A Lightweight Authentication Protocol for Wide-Range Drone Communications

Wanting Li
College of Computer Science
Shenyang Aerospace University
Shenyang, China
liwanting2@stu.sau.edu.cn

Maode Ma
College of Engineering
Qatar University
Qatar
mammdsg@ieee.org

Lijun Gao
College of Computer Science
Shenyang Aerospace University
Shenyang, China
gaolijun@sau.edu.cn

***Abstract*—The widespread potential of the Internet of Drones (IoD) across various domains is accelerating the development of technologies and innovative applications in multiple scenarios. Ubiquitous wireless connectivity makes it possible for Unmanned Aerial Vehicles (UAVs) to access real-time data in a difficult to reach or hazardous environment. Open network environments present a high security risk, which drastically reduces the success rate of UAVs in executing designated flight paths and transmitting real-time data. In order to address confidentiality and integrity in IoD communications, this paper proposes a lightweight and secure key negotiation protocol for wide-range UAV communications, called LAPW-DC. The protocol enables remote signaling between UAVs and Ground Stations (GS), as well as between UAVs, via Long-Term Evolution (LTE) networks, and solves the problem of independent use of the Physical Unclonable Function (PUF) technique for resisting physical capture over a wide area. Based on BAN logic and security evaluation against various common attacks, LAPW-DC is shown to enable secure communication in open network environments. Through a comparative study, we also demonstrate that LAPW-DC provides enhanced security with a lower communication and computational overhead compared to existing protocols.**

***Index Terms*—Internet of Drones (IoD), Long-Term Evolution (LTE), Unmanned Aerial Vehicles (UAVs), Multi-Domain, Security Protocol**

I. Introduction

The Internet of Things (IoT) connects smart devices, exchanges network information, and supports various domains such as smart agriculture, smart cities, smart transportation, and smart healthcare [1]. Unmanned Aerial Vehicles (UAVs), which serve as widely used sensing devices in IoT environments, form the Internet of Drones (IoD) through their integration with the IoT domain. Due to their autonomous, flexible, and stable flight capabilities, UAVs have been deployed for military surveillance, air pollution monitoring, agriculture, and smart city applications. UAV communications in open network environments are vulnerable to various attacks [2], including replay attacks, man-in-the-middle (MITM) attacks, and physical capture. Yu et al. [3] established an efficient and secure authentication mechanism based on the Physical Unclonable Function (PUF) for UAVs in smart cities to improve the security of UAV communication. It can be seen that PUF is often introduced in UAV authentication protocols to help UAVs defend against tampering attacks.

However, due to the limited communication distance of wireless networks, UAVs often cross areas controlled by multiple Ground Stations (GS) during mission execution. Some communication protocols deployed in single domain environments do not meet the requirement. Taking forest fires as an example, when UAVs handle such tasks, they need to call on the UAVs in the fire area. Especially when there are no available UAVs in airspace, nearby UAVs need to be called to assist in finding the location of the fire source, providing accurate positioning information or real-time monitoring of the fire and smoke situation, providing fire scene images and data, helping the command center understand the spread of the fire and choose appropriate response measures. Some communication protocols deployed in single domain environments do not meet the requirement. Recently, many UAV authentication protocols for multi-domain IoD have been used to fill this gap. Feng et al. [4] designed a lightweight blockchain-based lightweight authentication service for UAVs. However, blockchain technology involves frequent reading and writing of data, which can increase additional communication latency. Tanveer et al. [5] designed an authentication encryption based on PUF Elliptic Curve Cryptography (ECC) and hash functions are used to perform authentication key management (AKM). Designed to verify the authenticity of the user and then set the session key (SK) between the user and the particular UAV for unbreakable communication. The performance of UAVs is largely constrained by limited computational power, the protocol involves complex bilinear operations, obviously these do not apply to UAVs with low communication cost and limited computational resources. Bera et al. [6] proposed a protocol based on public key certificates for the secure collection of still images or real-time videos. However, certificate PKI (public key infrastructure)-based authentication schemes rely heavily on certificate authorities (CAs). Khalid et al. [7] proposed an anonymous switching authentication protocol. This protocol utilizes the Advanced Encryption Standard (AES) - Rivest Shamir Adleman (RSA) and public key certificates to provide secure key management and authentication schemes during UAV flight. The encryption-decryption operation of these two algorithms involves complex operations such as block operations or modulo operations, and although hybrid encryption can enhance security, they require high computational and storage resources, which is not practical for resource-constrained UAVs.

Therefore, most authentication schemes use lightweight hash functions or bitwise XOR operations to implement authentication mechanisms for multi-domain UAVs. Tian et al. [8] set up a new lightweight mutual authentication protocol based on PUF, which enables realizable communication for UAVs to collect and share data across multiple regions. This

ISBN 978-3-903176-72-0 © 2025 IFIP.

protocol, while considering the resource consumption caused by PUF synchronization in multi-domain environments, creates a severe storage burden in UAVs as well as GSs. Bhattarai et al. [9] uses hash functions and PUF. Implements secure transmission of data collected by UAVs to GSs and establishes separate SK for different types of data, but this also results in significant communication and computational costs.

