A Blockchain-Based Cross-Domain Authentication and Flight Trajectory Privacy Protection Scheme for Unmanned Aerial Vehicle Networks

Gongzhe Qiao, Panlong Yang, *Senior Member, IEEE*, Tong Ye, and Feiyu Han

***Abstract*—The rapid expansion of the low-altitude economy has propelled the increasing cross-domain applications of unmanned aerial vehicles (UAVs). During cross-domain missions, UAVs face challenges in identity management and trajectory privacy protection. The conventional centralized identity management model is susceptible to single-point failures and blockchain-based solutions suffer from performance bottlenecks. Also, the high dynamics of low-altitude networks further exacerbates the risk of trajectory data leakage. To address these problems, this article proposes a consortium blockchain (CBC)-based cross-domain authentication and flight trajectory privacy protection scheme, which includes cross-domain authentication, key agreement, dynamic identity changing, mutual authentication, and domain notification methods. The proposed blockchain-based method enables trusted cross-domain identity verification, preventing attackers from reconstructing full flight paths with partial information. Formal verification based on the real-or-random model is presented to prove the semantic security of the proposed method. Informal security analysis ensures that the proposed method resists major cyber-attacks. The performance of the proposed method is evaluated through simulations. The experimental results show that the proposed method has higher efficiency compared to the existing methods.**

***Index Terms*—Blockchain, cross-domain authentication, key agreement, trajectory privacy protection, unmanned aerial vehicle (UAV) network.**

NOMENCLATURE

DCC_i	Domain control center of the domain i.
d_j	UAV j.
FP	Flight path in the current domain.
$Pid^i_{d_j}$	ID of UAV d_j in the domain i.
SK_{d_j}	Private key of d_j.
PK_{d_j}	Public key of d_j.
SK_{DCC_i}	Private key of DCC_i.
PK_{DCC_i}	Public key of DCC_i.
$Sig_{DCC_i}()$	Digital signature function of DCC_i.
CBC	Consortium blockchain.
PBC_i	Private blockchain of the domain i.
$*PBH_{d_j}$	Block number of the PBC block that includes the task information of d_j.
$CNid_c$	ID of the current domain.
$CNid_n$	ID of the next domain.
$CNid_d$	ID of the destination domain.

Received 18 August 2025; revised 10 October 2025; accepted 27 October 2025. Date of publication 31 October 2025; date of current version 8 January 2026. This work was supported in part by The Startup Foundation for Introducing Talent of NUIST under Grant 1083142501012. *(Corresponding author: Panlong Yang.)*

Gongzhe Qiao, Panlong Yang, and Feiyu Han are with the School of Computer Science, School of Cyber Science and Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: qgz@nuaa.edu.cn; 003829@nuist.edu.cn; fyhan@nuist.edu.cn).

Tong Ye is with the College of Computer and Software, Nanjing University of Industry Technology, Nanjing 210023, China (e-mail: yetong@nuaa.edu.cn).

Digital Object Identifier 10.1109/JIOT.2025.3627629

I. INTRODUCTION

WITH the rapid development of the low-altitude economy, unmanned aerial vehicles (UAVs) have witnessed increasingly widespread applications across diverse domains, including urban air mobility (UAM), logistics delivery, emergency rescue, and environmental monitoring, thereby driving a substantial surge in cross-domain mission requirements [1]. As depicted in Fig. 1, when executing missions such as logistics delivery, UAVs require cross-domain authentication and communication with DCCs. Typically, three categories of communication behaviors are involved: UAV-to-UAV (U2U), UAV-to-infrastructure (U2I), and UAV-to-person (U2P) [2], [3]. However, UAVs face significant challenges in identity management and trajectory privacy protection during cross-domain missions [4], [5]. These issues have become key factors limiting the security and efficiency of low-altitude networks.

Currently, countries around the world are actively promoting the construction of low-altitude network infrastructure, and cross-domain flight of UAVs has become the norm. The differences among different airspace management entities and operation platforms complicate the identity authentication and management of UAVs. Meanwhile, high-precision sensors on UAVs can collect sensitive data such as location and trajectory in real time. Such data is vulnerable to theft by attackers through signal interception and trajectory correlation analysis, which not only threatens personal privacy but may also cause damage to national security and commercial interests [5].

Cross-domain flight requires UAVs to break through the restrictions of a single management domain and seamlessly navigate between domains under different administrative regions, controlled areas (e.g., airport clearance zones and military control zones), and operating entities (e.g., logistics enterprises and government departments). Their identity authentication and trajectory data need to be shared and interacted among multiple stakeholders. However, traditional

2327-4662 © 2025 IEEE. All rights reserved, including rights for text and data mining, and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Army Engineering Univ of PLA(f. PLA U of S&T). Downloaded on January 20,2026 at 08:23:16 UTC from IEEE Xplore. Restrictions apply.

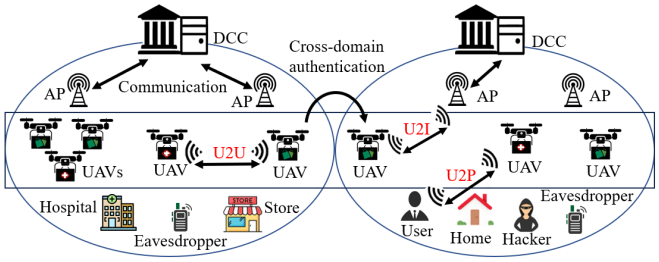

Fig. 1. Scenario of the UAV delivery and the communication types.

centralized identity management architectures, such as systems based on certificate authority (CA), have exposed defects in cross-domain scenarios, including single points of failure, high trust costs, and concentrated risks of privacy leakage [6].

Currently, UAV identity management and trajectory privacy protection in low-altitude networks face the following challenges.

1) In cross-domain scenarios, the identity authentication standards and protocols of different domain management entities (e.g., civil aviation administrations, local governments, and enterprises) are incompatible with each other. Users and UAVs are required to repeatedly register their identities when crossing domains. Meanwhile, the lack of a trusted data-sharing bridge between domains leads to low efficiency in identity verification and excessive exposure of identity information [1].
2) The traditional centralized identity management model is prone to single-point failure and fails to meet the dynamic access requirements of large-scale UAVs [6].
3) Flight trajectories of UAVs have the characteristics of spatiotemporal continuity and behavioral regularity. By integrating partial trajectory fragments (e.g., takeoff points and transit nodes) disclosed across multiple domains, attackers can reconstruct complete flight paths, thereby enabling long-term tracking of specific UAVs.

Existing studies [1], [6], [7], [8], [9] have attempted to introduce blockchain technology into identity management in low-altitude networks, enabling cross-domain identity registration and authentication through decentralized ledgers. However, most existing solutions either focus on identity verification within a single domain or adopt a public chain architecture, which leads to performance bottlenecks (e.g., the throughput of the Bitcoin blockchain is only 7 transactions per second) and thus cannot meet the requirements of real-time identity verification and high-frequency interaction of trajectory data in cross-domain scenarios.

In addition, the majority of existing studies [10], [11], [12] treat identity management and trajectory privacy as separate entities, failing to establish a collaborative protection mechanism for the two in cross-domain scenarios. This inadequacy renders them ineffective in defending against composite attacks that integrate identity association and trajectory inference. Furthermore, the high dynamics of low-altitude networks (such as the rapid movement of UAVs and frequent changes in network topology) lead to delayed key updates in traditional encryption algorithms, thereby further exacerbating the risk of trajectory data leakage. Conventional differential privacy and trajectory anonymization techniques face challenges in balancing the intensity of privacy protection and data utility in cross-domain scenarios.

To address the aforementioned challenges and issues, this article proposes a federated blockchain-based collaborative protection framework for identity obfuscation and flight trajectory privacy, tailored to the scenario of cross-domain UAV collaborative missions. The contributions are as follows.

1) To address the incompatibility of identity authentication protocols across domains, repeated identity registration, and the lack of trusted data-sharing mechanisms, this article proposes a unified cross-domain identity authentication framework for UAVs. This framework establishes interoperable authentication protocols, eliminates redundant registration processes for users and UAVs during cross-domain operations, and constructs a secure data-sharing bridge to enhance identity verification efficiency while reducing unnecessary exposure of identity information.
2) Aiming at the single-point failure vulnerability of traditional centralized identity management models and their inability to adapt to the dynamic access needs of large-scale UAVs, this article designs a distributed identity management architecture using blockchain. This architecture eliminates reliance on a central authority, enhances system robustness, and supports flexible and real-time access control to accommodate the dynamic characteristics of large-scale UAV operations. Compared with existing studies, the proposed scheme can not only verify the authenticity of identities but also validate the authenticity of missions.
3) To mitigate the risk of complete flight path reconstruction and long-term tracking of specific UAVs, this article develops a trajectory privacy protection mechanism. The hierarchical identity coding scheme is designed to map the real identity of UAVs to dynamically changing anonymous identifiers. Leveraging the consensus algorithm of the CBC, trusted verification of cross-domain identities is achieved, enabling the authentication process to be completed without disclosing the original identity, preventing attackers from integrating partial information to reconstruct full flight paths and thus safeguarding UAV trajectory privacy.

The structure of this article is as follows. Section II reviews the progress of related research. Section III constructs a cross-domain UAV CBC system model and presents the security model and security requirements. Section IV presents the detailed steps of the proposed method. Section V analyzes the security of the proposed method from both formal and informal perspectives. Section VI evaluates the performance of the proposed method through simulation experiments. Section VII concludes this article and outlines future directions.

