Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 7107015, 14 pages
https://doi.org/10.1155/2023/7107015

Research Article

A Novel and Efficient Authentication Scheme Based on UAV-UAV Environment

Yuanyuan Zhang, Lingzhe Meng, Jialing Gan, and Zhihao Huang

School of Computers, Hubei University of Technology, Wuhan 430068, China

Correspondence should be addressed to Yuanyuan Zhang; circle0519@hotmail.com

Received 8 October 2022; Revised 4 February 2023; Accepted 6 February 2023; Published 11 May 2023

Academic Editor: Le Kim Hung

Nowadays, unmanned aerial vehicles (UAVs) are used in various fields due to their high maneuverability and low cost of construction and use. With the development of UAV technology, it has become a trend for UAVs to cooperate with each other to complete assigned tasks. Multiple UAVs are combined according to a certain structure, and through the information sharing between them, a cooperative effect is generated to achieve intelligent collaborative task execution. However, information sharing is carried out on a public channel, so ensuring secure communication between UAVs is crucial. Moreover, UAVs are easily captured by an adversary, who can impersonate legitimate UAVs to disrupt communications if UAVs' internal secrets that are stolen. Therefore, we propose a lightweight authentication scheme based on physical unclonable function (PUF), to provide mutual authentication between UAVs. PUF is embedded in the unmanned aerial vehicle (UAV) to defend against physical capture attack. Furthermore, to evaluate the security and performance of our scheme, formal and informal security analyses and formal security verification of the scheme are performed, and the performance of the scheme is compared with existing UAV schemes. The above analyses show that our scheme has great advantages in terms of security and overheads.

1. Introduction

Nowadays, UAV has entered people's sights as a new product. A drone is an unmanned microaircraft, that is, an unmanned aerial vehicle which is operated using radio remote control technology and controls embedded in the drone [1]. UAV has the characteristics of low maintenance cost and wide deployment range, so it has been applied in various fields. In the prevention and control of infectious diseases, the task of spraying disinfectant on contaminated areas can be done by UAVs [2].

With the increasing difficulty and complexity of tasks, a single UAV cannot perform such tasks due to its short flight time, limited storage space, and other limitations. Therefore, the cooperation of multiple UAVs to complete the task has become a new mode to achieve the expansion of UAV mission capability [3]. In this mode, multiple UAVs with autonomous control capabilities form a relatively large UAV group. Information is shared among the UAVs within the group [4], thereby improving the efficiency of task execution and completing the assigned task with high quality. For example, in the field of disaster rescue, when UAVs carry out search and rescue work in mountainous areas, it is easy to block the signal and affect the communication due to the complex environment in these areas. This problem can be avoided by adopting the cooperative mode of multiple UAVs [5], that is, each UAV serves as a communication relay station, and UAVs communicate with each other to achieve information sharing. In addition to disaster rescue, the UAV group is also playing an important role in intelligent mining. The underground multi-UAV cooperation mode has the advantages of strong monitoring ability and wide monitoring range, which can effectively improve the monitoring efficiency. Moreover, the wireless multihop mode will solve the problem of limited communication distance of a single UAV, which is conducive to the transmission of detected information [6].

The mode of cooperative work and information sharing among UAVs provides great convenience for industrial production and social life. However, because the communication between UAVs is carried out on the public channel, the communication process is vulnerable to security threats [6]. These threats include impersonation attack, replay attack, and man-in-the-middle attack [7]. In addition, an adversary can eavesdrop on or tamper with information transmitted on the public channel to disrupt communications. Node authentication, which is divided into information authentication and identification authentication [8], is precisely the way to resist these security threats. Information authentication is to ensure the integrity of the information transmitted between two parties and that the information has not been maliciously tampered with. Identification authentication means that the communication parties verify whether the identity of the other party is authentic and credible, to prevent the adversary from participating in communication by impersonating legitimate entities [8].

In flight, UAVs not only have the above-mentioned security threats but also are prone to physical capture attack. An UAV in the air cannot be constantly monitored by staff, so it could be captured by an adversary who steals the UAV's secrets through power analysis attacks [9] and impersonates the UAV to participate in authentication. In recent years, to resist such attacks, physical unclonable function (PUF) has been embedded in the UAV. This function is a one-way function based on the challenge-response pair mechanism [10]. Inputting a challenge C to the function will calculate a response R, which is $R = \mathrm{PUF}(C)$. The manufacturing process of the PUF in each UAV is the same, but due to the tiny random changes inherent in the manufacturing process, the output of each function is different [11]; that is, PUF is used to make each UAV have its own fingerprint. This fingerprint cannot be cloned, because PUF is unclonable, and it is impossible to make two identical functions [12]. Furthermore, the adversary captures an UAV and enters a challenge into the PUF in the UAV. Since the response calculated by the PUF participates in the authentication as an intermediate value, the adversary still cannot extract the corresponding response. Combining the above advantages, PUF can resist physical capture attack and is suitable for identity authentication and key generation scenarios [13].

In order to resist the attacks easily encountered in the communication process of UAVs and realize the secure communication between UAVs, this paper proposes a lightweight mutual authentication scheme between UAVs based on PUF. The specific contributions of this scheme are described below:

(i) We propose an authentication and key agreement scheme suitable for Internet of drone (IoD) environment, which realizes mutual authentication between two UAVs. After the authentication, two parties discuss a session key. In addition, the introduction of PUF can ensure the physical security of the UAV

(ii) Our scheme is formally security analysis by applying the widely used real-or-random (ROR) model. This model is mainly used to ensure the semantic security of session key. Moreover, an informal security analysis is performed on our scheme which showed that it could withstand several known attacks

(iii) A detailed comparison is made between our scheme and existing related authentication schemes in terms of security, functional characteristics, and overheads. The results show that our scheme is efficient and security

The rest of this paper is roughly organized as follows. The related work related to UAV authentication is given in Section 2. In Section 3, we provide the system and threat models used by our scheme. Section 4 describes the specific steps of our scheme. Formal and informal security analyses and formal security verification of our scheme are shown in Section 5. In Section 6, our scheme is compared with existing similar schemes in terms of performance. Finally, Section 7 makes some important concluding remarks to the whole paper.

2. Related Work

With the diversification of user needs and the growth of the complexity of tasks, the collaborative work of multiple devices has become a reality, and the communication between devices will become more and more frequent [14]. However, communication between devices is subject to some malicious attacks. Therefore, identity authentication between devices is essential.

Semal et al. [15] proposed an IoD-based certificate-authenticated key agreement scheme to ensure identity authenticity and message integrity in UAVs' communication. However, computation overhead of this scheme is high. In order to reduce the overhead of device authentication, Malani et al. [16] proposed a device access control scheme. The scheme uses hash function and elliptic curve cryptography to realize mutual authentication between any two neighboring devices, but it cannot provide device anonymity and resist device impersonation attack. Another access control scheme using elliptic curve encryption and hash function techniques was proposed by Bera et al. [17], which is a lightweight scheme based on IoD environment. Two neighboring UAVs authenticate each other using certificates issued by the control room and negotiate a session key. Then, Chaudhry et al. [18] pointed out that the scheme of Bera et al. cannot provide protection against UAV impersonation attack, replay attack, and man-in-the-middle attack. To address these issues, Chaudhry et al. designed an improved certificate-based authentication scheme that guarantees mutual authentication and key agreement between UAVs. Unfortunately, an adversary can calculate the private key of the control room in the scheme. Armed with a private key, he/she can deploy a malicious UAV in IoD environment and simulate ground station server to communicate with legitimate UAVs [19]. A certificate-supported access control scheme between UAVs proposed by Das et al. [19]

