Hindawi
Security and Communication Networks
Volume 2022, Article ID 2330052, 19 pages
https://doi.org/10.1155/2022/2330052

Research Article

Lightweight Mutual Authentication Scheme Enabled by Stateless Blockchain for UAV Networks

Lingjun Kong,[1] **Bing Chen**,[1] **Feng Hu**,[1] **and Ji Zhang**[2]

[1]*University of Southern Queensland, Toowoomba, Australia*
[2]*Nanjing University of Aeronautics and Astronautics, Nanjing, China*

Correspondence should be addressed to Bing Chen; cb_china@nuaa.edu.cn

Received 25 April 2022; Revised 22 June 2022; Accepted 28 July 2022; Published 14 September 2022

Academic Editor: Yinbin Miao

The UAV network composed of resource-constrained lightweight UAV swarms can efficiently accomplish mission with time critical requirements in dynamic and complex environments. However, the trusted authentication of network nodes poses a huge challenge due to its own resource constraints, the lack of trusted centralized support, frequent joining or departure of UAVs to or from the network, and the presence of cyber-attacks. In this paper, we propose a stateless blockchain based on triple aggregatable subvector commitment and present a dynamic proof of trust authorization consensus mechanism with a periodic random selection of authorized nodes to guarantee the trustworthiness of mutual authentication of UAV nodes. Our proposed triple vector authentication solution solves several of the challenges mentioned above very well. The extensive experiments demonstrate that our blockchain-based authentication scheme enjoins significant advantages over the four schemes currently available for UAV network authentication in terms of single authentication latency, speed of energy consumption, average computational cost, and end-to-end latency.

1. Introduction

The UAV network is a mission-oriented, temporary mobile self-organizing network, consisting of a fleet of lightweight UAVs that collaborate with each other at low cost; with distributed, equal, and destruction-resistant characteristics, all drones are linked as peer entities, both as data processing hosts and to undertake message routing and forwarding functions, interdrone communication without base station forwarding, to complete data transmission in a multi-hop manner, capable of complex environments, and high timeliness. It has a wide range of practical applications, such as joint search and rescue, environmental surveys, emergency communications, and military missions. Lightweight UAV nodes have the advantage of efficient networking and easy deployment, but at the cost of limited resources in terms of energy supply, storage, and computing power, which makes UAV networks a special type of mobile self-organized networks and face more complex network threats than MANETs [1, 2].

Firstly, the use of wireless links makes the UAV network more vulnerable to attacks launched from the links, which can come from all directions, and any node can be targeted. Ways of compromise include revealing secret information, jamming information, and impersonating nodes. Each node therefore needs to be in direct or indirect contact with the adversary. Further, the autonomy of nodes in UAV networks, operating in an unpredictable environment, increases the risk of nodes being captured, compromised, and hijacked, and thus in addition to being subject to external attacks, attacks launched from within by compromised nodes are more difficult to detect and more dangerous. Therefore, the operation of any node must adhere to a certain pattern rather than immediately trusting its peers. Finally, the mobility of UAVs, complex mission environments, and mission needs all make UAVs frequent access to the network, resulting in dynamic changes in UAV network topology and size, leading to a network with no clear defensive boundaries and statically configured security solutions that are not applicable. At the same time, invalid

network node information leads to increased end-to-end latency and higher routing costs, increasing the number of mutual communication failures and reducing the overall performance of the network.

In conclusion, mission UAV networks in complex and unknown environments are inherently very vulnerable and dynamic, and such characteristics bring new challenges to their security defense. It is necessary to build a lightweight and trusted global trust platform on UAV networks to achieve efficient authentication and key management to secure UAV networks, while also meeting the requirements of real-time, robustness, and dynamic adaptability of ad hoc mission networks.

As a special mobile self-organizing network, the nodes of the UAV network are mainly authenticated based on the threshold secret sharing technology authentication mode, certificate chain authentication, blockchain-based authentication mode, and stateless blockchain based on the cryptographic accumulator method, but due to the limited resources of the UAV network, the dynamic nature of these methods are not good enough to meet the needs in terms of computing, bandwidth, storage, and energy supply.