It is worth considering that there are still implicit and unconsidered issues in numerous schemes. First, authentication protocols take into account the problem of resource cost while ensuring protection against multiple security attacks. In addition, differently establishing secure SK for different types of data collected by UAVs can effectively prevent all data from being accessed maliciously in its entirety due to partial secret disclosure. Second, how PUF-based noise authentication protocols ensure the independence between different GSs and how to synchronize the information during UAV registration in a way that consumes less communication cost.

Based on the promotion of the above issues, we have rationalized the protocol, the core of this paper as follows.

- We propose a lightweight and secure key negotiation protocol for wide-range UAV communications, called LAPW-DC. It enables UAV-GS mutual authentication and extends it to enable the protocol to establish secure sessions between any two UAVs on the network. It is crucial to consider the different types of data associated with UAV communication tasks and to ensure that appropriate security measures are applied during their transmission.
- LAPW-DC sets up independent usage mechanisms for PUF in different regions to achieve secure mutual authentication; The proposed mechanism effectively minimizes the overhead introduced by frequent information updates and prevents the leakage of sensitive data during the update process. Furthermore, it addresses the issue of excessive storage consumption in GS in the scheme [8].

This paper is structured as follows. Section II introduces the system model and the attack model. Section III, we present the proposed LAPW-DC. The security analysis is performed in Section IV. Section V conducted experiments to compare the performance and mechanism with related papers. The paper provides a summary in Section VI.

II. SYSTEM MODEL

A. System Model

UAVs are deployed in open network environments, and the Long Term Evolution (LTE) wireless network is widely used around the world and provides comprehensive technical specifications [10]. The designated infrastructure Evolved NodeB (eNB) is used to assist communication. As shown in Fig. 1, the system consists of eNBs with LTE infrastructure in different regions, legitimate UAVs, and adversaries. We divide the airspace into multiple flight areas and set up areas where UAVs need to cross multiple eNB controls when performing tasks. Subsequently, in the subsequent communication, the UAV collects various application information in the designated area and performs a secure data transmission. We made the following assumptions.

The potential application areas for UAV IoD are as follows. Task area 1: Smart city area; Task area 2: Agriculture and forest areas; Task area 3: Military region; Task area 4: Control command center;

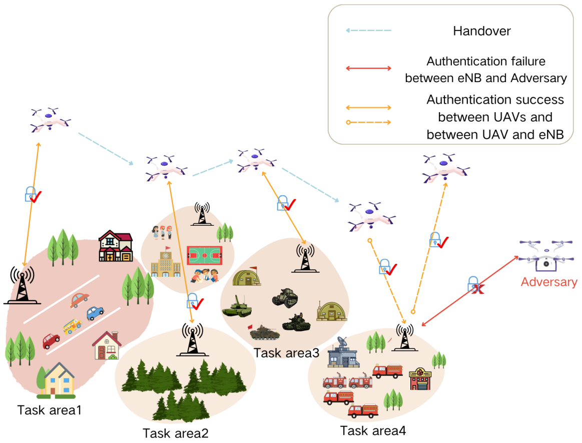
Handover
Authentication failure between eNB and Adversary
Authentication success between UAVs and between UAV and eNB
Adversary
Task area1
Task area2
Task area3
Task area4

Fig. 1. System Model

B. Attack Model

We consider the widely used Dolev-Yao (DY) threat model. Provided as follows, Adversary can not only capture, delete, or tamper the information generated during the communication process but also inject malicious data during the authentication process between the UAV and its associated GS. In LAPW-DC, there is a risk that the UAV falls into the hands of an adversary because it is not possible to monitor all areas, similar to areas that may be difficult or nearly impossible to reach in a land vehicle or on foot. UAV can also be tracked by the adversary. And once the UAV is physically captured by the adversary, various types of critical information stored by the damaged UAV can be extracted by applying a power analysis attack.

III. PROPOSED LAPW-DC

In this section, our proposed LAPW-DC to secure secure communication is described in detail. The notation of the LAPW-DC with their definitions is listed in Table I.

TABLE I
NOTATIONS AND DEFINITION OF THE PROPOSED PROTOCOL

Symbols	Definition
GID_{gs}, UID_u	Unique identities for eNB and UAV
ID_{gs}, ID_d	Temporary identifiers for eNB and UAV
gs_n, d_n	Random nonce generated by eNB and UAV
(C_u, R_u)	PUF challenge-response pair(CRP)
$H(.)$	One-way hash function
SK_u	SK between U and eNB
SK_{uv}	SK between U and V
tx	Transmit data of type tx
$\|\|$	Concatenation operation
xor	XOR operators

A. Mutual authentication between UAV and GSs

Our protocol LAPW-DC guarantees secure communication of UAVs in the LTE communication network, and the steps are shown in Fig. 2.

