

Article

Lightweight Drone-to-Ground Station and Drone-to-Drone Authentication Scheme for Internet of Drones

Qi Xie *  and Jilin Zhang

Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, Hangzhou 311121, China; 2022111011026@stu.hznu.edu.cn

* Correspondence: qixie@hznu.edu.cn

Abstract: The implementation of the Authentication and Key Agreement (AKA) protocol in the Internet of Drones (IoD) is crucial for enhancing the security and reliability of information transmission. However, almost all existing authentication protocols between drones and Ground Station (GS) may suffer from several attacks due to capture attacks. In addition, the authentication between drones requires the participation of GS, which not only increases the amount of computation and transmission but also faces challenges such as impersonation attacks, lack of privacy protection, and perfect forward security. Therefore, we propose a secure and lightweight drone-to-GS (D2G) and D2D AKA protocol with perfect forward secrecy for IoD. Our protocol integrates physical unclonable functions (PUF) symmetrically into GS and drones to protect secret information against capture attacks while ensuring that GS does not store secret information related to drones. Furthermore, the proposed protocol enables direct mutual authentication between drones in a symmetrical manner without GS involvement, improving security and efficiency, particularly in scenarios where drones must collaborate without GS connectivity. Formal security proof using the random oracle model confirms the protocol's resilience against various attacks. The performance analysis indicates that our scheme improves computational efficiency by an average of 39.44% compared to existing schemes that offer comparable security. Additionally, our approach incurs zero storage overhead during the GS authentication process. This protocol offers a secure and efficient solution for IoD, enhancing both security and scalability.



Academic Editors: Tomohiro Inagaki and Hsien-Chung Wu

Received: 8 March 2025

Revised: 24 March 2025

Accepted: 2 April 2025

Published: 5 April 2025

Citation: Xie, Q.; Zhang, J.

Lightweight Drone-to-Ground Station and Drone-to-Drone Authentication Scheme for Internet of Drones.

Symmetry **2025**, *17*, 556. <https://doi.org/10.3390/sym17040556>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: authentication protocol; Internet of Drones (IoD); drone-to-ground station; drone-to-drone; physical unclonable function (PUF)

1. Introduction

Drones, or Unmanned Aerial Vehicles (UAVs) are aircraft systems that operate without a human pilot, either remotely controlled by an operator or autonomously via pre-programmed flight paths. They are used in various fields such as surveillance, aerial photography, logistics, agriculture, and infrastructure inspection, offering significant benefits in terms of cost efficiency, operational flexibility, and access to hard-to-reach areas [1,2]. Drones typically operate autonomously or semi-autonomously, relying on communication with GS for navigation, control, and data transfer. This interaction forms the foundation of many modern drone applications, where security and reliability are crucial. The IoD extends the Internet of Things (IoT) concept to drones [3–6], enabling them to share data, communicate with one another, and integrate into broader systems and networks. This connectivity makes drones smarter, more autonomous, and capable of executing more complex tasks, creating a dynamic ecosystem where drones can interact and collaborate.

However, as drones become more integrated into critical infrastructure, the security vulnerabilities associated with their communication channels are increasingly concerning [7]. Drones communicate wirelessly with GS, other drones, and cloud-based platforms [8], making them vulnerable to various cyberattacks, including unauthorized access, data tampering, malicious interception, impersonation, man-in-the-middle, replay attacks, physical capture, and more [9]. To mitigate such risks, drone authentication and key agreement protocols have emerged as crucial mechanisms for ensuring secure communication between drones and other entities [10–12]. Authentication protocols verify the identity of drones and their communication partners, preventing unauthorized devices from interacting with the system. Key agreement protocols allow secure cryptographic keys to be shared between communicating drones or between a drone and GS, ensuring the confidentiality and integrity of exchanged information. Given the resource constraints of drones, such as limited computational power and energy supply, it is crucial that these AKA protocols [13–18] are lightweight and energy-efficient, without compromising security. Additionally, the protocols must be resilient against evolving threats, considering the increasing sophistication of cyberattacks targeting UAVs and their ground control systems.

Motivation and contribution: In recent years, numerous scholars have proposed various AKA schemes for IoD. However, almost all existing AKA schemes are unable to resist capture attacks from GS and drones; attackers can obtain secret information stored in GS and drones; thus, they can launch impersonation attacks, man-in-the-middle attacks, etc., and cannot achieve anonymity and perfect forward secrecy. On the other hand, the mutual authentication between drones requires the participation of GS, which increases communication and computation costs and may also be vulnerable to several attacks due to GS being captured. As the drone size increases, it also becomes impractical to expect GS to incur significant storage overhead for storing information related to the drone's registration and communication phases. Therefore, how to solve the above problems is a challenge. Our solution is the first scheme to propose such an idea, which can achieve various security attributes and lightweight requirements and is also applicable to the need for drones to cooperate in executing tasks when they cannot establish contact with ground stations. The main contributions of this paper are summarized as follows:

- A secure and lightweight D2G and D2D authentication and key agreement protocol with perfect forward secrecy for IoD is proposed.
- In order to enhance the security and privacy-preserving, we integrate PUF into GS and drones, respectively, to resist capture attacks from GS and drones. In addition, GS has no additional storage overhead for the registration and authentication process for drones. Furthermore, the mutual authentication between drones does not require the participation of GS, which is more secure and efficient.
- The proposed protocol guarantees to be secured against all known threats faced by IoD. The semantic security of the proposed protocol is formally proved under the random oracle model. Comparative analysis shows that our protocol can resist various known attacks, achieve perfect forward security and privacy protection, and maintain low computational costs.

There are three innovations in the work: (a) Ground stations and drones can complete mutual authentication without storing drones' information. This provides a strong condition for the scalability of the system. (b) The authentication between drones does not require the participation of ground stations. This effectively reduces the burden on the GS and allows drones to communicate with each other even if they travel outside the communication range of the GS. (c) The security of GS is taken into account. The work incorporates PUF into both the GS and drones. This integration serves as a robust defense

mechanism against capture attacks, significantly enhancing the overall security posture of the system.

The rest of this paper is organized as follows. Section 2 discusses the related works. In Section 3, the system model for IoD is introduced. Section 4 describes our proposed protocol. Section 5 provides a security proof of the protocol. In Section 6, a performance analysis of the protocol is also presented. Finally, we conclude the paper in Section 7.

2. Related Works

Recent efforts to secure drone networks have led to the development of various lightweight authentication protocols that address both emerging security challenges and the constraints of limited resources. Jan et al. [19] proposed a protocol specifically tailored for the IoD, emphasizing minimal overhead while ensuring robust security.

Several researchers have focused on encryption-based methods. Cheon et al. [20] introduced a homomorphic authenticated encryption technique that enables real-time data protection by allowing simultaneous encryption and verification. This approach safeguards confidentiality and integrity without imposing heavy computational demands. In a complementary direction, Jiang et al. [21] designed an intelligent authentication system that leverages behavioral analysis and prediction to identify abnormal drone activity, thereby effectively mitigating identity spoofing risks.

Blockchain technology has emerged as a promising solution for decentralized security. Tan et al. [22] developed a blockchain-assisted distributed authentication service for industrial drones, which offers tamper resistance while keeping the system lightweight. Additionally, Wang et al. [23] presented a blockchain-enhanced mutual authentication protocol that further secures drone communications, and García et al. [24] combined a μ Tesla-based approach with blockchain to protect broadcast communications within drone networks.

Other studies have explored alternative lightweight cryptographic mechanisms. Yu et al. [25] proposed an authentication protocol that employs physical unclonable functions (PUFs), offering an efficient solution for smart city applications where drones operate under strict resource constraints. In parallel, streamlined authentication and key agreement schemes have been put forward by Zhang et al. [26] and Wazid et al. [6], both aiming to balance robust security with low computational overhead. Moreover, Hussain et al. [27] introduced an efficient user access protocol that reinforces overall system reliability in dynamic drone environments.

In addition to protocol development, broader evaluations and adaptations for emerging network technologies have also been considered. Rodrigues et al. [28] provided a comprehensive review of various authentication methods for drone communications. Al-ladi et al. [29] introduced Drone-MAP, a protocol designed for drone-assisted 5G networks, which addresses the need for ultra-low latency and high security in next-generation communication systems. Furthermore, Wu et al. [30] developed an enhanced authentication framework optimized for 5G-enabled drone networks, underscoring the importance of robust security in high-speed settings.