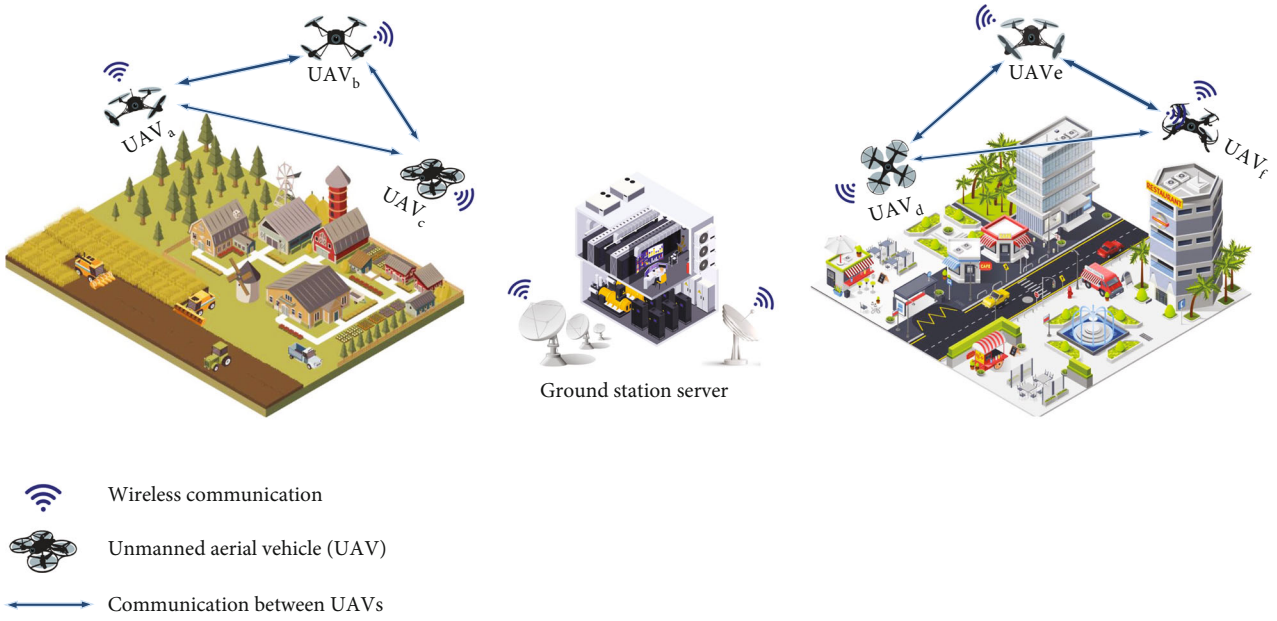

Figure 1: System model.

can solve the loopholes in Chaudhry et al.'s scheme. Das et al.'s scheme supports mutual authentication of UAVs and ensures the anonymity and untraceability of UAVs, but it cannot resist drone capture attack, and the overhead is relatively high. Based on the problem of high authentication overhead, Khan et al. [20] applied lightweight operations such as hyperelliptic curve cryptography and hash function. Their scheme, which enables the authentication of two UAVs and the addition of a new UAV, is superior in performance to several similar schemes above. The authentication scheme under vehicular ad hoc networks proposed by Wang et al. [21] also requires less overhead, because the scheme uses modular exponentiation and sets up a precomputed lookup table in vehicle-to-vehicle authentication to speed up verification.

In recent years, the physical security of device has received increasing attention. The devices in the above authentication schemes are vulnerable to physical capture attack, where an adversary can obtain secrets in the device to disrupt communications. To resist such attack, PUF has been introduced in recent studies. Yıldız et al. [22] used the PUF in a group authentication and key distribution scheme, and the role of the function is to provide a unique key for each device without storing any information on those devices. A lightweight mutual authentication scheme between smart meter node and server was proposed by Harishma et al. [23]. The PUF is embedded in smart meter node to resist physical capture attack and require less secure secret value to be stored on the device. Aiming at the environment of smart home, Xia et al. [24] proposed a group authentication and key agreement protocol based on PUF, which realizes the simultaneous access of multiple devices in smart home by using the Chinese residual theorem and other technologies. The scheme uses PUF to protect secret parameters stored in the memory of smart devices. A lightweight authentication and key establishment scheme (PUF-RAKE) based on PUF were proposed by Qureshi and Munir [25], which reduces resource consumption by applying PUF. Babu et al. [26] provided a new lightweight authentication protocol, which implements mutual authentication and session key negotiation between electric vehicle and charging system. In addition, the proposed protocol uses PUF to enhance the physical security of the device.

We use similar PUF in our IoD authentication scheme to ensure the physical security of the UAV that an adversary cannot simulate a legitimate UAV even if he/she captures this UAV. In our scheme, PUF is embedded in the UAV, and mutual authentication between UAVs is realized.

3. System and Threat Models

This section presents the system and threat models required for our scheme, which explain the workflow and applicability of the scheme.

3.1. System Model. The system model of the proposed authentication scheme between UAVs is shown in Figure 1. Under this model, there are two entities, which are the UAVs deployed to the IoD environment and the ground station server. The ground station server provides registration service for each UAV and generates parameters needed for authentication. UAVs equipped with sensors and communication facilities are registered on the ground station server and assigned to perform missions in urban, rural, or mountainous locations. Related drones in the same area can monitor data around the flight environment and can use the discovery function to connect with surrounding UAVs [20]. In this area, an UAV and a nearby UAV conduct mutual authentication and negotiate a session key. The two UAVs then use the key to communicate securely, enabling both parties to share information and complete specified tasks with high quality and efficiency.

Table 1: Symbols and their significance.

Symbols	Significance
DR_i, D_i	ith drone and its identity, respectively
$PUF_i(\cdot)$	Physical unclonable function (PUF) of DR_i
$(C_i, R)_i$	PUF challenge response pair of DR_i
GSS, SID	Ground station server and its identity, respectively
q	A large prime number
$E_q(a, b), U$	Elliptic curve and a base point over $E_q(a, b)$, respectively
s, P_{pub}	Private and public key of GSS, respectively
SK	Session key
$h_1(\cdot), h_2(\cdot)$	Collision-resistant one-way hash functions
$\oplus$	Bitwise XOR operation
$\|\|$	Concatenation operation

3.2. Threat Model. During the authentication process, one UAV communicates with another UAV over a public channel. According to the widely used Dolev–Yao (DY) threat model [27], this channel is wireless and insecure. An adversary can steal the messages exchanged between two parties, modify or delete them, and replay them to legitimate entities. The model also assumes that the communication parties are untrusted, and the adversary can simulate legitimate entities to participate in the communication.

The adversary also has the ability to know all the public parameters but not enough ability to know the private key of the ground station server. In addition, an UAV may be unmonitored while in the air, so the adversary can capture the UAV and use power analysis attacks [9] to gain access to its internal storage secrets.

4. Proposed Authentication Scheme

This section presents the proposed authentication and key agreement scheme. The scheme is composed of following four steps, i.e., setup phase, UAV registration phase, UAV-UAV authentication phase, and dynamic UAV addition phase. The symbols that appear in Table 1 are used to describe our scheme. Before describing, we first provide a brief introduction to elliptic curve cryptography, as it is one of the key techniques of the scheme.

We introduce an elliptic curve over a finite field $GF(q)$, where q is a large prime number representing the number of elements in $GF(q)$. The elliptic curve $E_q(a, b)$ is defined by the equation $y^2 = x^3 + ax + b \pmod q$, where the equation satisfies the conditions $a, b \in GF(q)$ and $\Delta = 4a^3 + 27b^2 \neq 0 \pmod q$, respectively [28]. A point O at infinity on $E_q(a, b)$, together with all the other points on $E_q(a, b)$, form a set $G = \{(x, y): x, y \in GF(q) | y^2 - x^3 - ax - b = 0\} \cup \{O\}$. It is easy to compute the point $Q = s \cdot U$ if you set the base point U on $E_q(a, b)$ and an integer s, but it is computationally difficult to find s from Q and U [29]. Calculating this point Q is equivalent to adding up multiple points U, as shown by this formula $Q = s \cdot U = U + U + \cdots + U$ (s times).

4.1. Assumptions. According to [6, 30], we indicate some assumptions required in our scheme, as shown below.

(i) The private key of the ground station server is assumed to be secure, and an adversary cannot obtain the key

(ii) Each legal UAV has a unique PUF embedded in it. The adversary capturing an UAV and tampering with its PUF will destroy the PUF [10], not get the expected response value, and fail to pass the authentication. Furthermore, the PUF used in our scheme is ideal

4.2. Setup Phase. The setup phase is done by the ground station server GSS. At this phase, GSS generates the parameters required by the system.

S1. GSS chooses an elliptic curve $E_q(a, b)$ over a finite field $GF(q)$ and a base point U over $E_q(a, b)$. It then selects $s \in Z_q^*$ as its own private key and computes its own public key $P_{pub} = s \cdot U$

S2. GSS chooses its own identity SID and two hash functions $h_1(\cdot): \{0, 1\}^* \longrightarrow Z_q^*$ and $h_2(\cdot): \{0, 1\}^* \longrightarrow \{0, 1\}^n$, where $h_1(\cdot)$ maps a string of arbitrary length to an integer, and $h_2(\cdot)$ maps a string of arbitrary length to a string of fixed length

S3. In the end, GSS keeps the private key s and identity SID and publishes $\{E_q(a, b), q, U, P_{pub}, h_1(\cdot), h_2(\cdot)\}$ as the system public parameters

4.3. UAV Registration Phase. During this phase, the ground station server GSS is responsible for the registration of each UAV. Suppose there are a total of σ UAVs, these UAVs are registered on GSS. After registration, they are deployed to the target area to perform tasks. The following are the detailed steps of UAV registration phase.