II. Related Work

A. Cryptographic-Based Identity Authentication Method

During mission execution, drones must undergo cross-domain authentication to verify their identity. To counter

Authorized licensed use limited to: Army Engineering Univ of PLA(f. PLA U of S&T). Downloaded on January 20,2026 at 08:23:16 UTC from IEEE Xplore. Restrictions apply.

potential security threats, researchers have developed cryptographic cross-domain authentication schemes. For instance, Tanveer et al. [13] proposed a robust authentication mechanism for the Internet of Drones (IoDs) by combining elliptic curve cryptography (ECC), symmetric encryption, and hash functions to defend against various attacks. In scenarios where attackers may intercept data from open network channels, Jan et al. [14] introduced an ECC-based authentication mechanism for the IoD with provable security guarantees. Rajamanickam et al. [15] implemented an elliptic curve cryptographic authentication mechanism designed to prevent insider compromises in IoD networks, thereby enhancing the security of IoD systems against multiple documented threats. Jawad et al. [16] proposed a lightweight UAV authentication system where a ground control station (GCS) verifies multiple UAVs using chaotic map-derived session keys tied to preregistered flight plans. Mahmood et al. [17] proposed a lightweight authentication protocol for the IoDs, integrating chaotic maps, hash functions, and physical unclonable functions (PUFs) to counter impersonation, replay, and physical cloning attacks. However, these approaches enhance security at the cost of increased computational overhead, as they require extensive parameter processing across devices, registration centers, and control centers.

B. Identity Management and Authentication Technology Based on Blockchain

The open and insecure nature of drone communications poses critical challenges to data integrity and authentication, driving the adoption of blockchain-enabled IoDs frameworks. Recent advancements in blockchain-based decentralized identity management have reshaped UAV authentication paradigms, replacing traditional centralized authorities with tamper-resistant smart contracts, addressing inherent vulnerabilities of centralized authentication systems, such as single-point failures. Jain et al. [18] systematically examined blockchain-based solutions for IoD vulnerabilities, offering experimental comparisons of consensus algorithms, security model analyses, and machine learning-integrated recommendations to advance resilient drone networks. Vardhan et al. [19] proposed a blockchain-enhanced lightweight authentication scheme for IoD devices, combining ECC-based mutual authentication with tamper-resistant smart cards to ensure anonymity and defend against brute-force and DoS attacks. Subramani et al. [20] proposed a blockchain-enabled authentication framework that ensures physical security and privacy preservation for drones, enabling rapid reauthentication through dynamic transfer of credential codes between UAV operators without requiring local secret key storage. Huang et al. [21] proposed BAKAS-UAV, a blockchain-assisted authentication and key agreement framework integrating elliptic curve cryptography and PUFs to support both hierarchical UAV-ground and peer-to-peer UAV authentication modes without ground station intermediation. To prevent valuable industrial data leakage, Tan et al. [7] designed a blockchain-assisted distributed and lightweight authentication service for industrial UAVs.

However, the above identity management and authentication framework mainly focuses on data security and neglects the management efficiency when facing a large number of drones. In addition, the blockchain-based methods have not been able to reasonably partition the data storage on the chain, leading to low query efficiency and data isolation. While prior studies have improved trustworthiness in UAV ecosystems, critical challenges persist in dynamic node enrollment, cross-domain identity interoperability, and real-time authentication latency.

C. Privacy Enhancement and Cross Domain Collaboration Technology

In low-altitude network environments, privacy-enhancing and cross-domain collaboration technologies play a pivotal role in ensuring UAV flight safety, protecting data privacy, and facilitating efficient cross-domain operations. These technologies aim to meet the complex requirements of cross-domain UAV operations while minimizing risks of identity information and flight trajectory data leakage. Current research has explored various approaches in privacy enhancement and cross-domain authentication. To protect data security in multiparty computation models, Pei et al. [8] proposed a blockchain-assisted verifiable secure multiparty data computing approach for privacy preservation to prevent privacy leakage when users and multiple participants share data. Chandran and Vipin [22] proposed an authentication and key agreement protocol for multi-UAV networks, grounded in PUF technology, which leverages PUF technology to enhance security. Sharma and Mehra [23] proposed a hyperelliptic curve and fuzzy extractor-based secure authentication protocol for IoT-based UAV networks. For the scenario of package delivery and data collection, Enayati et al. [10] proposed a privacy-preserving mechanism to randomize the UAV's trajectory, making observers confused to detect the UAV's destination. Wang et al. [24] proposed a lightweight UAV cross-domain authentication and key agreement scheme using symmetric encryption and hash functions, enabling direct authentication via tokens and secure key establishment with ground stations. Zhang et al. [25] proposed a blockchain-based certificateless cross-domain authentication and key agreement (CL-AKA) protocol for IoD, leveraging Chebyshev chaotic mapping to achieve robust security and resist known attacks. Xie et al. [26] proposed BASUV, a blockchain-based authentication scheme for UAV-assisted IoV systems, enabling secure decentralized certificate management while supporting dynamic UAV registration and removal. Cai et al. [27] proposed a robust cross-domain UAV RF fingerprinting (RFFI) method that leverages domain-invariant adversarial training and manifold-level regularization to extract class-specific features. Pu et al. [28] proposed ReBAS, a redactable blockchain-assisted application-aware authentication system for next-gen IoD, enabling secure drone authentication across dynamic flying zones during multitype data collection. Akram and Anaissi [29] presented a privacy-first crowdsourcing framework that combines differential privacy (DP) for provider anonymity with blockchain-based accountability, establishing a trustworthy data exchange platform for emergency drone services that balances privacy preservation with data utility.

However, current approaches still have limitations. While conventional encryption techniques ensure data confidentiality,

Authorized licensed use limited to: Army Engineering Univ of PLA(f. PLA U of S&T). Downloaded on January 20,2026 at 08:23:16 UTC from IEEE Xplore. Restrictions apply.

their substantial computational overhead may compromise flight performance and endurance for resource-constrained UAVs. Cross-domain authentication schemes relying on trusted third parties are vulnerable to single-point failures. Any compromise or malfunction of the central authority would paralyze the entire authentication system. Blockchain implementations face challenges of low consensus efficiency and excessive storage demands, rendering them unsuitable for large-scale, high-frequency cross-domain UAV operations. While DP protects trajectories through noise addition, its inherent privacy-utility tradeoff risks significant data distortion that could undermine subsequent trajectory-based analyses and operational decisions.

III. System Model, Security Model, and Security Requirements

A. System Model

The demand for secure and decentralized authentication in UAV networks necessitates a hierarchical blockchain architecture. As depicted in Fig. 2, the proposed system comprises multiple autonomous domains, each integrating a DCC, PBC nodes, access points (APs), and UAV fleets, with cross-domain coordination achieved through a CBC. The functional roles are defined as follows.

1) DCC acts as the core governance entity, managing domain-specific operations including UAV registration, dynamic credential issuance, and anomaly detection. It deploys edge-based smart contracts for real-time authentication while maintaining synchronized revocation lists with the PBC.
2) CBC operates as an interdomain ledger jointly maintained by participating DCCs. It stores immutable authentication records, executes cross-domain smart contracts, and validates interdomain transactions through Byzantine fault tolerance consensus.
3) PBC functions as a lightweight intradomain ledger managed by local DCC. It records UAV operational data (e.g., flight logs and energy status) and processes high-frequency authentication requests via optimized practical Byzantine fault tolerance (PBFT) consensus.
4) APs serve as blockchain-enabled authentication gateways. Equipped with lightweight verification modules, they validate UAV signatures through on-chain credentials and provide secure data offloading services.
5) UAVs as mobile network entities carry embedded hardware wallets storing identity certificates. During cross-domain mobility, they initiate authentication requests via APs and update operational status to PBC through DCC-authorized transactions.

The privacy-sensitive information recorded on PBC is not exposed across the entire blockchain network. CBC can ensure only relevant DCCs access and process cross-domain transaction information. In addition, the architecture facilitates blockchain network maintenance and management, further reducing maintenance costs.

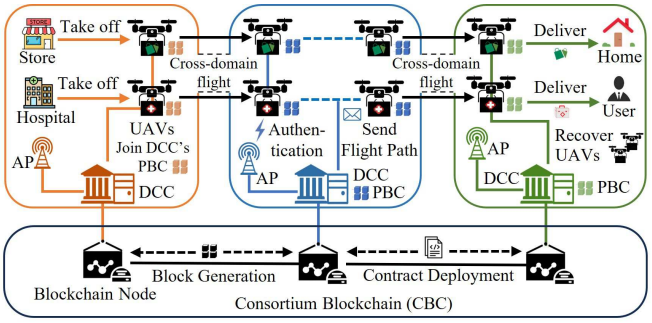

Fig. 2. System model based on CBC and domain PBC.

B. Adversary Model

In this system, we consider the well-accepted Dolev-Yao threat model to describe the behaviors of the adversary. This model assumes that wireless communication channels are insecure. Therefore, the adversary can access all the information exchanged by the drone during cross-domain authentication. The adversary has complete knowledge of the authentication protocol, can manipulate the open communication channel, and participate in the protocol execution. To be specific, the adversary has the ability to perform malicious operations, including eavesdropping, interception, replay attacks, data modification, and packet fabrication through the public channel. Such capabilities pose significant risks to the confidentiality, integrity, and availability of communications within the low-altitude network.

C. Security and Performance Requirements

The cross-domain authentication method for the UAVs has the following security and performance requirements.