Advanced protocols designed for large-scale drone deployments and swarm communications have also been explored. Bansal et al. [31] proposed SHOTS, a scalable authentication-attestation protocol that incorporates optimal trajectory planning to enhance both security and operational efficiency in drone swarms. Similarly, Javed et al. [32] investigated the use of blockchain as a certificate authority, aiming to mitigate vulnerabilities associated with centralized systems. Finally, Mishra et al. [33] introduced a secure key management framework that leverages blockchain and big data analytics for drones operating in networks beyond 5G, while Zhang et al. [34] demonstrated the potential of an

ECC-based lightweight authentication protocol to meet the dual demands of security and efficiency in modern drone applications.

Lastly, Xiao et al.'s scheme [35] allows mutual authentication between a drone and the GS, as well as between any two drones, establishing secure session keys in both cases. However, their protocol does not account for GS security, which is vulnerable to physical capture attacks, and it requires GS participation for drone-drone authentication. Li et al. [36] introduced CSECMAS, an efficient certificate signing-based authentication scheme that leverages elliptic curve cryptography for drone communication networks. Their approach focuses on providing robust security while minimizing computational overhead, making it well-suited for resource-constrained drone systems. Bansal and Sikdar [37] proposed a location-aware clustering method aimed at developing a scalable authentication protocol for drone swarms. By incorporating geographic information into the clustering process, their framework enhances scalability and streamlines the authentication process in large-scale drone deployments. Cho et al. [38] developed SENTINEL, a secure and efficient authentication framework tailored for drone communications. Their method emphasizes rapid and reliable authentication, ensuring that dynamic drone networks can maintain high levels of security without sacrificing operational efficiency. However, the protocol is vulnerable to physical capture attacks. Yu et al. [39] introduced LAKA-UAV, a lightweight authentication and key agreement scheme that leverages blockchain for cloud-assisted drone networks in flying ad-hoc environments. Their framework focuses on providing robust security with minimal computational overhead, making it suitable for dynamic and distributed drone communications. Bhattarai et al. [40] proposed a lightweight and anonymous, application-aware authentication and key agreement protocol designed specifically for the Internet of Drones. Their approach emphasizes user privacy and efficient credential management, addressing the unique challenges inherent in drone communication networks. Alkatheiri et al. [41] developed a lightweight authentication scheme based on PUF for drone networks. This method exploits the inherent uniqueness of PUFs to deliver a secure and resource-efficient solution for authenticating drones in diverse operational environments.

Overall, the security and privacy of drone communications in IoD have been the subject of various AKA protocols in recent years, but these existing schemes face challenges related to session key leakage, physical capture attacks, and inefficiency in UAV-to-UAV or UAV-to-GS communications. These existing protocols highlight the need for more efficient, secure, and resilient AKA schemes, especially for scenarios where UAVs must authenticate each other independently of the GS. Our proposed protocol addresses these gaps by providing mutual drone-to-drone authentication without requiring GS involvement, improving both security and efficiency. Some important related works are summarized in Table 1. The proposed scheme addresses the limitations of these previously proposed protocols listed in Table 1, such as the need for GS involvement for D2D authentication, GS physical capture attack, and perfect forward security.

Table 1. The summary of the related schemes for IoD.

Scheme	Year	Cryptographic Techniques	Advantages	Limits
[19]	2021	Utilize hash message authentication code	Protects the communication between drone and drone	Authentication requires GS
[20]	2018	Utilize homomorphic encryption	Guarantees the security against eavesdropping and forgery attacks	Vulnerable to session key leaks and insider attacks

Table 1. Cont.

Scheme	Year	Cryptographic Techniques	Advantages	Limits
[21]	2020	Utilize Kalman Trajectory Predicting Algorithm	Provides the government with intelligent control	Does not resist physical capture attack
[28]	2019	Utilize ECC	Provides mutual authentication between base station devices and UAVs	Does not resist physical capture attack
[6]	2019	Utilize fuzzy extractor	Provides three-factor security	Does not guarantee perfect backward secrecy
[27]	2023	Utilize one-way hash function	Provides mutual authentication for user and drone	Does not resist physical capture attack
[23]	2023	Utilize one-way hash function	Provides a lightweight blockchain-enhanced mutual authentication	Does not resist physical capture attack
[24]	2023	Utilize one-way hash function	Utilizes blockchain to manage drone authentication	Authentication requires GS
[33]	2023	Utilize one-way hash function	Provides an authentication key management framework with big data analytics	Does not resist physical capture attack
[34]	2023	Utilize ECC	Provides drone-GS authentication	Does not resist physical capture attack
[35]	2024	Utilize one-way hash function	Provides low computation overload	Does not resist GS capture attack
[36]	2022	Utilize ECC	Establishes a secure session between the GS and a UAV	Substantial computational overhead
[37]	2021	Utilize PUF	Uses K-Means clustering to construct UAV clusters	Does not resist replay attack, anonymity, and perfect forward secrecy

3. System Model

The system model, including the network model (overall architecture) and its corresponding threat model, is described as follows.

3.1. Network Model

The network model is shown in Figure 1, which contains a GS and drones. In Figure 1, drones have limited memory and compute capabilities when compared to the GS, and they communicate with each other over an insecure wireless channel.

The GS serves as the main command and control hub for the safe flight and guidance of drones. The GS often acts as the central hub for monitoring and controlling drone fleets. It coordinates flight paths, monitors real-time drone status (e.g., battery levels, GPS location, and system health), and adjusts operational parameters based on environmental conditions. The GS is responsible for overseeing drone missions, providing updates, and ensuring that drones follow assigned routes or complete specified tasks, such as surveillance or delivery. The GS collects and aggregates data transmitted by drones, which could include sensor data, images, videos, and telemetry. This data can be used for real-time analysis or stored for later processing. The GS processes this collected data to make decisions, such

as adjusting drone routes based on real-time data or performing predictive analytics to optimize drone operations.

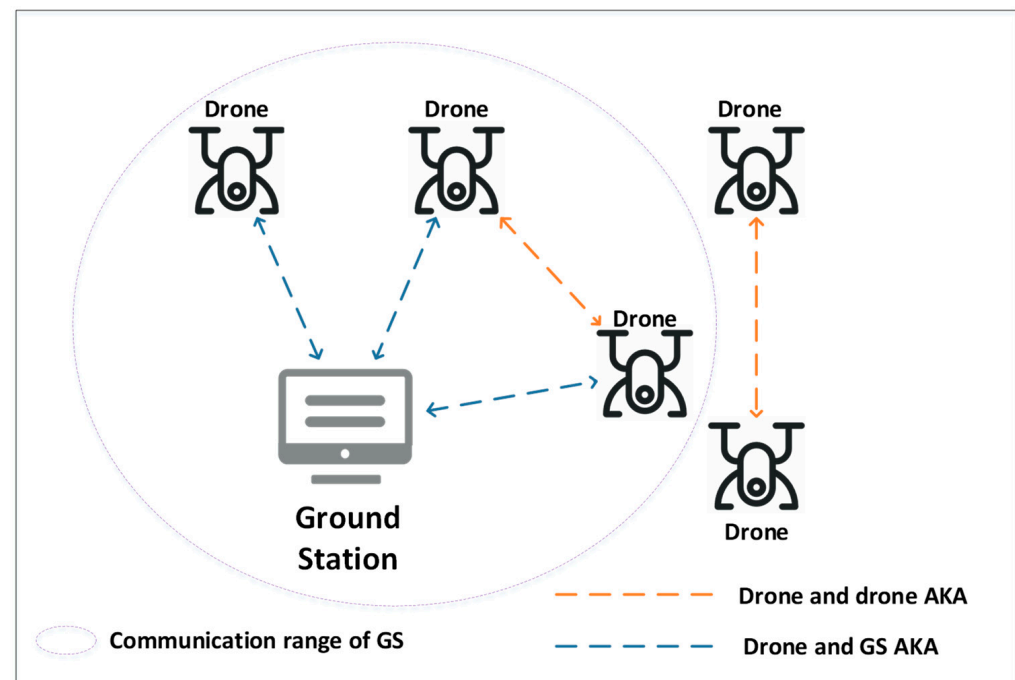


Figure 1. Network model.

Drones are the core components of IoD, where they perform various tasks related to surveillance, delivery, communication, and data collection. In the IoD ecosystem, drones are designed to work autonomously or in coordination with GS and other drones to complete complex operations. Drones in the IoD are often capable of autonomous flight, navigating based on pre-defined routes, real-time GPS data, and environmental sensing. They can adjust their paths dynamically based on obstacles or changes in the environment, making them highly adaptable in diverse situations. Drones can make decisions on-the-fly, such as selecting an optimal flight path or avoiding collisions, without the need for continuous remote control by GS.

In IoD ecosystem, the GS and drones work together to ensure efficient, secure, and reliable operations. Their collaboration is vital for tasks such as surveillance, delivery, data collection, and fleet management. In order to establish a secure communication session with the GS, a drone needs to perform the drone-GS AKA. In order to establish a secure communication session with another drone, a drone needs to perform the drone-drone AKA without the help of GS.