R1. For each UAV $DR_i (i = 1, \cdots, \sigma)$, GSS selects a random number $d_i \in Z_q^*$ for DR_i, and computes DR_i's identity $D_i = d_i \cdot U = (D_i^x, D_i^y)$, where D_i^x and D_i^y are the abscissa and ordinate of the point D_i, respectively. GSS further calculates $F_i = d_i + s \cdot h_1(SID || D_i^x) \bmod q$ using its own private key s. Then, GSS sends D_i, F_i, and its identity SID to DR_i through a secure channel

R2. After receiving the information from GSS, DR_i generates a challenge C_i, which is the input of the PUF_i embedded in DR_i, and obtains the corresponding response $R_i = PUF_i(C_i)$. Further, DR_i calculates $G_i = F_i \oplus h_2(R_i || D_i^y)$. Finally, it stores $\{D_i, G_i, C_i, SID\}$ in its own memory

Now each DR_i is ready for deployment. The UAV registration phase is briefed in Figure 2.

4.4. UAV-UAV Authentication Phase. Suppose there are two adjacent UAVs, called $DR_\alpha (1 \leq \alpha \leq \sigma)$ and $DR_\beta (1 \leq \beta \leq \sigma, \alpha \neq \beta)$. To ensure secure communication between the two UAVs, they need to authenticate each other and establish a session key for future communication after successful

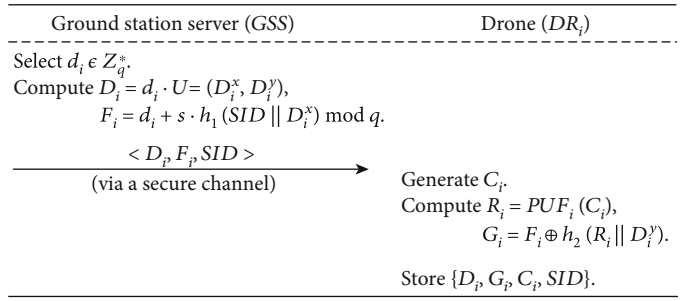

Figure 2: UAV registration phase.

authentication. Figure 3 shows the calculation operations performed and various information exchanged by DR_α and DR_β during the authentication process. The two UAVs perform the following steps for mutual authentication and key agreement.

A1. DR_α takes the challenge C_α stored in the memory as the input of the PUF_α and gets the corresponding response $R_\alpha = PUF_\alpha(C_\alpha)$. Then, it computes $F_\alpha = G_\alpha \oplus h_2(R_\alpha \| D_\alpha^y)$. D R_α creates a random number $k_\alpha \in Z_q^*$ and calculates $K_\alpha = k_\alpha \cdot U = (K_\alpha^x, K_\alpha^y)$, where K_α^x and K_α^y are the abscissa and ordinate of K_α. Further, it computes $J_\alpha = F_\alpha + k_\alpha \bmod q$

A2. DR_α dispatches the message $M_1 = <D_\alpha, K_\alpha, J_\alpha>$ to DR_β over a public channel

A3. After receiving M_1 from DR_α, DR_β firstly checks whether the formula $J_\alpha \cdot U = D_\alpha + P_{pub} \cdot h_1(SID \| D_\alpha^x) + K_\alpha$ holds. Note that

$$\begin{aligned} J_\alpha \cdot U &= (F_\alpha + k_\alpha) \cdot U = d_\alpha \cdot U + s \cdot U \cdot h_1(\mathrm{SID} \| D_\alpha^x) + k_\alpha \cdot U \\ &= D_\alpha + P_{pub} \cdot h_1(\mathrm{SID} \| D_\alpha^x) + K_\alpha. \end{aligned} \tag{1}$$

If it fails, DR_β rejects the authentication request. Otherwise, DR_β performs the step A4.

A4. DR_β inputs the challenge C_β into the PUF_β, and the function outputs the corresponding response $R_\beta = PUF_\beta(C_\beta)$. Then, DR_β computes $F_\beta = G_\beta \oplus h_2(R_\beta \| D_\beta^y)$, creates a random number $k_\beta \in Z_q^*$, and calculates $K_\beta = k_\beta \cdot U = (K_\beta^x, K_\beta^y)$, where K_β^x and K_β^y are the abscissa and ordinate of K_β. Finally, it calculates $J_\beta = F_\beta + k_\beta \bmod q$ and $L = J_\beta \oplus h_2(K_\alpha^x \| K_\alpha^y \| D_\alpha^x \| D_\beta^x)$

A5. DR_β transmits the message $M_2 = <D_\beta, K_\beta, L>$ to DR_α via an open channel

A6. On receiving M_2, DR_α computes $J_\beta = L \oplus h_2(K_\alpha^x \| K_\alpha^y \| D_\alpha^x \| D_\beta^x)$ and checks whether DR_β's identity is authentic by verifying $J_\beta \cdot U = D_\beta + P_{pub} \cdot h_1(\mathrm{SID} \| D_\beta^x) + K_\beta$. Note that

$$\begin{aligned} J_\beta \cdot U &= \left(F_\beta + k_\beta\right) \cdot U = d_\beta \cdot U + s \cdot U \cdot h_1\left(\mathrm{SID} \| D_\beta^x\right) + k_\beta \cdot U \\ &= D_\beta + P_{pub} \cdot h_1\left(\mathrm{SID} \| D_\beta^x\right) + K_\beta. \end{aligned} \tag{2}$$

If the verification is successful, DR_β passes the authentication of DR_α, and DR_α continues to the next step A7. Otherwise, this phase is terminated.

A7. DR_α computes $V = k_\alpha \cdot K_\beta = (V^x, V^y)$, where V^x and V^y are the abscissa and ordinate of V. It also calculates the session key $SK = h_2(V^x \| V^y \| D_\alpha^y \| D_\beta^y)$ and $W = h_2(SK \| K_\beta^x \| K_\beta^y \| D_\beta^x \| D_\beta^y)$

A8. DR_α sends the message $M_3 = <W>$ to DR_β through a public channel

A9. When DR_β receives M_3 from DR_α, it evaluates $V = k_\beta \cdot K_\alpha = (V^x, V^y)$ and $SK' = h_2(V^x \| V^y \| D_\alpha^y \| D_\beta^y)$ to verify that the formula $W = h_2(SK' \| K_\beta^x \| K_\beta^y \| D_\beta^x \| D_\beta^y)$ is equal. If the formula does not hold, DR_β terminates this authentication process. Otherwise, DR_β uses SK' as the current session key

In the end, DR_β stores the session key SK' for future communication with DR_α. Likewise, DR_α stores this key $SK(= SK')$ for communicating and sharing information with DR_β.

4.5. Dynamic UAV Addition Phase. The proposed scheme has the function of adding new UAVs to the network. Assuming that there is a new UAV DR_i^{new} to be deployed in the IoD environment, the UAV needs to perform the following steps to complete the registration on the ground station server GSS. In addition, messages are transmitted over a secure channel during the process.

U1. GSS chooses a random number $d_i^{new} \in Z_q^*$ for DR_i^{new} and computes DR_i^{new}'s identity $D_i^{new} = d_i^{new} \cdot U = (D_i^{x^{new}}, D_i^{y^{new}})$, where $D_i^{x^{new}}$ and $D_i^{y^{new}}$ are the abscissa and ordinate of the point D_i^{new}, respectively. Then, GSS calculates $F_i^{new} = d_i^{new} + s \cdot h_1(\mathrm{SID} \| D_i^{x^{new}}) \bmod q$. Finally, GSS transmits the messages D_i^{new}, F_i^{new}, and its identity SID to DR_i^{new}

U2. When receiving the messages from GSS, DR_i^{new} generates a challenge C_i^{new}. This challenge serves as the input value to the PUF_i^{new}, and the PUF_i^{new} outputs the response $R_i^{new} = PUF_i^{new}(C_i^{new})$. Furthermore, DR_i^{new} computes $G_i^{new} = F_i^{new} \oplus h_2(R_i^{new} \| D_i^{y^{new}})$. Finally, it stores $\{D_i^{new}, G_i^{new}, C_i^{new}, \mathrm{SID}\}$ in its own memory

The dynamic UAV adding process is shown in Figure 4. After the addition process is completed, the new UAV D R_i^{new} is deployed to the IoD environment, where it can