1) *Anonymity:* The method should ensure the anonymity of drones to prevent the adversary from recognizing the real identity of the UAVs from the intercepted authentication messages. The UAVs should avoid exposing unique identifiers (such as serial numbers, MAC addresses) in communication and use dynamic temporary IDs or anonymous certificates instead.
2) *Path Confidentiality:* When the UAVs perform tasks such as logistics distribution, military reconnaissance, and disaster monitoring, the flight paths may involve sensitive information, and it is necessary to ensure that the path information is not illegally obtained by the adversary. The comparison of attack scenarios with and without trajectory privacy protection is shown in Fig. 3.
3) *Cross-Domain Mutual Authentication:* The method should support mutual verification of legitimacy between the UAVs or ground stations in different security domains to prevent forgery attacks.
4) *Forward Security:* The proposed method should guarantee that even if an adversary intercepts all exchanged messages during the authentication phase, he cannot derive the long-term secret parameters or session keys of the UAVs or ground stations.
5) *Resistance to Replay Attacks:* During the communication of the UAVs, the adversary may intercept and reply to legitimate commands, such as control signals,

Authorized licensed use limited to: Army Engineering Univ of PLA(f. PLA U of S&T). Downloaded on January 20,2026 at 08:23:16 UTC from IEEE Xplore. Restrictions apply.

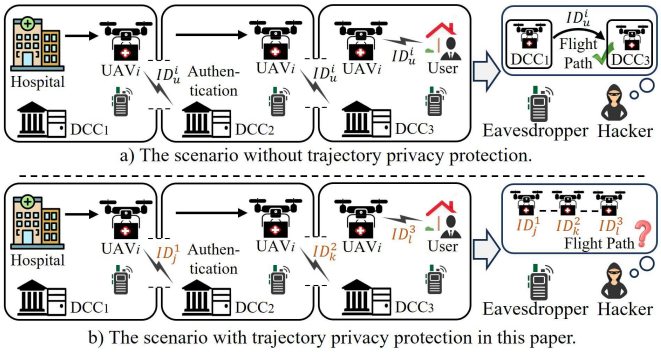

Fig. 3. Comparison of attack scenarios. (a) Scenario without trajectory privacy protection. (b) Scenario with trajectory privacy protection.

identity authentication messages, and navigation data, resulting in the UAV performing incorrect operations. The proposed method should ensure that the receiver only processes the latest instructions and rejects expired or duplicate messages.

6) *Resistance to Man-in-the-Middle Attacks:* The adversary may launch man-in-the-middle attacks through open channels. The attacks are difficult to detect actively by both communicating parties. The proposed method should ensure that the UAVs or ground stations verify each other's identities before communication, preventing the adversary from disguising themselves as each party.
7) *Resistance to Physical Capture Attacks:* The proposed method should provide a security protection mechanism to ensure that even if the UAVs are physically captured by the adversary, the secret parameters cannot be retrieved to affect the security of other UAVs or ground stations.
8) *Low Latency Communication:* Cross-domain operations require real-time data transmission, such as control instructions and status feedback, to avoid accidents caused by communication delay.
9) *Cross-Domain Protocol Compatibility:* Compatible with different regional communication standards, such as 4G/5G, satellite links, and LoRa, to ensure seamless cross-domain communication.

IV. Proposed Scheme

In this section, we give a detailed description of our scheme, which mainly consists of the registration mechanism, the cross-domain authentication method, the two-way authentication strategy, and the notification mechanism between domains. Detailed steps for each part are provided in Sections IV-A–IV-D.

A. Registration Mechanism

The registration mechanism is categorized into two types: initial registration of new UAVs or users and the UAV registration for task execution. For the convenience of introducing the proposed method, the symbols and definitions used are shown in Nomenclature. In the initial registration process, the information about the new UAV (including unique hardware codes MAC ID, model specifications, and UAV parameters) or user personal data (including usernames and passwords for client/application login and phone numbers) is stored in traditional databases to facilitate query and maintenance by staff. When the DCC receives a request for a delivery task, it identifies a suitable UAV from the available UAV database and completes the UAV registration for task execution. The UAV registration process for task execution includes the following steps.

Step 1: DCC_i selects a suitable UAV d_j with hardware ID mac_{d_j} to execute the mission. Furthermore, DCC_i computes the intradomain flight path and cross-domain path for the task based on the task information, derives the ID of the next domain Did_n, and calculates the estimated departure time from the current domain T_{out}.

Step 2: DCC_i assigns a unique ID in its domain to the UAV d_j, which is denoted as $\mathrm{Pid}^i_{d_j}$. In addition, DCC_i computes the pair of public key (PK_{d_j}) and private key (SK_{d_j}) for d_j. Moreover, DCC_i utilizes its own private key ($\mathrm{SK}_{\mathrm{DCC}_i}$) to generate a digital signature $\mathrm{Sig}_{\mathrm{DCC}_i}(\mathrm{Pid}^i_{d_j})$.

Step 3: DCC_i sends the flight path in the current domain (FP), the ID ($\mathrm{Pid}^i_{d_j}$), the private key of d_j (SK_{d_j}), the public key of DCC_i ($\mathrm{PK}_{\mathrm{DCC}_i}$), the public key of DCC_n ($\mathrm{PK}_{\mathrm{DCC}_n}$), the digital signature ($\mathrm{Sig}_{\mathrm{DCC}_i}(\mathrm{Pid}^i_{d_j})$), the domain PBC PBC_i = ($\mathrm{Pid}^i_{d_j}$, PK_{d_j}) and the block height PBH_{d_j} to UAV d_j via a secure channel. Then, DCC_i updates the PBC_i. We do not consider the identity transformation of UAVs within a domain. Therefore, the identifier of an UAV is the unique identifier in the current domain.

Step 4: DCC_i submits a mission request structured as mission = $\{\mathrm{Pid}^i_{d_j}, \mathrm{CNid}_c, \mathrm{CNid}_n, \mathrm{CNid}_d, T_{\mathrm{out}}\}$ to other DCCs on the CBC. Upon reaching consensus among CBC members, the mission is assigned a unique mission ID (Mid), and the CBC chain is updated with mission = $\{\mathrm{Mid}, \mathrm{Pid}^i_{d_j}, \mathrm{PK}_{d_j}, \mathrm{CNid}_c, \mathrm{CNid}_n, \mathrm{CNid}_d, T_{\mathrm{out}}\}$.

Step 5: UAV d_j flies along the planned path, updating its local PBC throughout the mission execution process. Simultaneously, DCC_i archives the mission's detailed information in the local database and removes d_j from the local available UAV database.

Furthermore, the following assumptions are made: 1) each DCC possesses the public keys of other DCCs, and the private key of each DCC remains undisclosed; 2) the private key of the UAV executing a task is secure from leakage; and 3) attackers cannot decrypt messages encrypted with public or private keys within a short time.

B. Cross-Domain Authentication Method

During mission-critical operations, UAVs exchange data with DCCs through insecure wireless links in public networks, where transmitted information constitutes sensitive data. To mitigate security risks and ensure confidentiality, a provably secure mutual authentication protocol with efficient key agreement is essential. Following successful mutual authentication, all subsequent communications are encrypted using the dynamically generated session keys.

The proposed authentication and key agreement (AKA) protocol is shown in Fig. 4, which comprises the following steps.

Authorized licensed use limited to: Army Engineering Univ of PLA(f. PLA U of S&T). Downloaded on January 20,2026 at 08:23:16 UTC from IEEE Xplore. Restrictions apply.

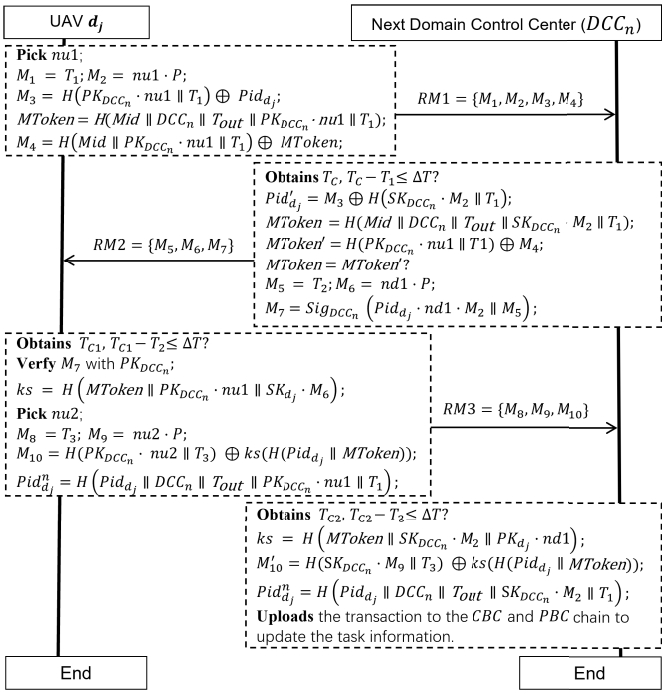

Fig. 4. Proposed authentication and key agreement protocol.

Step 1: The UAV initiates the AKA process.

The UAV d_j generates a 16-byte random number nu1 and the timestamp T_1. Each domain control node DCC_i maintains an electronic fence for a geographic area, and automatically changes its identity when the UAV moves to the next domain (beyond the electronic fence of the previous domain).

First, d_j calculates and generates $M_1 = T_1$, $M_2 = \mathrm{nu1} \cdot P$, $M_3 = H(\mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1} \| T_1) \oplus \mathrm{Pid}_{d_j}$. Where M_3 hides the identity of the UAV, which is encrypted using the target domain's public key. After that, d_j calculates and generates the mission token MToken in the target domain according to (1) and calculates $M_4 = H(\mathrm{Mid} \| \mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1} \| T_1) \oplus \mathrm{MToken}$, where the mission token is hidden in M_4

$$\mathrm{MToken} = H\left(\mathrm{Mid} \| \mathrm{DCC}_n \| T_{\mathrm{out}} \,\|\, \mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1} \,\|\, T_1\right). \quad (1)$$

In (1), $H()$ is the hash function, Mid is the ID of the mission, DCC_n is the ID of the target domain control node, T_{out} is the time limit for d_j executing the mission in the target domain, and $\mathrm{PK}_{\mathrm{DCC}_n}$ is the public key of DCC_n, T_1 is the timestamp.