3.2. Threat Model

We define the threat model as follows in accordance with the Dolev-Yao threat model [42] and Krawczyk (CK) threat model [43].

- The adversary A may be an internal attacker or a drone with a valid registration, in which case the attacker may transmit harmful messages or initiate impersonation attacks.
- A can also eavesdrop, modify, intercept, forge, delete, and replay the messages transmitted publicly.
- A can gain access to stored data by side-channel attacks on drones and GS, but cracking PUF is tough.

4. Proposed Protocol

The proposed scheme is organized into four phases: (1) System initialization. (2) Drone registration. (3) Drone-GS authentication and key agreement. (4) Drone-drone authentication and key agreement. (5) Pseudo-identity and public key update. (6) Drone revocation/reissue phase. Table 2 presents the notations used in this scheme.

Table 2. The notations used in this scheme.

Notation	Description
GS	Ground station
ID_s, ID_i	Identities of GS, $Drone_i$
PID_i, PID_j	Pseudo – identities of $Drone_i, Drone_j$
PID_i'	New pseudo – identity of $Drone_i$
P	The generator of the elliptic curve
x_s, Y_s	Private and public key of GS
d_i, Y_i	Private and public key of drone
$PUF()$	Physical unclonable function
Cha_i, Res_i	The challenge and response pair
$h(.)$	Hash function
$\oplus$	XOR operation
$ $	Concatenation
T_i	Timestamp of current time
$E_{SK}()/D_{SK}()$	Symmetric encryption/decryption function
SK_{is}	The session key between drone and GS
SK_{ij}	The session key between drones

4.1. System Initialization Phase

GS selects an elliptic curve $E(GF_q)$ and a base point P then selects its private key $x_s \in Z_q^*$ and a random number Cha_s and its identity ID_s , calculates $Res_s = PUF(Cha_s)$, $Q_s = x_s \oplus h(Res_s)$, $Y_s = x_s \cdot P$ as its public key, and stores $\{PUF(), Q_s, Cha_s\}$. GS selects one-way hash function $h(.)$. Finally, GS publishes the system parameters $\{q, P, Y_s, ID_s, h(.)\}$.

4.2. Drone Registration Phase

In this phase, A drone launches a registration application with GS before deployment in the IoD. The registration phase is shown in Figure 2.

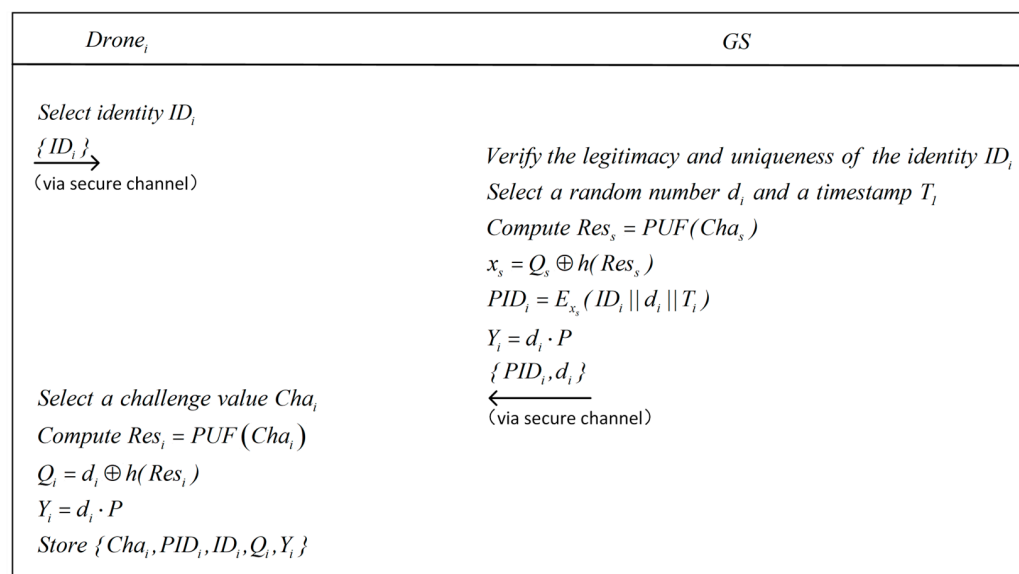


Figure 2. Drone registration phase.

The detailed description of the drone registration is as follows:

1. The drone selects its identity ID_i and sends its identity ID_i to GS via a secure channel.
2. On receiving the request from the drone, GS verifies the legitimacy and uniqueness of the identity ID_i , selects a random number d_i , calculates $Res_s = PUF(Cha_s)$, $x_s = Q_s \oplus h(Res_s)$, $PID_i = E_{x_s}(ID_i || d_i || T_i)$, $Y_i = d_i \cdot P$, where T_i is current time. Then, GS sends $\{PID_i, d_i\}$ to drone via a secure channel and adds Y_i in the revocation list.
3. The drone selects a challenge value Cha_i , calculates $Res_i = PUF(Cha_i)$, $Q_i = d_i \oplus h(Res_i)$, $Y_i = d_i \cdot P$, then the drone stores $\{Cha_i, PID_i, ID_i, Q_i, Y_i\}$.

4.3. Drone-GS Authentication and Key Agreement Phase

Ground station (GS) and drone authentication could enable GS to get the status of a drone, flight plan, GPS coordinates, and scope of regulations. The drone-GS authentication and key agreement phase is shown in Figure 3.

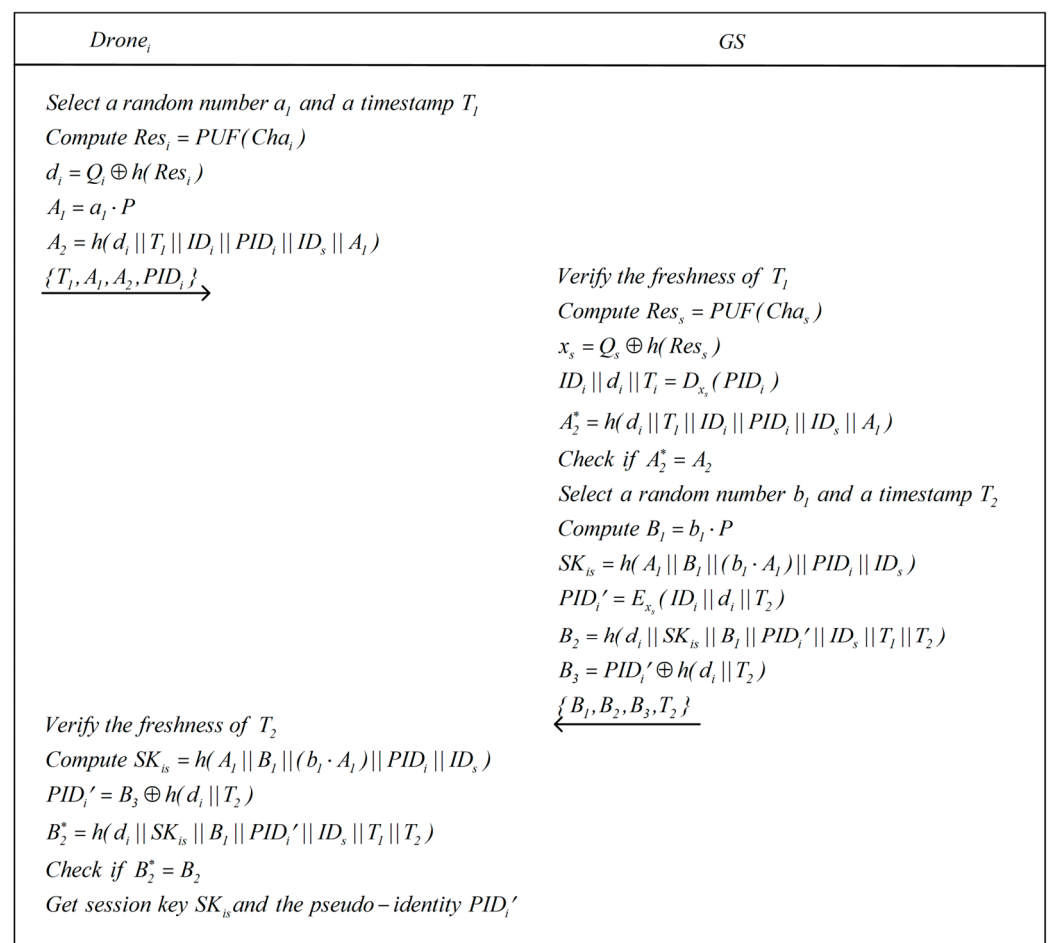


Figure 3. Drone-GS AKA phase.