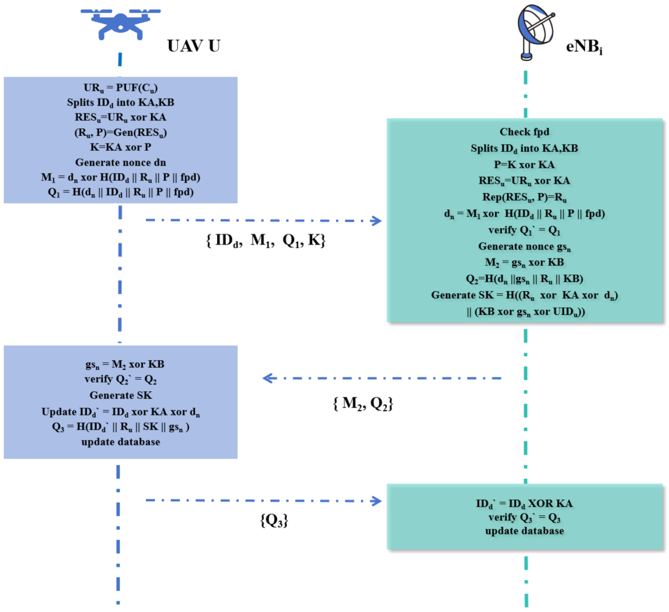

Fig. 2. Mutual Authentication between UAV and eNB$_i$

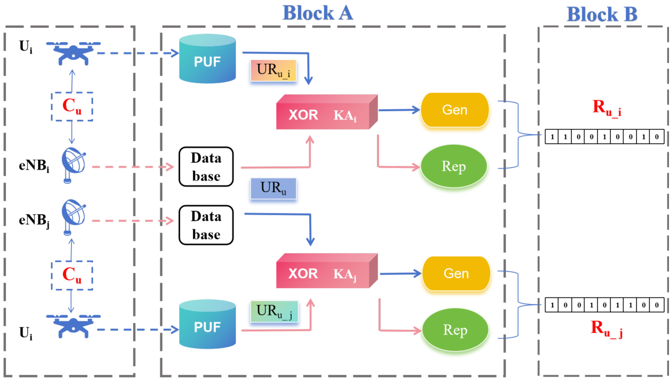

Fig. 3. Approach Overview

A1. Registration: The UAV selects its unique identifier UID_u and generates the pseudo-identity ID_d as ID_d = H(UID_u, n_1), where n_1 is a nonce generated randomly. The pseudo-identity ID_d is then split into two components, KA and KB, such that ID_d = KA xor KB, where KA and KB are randomly generated bit strings. Subsequently, U generates the challenge-response pair (CRP), deriving the secret response UR_u from the challenge C_u, such that UR_u = Puf(C_u). U sends the UID_u, ID_d along with the preprocessed response UR_u to the eNB for registration and storage. U also stores its pseudo-identity and the challenge C_u in its database. Finally, eNB counts the data types $Type = [t1, t2.....tm]$ and the flight plan fpd, through a secure channel to U and stores them in both databases.

A2. Mutual Authentication: Step 1: U $\rightarrow$ eNB$_i$: U uses PUF, UR_u = Puf(C_u), to generate UR_u. In order to implement a method that supports identity authentication for multi-domain IoD in the protocol, we preprocess the secret information UR_u, RES_u = UR_u xor KA. And use a fuzzy extractor to generate an auxiliary string P to resist the influence of noise. (R_u,P) = Gen(RES_u). Subsequently, ID_d was secretly divided into KA and KB. Encrypt the auxiliary string P using the decomposed information KA, K = KA xor P, to prevent sensitive information from being leaked to the adversary during transmission. U selects a random value dn and generates the information M_1. M_1 facilitates the secret transmission of the random number d_n. To declare the integrity of the information, the authentication code Q_1 is calculated based on the random number d_n, pseudonym ID_d, response R_u, auxiliary string P, and flight plan fpd. Finally, U sends Message1 = $\{ID_d, M_1, Q_1, K\}$ to eNB$_i$.

Step 2: eNB$_i$ $\rightarrow$ U : When eNB_i receives Message1, it traverses the database to find the fpd corresponding to ID_d and checks whether access to the region is required. If not, the session is terminated; otherwise, it continues with the subsequent operations. eNB$_i$ performs a decryption operation on the auxiliary string P. Subsequently, the fuzzy extractor is utilized to reproduce the final response R_u and decrypt d_n. The value of the message authentication code $Q_1^{'}$ is calculated on the basis of the known information. If it matches the received Q_1, it indicates that eNB$_i$ has successfully verified the legitimacy of U as well as the integrity of the message, and if it does not match, the authentication process is aborted. eNB$_i$ generates the random number gs_n and produces the message M_2. M_2 facilitates the secret transmission of the random number gs_n to U and confirms its legitimacy to U. To guarantee the correct delivery of the messages, the message authentication code Q_2 is computed based on secret information. Finally, SK can be computed. eNB$_i$ sends the Message2 = $\{M_2, Q_2\}$ to U.