Then, d_j sends the authentication request $\mathrm{RM1} = \{M_1, M_2, M_3, M_4\}$ to the control node DCC_n in the target domain.

Step 2: DCC_n receives the authentication request from d_j and replies.

After receiving the message $\mathrm{RM1} = \{M_1, M_2, M_3, M_4\}$, DCC_n obtains the current timestamp T_C and checks whether $T_C - T_1 \le \Delta T$ holds to determine if the message has exceeded the time limit to prevent replay attacks. If it holds, DCC_n starts the authentication process; otherwise, the process is terminated.

To authenticate the identity and mission information of d_j, DCC_n obtains the hidden UAV identity from the received message M_3 by $\mathrm{Pid}_{d_j}{}' = M_3 \oplus H(\mathrm{SK}_{\mathrm{DCC}_n} \cdot M_2 \| T_1)$, and authentication is performed compared to the identity of d_j on the domain blockchain. If they are consistent, the authentication process continues; otherwise, the process is terminated. Then, DCC_n queries the mission information of d_j on the blockchain, and generates mission token MToken for d_j by $\mathrm{MToken} = H(\mathrm{Mid} \| \mathrm{DCC}_n \| T_{\mathrm{out}} \| \mathrm{SK}_{\mathrm{DCC}_n} \cdot M_2 \| T_1)$. Then, the encrypted MToken′ in the received message M_4 is extracted by $\mathrm{MToken}' = H(\mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1} \| T_1) \oplus M_4$, which is compared with the value of MToken calculated by DCC_n. If they are consistent, DCC_n continues the authentication process; otherwise, the process is terminated.

After successful authentication, DCC_n sends a response message to d_j. First, DCC_n generates the current timestamp T_2 and random number nd1. Then, DCC_n generates messages $M_5 = T_2$, $M_6 = \mathrm{nd1} \cdot P$. After that, DCC_n generates the digitally signed message $M_7 = \mathrm{Sig}_{\mathrm{DCC}_n}(\mathrm{PK}_{d_j} \cdot \mathrm{nd1} \cdot M_2 \| M_5)$, and sends the response message $\mathrm{RM2} = \{M_5, M_6, M_7\}$ back to d_j.

Step 3: After receiving the reply, the UAV d_j authenticates DCC_n, generates the session key and the temporary identity of d_j in the current domain.

After receiving the message $\mathrm{RM2} = \{M_5, M_6, M_7\}$, d_j obtains the current timestamp T_{C1} and extracts T_2 from M_5 to check whether $T_{C1} - T_2 \le \Delta T$ holds. If it holds, the process continues; otherwise, it is terminated. Then, d_j verifies M_7 using the public key of DCC_n to authenticate the identity of DCC_n. If the verification is successful, the process continues; otherwise, d_j terminates the process. Then, d_j calculates the session key by $ks = H(\mathrm{MToken} \| \mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1} \| \mathrm{SK}_{d_j} \cdot M_6)$.

Then, d_j generates the random number nu2 and a timestamp T_3, and encrypts the hash value of Pid_{d_j} and Moken using the session key ks. After that, d_j generates messages $M_8 = T_3$, $M_9 = \mathrm{nu2} \cdot P$, $M_{10} = H(\mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu2} \| T_3) \oplus ks(H(\mathrm{Pid}_{d_j} \| \mathrm{MToken}))$, and sends the message $\mathrm{RM3} = \{M_8, M_9, M_{10}\}$ to DCC_n.

Finally, d_j generates $\mathrm{Pid}^n_{d_j}$ which is the temporary identity of d_j in the current domain. The method for d_j to generate $\mathrm{Pid}^n_{d_j}$ is shown in the following equation:

$$\mathrm{Pid}^n_{d_j} = H\left(\mathrm{Pid}_{d_j} \| \mathrm{DCC}_n \| T_{\mathrm{out}} \,\|\, \mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1} \,\|\, T_1\right) \quad (2)$$

where $H()$ is the hash function, Pid_{dj} represents the current ID of the UAV d_j in the current domain on the blockchain, DCC_n represents the ID of the target domain control node, and $\mathrm{PK}_{\mathrm{DCC}_n}$ is the public key of DCC_n. T_{out} is the time limit for d_j executing the task in the target domain.

Step 4: DCC_n receives the message and completes authentication, session key negotiation, and generates the temporary identity for d_j in the current domain.

Upon receiving the message, DCC_n obtains the current timestamp T_{C2} and extracts T_3 from M_5 to check whether $T_{C2} - T_3 \le \Delta T$ holds. Then, it computes the session key $ks = H(\mathrm{MToken} \| \mathrm{SK}_{\mathrm{DCC}_n} \cdot M_2 \| \mathrm{PK}_{d_j} \cdot \mathrm{nd1})$. Where $M_2 = \mathrm{nu1} \cdot P$, and $\mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1} = \mathrm{SK}_{\mathrm{DCC}_n} \cdot M_2$. Based on this, it calculates $M'_{10} = H(\mathrm{SK}_{\mathrm{DCC}_n} \cdot M_9 \| T_3) \oplus ks(H(\mathrm{Pid}^n_{d_j} \| \mathrm{MToken}))$. If M'_{10} matches the received M_{10}, authentication succeeds, and key negotiation is completed.

After that, DCC_n calculates the temporary identity of the UAV in the domain by $\mathrm{Pid}^n_{d_j} = H(\mathrm{Pid}_{d_j} \| \mathrm{DCC}_n \| T_{\mathrm{out}} \| \mathrm{SK}_{\mathrm{DCC}_n} \cdot M_2 \| T_1)$, and uploads it to the blockchain. Finally, DCC_n

Authorized licensed use limited to: Army Engineering Univ of PLA(f. PLA U of S&T). Downloaded on January 20,2026 at 08:23:16 UTC from IEEE Xplore. Restrictions apply.

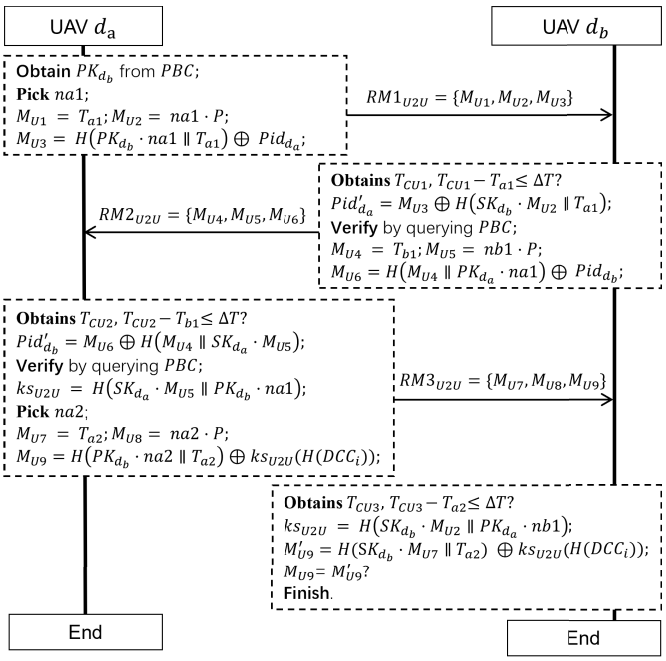

Fig. 5. Mutual authentication and key agreement for UAVs.

uploads the transaction mission′ to the CBC chain to update the task information.

C. Mutual Authentication and Key Agreement for UAVs

The authentication and key agreement process between the UAVs is shown in Fig. 5, which involves the following steps.

Step 1: Authentication Request Generation. The UAV d_a initiates the authentication process by sending a request to the UAV d_b. First, d_a queries the blockchain to retrieve d_b's public key PK_{d_b}. Subsequently, d_a generates a random number $na1$ and a timestamp T_{a1}. The following messages are then constructed: $M_{U1} = T_{a1}$, $M_{U2} = na1 \cdot P$, $M_{U3} = H(\mathrm{PK}_{d_b} \cdot na1 \| T_{a1}) \oplus \mathrm{Pid}_{d_a}$ Where M_{U3} contains the obfuscated identity Pid_{d_a}. After that, d_a transmits the authentication request message $\mathrm{RM1}_{U2U} = \{M_{U1}, M_{U2}, M_{U3}\}$ to d_b.

Step 2: Authentication Request Reception and Response by d_b. Upon receiving the authentication request message $\mathrm{RM1}_{U2U} = \{M_{U1}, M_{U2}, M_{U3}\}$, d_b generates the current timestamp T_{CU1} and verifies the timestamp T_{a1} in M_{U1} by checking whether $T_{CU\,1} - T_{a1} \leq \Delta T$ holds. This step ensures the message is within the valid time window to prevent replay attacks. If the condition is satisfied, the authentication process proceeds; otherwise, it is terminated. Next, d_b computes $\mathrm{Pid}_{d_a}{}' = M_{U3} \oplus H(\mathrm{SK}_{d_b} \cdot M_{U2} \| T_{a1})$to derive the domain identity $\mathrm{Pid}_{d_a}{}'$ of d_a. Subsequently, d_b queries the domain-PBC to verify whether the registered identity matches the derived identity, thereby confirming its authenticity.

After successful authentication, d_b sends a reply message to d_a. First, d_b generates the timestamp T_{b1} and the random number $nb1$. Then, d_b generates the messages $M_{U4} = T_{b1}$, $M_{U5} = nb1 \cdot P$, $M_{U6} = H(M_{U4} \| \mathrm{PK}_{d_a} \cdot na1) \oplus \mathrm{Pid}_{d_b}$. Where M_{U6} is the message containing the encrypted identity of d_a. After that, d_b sends the reply message $\mathrm{RM2}_{U2U} = \{M_{U4}, M_{U5}, M_{U6}\}$ to d_a.