The detailed description of the drone-GS authentication and key agreement phase is as follows:

1. The drone selects a random number a_i and a timestamp T_i , calculates $Res_i = PUF(Cha_i)$, $d_i = Q_i \oplus h(Res_i)$, $A_i = a_i \cdot P$, $A_2 = h(d_i || T_i || ID_i || PID_i || ID_s || A_i)$, and sends $\{T_i, A_i, A_2, PID_i\}$ to GS.
2. On receiving the information from the drone, GS verifies the freshness of T_i , calculates $Res_s = PUF(Cha_s)$, $x_s = Q_s \oplus h(Res_s)$, $ID_i || d_i || T_i = D_{x_s}(PID_i)$, $A_2^* = h(d_i || T_i || ID_i || PID_i || ID_s || A_i)$, then verifies if $A_2^* = A_2$, if not, reject it. Other-

- wise, GS selects a random number b_1 and a timestamp T_2 , calculates $B_1 = b_1 \cdot P$, $SK_{is} = h(A_1 || B_1 || (b_1 \cdot A_1) || PID_i || ID_s)$, $PID_i' = E_{x_s}(ID_i || d_i || T_2)$, $B_2 = h(d_i || SK_{is} || B_1 || PID_i' || ID_s || T_1 || T_2)$, $B_3 = PID_i' \oplus h(d_i || T_2)$, then sends $\{B_1, B_2, B_3, T_2\}$ to drone. The SK_{is} serves as a session key between the drone and GS.
3. On receiving the information from GS, the drone verifies the freshness of T_2 , then calculates $SK_{is} = h(A_1 || B_1 || (a_1 \cdot B_1) || T_2 || PID_i || ID_s)$, $PID_i' = B_3 \oplus h(d_i || T_2)$, $B_2^* = d_i || SK_{is} || B_1 || PID_i' || ID_s || T_1 || T_2$, then verifies if $B_2^* = B_2$, if it is valid, the drone gets the session key SK_{is} and updates the pseudo-identity PID_i' .

4.4. Drone-Drone Authentication and Key Agreement Phase

In this phase, AKA requests from one drone to another drone for future secure communication. The drone-drone authentication and key agreement phase is shown in Figure 4.

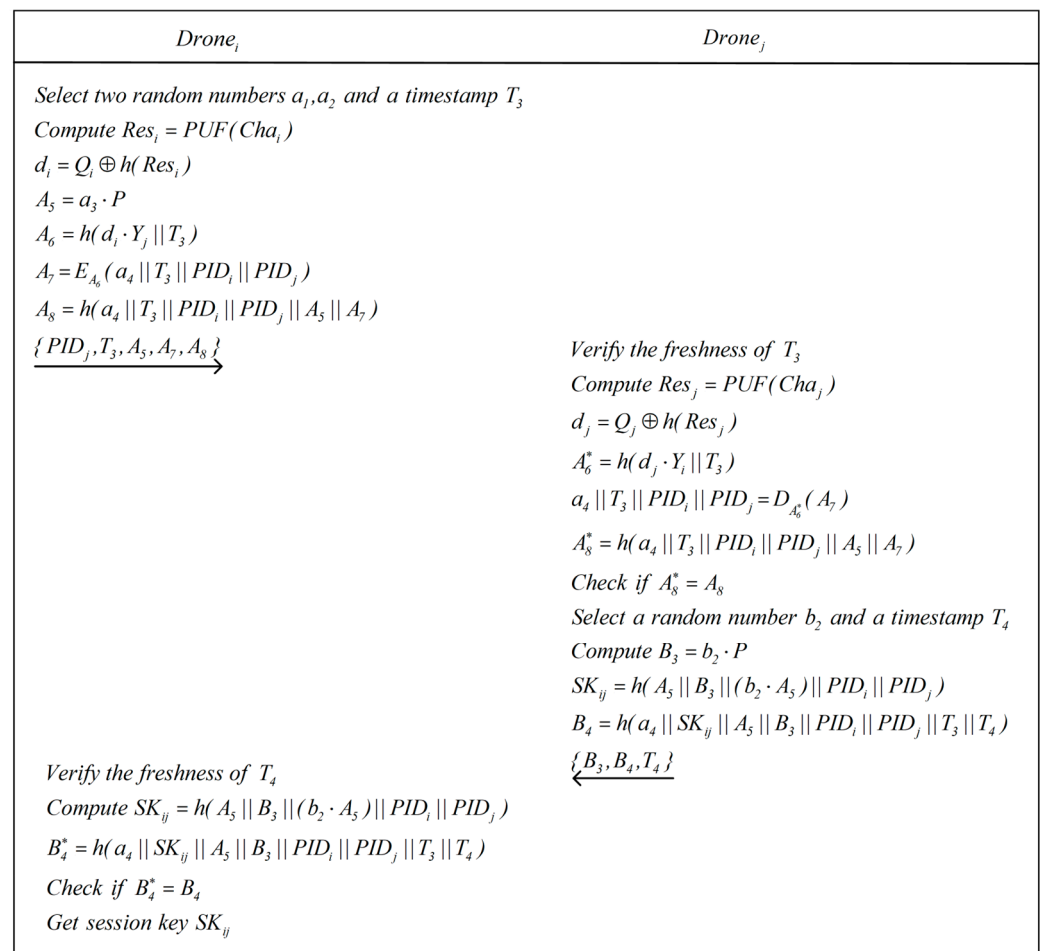


Figure 4. Drone-drone AKA phase.

The detailed description of the drone-drone authentication and key agreement phase is as follows:

1. Drone_i selects two random numbers a_3, a_4 and a timestamp T_3 , calculates $Res_i = h(Cha_i)$, $d_i = Q_i \oplus h(Res_i)$, $A_5 = a_3 \cdot P$, $A_6 = h(d_i \cdot Y_j || T_3)$, $A_7 = E_{A_6}(a_4 || T_3 || PID_i || PID_j)$, $A_8 = h(a_4 || T_3 || PID_i || PID_j || A_5 || A_7)$, sends $\{PID_j, T_3, A_5, A_7, A_8\}$ to Drone_j.
2. On receiving the information from Drone_i, the Drone_j verifies the freshness of T_3 , calculates $Res_j = PUF(Cha_j)$, $d_j = Q_j \oplus h(Res_j)$, $A_6^* = h(d_j \cdot Y_i || T_3)$, $a_4 || T_3 || PID_i || PID_j = D_{A_6^*}(A_7)$, $A_8^* = h(a_4 || T_3 || PID_i || PID_j || A_5 || A_7)$, then veri-

- fies if $A_8^* = A_8$, if not, reject it. Otherwise, $Drone_j$ selects a random number b_2 and a timestamp T_4 , calculates $B_3 = b_2 \cdot P$, $SK_{ij} = h(A_5 || B_3 || (b_2 \cdot A_5) || PID_i || PID_j)$, $B_4 = h(a_4 || SK_{ij} || A_5 || B_3 || PID_i || PID_j || T_3 || T_4)$, then sends $\{B_3, B_4, T_4\}$ to $Drone_i$. The SK_{ij} serves as a session key between the $Drone_i$ and $Drone_j$.
- On receiving the information from $Drone_j$, $Drone_i$ verifies the freshness of T_4 , calculates $SK_{ij} = h(A_5 || B_3 || (a_3 \cdot B_3) || PID_i || PID_j)$, $B_4^* = h(a_4 || SK_{ij} || A_5 || B_3 || PID_i || PID_j || T_3 || T_4)$, then verifies if $B_4^* = B_4$, if it is valid, $Drone_i$ gets the session key SK_{ij} .

4.5. Pseudo-Identity and Public Key Update Phase

To resist identity tracking attacks and protect the privacy of the vehicle, the temporary pseudo-identity and public key of the drone can be updated.

After the drone $Drone_i$ and GS complete the mutual authentication (please refer to Section 4.3) and gets session key SK_{is} , GS chooses d_i^{new} and current timestamp T_i^{new} , computes $PID_i^{new} = E_{x_s}(ID_i || d_i^{new} || T_i^{new})$, $B_5 = PID_i^{new} \oplus h(SK_{is} || T_5)$, $B_6 = d_i^{new} \oplus h(T_5 || SK_{is})$, $Y_i^{new} = d_i^{new} \cdot P$, and sends B_5 and B_6 to $Drone_i$ via a public channel.

After receiving B_5 and B_6 , $Drone_i$ computes PID_i^{new} and d_i^{new} from B_5 and B_6 , and computes $Q_i^{new} = d_i^{new} \oplus h(Res_i)$ and $Y_i^{new} = d_i^{new} \cdot P$, updates d_i and Y_i .