Step 3: U $\rightarrow$ eNB$_i$: When U receives message M_2, gs_n can be decrypted. The authentication code $Q_2^{'}$ is calculated to verify the legitimate identity of eNB$_i$. If the calculated $Q_2^{'}$ matches the received Q_2, the mutual authentication between U and eNB$_i$ is complete. Subsequently, the transmitted information is used to generate SK and compute the temporary identification $ID_d^{'}$ of the U for the new session. The message authentication code Q_3 is calculated based on secret information. And U sends the Message3 = $\{Q_3\}$ to eNB$_i$.

Step 4: eNB$_i$ $\rightarrow$ U : When eNB$_i$ receives M_3, the new pseudonym $ID_d^{'}$ of U is calculated to verify the message authentication code $Q_3^{'}$. If $Q_3^{'}$ matches the received Q_3, a pseudonym update operation is performed to store the SK in the database and update the pseudonym $ID_d^{'}$.

In addition, a PUF application to realize authentication in a multi-domain environment is also proposed in LAPW-DC. Fig. 3 shows the UAV U authenticates with two base stations eNB$_i$ and eNB$_j$ in two different domains. We have shortened the data length. Data processing as in block A is set up so that even if the same response C_u is chosen in two different domains,it still generates different secret values with randomization as shown in block B and R_u is used as response value for the generation of the secure session key. We have shortened the length of the data.

B. Mutual authentication between UAVs

We will briefly describe the mutual authentication process as shown in Fig. 4.

Step 1: U$_1$$\rightarrow$ eNB : In phase A2, a secure communication key SK_1 is established between UAV U$_1$ and eNB, and subsequently U$_1$ sends a request to eNB to establish a secure session with another UAV U$_2$.

Step 2: eNB $\rightarrow$U$_2$: The eNB_i recognizes the UAV U$_2$ referred to by U$_1$ and forwards an authentication request

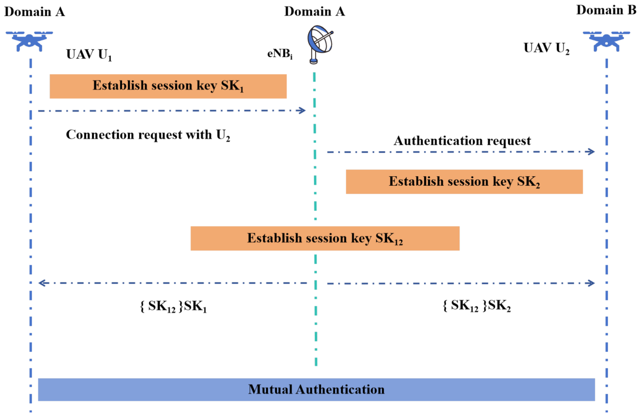

Fig. 4. Mutual Authentication between UAV U$_1$ and U$_2$

Req, H($Req||tx||ID_{d2}$) containing the Req string and a hash computed to contain the data type tx to the UAV U$_2$. The U$_2$ verifies the hash and initiates mutual authentication of the U$_2$ - eNB$_i$ as described in phase B to generate the SK_2 to establishment of communication.

Step 3: eNB $\rightarrow$U$_1$ eNB $\rightarrow$U$_2$: The eNB generates a new secret session key SK_{12}, the SK_{12} secure session key is set to SK_{12} = H($SK_1||SK_2||tx$), and encrypts SK_{12} using the session keys SK_1 and SK_2 and assigns it to U$_1$ and U$_2$, respectively. After these steps, both UAVs obtain the session key SK_{12}, and thus successfully establishing a secure communication session between U$_1$ and U$_2$.

IV. Security Evaluation

The correctness of the LAPW-DC protocol is formally verified using BAN logic, a widely adopted model for analyzing the security of authentication protocols. Furthermore, the protocol is rigorously evaluated against a range of common attacks, and its ability to achieve essential security goals is demonstrated. The analysis confirms that LAPW-DC provides effective protection for secure communications.

A. Logic Correctness Proof

In this section, BAN logic is employed to verify that the communicating entities can achieve mutual authentication and securely establish the session key (SK). The notations and inference rules used in the BAN logic analysis are summarized in Table II.

Message 1: $U \rightarrow \text{eNB} : ID_d, M_1, K, Q1 : \langle d_n, P\rangle R_u$
Message 2: $\text{eNB} \rightarrow U : M_2, Q_2 : \langle gs_n, d_n\rangle R_u, KB$
Message 3: $U \rightarrow \text{eNB} : Q_3 : \langle ID_d, gs_n\rangle R_u$

The message of the protocol is now idealized as follows:
$A1$: eNB $|\equiv U \overset{\text{Ru}}{\leftrightarrow} \text{eNB}$ $A2$: eNB $|\equiv \#d_n$
$A3$: U $|\equiv \text{eNB} \overset{\text{Ru}}{\leftrightarrow} U$ $A4$: U $|\equiv \#gs_n$ $A5$: eNB $|\equiv \#gs_n$

If LAPW-DC can achieve the following goals, then the protocol correctly realizes mutual authentication between U and eNB.

