A., Sridhar, S., & Zindros, D. (2024). On-chain timestamps are accurate. International Conference on Financial Cryptography and Data Security,

Wang, A., Zha, Z., Guo, Y., & Chen, S. (2019). Software-defined networking enhanced edge computing: A network-centric survey. *Proceedings of the IEEE*, *107*(8), 1500-1519.

Wang, D., Cao, Y., Lam, K.-Y., Hu, Y., & Kaiwartya, O. (2024). Authentication and key agreement based on three factors and PUF for UAVs-assisted post-disaster emergency communication. *IEEE internet of things journal*.

Yang, Z., Yang, Y., He, X., & Qi, W. (2024). Incremental coverage path planning method for UAV ground mapping in unknown area. *International Journal of Micro Air Vehicles*, *16*, 17568293241262323.

Yu, K., Feng, Z., Yu, J., Chen, T., Peng, J., & Li, D. (2024). Secure ultra-reliable and low latency communication in UAV-enabled NOMA wireless networks. *IEEE Transactions on Vehicular Technology*, *73*(10), 14908-14922.

Yu, S., Das, A. K., Park, Y., & Lorenz, P. (2022). SLAP-IoD: Secure and lightweight authentication protocol using physical unclonable functions for internet of drones in smart city environments. *IEEE Transactions on Vehicular Technology*, *71*(10), 10374-10388.

Yusop, M. I. M., Kamarudin, N. H., Suhaimi, N. H. S., & Hasan, M. K. (2025). Advancing passwordless authentication: A systematic review of methods, challenges, and future directions for secure user identity. *IEEE Access*.

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

Zhou, S., Liu, X., Tang, B., & Tan, G. (2024). Handover and coverage analysis in 3-D mobile UAV cellular networks. *IEEE internet of things journal*, *11*(18), 29911-29925.