4.6. Drone Revocation/Reissue Phase

The drone revocation phase is crucial in scenarios where a drone needs to be removed from the system's authorized list. This could be due to a drone being compromised, malfunctioning, or no longer needed. In this phase, the system must revoke the drone's access rights, ensuring it can no longer communicate with other components like GS or other drones.

The GS decrypts $ID_i || d_i || T_i$ based on the PID_i of the drone that needs to be revoked, calculates $Y_i = d_i \cdot P$, then adds Y_i to the revocation list that are already authenticated with GS. Then, if GS and other drones discover the Y_i of a revoked drone in the revocation list, they will refuse to communicate with it.

When a revoked drone needs to be reissued, it needs to re-initiate a registration request to GS for a new Y_i and PID_i . At this point, since the drone's Y_i is already on the revocation list, GS needs to decide whether to accept this registration request or not based on the actual situation. If it is deemed that the drone can be legally re-registered, then remove Y_i from the revocation list.

5. Security Proof

In this part, we first provide informal security proof for the proposed scheme. Then, we present a formal security proof for the proposed scheme using the random oracle model.

5.1. Informal Security Proof

5.1.1. Replay Attack

Timestamps and random numbers are associated with public messages. Replayed messages fail to meet freshness and integrity standards. The proposed protocol can resist replay attacks.

5.1.2. Impersonation Attack

In the drone-GS authentication and key agreement phase, suppose an adversary impersonates the drones to authenticate with GS and forges the message $\{T_1, A_1, A_2, PID_i\}$, where $A_1 = a_1 \cdot P$, $A_2 = h(d_i || T_1 || ID_i || PID_i || ID_s || A_1)$, a_1 and d_i are random numbers, ID_i and ID_s are identities of the drone and GS, PID_i is pseudo-identity of the drone. PID_i

will be updated after authentication. It is impossible to calculate A_2 without knowing d_i and ID_i .

In the drone-drone authentication and key agreement phase, suppose an adversary impersonates the drones to authenticate with another drone and forges the message $\{PID_j, T_3, A_5, A_7, A_8\}$, where $A_5 = a_3 \cdot P$, $A_6 = h(d_i \cdot Y_j || T_3)$, $A_7 = E_{A_6}(a_4 || T_3 || PID_i || PID_j)$, $A_8 = h(a_4 || T_3 || PID_i || PID_j || A_5 || A_7)$, a_3 and d_i are random numbers, PID_i and PID_j is pseudo-identities. PID_i will be updated after authentication. It is impossible to calculate A_6 without knowing d_i .

5.1.3. Drone Physical Capture Attack

Suppose an adversary has physically captured some drones; the adversary can retrieve stored information $\{Cha_i, PID_i, ID_i, Q_i, Y_i\}$ through power analysis attacks, where $Res_i = PUF(Cha_i)$, $d_i = Q_i \oplus h(Res_i)$. While the adversary can collect this information, attempting to probe or manipulate the integrated circuits of captured drones to retrieve the output responses of their PUFs will result in irreversible damage to the PUFs due to slight physical variances.

5.1.4. GS Physical Capture Attack

Similarly, suppose an adversary has physically captured GS; the adversary can retrieve stored information $\{Cha_s, Q_s\}$ through power analysis attacks, where $Res_s = PUF(Cha_s)$, $x_s = Q_s \oplus h(Res_s)$. While the adversary can collect this information, attempting to probe or manipulate the integrated circuits of captured drones to retrieve the output responses of their PUFs will result in irreversible damage to the PUFs due to slight physical variances.

5.1.5. Forward and Backward Secrecy

Assume the attacker has complete knowledge of the protocol's long-term keys. However, the random numbers used for session key agreements are not publicly available. Even if the attacker knows long-term keys, he cannot recover earlier or any future session keys.

5.1.6. MITM Attack

To undertake MITM attacks against the proposed protocol, an adversary must intercept and tamper with the communications. According to the preceding description, $\{T_1, A_1, A_2, PID_i\}$ and $\{PID_j, T_3, A_5, A_7, A_8\}$ are protected and unknown to the adversary. The adversary can intercept these messages but cannot modify them. Therefore, the proposed scheme can prevent MITM attacks.

5.1.7. Anonymity and Untraceability

In the proposed protocol, the pseudo-identity of a drone is $PID_i = E_{x_s}(ID_i || d_i || T_i)$, where x_s and T_i are secret values generated by GS. The pseudo-identities of drones are different and unlinkable. The adversary cannot obtain the real identity or trace the drone based on PID_i . Thus, the proposed protocol preserves anonymity and unlinkability.

5.1.8. Desynchronization Attack

The GS generates pseudo-identities on an individual basis. Suppose an attacker initiates assaults that disrupt drone pseudo-identity updates. The attacker interferes with the drone to receive the correct message from GS utilizing tampering and interception. However, this will not affect the drone's authentication. As a result, the suggested protocol can withstand desynchronization attacks.

5.1.9. ESL Attack

Even if an adversary obtains the long-term secret ID_i during the drone-GS authentication and key agreement phase, it is unable to compute the session because it lacks knowledge of a_1 or b_1 . And in the phase of drone-drone authentication and key agreement, it is also unable to compute the session key, because it does not know a_3 or b_2 .

5.1.10. Insider Attack

Because our solution utilizes PUF to protect the security of secret parameters in drones and GS, no internal or external attackers can obtain the secret parameters of drones and GS, thus resisting privileged insider attacks.

5.2. Formal Security Proof

We employ the random oracle model to show the proposed protocol's semantic security. The random oracle model is a theoretical construct used in the analysis of cryptographic protocols. It assumes that certain hash functions or other cryptographic primitives behave like an ideal random function. In this model, when a party queries the random oracle with an input, the oracle returns a uniformly distributed random output that has not been previously returned for any other input, and this random mapping is stored internally. It helps in simplifying the security analysis of protocols by abstracting away the complexity of real-world hash functions and providing a clean framework for proving security properties. In cryptographic security proofs within the random oracle model, a sequence of "games" is used to formally demonstrate that an adversary's advantage in breaking a scheme is negligible.

Definition 1. The participants are composed of Drone(D) and Ground Station(GS). In the i -th instance, the participants are denoted as In_{Di}^i (In_{Dj}^i), and In_{Gi}^i , respectively. The state Accept represents that an oracle receives a correct message. If two oracles are in Accept and the session keys have been agreed, the oracles get their session identities and participant identities. The oracles can be considered partners if their session keys and session identities are the same, and the participant identity is equal to each other's identity.

Definition 2. The queries simulate the capabilities of attackers.

$Execute(In_{Di}^i, In_{Gi}^i, In_{Dj}^i)$: All the messages transmitted openly can be intercepted by the adversary A.

$Send(In_{Di}^i, In_{Gi}^i, In_{Dj}^i, m)$: A forges and sends the message m to In_{Di}^i , In_{Gi}^i or In_{Dj}^i , if m is correct, In_{Di}^i , In_{Gi}^i or In_{Dj}^i responses A.

$Reveal(In_{Di}^i, In_{Gi}^i, In_{Dj}^i)$: A can get the session keys between In_{Di}^i , In_{Gi}^i and In_{Dj}^i .

$Test(In_{Di}^i, In_{Gi}^i, In_{Dj}^i, r)$: This query is only permitted to be run once. which creates a random bit r , and if $r = 1$, returns the real session key; otherwise, returns a random number.

$Corrupt(In_{Di}^i, In_{Dj}^i)$: Which simulates the side-channel attack on the drone, and returns the stored information $\{Cha_i, PID_i, ID_i, Q_i, Y_i\}$.

$CorruptGS(In_{Gi}^i)$: Which simulates the attack of capturing GS, and returns the stored information $\{Cha_s, Q_s\}$.

Definition 3. A is allowed to execute at most once $Test(In_{Di}^i, In_{Gi}^i, In_{Dj}^i, r)$ and multiple other queries to determine the correctness of the return value of $Test(In_{Di}^i, In_{Gi}^i, In_{Dj}^i, r)$. That is A guesses the random bit r generated by $Test(In_{Di}^i, In_{Gi}^i, In_{Dj}^i, r)$. The possibility is $Adv_P^A = |2Pr[Suc(A)] - 1|$, $Adv_P^A < \eta$ represents the protocol is secure, where η is sufficiently small.

Theorem 1. The advantage of obtaining the session key in polynomial time by A is:

$$Adv_P^A \leq \frac{q_H^2}{2^{l_H}} + \frac{(q_{SE} + q_{EX})^2}{n} + 2Adv_{ECDLP}^A + 2q_{SE}Adv_{PUF}^A$$

where q_H , q_{SE} and q_{EX} represents the times of executing Hash, Send, and Execute, respectively. l_H and n are the length of hash and transcripts. The advantage of breaking PUF and ECDLP by Adv_{PUF}^A and Adv_{ECDLP}^A , respectively.