- $G1$: U $|\equiv$ eNB $\overset{\text{SK}}{\leftrightarrow} U$
- $G2$: eNB $|\equiv U \overset{\text{SK}}{\leftrightarrow}$ eNB

Claim 1. U believes that SK is a good secret key between U and eNB.

Message 1: we obtain:

$$\text{eNB} \triangleleft \langle d_n, P_u\rangle R_u \tag{1}$$

The message meaning rule R3 is applied to (1) and A1, and eNB believes that U has said d_n and P_u.

$$\text{eNB} \mid\equiv U \sim \langle d_n, P_u\rangle \tag{2}$$

The random number rule R4 is applied to (2) and A2 to obtain: eNB believes U believes d_n, P_u.

$$\text{eNB} \mid\equiv U \mid\equiv \langle d_n, P_u\rangle \tag{3}$$

The belief rule R8 applied to (3) derive: eNB believes U believes d_n.

$$\text{eNB} \mid\equiv U \mid\equiv \langle d_n\rangle \tag{4}$$

Message 2: we obtain:

$$U \triangleleft \langle gs_n, d_n, KB\rangle R_u \tag{5}$$

Following the reasoning of (2), (3), and (4) above, the message meaning rule R3, random number rule R4, and belief rule R8 are applied to equations (5), A3 and A4, resulting in: U believes eNB believes d_n gs_n.

$$U \mid\equiv \text{eNB} \mid\equiv \langle \text{gs}_n, d_n\rangle \tag{6}$$

From A4, applying the random number rule R15, SK=H((R_u xor KA xor d_n) || (KB xor gs_n xor UID_u)): U believes that SK is fresh.

$$U \mid\equiv \#SK \tag{7}$$

The session key rule is applied to (6) and (7) to obtain the target G1:

$$U \mid\equiv \text{eNB} \overset{\text{SK}}{\leftrightarrow} U \tag{8}$$

Claim 2. eNB believes that SK is a good secret key between U and eNB.

Message 3: we obtain:

$$\text{eNB} \triangleleft \langle ID_d, gs_n\rangle R_u \tag{9}$$

Following the reasoning in (2), (3), and (4) above, the message meaning rule R3, random number rule R4, and belief rule R8 are applied to (9), A1, and A5, resulting in eNB believing U believing gs_n.

$$\text{eNB} \mid\equiv U \mid\equiv gs_n \tag{10}$$

The belief rule R6 is applied to (4) and (10) to obtain eNB belief U belief gs_n, d_n.

$$\text{eNB} \mid\equiv U \mid\equiv \langle gs_n, d_n\rangle \tag{11}$$

According to A5, the application of belief rules R15, SK=H((R_u xor KA xor d_n) || (KB xor gs_n xor UID_u)), eNB believes that SK is fresh.

$$\text{eNB} \mid\equiv \#SK \tag{12}$$

The session key rule is applied to (11) and (12) to obtain the target G2.

$$\text{eNB} \mid\equiv U \overset{\text{SK}}{\leftrightarrow} \text{eNB} \tag{13}$$

From equations (8) and (13), it can be seen that LAPW-DC meets the security objectives, and both the UAV U and the eNB believe that they share a fresh session key SK with each other.

TABLE II
COMMON SYMBOLS AND RULES OF BAN LOGIC

Symbols	Definition	Symbols	Definition	Symbols	Definition
$P \mid\equiv X$	P believes in X	$\langle X\rangle Y$	Linkage between X and Y	$\frac{P\mid\equiv\#X, P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$	R4,Random Number Rules
$P \triangleleft X$	P received X	$\{X\}Y$	K encryption X	$\frac{P\mid\equiv X, P\mid\equiv Y}{P\mid\equiv (X,Y)}$	R6,Rules of Faith
$P \mid\sim X$	P once said X	$P \overset{X}{\leftrightarrow} Q$	X is the secret shared by P and Q	$\frac{P\mid\equiv Q\mid\equiv (X,Y)}{P\mid\equiv Q\mid\equiv X}$	R8,Rules of Faith
$\#(X)$	X is fresh	$\frac{P\mid\equiv Q\overset{K}{\leftrightarrow}P, P\triangleleft\{X\}K}{P\mid\equiv Q\mid\sim X}$	R1,Message Secrecy Rules	$\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$	R15,News Freshness Rules
$P \overset{K}{\leftrightarrow} Q$	K is the shared key between P and Q	$\frac{P\mid\equiv Q\overset{Y}{\leftrightarrow}P, P\triangleleft\{X\}Y}{P\mid\equiv Q\mid\sim X}$	R3,Deduction of Message Confidentiality Rules	$\frac{P\mid\equiv\#K, P\mid\equiv Q\mid\equiv X}{P\mid\equiv Q\overset{K}{\leftrightarrow}P}$	Session Key Rules, X is the parameter

B. Qualitative Security Analysis

This section explains the security features and attack resistance capabilities of the proposed solution, as well as a detailed examination of the proposed security features(SF).