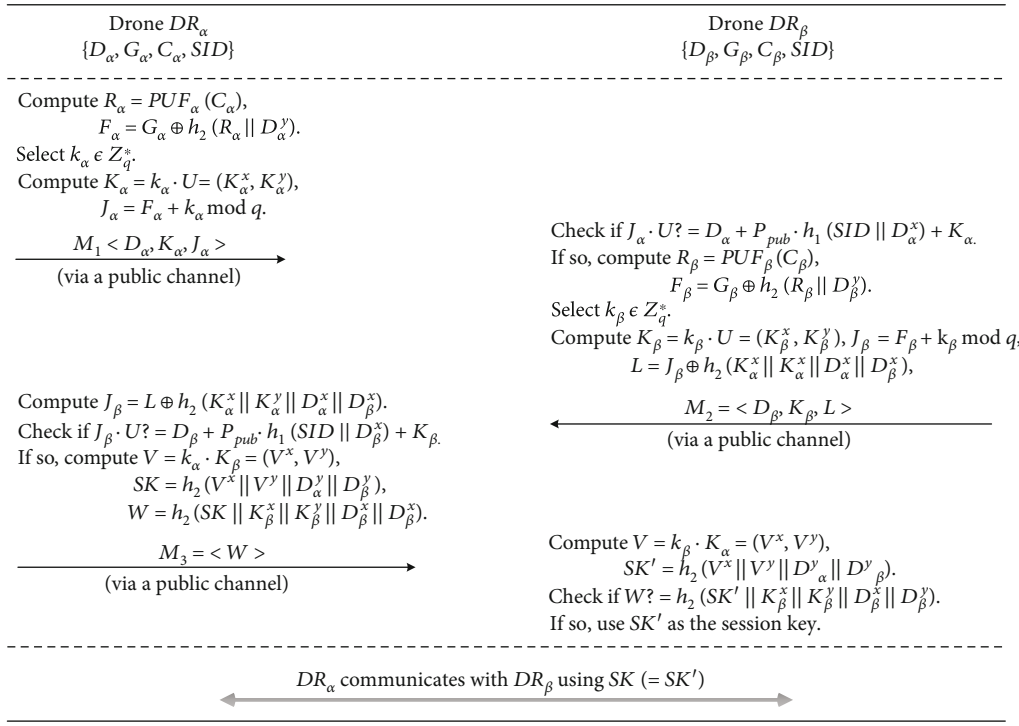

Figure 3: UAV-UAV authentication phase.

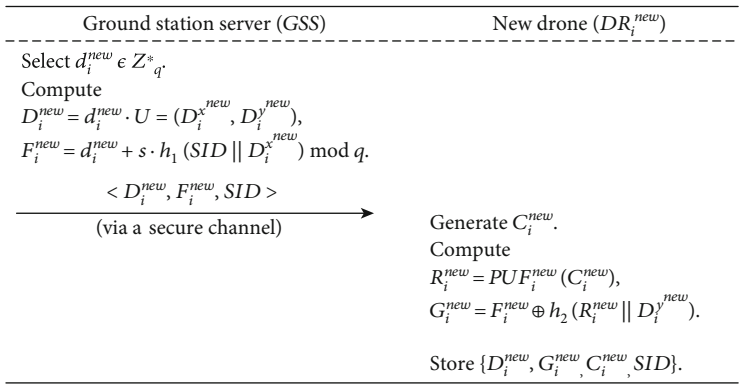

Figure 4: Dynamic UAV addition phase.

perform the steps in Section 4 for mutual authentication with surrounding UAVs.

5. Security Analysis

This section presents security analyses that we perform on the proposed scheme. First, the widely applied real-or-random (ROR) model [31] is used for formal security analysis of our scheme. Then, the informal security analysis of our scheme is given. Finally, Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [32] is used for formal security verification. Through these analyses, we conclude that the scheme is secure.

5.1. Formal Security Analysis Using ROR Model. The ROR model is applied in a formal security analysis to demonstrate the security of the session key (SK) of our authentication and key agreement (AKE) scheme.

Under the ROR model, an adversary A interacts with the l th instance of a participant, say P^l. There are two participants in our scheme, namely, the UAV DR_α and the UAV DR_β. Both entities are involved in mutual authentication and key agreement. $P^l_{DR_\alpha}$ and $P^j_{DR_\beta}$ represent the lth instance of DR_α and the jth instance of DR_β, respectively. Furthermore, in this proof, we model collision-resistant cryptographic one-way hash functions $h_1(\cdot)$ and $h_2(\cdot)$ and an ideal PUF function as random oracles, called $Hash_1$, $Hash_2$, and PUF, respectively. All participants including A have access to both hash functions and PUF.

The ROR model uses the elements shown below to perform [33]:

(i) *Execute*($P^l_{DR_\alpha}$, $P^j_{DR_\beta}$): it is modeled as an eavesdropping attack, and through this query, A can obtain

messages (M_1, M_2, and M_3) exchanged between $P^l_{DR_\alpha}$ and $P^j_{DR_\beta}$

(ii) *Send(* P^l, Msg*)*: it is modeled as an active attack. A executes this query, sends the message Msg to the instance P^l, and then receives a reply message based on Msg

(iii) *Reveal (*$P^l_{DR_\alpha}$ / $P^j_{DR_\beta}$*)*: through this query, A is able to obtain the current session key SK established between $P^l_{\mathrm{DR}_\alpha}$ (or $P^j_{\mathrm{DR}_\beta}$) and its associated participants

(iv) *Freshness*: the instance $P^l_{\mathrm{DR}_\alpha}$ or $P^j_{\mathrm{DR}_\beta}$ is fresh, if A does not use the Reveal($P^l_{\mathrm{DR}_\alpha}/P^j_{\mathrm{DR}_\beta}$) query to obtain the session key between two instances [34]

(v) Test($P^l_{\mathrm{DR}_\alpha}/P^j_{\mathrm{DR}_\beta}$): A executes a Test query for the instance $P^l_{\mathrm{DR}_\alpha}$ (or $P^j_{\mathrm{DR}_\beta}$)'s session key SK. Then, an unbiased coin $c \in \{0, 1\}$ is thrown, if SK has been established and is fresh: (1) $c = 1$, A will receive the session key SK; (2) $c = 0$, A will receive a random number with the same length as SK. Otherwise, A will receive null ($\perp$). Moreover, for an instance, A can only execute the Test query once [35]

In the following, we give definitions of elliptic curve decisional Diffie-Hellman problem (ECDDHP) and the semantic security of session key, as well as the assumption of PUF unclonability required in the proof.

Definition 1 (ECDDHP). Let $E_q(a, b)$: $y^2 = x^3 + ax + b \bmod (q)$ be an elliptic curve over a finite field GF(q), and T is a base point on $E_q(a, b)$. The ECDDHP is to give a quadruple $(T, x_1 \cdot T, x_2 \cdot T, x_3 \cdot T)$ and determine whether $x_3 = x_1 * x_2$ or x_3 is a uniform random value, where $x_1, x_2, x_3 \in Z^*_q$.

Definition 2 (Semantic security of session key). Under the ROR model, A needs to distinguish whether a value is the instance's session key or a random number. In addition, the adversary can perform multiple Test queries on multiple UAV instances. At the end of the game, A has to return a guessed bit c'. If the condition $c' = c$ is met, then, he/she wins the game. We represent SUCC as the event in which A wins a game. A's advantage of winning this game in polynomial time t becomes $\mathrm{Adv}^{\mathrm{AKE}}_\delta(t) = |2 \Pr[\mathrm{SUCC}] - 1|$, where δ represents our scheme. We say that in the ROR model, if this condition $\mathrm{Adv}^{\mathrm{AKE}}_\delta(t) \le \mu$ is satisfied, where $\mu > 0$ is a sufficiently small real number, and then, δ is semantic security [34].

Assumption (PUF unclonability assumption). A PUF is defined as inputting a string of length e_1 and outputting an arbitrary string of length e_2, that is, $\{0, 1\}^{e_1} \longrightarrow \{0, 1\}^{e_2}$. The security of this function can be determined by *challenge – responsegame* described below. This *game* mainly consists of two phases [33]:

Phase 1: A selects a random challenge C_j that has not been queried before.

Phase 2: A is allowed to obtain response corresponding to other challenges except the challenge C_j. A then outputs the guessed response R'_j based on the challenge C_j.

The correct response to C_j is $R_j = PUF_j(C_j)$. The condition for A to win the game is that $R'_j = R_j$. Therefore, we say $Adv^{PUF}_\delta(e_2) = \Pr[R'_j = R_j] \le 1/2^{e_2}$, where e_2 is the length of R_j and e_2 is also a big positive integer [36]. From this, it can be concluded that the probability of A guessing the correct response is negligible.

In Theorem 1, the semantic security of session key established by our scheme is proved using the queries described above.

Theorem 1. *Let a polynomial time adversary A run in time t against our scheme δ. Here,* q_{Hash_1}, q_{Hash_2}, *and* q_{Puf} *denote the number of* $Hash_1$ *queries,* $Hash_2$ *queries, and PUF queries, respectively.* $|HASH_1|$, $|HASH_2|$, *and* $|PUF|$ *denote the range space of* $h_1(\cdot)$, $h_2(\cdot)$, *and PUF, respectively. Furthermore, Ad* $v^{ECDDHP}_\delta(t)$ *means that A breaks the advantage of ECDDHP. Then, the advantage of A in breaking δ's semantic security to obtain the session key SK generated between two UAVs can be estimated as*

$$Adv^{AKE}_\delta(t) \le \frac{q^2_{Puf}}{|PUF|} + \frac{q^2_{Hash_1}}{|HASH_1|} + \frac{q^2_{Hash_2}}{|HASH_2|} + 2Adv^{ECDDHP}_\delta(t). \tag{3}$$

Proof. The proof of Theorem 1 is similar to the proofs given in [16, 33]. In this proof, we define the following four games, called Game_φ ($\varphi = 0, 1, 2, 3$). In addition, SUCC_φ represents the event that A guesses the correct bit c in Game_φ. The detailed descriptions of these games are given below.