Proof of Theorem 1. The games $Game_i$ ($0 \leq i \leq 4$) are defined to simulate the attacks launched by A . Win_i ($0 \leq i \leq 4$) means A guesses the random bit r in the $Game_i$. The games are defined as:

$Game_0$: This game simulates the real attack first launched by A . According to the definition, we get:

$$Adv_P^A = |2Pr[Win_0] - 1|, \quad (1)$$

$Game_1$: This game simulates the eavesdropping attack. A gets all the messages transmitted publicly. Then, A guesses the random bit r . However, because of the ECDLP, the attacker cannot judge the association between the captured messages and the session keys. Therefore, we get:

$$Pr[Win_0] = Pr[Win_1], \quad (2)$$

$Game_2$: This game simulates the collision attack on the transcripts and hash results, according to the definition of the birthday paradox, the probability of hash collision is less than $\frac{q_H^2}{2^{l_H+1}}$, and the collision probability of other transcripts is less $\frac{(q_{SE}+q_{EX})^2}{2n}$, Therefore, we have:

$$Pr[Win_2] - Pr[Win_1] \leq \frac{q_H^2}{2^{l_H+1}} + \frac{(q_{SE} + q_{EX})^2}{2n}, \quad (3)$$

$Game_3$: This game simulates A executes $Corrupt(In_{Di}^i, In_{Dj}^i)$ and $CorruptGS(In_{Gi}^i)$ to obtain the stored information $\{Cha_i, PID_i, ID_i, Q_i, Y_i\}$ in the drone and $\{Cha_s, Q_s\}$ in GS, where $Res_i = PUF(Cha_i)$, $d_i = Q_i \oplus h(Res_i)$. If A wants to obtain the valuable parameters, he must guess d_i or break PUF. Suppose the probability of breaking PUF by A is Adv_{PUF}^A . Therefore, we have:

$$Pr[Win_3] - Pr[Win_2] \leq q_{SE}Adv_{PUF}^A, \quad (4)$$

$Game_4$: A can obtain $A_5 = a_3 \cdot P$, $B_3 = b_2 \cdot P$, which are used for session keys agreements. This game simulates that A calculates the session keys according to the transcripts. We have:

$$Pr[Win_4] - Pr[Win_3] \leq Adv_{ECDLP}^A, \quad (5)$$

The session keys are generated independently and randomly. Hence, the advantage of guessing r is equal to guessing the session key. We have:

$$Pr[Win_4] = \frac{1}{2}, \quad (6)$$

Combining the above formulas, we have:

$$\frac{1}{2}Adv_P^A = |Pr[Win_0] - \frac{1}{2}| \leq \frac{q_H^2}{2^{l_H+1}} + \frac{(q_{SE} + q_{EX})^2}{2n} + Adv_{ECDLP}^A + q_{SE}Adv_{PUF}^A$$

$$Adv_P^A \leq \frac{q_H^2}{2^{l_H}} + \frac{(q_{SE} + q_{EX})^2}{n} + 2Adv_{ECDLP}^A + 2q_{SE}Adv_{PUF}^A$$

Equations (1)–(6) combined with the final proof typically serve to demonstrate the security properties of the proposed authentication and key agreement protocol. The final proof in ROM typically leverages these equations to conclude that an adversary’s advantage in breaking the protocol is negligible, thereby confirming its robustness. $\square$

5.3. Security Comparison

Table 3 compares the security aspects of the proposed scheme to other relevant AKA protocols for IoD [17,34,35,37]. We choose metrics A1 through A8 to compare the security of the protocols. These metrics are important indicators of protocol security. Failure to meet these security metrics can cause very serious harm to the system.

Table 3. Security comparison.

Feature	[17]	[34]	[35]	[37]	Ours
A1	X	X	✓	✓	✓
A2	X	✓	✓	X	✓
A3	X	✓	✓	✓	✓
A4	✓	✓	✓	✓	✓
A5	X	X	X	X	✓
A6	✓	✓	✓	✓	✓
A7	✓	✓	✓	X	✓
A8	X	✓	X	X	✓

✓: Resist (Attacks); X: Suffer (Attacks). A1: drone physical capture attack; A2: replay attack; A3: desynchronization attack; A4: MITM attack; A5: GS physical capture attack; A6: session key disclosure attack; A7: anonymity and untraceability; A8: perfect forward secrecy.

In [17], the lack of timestamps used in the drone-GS authentication phase can easily lead to replay attacks, the lack of PUF challenge-response values to defend against physical capture attacks by drones and GS, and the lack of mechanisms such as pseudonyms to defend against desynchronization attacks. In [34], neither the drones nor the GS use physical unclonable functions to defend against physical capture attacks. In [35], this scheme uses only physically unclonable functions for drones and does not take into account the security of the GS, which is therefore vulnerable to physical capture attacks. In [37], similarly, no PUF challenge-response value is applied to the GS, leaving the GS vulnerable to physical capture attacks, and this scheme drone-GS phase lacks a timestamping mechanism, leading to vulnerability to replay attacks. The lack of Diffie-Hellman secret value in the negotiation of the session key phase results in no forward security for these schemes in [17,35,37]. Moreover, this protocol does not dynamically update the identity and does not achieve untraceability.

6. Performance Analysis

In this section, we compare the performance between the proposed protocol and the related protocols [17,34–36]. We compare these articles because they are recent studies that introduce innovative solutions to problems in the IoD, each offering valuable insights.

In [17], they propose a lightweight and privacy-preserving mutual AKA protocol for IoD environments. This protocol employs PUF and a chaotic system to accomplish mutual authentication and establish a secure session key between communication entities in the IoD. This protocol is a big improvement in operational efficiency, but it is vulnerable to a variety of attacks such as replay attacks. In [34], they claim to have proposed a lightweight protocol based on ECC for drone authentication, but the system operates inefficiently, and this protocol is vulnerable to physical capture attacks. The same issues as those in the scheme in [36] still exist. In [35], this protocol they proposed dramatically

improves the computational efficiency but does not take into account the security of GS. GS is vulnerable to physical capture attacks, and every authentication between drones requires the participation of GS, making the system less efficient and scalable. We propose an innovative solution to address intractable security problems while minimizing time-consuming computations. Additionally, our approach avoids adding storage overhead to the ground station (GS) as the number of drones increases.

We evaluate the communication efficiency of [17,34–36] by counting the number of exchanged messages. By analyzing the communication sequence diagrams from [17,34–36], we first determine the messages exchanged in a single drone scenario and then calculate the total number of messages for a network of 100 drones. In [17], between a drone and GS, the drone first sends an authentication request to GS, which verifies the message's legitimacy and responds. The drone then verifies the response before sending a final message back to GS in the authentication process. This process requires three messages for a single drone application. For a network of 100 drones, a total of 300 messages are needed. In the case of authentication between two drones, one drone initiates the request-response phase with GS, exchanging two messages. Then, it communicates with the other drone through GS, exchanging four more messages. In total, six messages are required for a single drone interaction, and 600 messages are needed for a network of 100 drones. In [34], only the authentication and key negotiation phases of drones and GS are considered. Five message interactions are required in an application scenario with one drone and 600 messages in a scenario with 100 drones. In [35], the authentication between the drone and GS requires only one request and one response message, while authentication between drones involves four message exchanges. For a single drone application scenario, this results in 2 messages, and for 100 drones, a total of 200 and 400 messages are exchanged, respectively. In [36], the drone and GS authentication involves the Certificate Authority, requiring 5 messages for a single drone application scenario and 500 messages for a network of 100 drones. In our scheme, both Drone-GS authentication and Drone-to-Drone authentication require only one request and one response message. This means that for a scenario with one drone, two messages are exchanged, and for a network of 100 drones, 200 messages are needed. Our scheme significantly outperforms other schemes in terms of communication efficiency and scalability, both for Drone-to-Drone and Drone-to-GS authentication. These results are demonstrated in Figure 5.