SF1.Resistance to known attacks

In LAPW-DC, an adversary cannot impersonate a UAV, as it lacks the CRP stored in the UAV's memory. Similarly, it cannot masquerade as GS without access to the secret value UR_u stored in the GS database. As a result, masquerade and MITM attacks are effectively mitigated. Furthermore, even if a UAV is physically captured, any tampering attempt would alter the inherent characteristics of its PUF, rendering it inoperable. So node tampering attacks and cloning attacks cannot be successfully carried out. For replay attacks, as the new pseudonym will be used for a new authentication session, the adversary cannot access this new information, so our protocol is also secure against replay attacks. Since the new pseudonym will be used for a new authentication session, the adversary cannot access this new information, so our protocol is also secure against replay attacks.

SF2.No clock synchronization

We use random numbers to ensure the freshness of messages. LAPW-DC does not suffer from time delay and clock synchronization. Therefore the proposed protocol avoids these problems.

SF3.Mutual authentication

The final response R_u is combined with securely encrypted information d_n, gs_n, and shared information KA, KB between the UAV and the GS to generate SK. If opponent A wants to disguise as a legitimate UAV, A must have a legitimate value R_u and secret information KA, KB. Even if opponent A physically captures the UAV, they cannot obtain the correct R_u to calculate the SK. Similarly, the UAV verifies that the GS has confirmed Q_2, and A cannot calculate these values. Therefore, mutual authentication can only be done between the UAV and the GS.

SF4.Forward secrecy and backward secrecy

In LAPW-DC, if the adversary A breaks the current session key SK, A also cannot obtain the information R_u for the next session. A will not even be able to track the UAV, much less jeopardize any future session. Also, A can't infer any of the required secret information used to generate the previous session key based on the information from the current session, since this secret information has different values in different sessions. LAPW-DC guarantees complete forward-backward secrecy.

SF5.Ephemeral Secrets Leakage attack(ESL)

In LAPW-DC, SK is used for the authentication phase, which includes long-term and short-term secrets. Therefore, to break the SK, adversary A must know both the long-term secret and the short-term secret. Therefore, our solution LAPW-DC can resist ESL attacks.

SF6.Addressing De-Synchronization Attacks

After the UAV-GSs authentication phase, it will send a confirmation string Ack and a hash of Ack calculated as H(Ack$||gs_n||d_n$) to the UAV. If it is not satisfied, then U assumes that GS has not received the Message3 and sends it to GS repeatedly. After several attempts, if the UAV still does not receive any message, it will not update the temporary identity ID_d and discards the auxiliary message $UR_u^{'}$ sent to GS. This will lead to the same result as discussed above even if Message3 is blocked or not received by the GS due to other circumstances. If GS receives the Message3, it updates the temporary identifier $ID_d^{'}$ and its database. It will also retain temporary identity ID_d. When the UAV initiates authentication again, the GS will receive the ID_d or $ID_d^{'}$ to determine whether the U has updated its temporary identification. If $ID_d^{'}$ is received, GS will delete ID_d, and if $ID_d^{'}$ is received, GS will delete $ID_d^{'}$. The above setup effectively solves the de-synchronization attack and ensures the availability of the system when Message3 is not received by GS. This mechanism prevents de-synchronization and ensures system availability.

SF7.Authentication mechanisms for multi-domain IoD

In the protocol LAPW-DC, the cryptographic of random numbers d_n and gs_n makes its confidentiality proved. And we achieve the goal of applying PUF for authentication in multi-domain environment by using fuzzy extractors in combination with secret messages, so that each session use different Ru. Thus, our scheme is able to support mutual authentication under multiple GSs control areas.

SF8.Suitable for specific task types

LAPW-DC ensures security and continuity when exchanging data between UAVs by establishing security keys for specific mission types during mutual UAV authentication. By establishing a different SK for each data type, all types of data are prevented from being accessed maliciously all by partial secret disclosure.

C. Comparison of Security Features

This section aims to demonstrate the comparison of security features between the proposed LAPW-DC scheme and the competing scheme [2]–[9]. Table III presents a comparison of the standards discussed in section B.

V. PERFORMANCE EVALUATION

A. Experiment Design

In order to implement LAPW-DC and compare it with existing authentication schemes, performance evaluations were conducted on Intel (R) Core (TM) i5-1135G7 CPU, 2.40GHz, 16GB RAM, Windows 11 system for servers. Referring to

TABLE III
COMPARISON OF SECURITY FEATURES

Scheme	SF1	SF2	SF3	SF4	SF5	SF6	SF7	SF8
SecAuth [2]	Y	Y	Y	Y	Y	Y	N	N
SLAP [3]	Y	Y	Y	Y	N	Y	N	N
BADLA [4]	N	Y	Y	Y	Y	Y	N	N
RAMP [5]	Y	N	Y	Y	Y	N	N	N
ACPBS [6]	Y	Y	Y	Y	Y	N	N	N
HOOPE [7]	Y	Y	Y	Y	Y	Y	N	N
RPMAP [8]	Y	Y	Y	Y	Y	N	Y	N
LAAKA [9]	Y	N	Y	Y	N	Y	N	Y
LAPW-DC	Y	Y	Y	Y	Y	Y	Y	Y