Game $Game_0$: the game is simulated as an actual attack on our scheme δ by A under the ROR model. Here, it can be concluded as

$$\mathrm{Adv}^{\mathrm{AKE}}_\delta(t) = |2 \Pr[\mathrm{SUCC}_0] - 1|. \tag{4}$$

Game Game_1: in this game, an eavesdropping attack is simulated; that is, A can intercept all communication messages in UAV-UAV authentication phase through the execute query. After A obtains these messages ($M_1 = < D_\alpha, K_\alpha, J_\alpha >$, $M_2 = < D_\beta, K_\beta, L >$, $M_3 = < W >$), he/she tries to establish a session key $\mathrm{SK} = h_2(V^x \| V^y \| D^y_\alpha \| D^y_\beta)$ between DR_α and DR_β. A then executes the test query and guesses the value of c.

The constructed session key SK is made with V^x, V^y, D^y_α, and D^y_β, where D^y_α and D^y_β can be known by A. Therefore, A also needs to know about $V = (V^x, V^y)$. Here, $V = k_\alpha \cdot K_\beta = k_\beta \cdot K_\alpha$, where K_α and K_β can be intercepted by A.

However, it is difficult for A to compute k_α and k_β because he/she cannot extract k_α and k_β from $K_\alpha = k_\alpha \cdot U$ and $K_\beta = k_\beta \cdot U$, respectively. It follows that even if A steals communication messages M_1, M_2 and M_3, he/she cannot calculate SK; that is, the probability of A winning the game Game_1 does not increase. Since the games Game_1 and Game_0 are indistinguishable, the following conclusion is drawn:

$$\Pr[\text{SUCC}_1] = \Pr[\text{SUCC}_0]. \tag{5}$$

Game Game_2: the game Game_2 adds PUF query on the basis of Game_1. The session key established between the two UAVs $D\text{R}_\alpha$ and DR_β is $\text{SK} = h_2(V^x \| V^y \| D_\alpha^y c \| D_\beta^y)$. The way to figure out the correct SK is A to calculate $V = k_\alpha \cdot K_\beta = (V^x, V^y)$ or $V = k_\beta \cdot K_\alpha = (V^x, V^y)$. K_α and K_β are what A can get, and all that is left is to compute k_β or k_α.

Take calculating k_α as an example, A can obtain $J_\alpha = F_\alpha + k_\alpha$ through the execute query and calculate $F_\alpha = G_\alpha \oplus h_2(R_\alpha \| D_\alpha^y)$ through J_α, where G_α and D_α^y are both known by A. In order to obtain $R_\alpha = \text{PUF}_\alpha(C_\alpha)$, A needs multiple PUF queries to find collisions. In our scheme, we assume that PUFs used are secure and that the probability of A guessing the correct response is negligible as described in Section 5. This leads to the following results:

$$|\Pr[\text{SUCC}_1] - \Pr[\text{SUCC}_2]| \le \frac{q_{\text{Puf}}^2}{2|\text{PUF}|}. \tag{6}$$

Game Game_3: this game is treated as an active attack, with the send query, the Hash_1 query and the Hash_2 query added base on Game_2.

A performs multiple Hash_1 and Hash_2 queries to find hash collisions because he/she wants to trick legitimate instances into receiving tampered messages. Messages exchanged (M_1, M_2, and M_3) between two UAVs are safeguarded by collision-resistant one-way hash functions ($h_1(\cdot)$, $h_2(\cdot)$). Since these messages all apply the random numbers, identity information, and secret credentials, there is no collision here when the Send, Hash_1, and Hash_2 queries are executed by A.

On the other hand, $\text{SK} = h_2(V^x \| V^y \| D_\alpha^y \| D_\beta^y)$ and $V = k_\alpha \cdot K_\beta = k_\beta \cdot K_\alpha = (V^x, V^y)$, where A can know D_α^y, D_β^y, K_α, and K_β in the execute query. The fact that A computes $k_\alpha \cdot K_\beta$ or $k_\beta \cdot K_\alpha$ from $K_\alpha = k_\alpha \cdot U$ and $K_\beta = k_\beta \cdot U$ is computationally infeasible for A because it is equivalent to A solving the hard problem ECDDHP (see Definition 1) in polynomial time t. Therefore, based on the birthday paradox of hash functions and the intractability of ECDDHP, we can infer the following results:

$$\begin{aligned} &|\Pr[\text{SUCC}_2] - \Pr[\text{SUCC}_3]| \\ &\quad \le \frac{q_{\text{Hash}_1}^2}{2|\text{HASH}_1|} + \frac{q_{\text{Hash}_2}^2}{2|\text{HASH}_2|} + \text{Adv}_\delta^{\text{ECDDHP}}(t). \end{aligned} \tag{7}$$

In the above game, A simulates all queries. After executing the test query, he/she needs to guess the bit c to win the game. Here, we can get

$$\Pr[\text{SUCC}_3] = \frac{1}{2}. \tag{8}$$

□

Combining Equations (4), (5), and (8), the following derivation can be obtained:

$$\begin{aligned} \frac{1}{2}\text{Adv}_\delta^{\text{AKE}}(t) &= \left|\Pr[\text{SUCC}_0] - \frac{1}{2}\right| = \left|\Pr[\text{SUCC}_1] - \frac{1}{2}\right| \\ &= |\Pr[\text{SUCC}_1] - \Pr[\text{SUCC}_3]|. \end{aligned} \tag{9}$$

Applying the trigonometric inequalities in Equations (6) and (7) and the derived formula (9), the following is obtained:

$$\begin{aligned} \frac{1}{2}\text{Adv}_\delta^{\text{AKE}}(t) &= |\Pr[\text{SUCC}_1] - \Pr[\text{SUCC}_3]| \\ &\le |\Pr[\text{SUCC}_1] - \Pr[\text{SUCC}_2]| \\ &\quad + |\Pr[\text{SUCC}_2] - \Pr[\text{SUCC}_3]| \\ &\le \frac{q_{\text{Puf}}^2}{2|\text{PUF}|} + \frac{q_{\text{Hash}_1}^2}{2|\text{HASH}_1|} + \frac{q_{\text{Hash}_2}^2}{2|\text{HASH}_2|} \\ &\quad + \text{Adv}_\delta^{\text{ECDDHP}}(t). \end{aligned} \tag{10}$$

Finally, we obtain

$$\begin{aligned} \text{Adv}_\delta^{\text{AKE}}(t) \le \frac{q_{\text{Puf}}^2}{|\text{PUF}|} + \frac{q_{\text{Hash}_1}^2}{|\text{HASH}_1|} + \frac{q_{\text{Hash}_2}^2}{|\text{HASH}_2|} \\ + 2\text{Adv}_\delta^{\text{ECDDHP}}(t). \end{aligned} \tag{11}$$

5.2. Informal Security Analysis. Through the discussion in this section, we show that our scheme is resistant to the attacks described below and ensures both forward and backward secrecy of the session key.

5.2.1. Replay Attack. We consider that during UAV-UAV authentication phase, an adversary A may capture $M_1 = <D_\alpha, K_\alpha, J_\alpha>$, $M_2 = <D_\beta, K_\beta, L>$, and $M_3 = <W>$ in order to perform replay attack by resending them to receivers. However, this attack will fail due to the participation of random numbers. Let us take the message M_2 for example. DR_α sends $D_\alpha = (D_\alpha^x, D_\alpha^y)$ and $K_\alpha = (K_\alpha^x, K_\alpha^y)$ to DR_β. When DR_β .receives these information, it calculates $L = J_\beta \oplus h_2(K_\alpha^x \| K_\alpha^y \| D_\alpha^x \| D_\beta^x)$ and transmits $M_2 = <D_\beta, K_\beta, L>$ to DR_α. After receiving the message, DR_α calculates $J_\beta = L \oplus h_2(K_\alpha^x \| K_\alpha^y \| D_\alpha^x \| D_\beta^x)$ and verifies that $J_\beta \cdot U = D_\beta + P_{\text{pub}} \cdot h_1(\text{SID} \| D_\beta^x) + K_\beta$ holds through D_α and K_α generated previously. If the formula holds, the received L that contains the correct random number K_α^x, K_α^y, D_α^x, and DR_α considers the message M_2 from DR_β to be new and receives it. This way, if A replays M_2, DR_α will perform the verification operation and get the result that the message is replayed. Similarly, this

method is used to prevent the replay of other messages. Through the above discussion, our scheme is able to resist replay attack.