Step 3: Upon receiving the response, the UAV d_a authenticates d_b and generates the session key. After receiving the message $\mathrm{RM2}_{U2U} = \{M_{U4}, M_{U5}, M_{U6}\}$, the UAV d_a generates the current timestamp T_{CU2} and verifies the timestamp T_{b1} in M_{U4} by checking whether $T_{\mathrm{CU2}} - T_{b1} \leq \Delta T$ holds. If valid, the process continues; otherwise, it terminates. Subsequently, d_a computes $\mathrm{Pid}_{d_b}{}' = M_{U6} \oplus H(M_{U4} \| \mathrm{SK}_{d_a} \cdot M_{U5})$ and queries the blockchain to retrieve the identity information of the UAV d_b. This retrieved information is then compared with $\mathrm{Pid}_{d_b}{}'$ to authenticate UAV d_b's identity. If the authentication is successful, the process continues; otherwise, it is terminated.

The UAV d_a then computes the session key $ks_{U2U} = H(\mathrm{PK}_{d_b} \cdot na1 \| \mathrm{SK}_{d_a} \cdot M_{U5})$. Subsequently, d_a generates a random number $na2$ and a timestamp T_{a2}, and encrypts the hash of the current domain's ID using ks_{U2U}. The UAV d_a then constructs the following message components: $M_{U7} = T_{a2}$,$M_{U8} = na2 \cdot P$, $M_{U9} = H(\mathrm{PK}_{d_b} \cdot na2 \| T_{a2}) \oplus ks_{U2U}(H(\mathrm{DCC}_i))$.

Finally, d_a assembles the acknowledgment message $\mathrm{RM3}_{U2U} = \{M_{U7}, M_{U8}, M_{U9}\}$ and transmits it to d_b.

Step 4: Authentication and session key agreement by UAV d_b. Upon receiving the message, UAV d_b generates the current timestamp T_{CU3} and verifies the timestamp T_{a2} in M_{U7} by checking whether $T_{\mathrm{CU3}} - T_{a2} \leq \Delta T$ holds. If valid, the process continues; otherwise, it terminates. After that, d_b proceeds to compute the session key by $ks_{U2U} = H(\mathrm{SK}_{d_b} \cdot M_{U2} \| \mathrm{PK}_{d_a} \cdot nb1)$. Subsequently, d_b calculates $M_{U9}{}' = H(\mathrm{SK}_{d_b} \cdot M_{U7} \| T_{a2}) \oplus ks_{U2U}(H(\mathrm{DCC}_i))$. If $M_{U9}{}'$ matches the received M_{U9}, the authentication is successful and the key agreement is completed.

D. Notification Mechanism Between Domains

When an UAV completes cross-domain authentication and continues to perform the task, DCC_n needs to publish a transaction mission′ to the CBC chain to update the task information. After reaching a consensus, a DCC packages a certain number of transactions and generates a new block on the CBC chain. The DCCs query the CBC chain at regular intervals and obtain the task information of UAVs flying to their domains. In this way, the DCCs can plan the path for the UAVs in advance. The specific method is as follows.

Step 1: DCC_n query task information on the CBC chain from the height of the last queried block. By comparing its own ID and the next domain ID in the transaction (mission. CNid_n), DCC_n determines whether the next domain in the transaction is itself and saves the related task information. In this way, DCC_n obtains the task information of upcoming UAVs from the domain with ID CNid_c and updates the height of the last queried block.

Step 2: DCC_n preprocesses the tasks, plan a flight path according to task information, and obtain the ID of the next domain CNid'_n. In addition, DCC_n calculates the expected flight time of the UAV within the domain for updating T'_{out} in subsequent transactions. Then, DCC_n generates an incomplete CBC chain transaction, mission = $\{\mathrm{Pid}^i_{d_j}, \mathrm{CNid}'_c, \mathrm{CNid}'_n, \mathrm{CNid}_d, T'_{\mathrm{out}}\}$.

Step 3: When the UAV has passed the cross-domain authentication, DCC_n updates and publishes the transaction mission on the CBC chain. Also, DCC_n updates the domain private

Authorized licensed use limited to: Army Engineering Univ of PLA(f. PLA U of S&T). Downloaded on January 20,2026 at 08:23:16 UTC from IEEE Xplore. Restrictions apply.

chain PBC for mutual authentication of UAVs within the domain.

Due to the time-sensitive nature of the UAV task information stored in PBC, it is possible to reduce on-chain storage costs by regularly migrating historical data to offline storage or pruning PBC's historical data.

V. Security Analysis

Section IV outlined the adversary model and security requirements for the UAVs. In this section, the security analysis initiates with formal verification of the proposed communication protocols using the real-or-random (ROR) model. In addition, the informal security analysis is performed to guarantee that the proposed method is resilient to various well-known cyber-attacks.

A. Formal Security Analysis

1) Correctness of the session key ks: Theorem 1: If the domain control node and the UAV honestly execute the proposed AKA protocol, the session keys computed by d_j and DCC_n are identical: $ks_{d_j} = ks_{\mathrm{DCC}_n}$.

Proof: In the UAV-2-GCS authentication and key agreement (AKA) protocol proposed in Section IV-B, mutual authentication occurs between the domain control node DCC_n and the UAV d_j. The protocol executes as follows.

1) The UAV d_j initiates the AKA process.
2) DCC_n verifies d_j's authenticity.
3) The UAV d_j verifies DCC_n's authenticity and generates the shared session key by $ks_{dj} = H(\mathrm{MToken}\| \mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1}\| \mathrm{SK}_{d_j} \cdot M_6)$, where nu1 is the random number generated by d_j, $\mathrm{PK}_{\mathrm{DCC}_n}$ represents $\mathrm{SK}_{\mathrm{DCC}_n} \cdot P$. M_6 derived as $\mathrm{nd1} \cdot P$, where nd1 is the random number generated by DCC_n.
4) Subsequently, DCC_n authenticates d_j and computes the corresponding session key by $ks_{\mathrm{DCC}_n} = H(\mathrm{MToken}\| \mathrm{SK}_{\mathrm{DCC}_n} \cdot M_2\| \mathrm{PK}_{d_j} \cdot \mathrm{nd1})$, where M_2 derived as $\mathrm{nu1} \cdot P$, PK_{d_j} represents $\mathrm{SK}_{d_j} \cdot P$. These operations yield the following derived equations:

$$\begin{aligned} ks_{d_j} &= H\left(\mathrm{MToken} \,\|\, \mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1} \,\|\, \mathrm{SK}_{d_j} \cdot M_6\right) \\ &= H\left(\mathrm{MToken} \,\|\, \mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1} \,\|\, \mathrm{SK}_{d_j} \cdot \mathrm{nd1} \cdot P\right) \\ &= H\left(\mathrm{MToken} \,\|\, \mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1} \,\|\, \mathrm{SK}_{d_j} \cdot P \cdot \mathrm{nd1}\right) \\ &= H\left(\mathrm{MToken} \,\|\, \mathrm{SK}_{\mathrm{DCC}_n} \cdot M_2 \,\|\, \mathrm{PK}_{d_j} \cdot \mathrm{nd1}\right) \\ &= ks_{\mathrm{DCC}_n}. \end{aligned} \tag{3}$$

Since $M_2 = \mathrm{nu1} \cdot P$ and $M_6 = \mathrm{nd1} \cdot P$, the inputs to the hash function are identical, hence $ks_{d_j} = ks_{\mathrm{DCC}_n}$.

2) Semantic security of the session key *ks*.

The semantic security of the session key *ks* is formally analyzed via the widely used random oracle model (ROM). The components of the ROM are described as below.

1) *Participants:* The UAV d_j equipped with private key SK_{d_j} and public key $\mathrm{PK}_{d_j} = \mathrm{SK}_{d_j} \cdot P$ and the DCC DCC_n equipped with private key $\mathrm{SK}_{\mathrm{DCC}_n}$ and public key $\mathrm{PK}_{\mathrm{DCC}_n} = \mathrm{SK}_{\mathrm{DCC}_n} \cdot P$.
2) *Security Model and Assumptions:* a) *ROM:* Hash function H is modeled as an ideal random oracle. All parties, including adversaries, can access H via queries. b) *Computational assumptions:* Elliptic curve discrete logarithm problem (ECDLP): Given P and $Q = a \cdot P$, computing a is computationally infeasible. c) *Computational Diffie-Hellman (CDH) assumption:* Given P, $a \cdot P$, and $b \cdot P$, computing $a \cdot b \cdot P$ is computationally infeasible.
3) *Formal Security Definitions:* a) *Experiment* $\mathrm{Exp}_{\mathcal{A}}(1^k, b)$*, where* $b \in \{0, 1\}$*:* In the experiment, first, system parameters and keys for d_j and DCC_n are generated. The adversary $\mathcal{A}$ can make queries to the Hash oracle H. When $\mathcal{A}$ requests a challenge, if $b = 1$, the challenger returns the real session key *ks*. If $b = 0$, the challenger returns a random value $r \leftarrow_R \{0, 1\}^{|ks|}$. $\mathcal{A}$ outputs a bit b'. The experiment output is 1 if $b' = b$, otherwise 0. b) *Semantic security of session key:* The session key *ks* is semantically secure if for any probabilistic polynomial-time adversary $\mathcal{A}$, the advantage in distinguishing between the real session key and a random value is negligible

$$\begin{aligned} \mathrm{Adv}_{\mathcal{A}} &= \left|\Pr\left[\mathrm{Exp}_{\mathcal{A}}\left(1^k, 1\right) = 1\right] - \Pr\left[\mathrm{Exp}_{\mathcal{A}}\left(1^k, 0\right) = 1\right]\right| \\ &\leq \mathrm{negl}\,(k)\,. \end{aligned} \tag{4}$$

4) *Formal Proof: Theorem 2:* Under the ROM and the CDH assumption, the session key *ks* generated by the UAV-DCC authentication protocol is semantically secure. *Proof:* We prove this theorem by constructing a sequence of games and showing that the adversary's advantage in distinguishing between consecutive games is negligible. *Game 0:* Real protocol execution.