TABLE IV
SYSTEM PARAMETERS

Parameter	Value
Horizontal area	1500 m x 1500 m
Hover height	$h = 1000$ m
Speed of transmission	$c = 3 \times 10^8$ m/s
System bandwidth	10 MHz UL, 20 MHz DL
Number of UAV	$\{10, 20 \ldots\}$

TABLE V
COMPARISON OF COMPUTATIONAL COSTS

Scheme	UAV	GS	Time(ms)
RPMA[8]	$5T_h$+T_{puf}+T_g+T_e	$5T_h$+T_r+T_e	0.4462
LAAKA[9]	$13T_h$+$2T_{puf}$	$11T_h$	0.3896
LAPW-DC	$5T_h$+T_{puf}+T_g	$5T_h$+T_r	0.1814

TABLE VI
COMPARISON OF MESSAGE SIZE

Scheme	Message exchange	K(bits)
RPMAP[8]	U–^{384}→GS–^{576}→U–^{480}→GS	1440
LAAKA[9]	U–^{832}→GS–^{672}→U–^{992}→GS	2496
LAPW-DC	U–^{640}→GS–^{320}→U–^{160}→GS	1120

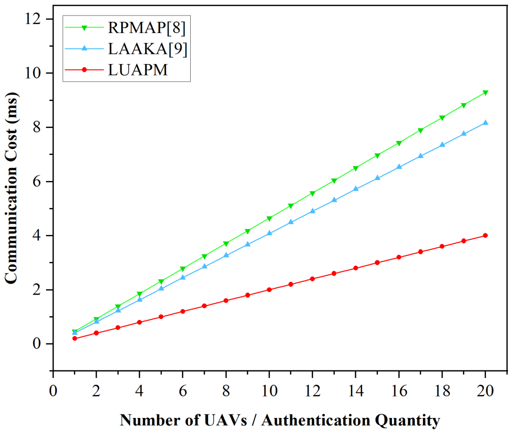

Fig. 5. Comparison of Communication Cost

[11], [12], the parameters used for the simulation setup are shown in Table IV. And various operations and runtimes are as follows.

- Hash computation time:T_h=0.0162ms;
- Time of Gen() in fuzzy extractor: T_g=0.016ms;
- Time of Rep() in the fuzzy extractor: T_r=0.003ms;
- Fuzzy extractor time: T_f=0.019ms;
- The extractor time : T_e=0.1324ms;
- PUF computation time: T_{puf}=0.0004ms;

B. Computation Cost

LAPW-DC is compared with RPMAP [8] and LAAKA [9], which are also dedicated to authentication mechanisms set up in the context of communication areas controlled by multiple GSs. And as shown in Table 6, the computational cost required to set up our protocol is only 0.1814 ms, which is significantly better than others.

C. Communication Cost

We compared the communication cost of the RPMAP [8] and LAAKA [9], and found that the total delay of the link is the sum of the T_p and T_t. In alignment with the approach presented in [12], this study follows the 3GPP model for aerial vehicles in LTE, as specified in Technical Report TR 36.777 [13]. The relevant parameters for calculating the communication cost are shown in Table V.

- Propagation Delay: T_p is the delay incurred by hiUAV-GSs communication to propagate data over a distance d.
$$T_p = \frac{d}{c}$$
- Transmission Delay: T_t is the delay incurred in transmitting K-bit information over the UAV-GSs communication.
$$T_t = \frac{K}{R}$$

To facilitate the computation of the value of K in each protocol, we set the identity, random number, output of the hashing, and timestamp of each entity to 160, 160, 160 and 32 bits, respectively. We used the PUF proposed in literature [6] as well as in literature [8] shown that this PUF can give a 320-bit response R_u when the 32-bit challenge C_u is input. We follow [14] and consider that the public parameter, that is, the auxiliary function, should be set to 160 bits, and that the acceptable error value of PUF should be 8 bits.

When the GS is authenticated with the UAV, the required message size is compared between the LAPW-DC and existing schemes. As shown in Table VI, the communication cost of LAAKA [9] is the highest at 2496 bits, while the communication cost of LAPW-DC is the lowest at 1120 bits.

We perform simulations to model the total time required by the protocols and use it as an evaluation metric, which includes the computational cost and the time cost by the communication. The variation of the simulation modeling results for each protocol with an increasing number of UAVs or authentications is shown in Fig. 5. It is obvious that LAPW-DC has less communication consumption compared to the schemes of RPMAP [8] and LAAKA [9].

D. Comparison of Multi-Domain Authentication Mechanisms

We considered the complexity, time cost, and GS storage cost of PUF's independent usage mechanism for multi-domain IoD. As shown in Table VII, our mechanism is superior to RPMAP [8] and LAAKA [9] in all aspects.

For comparison,we set n=3 as mentioned in [8] and the result is shown in Fig. 6. In our proposed LAPW-DC, the secret information transmitted to GS is the intermediate parameter UR_u of R_u, which strengthens the security and avoids the direct transmission of R_u, the information for generating SK, between GSs in LAAKA [9].