5.2.2. Man-in-the-Middle Attack. Under this attack, a man-in-the-middle adversary A will intercept the communication information between UAV DR_α and UAV DR_β and then modify these messages in an attempt to make the tampered messages accepted by legitimate entities. Suppose that A obtains the message $M_1 = <D_\alpha, K_\alpha, J_\alpha>$ during UAV-UAV authentication phase. In order to tamper with M_1 to become a valid message $M_{1A} = <D_\alpha, K_{\alpha A}, J_{\alpha A}>$, A needs to select a new random number $k_{\alpha A} \in Z_q^*$ and compute $K_{\alpha A} = k_{\alpha A} \cdot U = (K_{\alpha A}^x, K_{\alpha A}^y)$, $J_{\alpha A} = F_\alpha + k_{\alpha A} \bmod q$. However, computing a legitimate $J_{\alpha A}$ is difficult for A because he/she does not know DR_α's secret parameter F_α. For the other two messages M_2 and M_3, the adversary tries to modify them, and similar situations as M_1 occurs. It can be concluded that A tampering with the communication information will fail, and man-in-the-middle attack is successfully defended by our scheme.

5.2.3. UAV Capture and Impersonation Attacks. As described in the threat model of Section 3, an adversary A possesses the capability to capture a legitimate UAV flying in the air and apply power analysis attacks [9] to obtain secret parameters inside the UAV.

Here, we assume that A captures the UAV DR_β and steals $\{D_\beta, G_\beta, C_\beta, \mathrm{SID}\}$ from it. In order to successfully simulate DR_β, the requirements for A are to generate a valid message $M_2 = <D_\beta, K_\beta, L>$ and send M_2 to DR_α, where D_β is known by A. Moreover, A chooses a new random number $k_\beta \in Z_q^*$ and computes $K_\beta = k_\beta \cdot U = (K_\beta^x, K_\beta^y)$. Then, the remaining problem is that A needs to calculate L, which is not feasible for A. The reason is because A calculates a valid L to obtain J_β. Further, he/she needs to compute $F_\beta = G_\beta \oplus h_2(R_\beta \| D_\beta^y)$, where both G_β and D_β^y can be obtained by A. However, even if A captures DR_β, he/she cannot compute the response $R_\beta = \mathrm{PUF}_\beta(C_\beta)$ based on C_β. Due to the unclonability of PUF, A cannot produce identical PUF_β and the same response R_β. Furthermore, if the hardware of DR_β is damaged, A still cannot get the expected response R_β. Therefore, A cannot successfully simulate a legitimate UAV.

5.2.4. Session Key Forward and Backward Secrecy. In our scheme, the session key between UAV DR_α and UAV DR_β is $SK = h_2(V^x \| V^y \| D_\alpha^y \| D_\beta^y)$, where $V = k_\alpha \cdot K_\beta = k_\beta \cdot K_\alpha = (V^x, V^y)$. If an adversary A wants to calculate the correct SK, he/she needs to extract k_α or k_β from known K_α or K_β. However, this is difficult for A, because obtaining k_α or k_β from $K_\alpha = k_\alpha \cdot U$ or $K_\beta = k_\beta \cdot U$ is equivalent to solving elliptic curve discrete logarithm problem. Therefore, computing the current session key is not feasible for A. Obviously, k_α and k_β in each session are regenerated, so even if the current session key is stolen by A, he/she cannot guess the previously established session key. Furthermore, this has no effect on the security of future session key. Therefore, our scheme can achieve forward and backward secrecy of the session key.

5.2.5. Privileged Insider Attack. Suppose an insider privileged person becomes an adversary A who is able to gain access to the data stored in the ground station server GSS, but he/she could not get the private key s that belonged to GSS. Before each UAV can be deployed to the environment, it needs to be registered on GSS. After the registration process is over, the UAV stores the authentication-related parameters in the memory, and GSS deletes the secret credentials related to the UAV from its own memory. In this way, A cannot obtain secret parameters related to the authentication of the UAV. In addition, A attempts to deploy a fake UAV DR_α into the existing network and communicate with a legitimate drone. To carry out this attack, A needs to select a random number $d_A \in Z_q^*$ for DR_α and compute $D_A = d_A \cdot U = (D_A^x, D_A^y)$ and $F_A = d_A + s \cdot h_1(\mathrm{SID} \| D_A^x)$. However, computing F_A is a computationally difficult task for A, because he/she does not have enough power to obtain GSS's private key s. As a result, the deployment of malicious UAVs with such attack will be defended against our scheme. According to the above discussion, our scheme provides corresponding protection against privileged insider attack.

5.3. Formal Security Verification Using AVISPA Tool. In this section, we use the AVISPA tool to verify whether our scheme can resist replay attack and man-in-the-middle attack.

AVISPA is an automatic touch-tone formal validation tool for Internet security protocols and applications that provides a modular and expressive language to appoint protocols and their security attributes [32]. The tool performs automatic analysis through the integration of four backends. These backends include OFMC, CL-AtSe, SATMC, and TA4SP [37]. In this verification tool, the high-level protocol specification language (HLPSL) is used. The language is mainly used to model protocols, and the formal semantics of this language is based on Lamport's temporal logic of actions [38]. After modeling, the HLPSL code will be converted to an intermediate format (IF), which is then entered in one of four backends for automatic analysis. In the end, we obtain secure or insecure result.

In the implementation of our scheme, we have three basic roles, namely, an UAV DR_α, another UAV DR_β, and the ground station server GSS. There is also an intruder, denoted by i, who is also a participant in scheme execution. In addition to the above, there are also the roles for the session, environment and goal.

We have implemented our scheme using HLPSL and then selected OFMC and CL-AtSe backends for automatic analysis. The SATMC and TA4SP backends were not chosen because they do not support bitwise XOR operations. In order to check whether the replay attack can be resisted by our scheme, the backends verify that the legal agents can execute the scheme to search a passive adversary (intruder i) and then provide i with information related to some

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/UAV_Auth.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00 s
  searchTime: 0.15 s
  visitedNodes: 88 nodes
  depth: 8 plies
```

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/UAV_Auth.if
GOAL
  As Specified
BACKEND
  CL-AtSe

STATISTICS

  Analysed : 17 states
  Reachable : 6 states
  Translation : 0.01 seconds
  Computation : 0.01 seconds
```

Figure 5: Simulation results using OFMC and CL-AtSe backends.

Table 2: Comparison of communication costs.

Scheme	Transmitted messages (in bits)	Total cost (in bits)
Malani et al. [16]	$SD_\alpha \xrightarrow{992} SD_\beta \xrightarrow{1152} SD_\alpha$	2144
Chaudhry et al. [18]	$DR_\alpha \xrightarrow{832} DR_\beta \xrightarrow{832} DR_\alpha$	1664
Das et al. [19]	$DR_\alpha \xrightarrow{672} DR_\beta \xrightarrow{832} DR_\alpha \xrightarrow{192} DR_\beta$	1696
Our scheme	$DR_\alpha \xrightarrow{800} DR_\beta \xrightarrow{800} DR_\alpha \xrightarrow{160} DR_\beta$	1760

Table 3: Comparison of storage costs.

Scheme	Smart (sensing) device/UAV side
Malani et al. [16]	1600 bits
Chaudhry et al. [18]	1280 bits
Das et al. [19]	1280 bits
Our scheme	672 bits

normal sessions between the legitimate agents. In addition, the backends also need to verify the possibility of man-in-the-middle attack. Finally, we have obtained the simulation results, as shown in Figure 5. It can be clearly seen that our scheme provides protection against replay attack and man-in-the-middle attack.

6. Performance Comparison

In this section, we show the comparison between our scheme and existing similar schemes in terms of performance and security. Here, we have selected three recent authentication schemes [16, 18, 19] for comparison, all of which apply a similar system framework to our scheme.

6.1. Comparison of Communication Costs. In this section, we consider the bit size of messages exchanged between two devices when they authenticate each other. Here, we firstly set the bit value of each parameter, such as the identity of the device, random number, the output of hash function (if SHA-1 is used), and timestamp to be 160, 160, 160, and 32 bits, respectively. In addition, the size of the point on the elliptic curve $E_q(a, b)$: $y^2 = x^3 + ax + b \pmod q$ is 320 bits, where q is a large prime number of 160 bits [30]. The element in Z_p^* has 160 bits. We also consider embedding the PUF proposed in [39] on the UAV used in our scheme. A 32-bit challenge serves as input to this PUF, which outputs a corresponding 320-bit response [6].