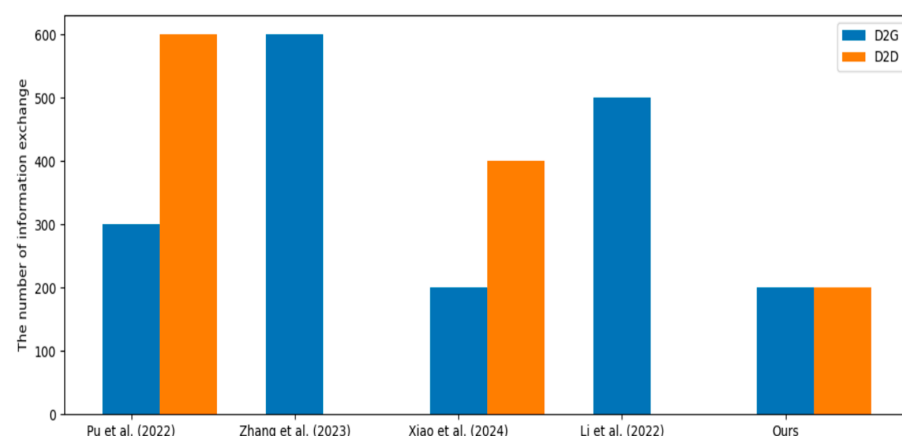


Figure 5. Comparison of information exchange number with existing schemes [17,34–36].

The size of the information exchanged is also considered as a factor of communication efficiency. We consider that the sizes of ID, ECC key, timestamp, hash code, random number, secret number, Henon map value, PUFchallenge, and PUF response are 64 bits, 160 bits, 32 bits, 256 bits, 60 bits, 192 bits, 256 bits, 32 bits, and 320 bits. In the drone-GS AKA phase,

the cost in our protocol is $\{32 + 160 + 256 + 64\} + \{160 + 256 + 256 + 32\} = 1216$ bits, while [17] requires $\{256 + 256 + 256 + 256 + 256 + 256 + 256\} = 1792$ bits, ref. [34] requires 2600 bits, ref. [35] requires $\{64 + 60 + 256 + 32 + 256\} + \{64 + 256 + 256 + 256\} = 1500$ bits, and ref. [36] requires at least 2944 bits. The communication efficiency of our protocol has improved by at least 44.9%. Table 4 shows the communication cost of these protocols. Therefore, our protocol is optimal in terms of communication efficiency and satisfies the lightweight requirement. These results are demonstrated in Figure 6.

Table 4. Communication cost.

Schemes	No. of Messages (Drone-GS)	No. of Messages (Drone-Drone)	Communication Cost (bits)
[17]	3	6	1792
[34]	6	-	2600
[35]	2	4	1500
[36]	5	-	2944
Ours	2	2	1216

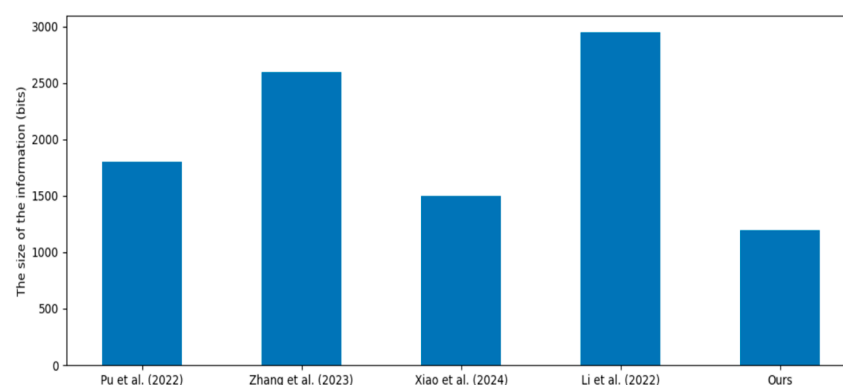


Figure 6. Comparison of computational costs with existing schemes [17,34–36].

To simulate the computing performance of mobile devices in an IoD environment, let T_H be the time of the hash operation, T_{SE} be the time of the symmetric encryption/decryption operation, T_{ECC} be the time cost of ECC operation. These specific performance metrics are among the more time-consuming of the protocols and often determine the performance of the entire system. In the environment of a Windows 10 64-bit laptop, Intel (R) Core (TM) i5-6300HQ CPU @ 2.30 GHz, 12 GB RAM, we get $T_H \approx 0.068$ ms, $T_{ECC} \approx 2.501$ ms, $T_{SE} \approx 0.56$ ms. In the environment of Raspberry Pi 4B, $T_H \approx 0.019$ ms, $T_{ECC} \approx 2.610$ ms, $T_{SE} \approx 0.511$ ms. Although the values of these metrics vary depending on the CPU, memory, and operating system, they illustrate an approximate relationship between the values of the various metrics.

Table 5 provides a comparison of computational costs for the proposed scheme and related schemes. Although the computational overhead of our proposed protocol is not optimal, this scheme ensures a wider variety of security. Efficiency makes sense only when security is ensured.

Table 5. Computation cost.

Schemes	Drone	GS	Total	Times (ms)
[17]	$11T_H$	$11T_H$	$22T_H$	1.496
[34]	$8T_H + 3T_{ECC} + 2T_{SE}$	$8T_H + 3T_{ECC} + 2T_{SE}$	$16T_H + 6T_{ECC} + 4T_{SE}$	18.334
[35]	$8T_H$	$9T_H$	$17T_H$	1.156
[36]	-	-	$5T_H + 6T_{ECC} + 2T_{SE}$	16.16
Ours	$5T_H + 2T_{ECC}$	$5T_H + 2T_{ECC} + 2T_{SE}$	$10T_H + 4T_{ECC} + 2T_{SE}$	11.804

7. Conclusions

We have proposed a secure and lightweight AKA protocol for IoD, effectively addressing critical security threats such as capture attacks, impersonation, and privacy breaches. By integrating PUF and enabling direct drone-to-drone authentication without GS involvement, our protocol enhances both security and efficiency. Additionally, it guarantees perfect forward secrecy, ensuring that past communications remain secure even if future cryptographic keys are compromised. Performance analysis indicates that our scheme improves computational efficiency by an average of 31.3% and communication efficiency by an average of 39.44% compared to existing schemes that offer comparable security. Furthermore, our protocol achieves zero storage overhead for GS authentication, further optimizing resource utilization. Formal security proof validates its robustness, making it a reliable and scalable solution for IoD deployments. In practical applications, this protocol strengthens authentication mechanisms in drone networks, enabling secure, efficient, and scalable communication. This is particularly beneficial for applications such as surveillance, disaster response, and logistics, where reliable and low-latency authentication is essential.

The limitation of our protocol is that it does not consider cross-domain scenarios. Future research will focus on developing cross-domain drone-to-GS authentication schemes that eliminate the need for GS to store drone information, as well as cross-domain drone-to-drone authentication mechanisms that operate without GS involvement. These advancements will further enhance the scalability and flexibility of IoD authentication systems.

Author Contributions: Q.X., writing—review and editing, resources, supervision, and funding acquisition; J.Z., writing—original draft. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Hangzhou Joint Fund of the Zhejiang Provincial Natural Science Foundation of China (Grant No. LHZSZ24F020002) and the National Natural Science Foundation of China (Grant No. U21A20466).

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Rodrigues, M.; Amaro, J.; Osório, F.S.; RLJC, B.K. Authentication methods for UAV communication. In Proceedings of the 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 29 June–3 July 2019; pp. 1210–1215.
2. Chamola, V.; Hassija, V.; Gupta, V.; Guizani, M. A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. *IEEE Access* **2020**, *8*, 90225–90265. [\[CrossRef\]](#)
3. Liu, X.; Li, Z.; Zhao, N.; Meng, W.; Gui, G.; Chen, Y.; Adachi, F. Transceiver design and multihop D2D for UAV IoT coverage in disasters. *IEEE Internet Things J.* **2018**, *6*, 1803–1815. [\[CrossRef\]](#)
4. Gharibi, M.; Boutaba, R.; Waslander, S.L. Internet of drones. *IEEE Access* **2016**, *4*, 1148–1162. [\[CrossRef\]](#)
5. Hall, R.J. An internet of drones. *IEEE Internet Comput.* **2016**, *20*, 68–73. [\[CrossRef\]](#)
6. Abdelmaboud, A. The internet of drones: Requirements, taxonomy, recent advances, and challenges of research trends. *Sensors* **2021**, *21*, 5718. [\[CrossRef\]](#) [\[PubMed\]](#)
7. Wazid, M.; Das, A.K.; Kumar, N.; Vasilakos, A.V.; Rodrigues, J.J.P.C. Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment. *IEEE Internet Things J.* **2018**, *6*, 3572–3584. [\[CrossRef\]](#)
8. Yang, W.; Wang, S.; Yin, X.; Wang, X.; Hu, J. A review on security issues and solutions of the internet of drones. *IEEE Open J. Comput. Soc.* **2022**, *3*, 96–110. [\[CrossRef\]](#)
9. He, D.; Chan, S.; Guizani, M. Communication security of unmanned aerial vehicles. *IEEE Wirel. Commun.* **2016**, *4*, 134–139. [\[CrossRef\]](#)
10. Altawy, R.; Youssef, A.M. Security, privacy, and safety aspects of civilian drones: A survey. *ACM Trans. Cyber-Phys. Syst.* **2016**, *1*, 1–25. [\[CrossRef\]](#)
11. Pu, C. Jamming-resilient multipath routing protocol for flying ad hoc networks. *IEEE Access* **2018**, *6*, 68472–68486. [\[CrossRef\]](#)