TABLE VII
COMPARATIVE ANALYSIS OF ALGORITHMS FOR MULTI-DOMAIN MECHANISMS

Scheme	Complexity	GS Memory Cost	Time Cost
RPMAP[8]	$O(n+1)-O(2n)$	352n	0.1324 ms
LAAKA[9]	——	352	——
UATM	$O(n)$	320	0.0067 ms

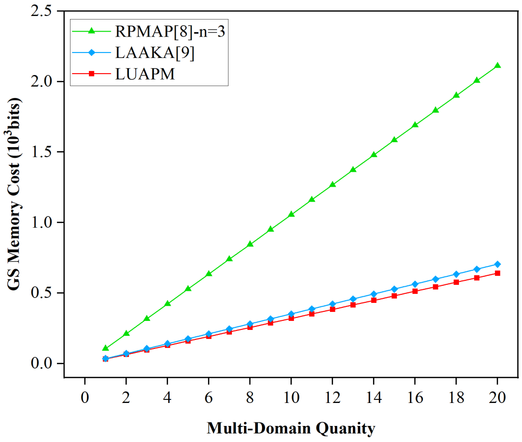

Fig. 6. Comparison of Memory Cost

VI. CONCLUSION

In this paper, we have proposed a lightweight mutual authentication protocol that supports secure UAV-GSs and UAV-UAV communication for wide-range IoD in LTE wireless networks. LAPW-DC not only proposes authentication mechanisms applicable to multi-domain environments but also sets different secure communication keys for different types of data in UAV-UAV sessions. In addition, we conducted security evaluations of the LAPW-DC to verify its high security and generality, and the LAPW-DC is competitive with other existing authentication papers in terms of computation and communication consumption costs. Therefore, we believe that LAPW-DC is a very effective and feasible authentication scheme.

REFERENCES

[1] J. Yao and N. Ansari, “Wireless Power and Energy Harvesting Control in IoD by Deep Reinforcement Learning,” in *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 980-989, June 2021.

[2] T. Alladi, Naren, G. Bansal, V. Chamola and M. Guizani, “SecAuthUAV: A Novel Authentication Scheme for UAV-Ground Station and UAV-UAV Communication,” in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15068-15077, Dec. 2020.

[3] S. Yu, A. K. Das, Y. Park and P. Lorenz, “SLAP-IoD: Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments,” in *IEEE Transactions on Vehicular Technology*, vol. 71, no. 10, pp. 10374-10388, Oct. 2022.

[4] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K.R. Choo, “Blockchain-based crossdomain authentication for intelligent 5G-enabled internet of drones,” *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, 2021.

[5] M. Tanveer, A. U. Khan, N. Kumar and M. M. Hassan, “RAMP-IoD: A Robust Authenticated Key Management Protocol for the Internet of Drones,” in *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 1339-1353, Jan. 15, 2022.

[6] B. Bera, A. K. Das, S. Garg, M. Jalil Piran and M. S. Hossain, “Access Control Protocol for Battlefield Surveillance in Drone-Assisted IoT Environment,” in *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2708-2721, Feb. 15, 2022.

[7] H. Khalid et al., “HOOPOE: High Performance and Efficient Anonymous Handover Authentication Protocol for Flying Out of Zone UAVs,” in *IEEE Transactions on Vehicular Technology*, vol. 72, no. 8, pp. 10906-10920, Aug. 2023.

[8] Tian C., Jiang Q., Li T., et al., “Reliable PUF-based mutual authentication protocol for UAVs towards multi-domain environment,” *Comput. Networks*, 2022.

[9] I. Bhattarai, C. Pu, K.-K. Raymond Choo and D. Korać, “A Lightweight and Anonymous Application-Aware Authentication and Key Agreement Protocol for the Internet of Drones,” in *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19790-19803, June 1, 2024.

[10] 3GPP TS 38.331. *Radio Resource Control (RRC) protocol specification (Release 15)*. 2019.

[11] W. A. Nelson, S. R. Yeduri, A. Jha, A. Kumar and L. R. Cenkeramaddi, “RL-Based Energy-Efficient Data Transmission Over Hybrid BLE/LTE/Wi-Fi/LoRa UAV-Assisted Wireless Network,” in *IEEE/ACM Transactions on Networking*, vol. 32, no. 3, pp. 1951-1966, June 2024.

[12] A. Zaki-Hindi, I. Z. Kovács, R. Amorim and J. Wigard, “Measurement Reporting Enhancement for 5G Cellular-Connected Aerial Vehicles,” in *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Toronto, ON, Canada, 2023, pp. 1-6.

[13] 3GPP TR 36.777 V15.0.0. *Study on Enhanced LTE Support for Aerial Vehicles (Release 15)*. 2017.

[14] Zhang Y., Meng L., Meng Z. W., “A secure and lightweight batch authentication scheme for Internet of Drones environment,” *Vehicular Communications*, 2023.