Table 2 shows the comparison of our scheme with other similar schemes in terms of communication cost. In the UAV-UAV authentication phase, our scheme requires three messages $M_1 = <D_\alpha, K_\alpha, J_\alpha>$, $M_2 = <D_\beta, K_\beta, L>$, and $M_3 = <W>$, where the sizes of M_1, M_2, and M_3 are 800, 800, and 160 bits, respectively. Thus, the total communication overhead is $(800 + 800 + 160) = 1760$ bits. In addition, the scheme of Malani et al. [16], the scheme of Chaudhry et al. [18], and the scheme of Das et al. [19] demand the communication costs of 2144 bits, 1664 bits, and 1696 bits, respectively. It can be seen from the above description that the communication cost of our scheme is lower than that of Malani et al.'s scheme, 96 bits (=0.0000114 MB) more than that of Chaudhry et al.'s scheme ,and 64 bits (=0.00000763 MB) more than that of Das et al.'s scheme. The extra cost of our scheme is within 0.0001 MB. Therefore, even if our scheme is more than the schemes of Chaudhry et al. and Das et al., it has little effect on the performance of the UAV.

6.2. Comparison of Storage Costs. When an UAV DR_i is registered on the ground station server GSS, it needs to store some secret parameters into memory for authentication with neighboring UAVs. This section provides a comparison of the amount of storage space required by a device in the device registration phase between our scheme and other related schemes.

In our scheme, DR_i stores the credentials $\{D_i, G_i, C_i, \text{SID}\}$, which require $(320 + 160 + 32 + 160) = 672$ bits. The storage overhead of the device in Malani et al.'s scheme [16] is 1600 bits. The UAVs that complete the registration task in Chaudhry et al.'s scheme [18] and Das et al.'s scheme [19] both need to store 1280-bit secret parameters. Table 3

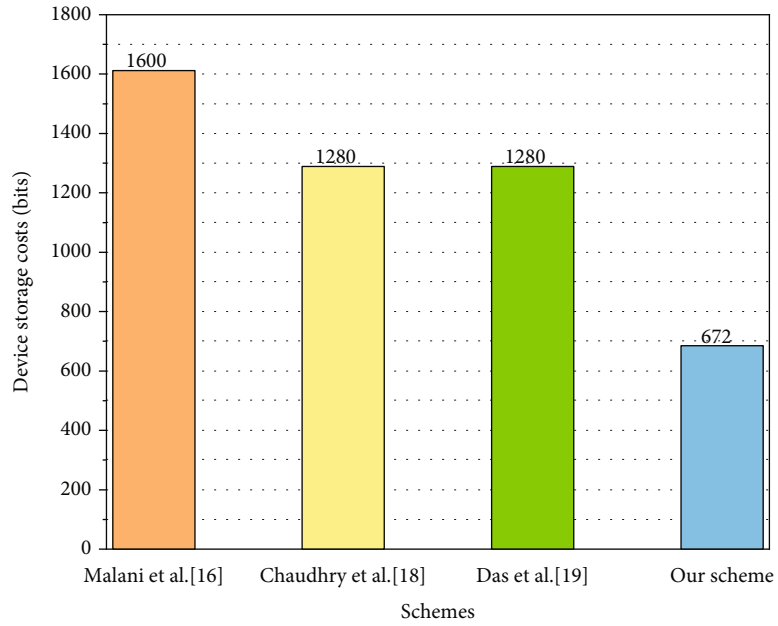

Figure 6: Comparison of device storage costs.

Table 4: Comparison of computation costs.

Scheme	Smart (sensing) device/UAV cost	Total cost
Malani et al. [16]	$6T_{mu} + 2T_{ad} + 8T_h$	$12T_{mu} + 4T_{ad} + 16T_h \approx 62.752$ ms
Chaudhry et al. [18]	$5T_{mu} + 2T_{ad} + 4T_h$	$10T_{mu} + 4T_{ad} + 8T_h \approx 52.176$ ms
Das et al. [19]	$6T_{mu} + 2T_{ad} + 9T_h + 1T_{poly}$	$12T_{mu} + 4T_{ad} + 18T_h + 2T_{poly} \approx 64.476$ ms
Our scheme	$4T_{mu} + 2T_{ad} + 5T_h + 1T_{puf}$	$8T_{mu} + 4T_{ad} + 10T_h + 2T_{puf} \approx 42.2208$ ms

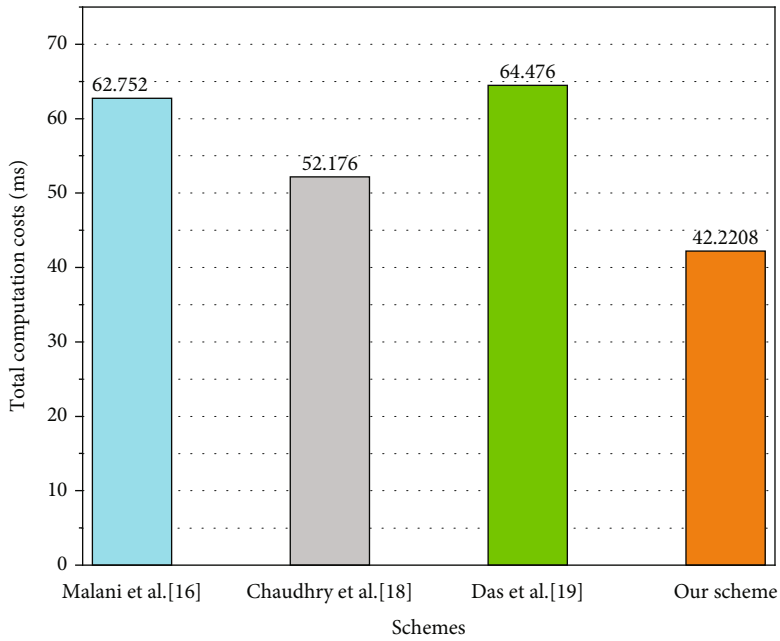

Figure 7: Comparison of total computation costs.

Table 5: Comparison of security and functionality features.

Feature	Malani et al. [16]	Chaudhry et al. [18]	Das et al. [19]	Our scheme
FE_1	√	√	√	√
FE_2	×	×	×	√
FE_3	×	×	×	√
FE_4	×	×	×	√
FE_5	√	×	×	√
FE_6	√	×	×	√
FE_7	√	√	√	√
FE_8	√	√	√	√
FE_9	√	√	√	√
FE_{10}	√	×	×	√
FE_{11}	√	×	√	√

Note: FE_1: replay attack; FE_2: man-in-the-middle attack; FE_3: device impersonation attack; FE_4: device capture attack; FE_5: privileged insider attack; FE_6: private key leakage attack of control room or ground station server; FE_7: session key forward and backward secrecy; FE_8: mutual authentication; FE_9: key agreement; FE_{10}: support dynamic device addition; FE_{11}: provide formal security verification by using AVISPA tool. √: a scheme resists an attack, or it supports a function; ×: a scheme does not resist an attack, or it does not support a function.

and Figure 6 provide a comparison of our scheme and other schemes in terms of storage cost. Obviously, our scheme requires less storage cost than these schemes [16, 18, 19].

6.3. Comparison of Computation Costs. This section describes how the proposed scheme compares with other related schemes [16, 18, 19] in terms of computation cost. To measure the computation time, we set up a simulation environment. We used a computer with an Intel i5-10300H processor and 16 gigabytes memory running Windows 10 operating system to represent an UAV DR_i or a smart (sensing) device. Moreover, we apply the MIRACL library to obtain the computation time of various operations. The following operations are performed on a computer representing an UAV or device. After the experiment, the specific time of each operation is shown as follows:

(i) Point multiplication on elliptic curve: $T_{mu} \approx 5.04$ ms

(ii) Point addition on elliptic curve: $T_{ad} \approx 0.32$ ms

(iii) Hash function calculation: $T_h \approx 0.062$ ms

(iv) PUF calculation: $T_{PUF} \approx 0.0004$ ms [6]

(v) Modular multiplication in the finite field GF(q): $T_m \approx 0.008$ ms

(vi) A t-degree univariate polynomial evaluation over the finite field GF(q): $T_{poly} \approx tT_m \approx 0.008t \approx 0.8$ ms (suppose $t = 100$) [19]

The comparison of computation costs between our scheme and other schemes is shown in Table 4 and Figure 7. In the mutual authentication phase between devices, the total computation costs required by Malani et al.'s scheme [16], Chaudhry et al.'s scheme [18], and Das et al.'s scheme [19] are $12T_{mu} + 4T_{ad} + 16T_h \approx 62.752$ ms, $10T_{mu} + 4T_{ad} + 8T_h \approx 52.176$ms, and $12T_{mu} + 4T_{ad} + 18T_h + 2T_{poly} \approx 64.476$ ms, respectively. However, the computation cost of our scheme in the UAV authentication phase is $8T_{mu} + 4T_{ad} + 10T_h + 2T_{PUF} \approx 42.2208$ ms. It can be clearly seen that the computation cost of our scheme is smaller than that of the other three schemes, and the authentication efficiency is higher.