This game models the real execution of the protocol. The challenger generates the session key *ks* according to the protocol specification.

Game 1: Replace the output of H with random value. Instead of computing *ks*, the challenger samples a random value $r \leftarrow_R \{0, 1\}^{|ks|}$ and uses r as the session key.

Lemma 1: Assuming H is a random oracle, the adversary's advantage in distinguishing between Game 0 and Game 1 is negligible.

Proof: If the adversary can distinguish between these two games, it implies the ability to distinguish the output of H from a random value, which contradicts the random oracle assumption.

Game 2: Simulate $\mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1}$, $\mathrm{SK}_{d_j} \cdot M_6$. In this game, we simulate the values $\mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1}$ and $\mathrm{SK}_{d_j} \cdot M_6$ without using the private keys $\mathrm{SK}_{\mathrm{DCC}_n}$ and SK_{d_j}. Instead, we use the CDH assumption to generate these values.

Lemma 2: Under the CDH assumption, the adversary's advantage in distinguishing between Game 1 and Game 2 is negligible.

Proof: If the adversary can distinguish between these two games, it implies the ability to solve the CDH problem, which contradicts the CDH assumption. Specifically, given $\mathrm{PK}_{\mathrm{DCC}_n} = \mathrm{SK}_{\mathrm{DCC}_n} \cdot P$ and $M_2 = \mathrm{nu1} \cdot P$, computing $\mathrm{SK}_{\mathrm{DCC}_n} \cdot M_2$ (or equivalently $\mathrm{PK}_{\mathrm{DCC}_n} \cdot \mathrm{nu1}$) is CDH-hard. Similarly, given $\mathrm{PK}_{d_j} = \mathrm{SK}_{d_j} \cdot P$ and $M_6 = \mathrm{nd1} \cdot P$, computing $\mathrm{SK}_{d_j} \cdot M_6$ is CDH-hard.

Authorized licensed use limited to: Army Engineering Univ of PLA(f. PLA U of S&T). Downloaded on January 20,2026 at 08:23:16 UTC from IEEE Xplore. Restrictions apply.

Game 3: Use random value for challenge. In this game, the challenger directly uses a random value for the session key, completely independent of the protocol execution.

Lemma 3: The adversary's advantage in distinguishing between Game 2 and Game 3 is negligible.

Proof: In Game 2, the session key is derived from simulated values that are computationally indistinguishable from the real values. In Game 3, the session key is a truly random value. By the indistinguishability of the simulated values (from the CDH assumption) and the random oracle property of H, the adversary cannot distinguish between these two games.

Conclusion: the adversary's advantage in distinguishing the real session key from a random value in the original protocol (Game 0) is negligible. Therefore, the session key *ks* is semantically secure.

B. Informal Security Analysis

As described below, the properties and security of the proposed methods, considering well-known security attacks, are analyzed. Also, the security analysis and comparison results are shown in Table I.

1) *Anonymity:* With the benefit of domain private chains and the identity update mechanism, UAVs use temporary identities within the domain for communication and authentication. Therefore, attackers cannot infer the real identity of the UAVs during the authentication process, which can ensure the anonymity of the UAVs.
2) *Mutual Authentication:* The proposed method can achieve mutual authentication between DCCs and UAVs, as well as between UAVs. The security property ensures that only two normal participants can authenticate each other and reach a consensus on the session key.
3) *Task Authentication:* Even if the identity is genuine, attackers may hijack legitimate UAVs and fly them to other domains. While the proposed method can verify the legality of the task through MToken.
4) *Decentralization:* Through the deployment of the private chain and consortium chain, cross-domain authentication and mutual authentication between UAVs do not require authentication through an authentication center.
5) *Session Key Agreement:* The proposed method can not only achieve secure authentication for both parties, but also achieve correct session key attainment for further communication needs.
6) *Path Confidentiality:* UAVs use different identities in each domain, and even if attackers can eavesdrop communication information within each domain, they cannot infer the complete flight path of a UAV from the obtained data, thus ensuring the confidentiality of the path.
7) *Path Preplanning:* By updating tasks on the consortium chain, the DCC of the next domain can be informed in advance of the upcoming UAVs and their expected arrival time, thus enabling path planning in advance.
8) *Resistance to Replay Attacks:* Attackers may capture and replay all the messages of a communication session. During the authentication process, DCCs and UAVs use a fresh random number and timestamp mechanism, which is not valid in the next round session. Therefore, attackers cannot successfully execute replay attacks.
9) *Resistance to Man-in-the-Middle Attacks:* Attackers may intervene between communication parties to intercept, tamper with, or forge communication data. While the messages are protected by a public–private key mechanism. Even if the data are captured, attackers cannot generate the correct authentication messages in a short period of time.
10) *Resistance to Physical Capture Attacks:* Attackers may physically disrupt the UAVs' flight and capture the UAVs. However, the task information stored by UAVs only includes temporary identities and flight paths within the domain. Therefore, attackers are unable to determine the destination and complete flight path of the task.
11) *Resistance to Impersonation Attacks:* Attackers may eavesdrop on the authentication messages and impersonate a legitimate device to deceive other devices. While attackers cannot derive the private key and other secret parameters to generate an authentication message that can be verified. Therefore, it is difficult to implement an impersonation attack.
12) *Resistance to Forgery Attack:* Attackers may generate an illegal or false ID to deceive UAVs or DCCs. While the DCCs and UAVs can query the CBC chain or PBC chain to confirm identity. In addition, it is difficult for attackers to forge identity on the CBC chain or compromise more than 50% of nodes to tamper the PBC chain.

VI. Performance Analysis

In this section, we build a testing environment and evaluate the performance of the proposed method from the perspective of computation overhead and communication overhead with other relevant existing methods.

A. Experimental Settings

We analyzed the performance of the proposed scheme by conducting simulation experiments. The configuration of the PC for the experiments is: CPU: Intel Core Ultra 7 155H, RAM: 32 GB, OS: Ubuntu 20.04, 64-bit. Also, the testing environment is based on the Truffle (version: 5.11.5) and Ganache (version: 2.7.1), Node.js (version: 18.18.0), and Web3.js (version: 1.10.0). To further evaluate the feasibility of the proposed scheme, we used a Raspberry Pi 4B to simulate the UAVs, which is widely used in the existing studies. The configuration of the Raspberry Pi 4B is: CPU: Quad-core Cortex-A72, RAM: 8 GB, OS: Ubuntu 20.04, 64-bit. We use Python libraries to implement cryptographic primitives for evaluating the performance overhead on Raspberry Pi 4B and PC platforms.

B. Computation Overhead Analysis

To evaluate the computational overhead of the proposed method, we estimate the total execution time of cryptographic primitive operations involved in the proposed and compared

Authorized licensed use limited to: Army Engineering Univ of PLA(f. PLA U of S&T). Downloaded on January 20,2026 at 08:23:16 UTC from IEEE Xplore. Restrictions apply.

TABLE I
COMPARATIVE STUDY ON SECURITY PROPERTIES

Security properties	[30]	[9]	[31]	[21]	Ours
SP1	×	×	✓	✓	✓
SP2	✓	✓	✓	✓	✓
SP3	×	×	×	×	✓
SP4	✓	✓	×	✓	✓
SP5	✓	✓	✓	✓	✓
SP6	×	×	×	✓	✓
SP7	×	×	×	×	✓
SP8	✓	✓	✓	✓	✓
SP9	✓	✓	✓	✓	✓
SP10	×	×	✓	✓	✓
SP11	✓	✓	✓	✓	✓
SP12	✓	✓	✓	✓	✓

Notes: **SP1**: Anonymity; **SP2**: Mutual Authentication; **SP3**: Task Authentication; **SP4**: Decentralization; **SP5**: Session Key Agreement; **SP6**: Path Confidentiality; **SP7**: Path pre-planning; **SP8**: Resistance to replay attacks; **SP9**: Resistance to Man-in-the-Middle attacks; **SP10**: Resistance to physical capture attacks; **SP11**: Resistance to impersonation attacks; **SP12**: Resistance to forgery attack.

TABLE II
COMPUTATIONAL OVERHEAD OF THE MAIN OPERATIONS

Operation	DCC side (ms)	UAV side (ms)
T_h	0.0012	0.0043
T_{eca}	0.0196	0.0792
T_{ecm}	0.0971	0.2979
T_{enc}	0.0055	0.0323
T_{dec}	0.0053	0.0354
T_{sig}	0.1250	0.7321
T_{sv}	0.2517	0.9732
T_{fg}	650.3865	1936.7562
T_{fr}	136.4712	792.5621
T_{puf}	0.5727	1.6479
T_{bp}	8.9376	27.7323

methods. Simple operations, such as the concatenation operation, were not taken into consideration because of their low computational expense. The symbols and explanations are listed as follows. T_h: one-way hash function; T_{eca}: elliptic curve point addition; T_{ecm}: elliptic curve point multiplication; T_{enc}: AES encryption; T_{dec}: AES decryption; T_{sig}: Ed25519 signature; T_{sv}: signature verification; T_{fg}: fuzzy extractor generation; T_{fr}: fuzzy extractor reproduce; T_{puf}: physical unclonable function; and T_{bp}: bilinear pairing. The computational overhead of the above operations is shown in Table II. The time cost in the table is the average cost of executing the corresponding operation 10 000 times on the corresponding platform.