12. Michailidis, E.T.; Vouyioukas, D. A review on software-based and hardware-based authentication mechanisms for the internet of drones. *Drones* **2022**, *6*, 41. [\[CrossRef\]](#)
13. Huang, Y.; Mu, J.; Wang, Y.; Zhao, R. A Review of Authentication Methods in Internet of Drones. In Proceedings of the 2023 International Conference on Networking and Network Applications (NaNA), Qingdao, China, 18–21 August 2023; pp. 7–12.
14. Ashrif, F.F.; Sundararajan, E.A.; Ahmad, R.; Hasan, M.K.; Yadegaridehkordi, E. Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction. *J. Netw. Comput. Appl.* **2024**, *221*, 103759. [\[CrossRef\]](#)
15. Mall, P.; Amin, R.; Das, A.K.; Leung, M.T.; Choo, K.K.R. PUF-based authentication and key agreement protocols for IoT, WSNs, and smart grids: A comprehensive survey. *IEEE Internet Things J.* **2022**, *9*, 8205–8228. [\[CrossRef\]](#)
16. Hasan, M.K.; Weichen, Z.; Safie, N.; Ahmed, F.R.A.; Ghazal, T.M. A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. *IEEE Access* **2024**, *12*, 61642–61666. [\[CrossRef\]](#)
17. Soni, M.; Singh, D.K. LAKA: Lightweight authentication and key agreement protocol for internet of things based wireless body area network. *Wirel. Pers. Commun.* **2022**, *127*, 1067–1084.
18. Pu, C.; Wall, A.; Choo, K.K.R.; Ahmed, I.; Lim, S. A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of Drones environment. *IEEE Internet Things J.* **2022**, *9*, 9918–9933. [\[CrossRef\]](#)
19. Hajian, R.; Haghighat, A.; Erfani, S.H. A secure anonymous D2D mutual authentication and key agreement protocol for IoT. *Internet Things* **2022**, *18*, 100493. [\[CrossRef\]](#)
20. Jan, S.U.; Qayum, F.; Khan, H.U. Design and analysis of lightweight authentication protocol for securing IoD. *IEEE Access* **2021**, *9*, 69287–69306. [\[CrossRef\]](#)
21. Cheon, J.H.; Han, K.; Hong, S.M.; Kim, H.J.; Kim, J.; Kim, S.; Seo, H.; Shim, H.; Song, Y. Toward a secure drone system: Flying with real-time homomorphic authenticated encryption. *IEEE Access* **2018**, *6*, 24325–24339. [\[CrossRef\]](#)
22. Jiang, C.; Fang, Y.; Zhao, P.; Panneerselvam, J. Intelligent UAV identity authentication and safety supervision based on behavior modeling and prediction. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6652–6662. [\[CrossRef\]](#)
23. Wang, W.; Han, Z.; Gadekallu, T.R.; Raza, S.; Tanveer, J.; Su, C. Lightweight blockchain-enhanced mutual authentication protocol for UAVs. *IEEE Internet Things J.* **2023**, *11*, 9547–9557. [\[CrossRef\]](#)
24. García, J.C.P.; Benslimane, A.; Braeken, A.; Su, Z. μ Tesla-Based Authentication for Reliable and Secure Broadcast Communications in IoD Using Blockchain. *IEEE Internet Things J.* **2023**, *10*, 18400–18413. [\[CrossRef\]](#)
25. Tan, Y.; Wang, J.; Liu, J.; Kato, N. Blockchain-assisted distributed and lightweight authentication service for industrial unmanned aerial vehicles. *IEEE Internet Things J.* **2022**, *9*, 16928–16940. [\[CrossRef\]](#)
26. Zhang, Y.; He, D.; Li, L.; Chen, B. A lightweight authentication and key agreement scheme for Internet of Drones. *Commun.* **2020**, *154*, 455–464. [\[CrossRef\]](#)
27. Hussain, S.; Farooq, M.; Alzahrani, B.A.; Albeshri, A.; Alsubhi, K.; Chaudhry, S.A. An efficient and reliable user access protocol for Internet of Drones. *IEEE Access* **2023**, *11*, 59688–59700. [\[CrossRef\]](#)
28. Yu, S.; Das, A.K.; Park, Y. SLAP-IoD: Secure and lightweight authentication protocol using physical unclonable functions for internet of drones in smart city environments. *IEEE Trans. Veh. Technol.* **2022**, *71*, 10374–10388. [\[CrossRef\]](#)
29. Alladi, T.; Venkatesh, V.; Chamola, V.; Chaturvedi, N. Drone-MAP: A novel authentication scheme for drone-assisted 5G networks. In Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 10–13 May 2021; pp. 1–6.
30. Wu, T.; Guo, X.; Chen, Y.; Kumari, S.; Chen, C. Amassing the security: An enhanced authentication protocol for drone communications over 5G networks. *Drones* **2021**, *6*, 10. [\[CrossRef\]](#)
31. Bansal, G.; Chamola, V.; Sikdar, B. SHOTS: Scalable secure authentication-attestation protocol using optimal trajectory in UAV swarms. *IEEE Trans. Veh. Technol.* **2022**, *71*, 5827–5836. [\[CrossRef\]](#)
32. Javed, S.; Khan, M.A.; Abdullah, A.M.; Alsirhani, A.; Alomari, A.; Noor, F.; Ullah, I. An efficient authentication scheme using blockchain as a certificate authority for the internet of drones. *Drones* **2022**, *6*, 264. [\[CrossRef\]](#)
33. Mishra, A.K.; Wazid, M.; Singh, D.P.; Das, A.K.; Singh, J.; Vasilakos, A.V. Vasilakos. Secure Blockchain-Enabled Authentication Key Management Framework with Big Data Analytics for Drones in Networks Beyond 5G Applications. *Drones* **2023**, *7*, 508. [\[CrossRef\]](#)
34. Zhang, S.; Liu, Y.; Han, Z.; Yang, Z. A lightweight authentication protocol for UAVs based on ECC scheme. *Drones* **2023**, *7*, 315. [\[CrossRef\]](#)
35. Xiao, Y.; Tao, Y. SLAKA-IoD: A Secure and Lightweight Authentication and Key Agreement Protocol for Internet of Drones. *Drones* **2024**, *8*, 374. [\[CrossRef\]](#)
36. Li, L.; Lian, X.; Wang, Y.; Tan, L. CSECMAS: An efficient and secure certificate signing based elliptic curve multiple authentication scheme for drone communication networks. *Appl. Sci.* **2022**, *12*, 9203. [\[CrossRef\]](#)
37. Bansal, G.; Sikdar, B. Location aware clustering: Scalable authentication protocol for UAV swarms. *IEEE Netw. Lett.* **2021**, *3*, 177–180. [\[CrossRef\]](#)

38. Cho, G.; Cho, J.; Hyun, S.; Kim, H. SENTINEL: A Secure and Efficient Authentication Framework for Unmanned Aerial Vehicles. *Appl. Sci.* **2020**, *10*, 3149. [[CrossRef](#)]
39. Yu, S.; Lee, J.; Sutrala, A.K.; Das, A.K.; Park, Y. LAKA-UAV: Lightweight authentication and key agreement scheme for cloud-assisted Unmanned Aerial Vehicle using blockchain in flying ad-hoc networks. *Comput. Netw.* **2023**, *224*, 109612. [[CrossRef](#)]
40. Bhattarai, I.; Pu, C.; Choo, K.-K.R.; Korać, D. A Lightweight and Anonymous Application-Aware Authentication and Key Agreement Protocol for the Internet of Drones. *IEEE Internet Things J.* **2024**, *11*, 19790–19803. [[CrossRef](#)]
41. Alkathiri, M.S.; Saleem, S.; Alqarni, M.A.; Aseeri, A.O.; Chauhdary, S.H.; Zhuang, Y. A Lightweight Authentication Scheme for a Network of Unmanned Aerial Vehicles (UAVs) by Using Physical Unclonable Functions. *Electronics* **2022**, *11*, 2921. [[CrossRef](#)]
42. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [[CrossRef](#)]
43. Canetti, R.; Krawczyk, H. Universally composable notions of key exchange and secure channels. In Proceedings of the Advances in Cryptology—EUROCRYPT 2002: International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, 28 April–2 May 2002; pp. 337–351.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.