6.4. Comparison of Security and Functionality Features. In this section, our scheme compares with Malani et al.'s scheme [16], Chaudhry et al.'s scheme [18], and Das et al.'s scheme [19] in terms of security and functionality features. Table 5 provides the results of the comparison. As can be seen from the table, the schemes of Malani et al., Chaudhry et al., and Das et al. cannot resist man-in-the-middle attack, device impersonation, and capture attacks. Furthermore, Chaudhry et al.'s scheme and Das et al.'s scheme cannot successfully defend against privileged insider attack, and the private key of the control room in both schemes can be obtained by an adversary. However, our scheme achieves all the features mentioned in Table 5 and is more secure than the other three schemes.

Combining the above descriptions, it can be concluded that our scheme has greater advantages than the other three schemes [16, 18, 19] in terms of storage cost, computation cost, security, and functionality features.

7. Conclusion

The mode of multiple UAVs working together and sharing information has been widely used in various fields, so ensuring the communication security between UAVs is the top priority. In order to achieve this goal, this paper proposes a novel and lightweight authentication and key agreement scheme, which is suitable for the scenario of authentication between two UAVs. The scheme also applies PUF to defend against physical capture attack against UAVs. Our scheme has undergone formal security analysis (using the ROR model), formal security verification (using the AVISPA tool), and informal security analysis, which concluded that the scheme is well protected against some attacks such as replay attack and device impersonation attack. Moreover, compared with existing similar schemes, our scheme requires lower storage and computation costs and higher security. Therefore, the proposed scheme is very suitable in the environment of mutual authentication between UAVs.

In the future, we hope to evaluate the performance of our scheme in a real-world environment. This evaluation will help us adapt the proposed scheme to provide better security and performance when deploying UAVs in the environment. However, it is important to note that technical issues of communication between UAVs need to be solved when running our scheme in a real environment. The first is to solve the power supply of the communication module, the second is to complete the hardware and software

configuration of the UAV and communication module, and the last difficulty is the shortage of spectrum resources.

Data Availability

The data used to support the findings of this study are included within the article

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China under grant nos. 61701173, 61802445, 62072134, and U2001205 and the Key Research and Development Program of Hubei Province under grant no. 2021BEA163.

References

[1] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy et al., "Internet of drones security and privacy issues: taxonomy and open challenges," *Access*, vol. 9, pp. 57243–57270, 2021.

[2] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact," *Access*, vol. 8, pp. 90225–90265, 2020.

[3] V. Sharma, "Advances in drone communications, state-of-the-art and architectures," *Drones*, vol. 3, no. 1, p. 21, 2019.

[4] F. Noor, M. A. Khan, A. Al-Zahrani, I. Ullah, and K. A. Al-Dhlan, "A review on communications perspective of flying ad-hoc networks: key enabling wireless technologies, applications, challenges and open research topics," *Drones*, vol. 4, no. 4, p. 65, 2020.

[5] X. Liu, Z. Li, N. Zhao et al., "Transceiver design and multihop D2D for UAV IoT coverage in disasters," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1803–1815, 2019.

[6] T. Alladi, G. Naren, V. C. Bansal, and M. Guizani, "SecAuthUAV: a novel authentication scheme for UAV-Ground Station and UAV-UAV communication," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15068–15077, 2020.

[7] V. Chamola, P. Kotesh, A. Agarwal, N. G. Naren, and M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad Hoc Networks*, vol. 111, article 102324, 2021.

[8] W. Hong, L. Jianhua, L. Chengzhe, and W. Zhe, "A provably secure aggregate authentication scheme for unmanned aerial vehicle cluster networks," *Peer-to-Peer Networking and Applications*, vol. 13, no. 1, pp. 53–63, 2020.

[9] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[10] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Design Automation Conference, DAC'07, 44th ACM/IEEE*, pp. 9–14, San Diego California, 2007.

[11] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: enhancing IoT security through authentication of wireless nodes using *in-situ* machine learning," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388–398, 2019.

[12] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for V2G using physical unclonable function," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7234–7246, 2020.

[13] C. Herder, M. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[14] Z. Shang, M. Ma, and X. Li, "A secure group-oriented device-to-device authentication protocol for 5G wireless networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 11, pp. 7021–7032, 2020.

[15] B. Semal, K. Markantonakis, and R. N. Akram, "A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks," in *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, pp. 1–8, London, UK, 2018.

[16] S. Malani, J. Srinivas, A. K. Das, K. Srinathan, and M. Jo, "Certificate-based anonymous device access control scheme for IoT environment," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9762–9773, 2019.

[17] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of drones deployment," *Computer Communications*, vol. 153, pp. 229–249, 2020.

[18] S. A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A. K. Bashir, and Y. B. Zikria, "GCACS-IoD: a certificate based generic access control scheme for Internet of drones," *Computer Networks*, vol. 191, article 107999, 2021.

[19] A. K. Das, B. Bera, M. Wazid, S. S. Jamal, and Y. Park, "IGCACS-IoD: an improved certificate-enabled generic access control scheme for internet of drones Deployment," *Access*, vol. 9, pp. 87024–87048, 2021.

[20] M. A. Khan, I. Ullah, N. Kumar et al., "An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4839–4851, 2021.

[21] P. Wang, C.-M. Chen, S. Kumari, M. Shojafar, R. Tafazolli, and Y.-N. Liu, "HDMA: hybrid D2D message authentication scheme for 5G-enabled VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5071–5080, 2021.

[22] H. Yıldız, M. Cenk, and E. Onur, "PLGAKD: a PUF-based lightweight group authentication and key distribution protocol," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5682–5696, 2021.

[23] B. Harishma, P. Mathew, S. Patranabis et al., "Safe is the new smart: PUF-based authentication for load modification-resistant smart meters," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 663–680, 2022.

[24] Y. Xia, R. Qi, S. Ji, J. Shen, T. Miao, and H. Wang, "An identity authentication scheme based on SM2 algorithm in UAV communication network," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 7537764, 10 pages, 2022.

[25] M. A. Qureshi and A. Munir, "PUF-RAKE: a PUF-based robust and lightweight authentication and key establishment protocol," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2457–2475, 2022.

[26] P. R. Babu, A. G. Reddy, B. Palaniswamy, and A. K. Das, "EV-PUF: lightweight security protocol for dynamic charging system of electric vehicles using physical unclonable functions," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 5, pp. 3791–3807, 2022.

[27] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[28] A. Cilardo, L. Coppolino, N. Mazzocca, and L. Romano, "Elliptic curve cryptography engineering," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 395–406, 2006.

[29] N. A. Mehrabi, C. Doche, and A. Jolfaei, "Elliptic curve cryptography point multiplication core for hardware security module," *IEEE Transactions on Computers*, vol. 69, no. 11, pp. 1707–1718, 2020.

[30] G. Thumbur, N. B. Gayathri, P. V. Reddy, M. Z. U. Rahman, and A. Lay-Ekuakille, "Efficient pairing-free identity-based ADS-B authentication scheme with batch verification," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 5, pp. 2473–2486, 2019.

[31] M. Abdalla, P. Fouque, and D. Pointcheva, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography - PKC 2005*, pp. 65–84, Springer, Berlin, Heidelberg, 2005.

[32] A. Muñoz, A. Maña, and D. Serrano, "AVISPA in the validation of ambient intelligence scenarios," in *2009 International Conference on Availability, Reliability and Security*, pp. 420–426, Fukuoka, Japan, 2009.

[33] P. Gope and B. Sikdar, "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13621–13630, 2020.

[34] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 391–406, 2020.

[35] X. Li, S. Liu, S. Kumari, and C.-M. Chen, "PSAP-WSN: a provably secure authentication protocol for 5G-based wireless sensor networks," *CMES-Computer Modeling in Engineering & Sciences*, vol. 135, no. 1, p. 711, 2023.

[36] Y. Zhang, Z. Huang, Q. Zhu, and L. Meng, "Patient family binding and authentication scheme with privacy protection for E-health system," *Networks*, vol. 2022, article 1883293, pp. 1–12, 2022.

[37] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous secure framework in connected smart home environments," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 968–979, 2017.

[38] Y. Chevalier, L. Compagna, J. Cuellar et al., "A high level protocol specification language for industrial security-sensitive protocols," in *Workshop on Specification and Automated Processing of Security Requirements - SAPS'2004*, pp. 193–205, Linz, Austria, 2004.

[39] X. Zhao, Q. Zhao, Y. Liu, and F. Zhang, "An ultracompact switching-voltage-based fully reconfigurable RRAM PUF with low native instability," *IEEE Transactions on Electron Devices*, vol. 67, no. 7, pp. 3010–3013, 2020.