In our cross-domain authentication method, the computational overhead of DCCs and UAVs are as follows: for GCS: $7T_h + 6T_{ecm} + T_{enc} + T_{\text{sig}} = 0.7215$ ms, for UAVs: $7T_h + 5T_{ecm} + T_{enc} + T_{sv} = 2.5251$ ms. In our UAV-UAV authentication method, the computational overhead of UAVs is: $10T_h + 10T_{ecm} + 2T_{enc} = 3.0866$ ms. The comparison analysis of the computational overhead of our method with existing methods [9], [21], [30], and [31], is presented in Table III and Fig. 6. In [9], the ground station only provides a mutual authentication platform between UAVs, so the authentication between the ground station and the UAV is not involved.

C. Communication Overhead Analysis

To evaluate the communication overhead of the proposed method, we specify the size of the communication parameters involved in the proposed and compared methods. The identity,

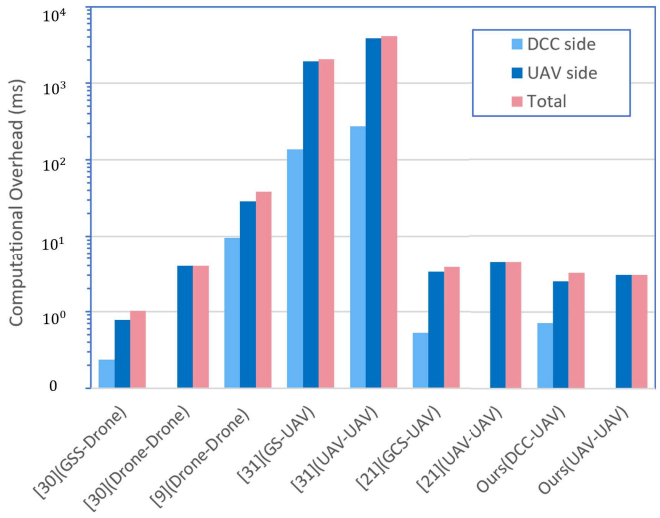

Fig. 6. Computational overhead comparison of different methods.

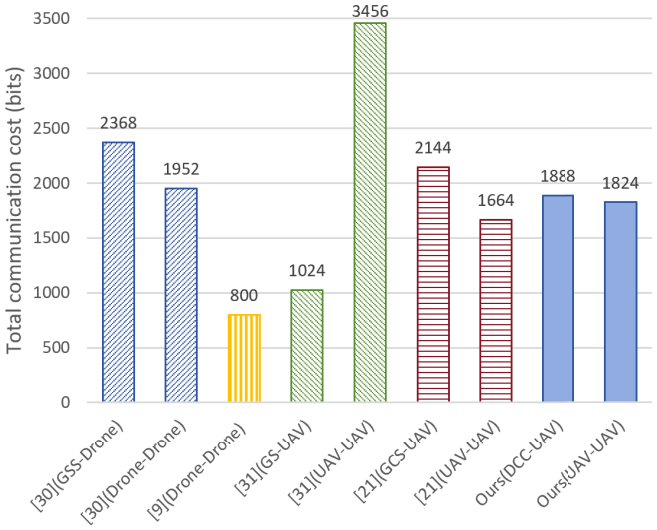

Fig. 7. Communication overhead comparison of different methods.

timestamp, elliptic curve points, random number, signature size, the digest of the hash function, the challenge/response, and plaintext/ciphertext as 160 bits, 32 bits, 320 bits, 160 bits, 64 bits, 256 bits, 128 bits, and 128 bits, respectively. Also, we analyze the number of communicated messages (bits) transmitted in our method and compare it with existing authentication methods. The comparison analysis of the communication overhead of our method with existing methods [9], [21], [30], and [31], is presented in Fig. 7. Specifically, the communicated messages in our method (DCC-UAV) are: RM1 = $\{M_1, M_2, M_3, M_4\} = 32 + 320 + 256 + 256 = 864$ bits; RM2 = $\{M_5, M_6, M_7\} = 32 + 320 + 64 = 416$ bits; and RM3 = $\{M_8, M_9, M_{10}\} = 32 + 320 + 256 = 608$ bits. The total communication cost is $864 + 416 + 608 = 1888$ bits. The communicated messages in our method (UAV-UAV) are: $\text{RM1}_{U2U} = \{M_{U1}, M_{U2}, M_{U3}\} = 32 + 320 + 256 = 608$; $\text{RM2}_{U2U} = \{M_{U4}, M_{U5}, M_{U6}\} = 32 + 320 + 256 = 608$; and $\text{RM3}_{U2U} = \{M_{U7}, M_{U8}, M_{U9}\} = 32 + 320 + 256 = 608$. The total communication cost is 1824 bits. In [28], the key dis-

Authorized licensed use limited to: Army Engineering Univ of PLA(f. PLA U of S&T). Downloaded on January 20,2026 at 08:23:16 UTC from IEEE Xplore. Restrictions apply.

TABLE III
COMPUTATIONAL OVERHEAD COMPARISON

Methods	DCC side	UAV side
[30](GSS-Drone)	$9T_h + 2T_{ecm} + T_{eca} + T_{enc} + T_{dec} \approx 0.2354\ ms$	$9T_h + 2T_{ecm} + T_{eca} + T_{enc} + T_{dec} \approx 0.7814\ ms$
[30](Drone-Drone)	-	$12T_h + 12T_{ecm} + 4T_{eca} \approx 3.9432\ ms$
[9](Drone-Drone)	$2T_{sig} + T_{bp} \approx 9.6596\ ms$	$T_{enc} + T_{dec} + 4T_{ecm} + T_{bp} \approx 28.9916\ ms$
[31](GS-UAV)	$4T_h + T_{fr} \approx 136.4760\ ms$	$4T_h + T_{fg} \approx 1936.7734\ ms$
[31](UAV-UAV)	$10T_h + 2T_{fr} \approx 272.9544\ ms$	$10T_h + 2T_{fg} + 2T_{puf} \approx 3876.8512\ ms$
[21](GCS-UAV)	$5T_h + 5T_{ecm} + 2T_{eca} \approx 0.5307\ ms$	$4T_h + 5T_{ecm} + 2T_{eca} + T_{puf} \approx 3.3130\ ms$
[21](UAV-UAV)	-	$6T_h + 14T_{ecm} + 4T_{eca} \approx 4.5132\ ms$
Ours(DCC-UAV)	$7T_h + 6T_{ecm} + T_{enc} + T_{sig} \approx 0.9575\ ms$	$7T_h + 5T_{ecm} + T_{enc} + T_{sv} \approx 1.5812\ ms$
Ours(UAV-UAV)	-	$10T_h + 10T_{ecm} + 2T_{enc} \approx 3.0866\ ms$

Notes: "-" means DCC side does not perform any operation.

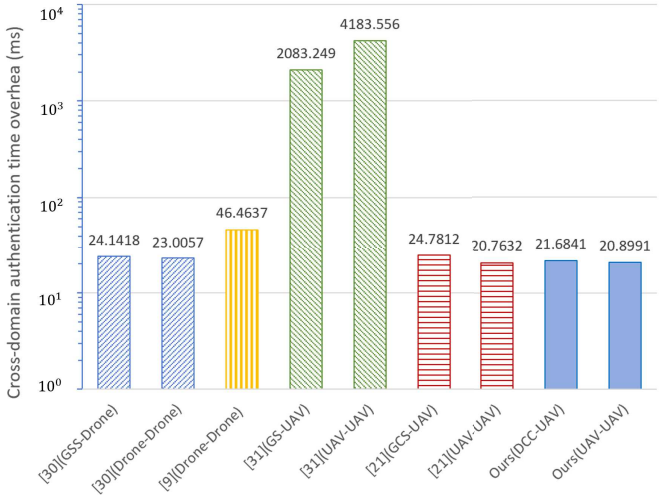

Fig. 8. Comparison of cross-domain authentication time overhead.

tribution process and authentication process are independent, and we only consider the messages transmitted during the authentication process.

D. Cross-Domain Authentication Time Overhead

The total cross-domain authentication time overhead includes the computational time and communication time. Based on the results above, we first evaluated the communication time overhead, which mainly includes transmission delay and propagation delay. The transmission delay can be expressed as the ratio of data size to transmission rate. The wireless network transmission rate, such as 4G (LTE), varies from several Mb to several Gb per second. For convenience, in the comparison analysis, we set the transmission rate is 100 Mbps. The transmission time taken by [30](GSS-Drone), [30](Drone-Drone), [9](Drone-Drone), [31](GS-UAV), [31](UAV-UAV), [21](GCS-UAV), [21](UAV-UAV), Ours(DCC-UAV), and Ours(UAV-UAV) is 23.125, 19.0625, 7.8125, 10, 33.75, 20.9375, 16.25, 18.4375, and 17.8125 ms, respectively. The propagation delay can be expressed as the ratio of the distance between two sides of the communication to the propagation speed of the wave in a vacuum. Generally, the range of the domain is relatively small and the propagation delay can be ignored. Therefore, the total cross-domain authentication time overhead includes the computational time and transmission time. And the cross-domain authentication time overhead of different methods is shown in Fig. 8. It can be seen that the proposed method has advantages in terms of authentication time.

VII. CONCLUSION

When executing missions such as logistics delivery, UAVs require cross-domain authentication to enter the next domain. However, in the process of cross-domain authentication, UAVs are vulnerable to eavesdropping attacks, which can reveal the trajectories of missions and expose users' privacy. To address this problem, we proposed a blockchain-based cross-domain authentication and flight trajectory privacy protection scheme for UAV networks. The proposed scheme includes a registration mechanism, a cross-domain authentication method, a mutual authentication and key agreement method, and a notification mechanism between domains. By taking advantage of blockchain, PKI, elliptic curve, and signature, the proposed method can ensure path confidentiality and prevent various network attacks. Furthermore, the notification mechanism between domains enables DCCs to plan paths in advance and improve the efficiency of UAV mission execution. Experiment results show that the proposed method has advantages in terms of the total cross-domain authentication time cost.

REFERENCES

[1] H. Pan, P. Cao, W. Wang, Y. Liu, and Z. Yin, "Blockchain-assisted cross-domain authentication and access control for low-altitude UAV," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Aug. 2023, pp. 1–6.

[2] A. Hamissi and A. Dhraief, "A survey on the unmanned aircraft system traffic management," *ACM Comput. Surv.*, vol. 56, no. 3, pp. 1–37, Mar. 2024.

[3] K. Xue, X. Luo, Y. Ma, J. Li, J. Liu, and D. S. L. Wei, "A distributed authentication scheme based on smart contract for roaming service in mobile vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 5284–5297, May 2022.

[4] Q. Xie and H. Wang, "PUF-based secure and efficient anonymous authentication protocol for UAV towards cross-domain environments," *Drones*, vol. 9, no. 4, p. 260, Mar. 2025.

[5] B. Liu, W. Ni, R. P. Liu, Y. J. Guo, and H. Zhu, "Privacy-preserving routing and charging scheduling for cellular-connected unmanned aerial vehicles," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 54, no. 8, pp. 4929–4941, Aug. 2024.

[6] B. Chai, J. Yu, B. Yan, Y. Yu, and S. Wang, "BSCDA: Blockchain-based secure cross-domain data access scheme for Internet of Things," *IEEE Trans. Netw. Service Manage.*, vol. 21, no. 4, pp. 4006–4023, Aug. 2024.

[7] Y. Tan, J. Wang, J. Liu, and N. Kato, "Blockchain-assisted distributed and lightweight authentication service for industrial unmanned aerial vehicles," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16928–16940, Sep. 2022.

Authorized licensed use limited to: Army Engineering Univ of PLA(f. PLA U of S&T). Downloaded on January 20,2026 at 08:23:16 UTC from IEEE Xplore. Restrictions apply.

[8] H. Pei, P. Yang, M. Du, Z. Liang, and Z. Hu, "Blockchain-assisted verifiable secure multi-party data computing," *Comput. Netw.*, vol. 253, Nov. 2024, Art. no. 110712.
[9] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K.-R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled Internet of Drones," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022.
[10] S. Enayati, D. Goeckel, A. Houmansadr, and H. Pishro-Nik, "Location privacy protection for UAVs in package delivery and IoT data collection," *IEEE Internet Things J.*, vol. 10, no. 23, pp. 20586–20601, Dec. 2023.
[11] Z. Li et al., "A secure and efficient UAV network defense strategy: Convergence of blockchain and deep learning," *Comput. Standards Interface*, vol. 90, Aug. 2024, Art. no. 103844.
[12] A. Yao, S. Pal, C. Dong, X. Li, and X. Liu, "A framework for user biometric privacy protection in UAV delivery systems with edge computing," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops Affiliated Events (PerCom Workshops)*, Mar. 2024, pp. 631–636.
[13] M. Tanveer, A. Alkhayyat, A. Naushad, A. U. Khan, N. Kumar, and A. G. Alharbi, "RUAM-IoD: A robust user authentication mechanism for the Internet of Drones," *IEEE Access*, vol. 10, pp. 19836–19851, 2022.
[14] S. U. Jan, I. A. Abbasi, F. Algarni, and A. S. Khan, "A verifiably secure ECC based authentication scheme for securing IoD using FANET," *IEEE Access*, vol. 10, pp. 95321–95343, 2022.
[15] S. Rajamanickam, S. Vollala, and N. Ramasubramanian, "EAPIOD: ECC based authentication protocol for insider attack protection in IoD scenario," *Secur. Privacy*, vol. 5, no. 5, p. 248, Sep. 2022.
[16] A. T. Jawad, R. Maaloul, and L. Chaari, "Authentication communication by using visualization cryptography for UAV networks," *Comput. Standards Interface*, vol. 92, Mar. 2025, Art. no. 103918.
[17] K. Mahmood, Z. Ghaffar, M. Farooq, K. Yahya, A. K. Das, and S. A. Chaudhry, "A security enhanced chaotic-map-based authentication protocol for Internet of Drones," *IEEE Internet Things J.*, vol. 11, no. 12, pp. 22301–22309, Jun. 2024.
[18] A. Jain et al., "A walkthrough of blockchain-based Internet of Drones architectures," *IEEE Internet Things J.*, vol. 11, no. 21, pp. 34924–34940, Nov. 2024.
[19] A. V. Vardhan, S. Mohanty, and M. Pradhan, "A lightweight blockchain-enabled authentication scheme for securing Internet of Drones devices," in *Proc. IEEE Int. Conf. Smart Power Control Renew. Energy (ICSPCRE)*, Jul. 2024, pp. 1–6.
[20] J. Subramani, A. Maria, A. S. Rajasekaran, and J. Lloret, "Physically secure and privacy-preserving blockchain enabled authentication scheme for Internet of Drones," *Secur. Privacy*, vol. 7, no. 3, p. 364, May 2024.
[21] K. Huang, H. Hu, and C. Lin, "BAKAS-UAV: A secure blockchain-assisted authentication and key agreement scheme for unmanned aerial vehicles networks," *IEEE Internet Things J.*, vol. 11, no. 22, pp. 36858–36883, Nov. 2024.
[22] I. Chandran and K. Vipin, "A PUF secured lightweight mutual authentication protocol for multi-UAV networks," *Comput. Netw.*, vol. 253, Nov. 2024, Art. no. 110717.
[23] J. Sharma and P. S. Mehra, "HCFAIUN: A novel hyperelliptic curve and fuzzy extractor-based authentication for secure data transmission in IoT-based UAV networks," *Veh. Commun.*, vol. 49, Oct. 2024, Art. no. 100834.
[24] X. Wang, W. Wang, Y. Liu, and P. Cao, "Anonymous cross-domain authentication and key agreement scheme for UAV," in *Proc. IEEE Global Commun. Conf.*, Dec. 2024, pp. 3595–3600.
[25] J. Zhang, X. Chen, Q. Cheng, X. Chen, and X. Luo, "An enhanced certificateless blockchain-assisted authentication and key agreement protocol for Internet of Drones," *IEEE Trans. Netw. Sci. Eng.*, vol. 12, no. 4, pp. 3065–3081, Jul. 2025.
[26] M. Xie, Z. Chang, H. Li, and G. Min, "BASUV: A blockchain-enabled UAV authentication scheme for Internet of Vehicles," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 9055–9069, 2024.
[27] Z. Cai, G. Lu, Y. Wang, G. Gui, and J. Sha, "Robust cross-domain UAV RFFI method using domain-invariant adversarial learning and manifold regularization," *IEEE Trans. Cognit. Commun. Netw.*, early access, Apr. 16, 2025, doi: 10.1109/TCCN.2025.3561305.
[28] C. Pu, A. Bilal, N. Park, J. Seol, and K.-K.-R. Choo, "A redactable blockchain-assisted application-aware authentication system for Internet of Drones," *IEEE Internet Things J.*, vol. 12, no. 14, pp. 27206–27221, Jul. 2025.
[29] J. Akram and A. Anaissi, "Privacy-first crowdsourcing: Blockchain and local differential privacy in crowdsourced drone services," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jul. 2024, pp. 1412–1414.
[30] B. Bera, A. K. Das, and A. K. Sutrala, "Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment," *Comput. Commun.*, vol. 166, pp. 91–109, Jan. 2021.
[31] R. Karmakar, G. Kaddoum, and O. Akhrif, "A PUF and fuzzy extractor-based UAV-ground station and UAV-UAV authentication mechanism with intelligent adaptation of secure sessions," *IEEE Trans. Mobile Comput.*, vol. 23, no. 5, pp. 3858–3875, May 2024.

Gongzhe Qiao received the B.S. degree in information security engineering and the B.A. degree in new media communication science from Shanghai Jiao Tong University, Shanghai, China, in 2017, and the Ph.D. degree in cyberspace security from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2024.

He is currently a Lecturer with the School of Computer Science, Nanjing University of Information Science and Technology, Nanjing. His research interests include cyberspace security, UAV network authentication, and information system risk assessment.

Panlong Yang (Senior Member, IEEE) is a Professor at Nanjing University of Information Science and Technology, Nanjing, China. Since 2012, he has supervised 50 master's and Ph.D. candidate students, including two excellent dissertation winners in Jiangsu Province and the PLA education system. He has been supported by the National Key Development Project and NSFC projects. He has published over 200 papers.

Dr. Yang served as a TPC Member of INFOCOM. He has been nominated by ACM MobiCom 2009 for the best demo honored mention awards, and won the best paper awards in IEEE MSN and MASS. He has served as a General Chair of IEEE BigCom and a TPC Chair of IEEE MSN.

Tong Ye received the B.S. and Ph.D. degrees in computer science and technology from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2017 and 2024, respectively.

She is currently a Lecturer at the College of Computer and Software, Nanjing University of Industry Technology, Nanjing. Her current research interests include IoT security, formal modeling, and model-driven security.

Feiyu Han received the B.S. degree from the School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, China, in 2019, and the Ph.D. degree from the School of Computer Science and Technology, University of Science and Technology of China, Hefei, China, in 2024.

He is currently an Associate Professor at the School of Computer Science, Nanjing University of Information Science and Technology, Nanjing. His research interests span across wireless sensing, mobile computing, and low-power communication.

Authorized licensed use limited to: Army Engineering Univ of PLA(f. PLA U of S&T). Downloaded on January 20,2026 at 08:23:16 UTC from IEEE Xplore. Restrictions apply.