In the stateless authentication blockchain recommended in this paper, UAV nodes establish the local trust degree of neighboring nodes by monitoring each other's forwarding behavior with neighboring nodes. The network periodically performs data consensus on the local trust degree of the authorized agent node group and completes a decision consensus based on this; i.e., it counts the global trust degree of nodes, elects a new round of authorized agent groups, and resets the three-vector commitment weights. A new block is created with the decision consensus result, and the UAV blockchain network system is updated. Through the identity vector commitment in the new block, untrustworthy nodes are identified and isolated from the network, maximizing the availability and trustworthiness of the network nodes actually involved in the mission and enabling a new round of UAV identity authentication. The decision consensus result is stored in the blockchain, while local trust transactions as data consensus can be discarded after the decision consensus is reached and do not need to be on the chain, so the identity blockchain for UAVs is stateless and lightweight for fast authentication of inter-UAV communication.

The main contributions of this work are as follows:

(i) First, we introduce the new concept of triple vector commitment stateless blockchain in UAV networks. Using an aggregatable subvector commitment technology, the blockchain only records the dynamic changes of identity commitments in triple vectors instead of every authentication transaction. This not only enables lightweight blockchain storage, but also avoids the massive amount of recalculation in individual vector commitment due to membership changes. It greatly reduces the computational and communication overhead incurred by UAVs frequently entering and leaving the network and the isolation of untrustworthy nodes.

(ii) Second, we propose a novel dynamic multicenter trust authorization proof consensus mechanism, where a set of agent nodes are periodically elected as a blockchain consensus committee among all UAVs that have been registered to the mission network. The committee members are randomly and dynamically replaced periodically to sense the UAV flight dynamics in real time and monitor the nodes' reports on the abnormal forwarding behavior of their own neighboring nodes. New block generation and consensus are either achieved periodically or triggered to complete in time according to node identity status changes. This not only ensures consensus efficiency, but also significantly reduces the risk of blockchain consensus master nodes being tracked and locked, and improves the security of the consensus process.

(iii) Third, we propose the method of local mutual authentication of blockchain nodes. In each period of the blockchain, any node of the UAV network is a peer-to-peer full node. The UAVs only need to provide their own commitment witness to achieve localized two-way authentication which only involves giving the existence of vector commitment instead of traversing the whole blockchain. This reduces both the computational and communication complexities of UAV mutual authentication to a constant level.

(iv) We compare our scheme with several major existing MANET node authentication schemes, including remote direct anonymous authentication, threshold key sharing authentication, certificate-coin authentication by blockchain token method, and blockchain authentication based on cryptographic accumulator. The extensive experimental results demonstrate that our proposed scheme outperforms other competitive schemes in terms of single-step authentication latency, energy consumption, authentication computational overhead, and end-to-end latency.

The rest of paper is organized as follows. The related work is discussed in Section 2. The system model, including the network model, the threat model, and the blockchain model, is elaborated in Section 3. Section 4 describes the design details of our proposed vector commitment-based lightweight authentication scheme for stateless blockchains. In Section 5, the safety certification and performance analysis on our proposed scheme are conducted. Simulation results and analysis are illustrated in Section 6. Finally, the conclusion is presented in Section 7.

2. Related Works

For the distributed, self-organized, and autonomous characteristics of self-organized networks, according to different application models, domestic and international research mainly includes the authentication model based on threshold secret sharing technology [3], certificate chain-

based authentication, and blockchain-based authentication model.

In [4], the UAV remotely connects to the control center via a 4G wireless network using direct anonymous attestation (DAA) for remote authentication. However, this method requires the support of a remote center and is not very scalable. Using the threshold secret sharing technique, [5] proposed a distributed certificate-based authentication model where the certificate is partitioned into n shares, a share is allocated to the node acting as a distributed certificate authority (D-CA), and t of these shares are collected at authentication time to reconstruct the certificate. In the scheme proposed by Yi and Krave [6], the node uses flooding to send a certificate request (CREQ) and the D-CA responds with a certificate reply (CREP) as a response. The successful collection of t copies of the certificate shares node, and the user reconstructs the complete certificate. A valid certificate indicates successful authentication. This approach increases the communication overhead of the network and does not protect against black hole attacks launched by resource-powered malicious nodes.

[7–9] proposed to apply identity-based public key cryptosystems to MANETs, introducing distributed cryptography to propose a fully distributed identity-based scheme, and each node performs the process of issuing and managing certificates and maintains a certificate repository. The nodes complete mutual authentication through the chain of authentication formed by the certificate repository. The advantage is that there is no need for a certification center to authorize the management of worker certificates, avoiding the risk of a single point of failure. But the introduction of private key generators (PKGs) caused key escrow problems and the risk of impersonation attacks. Certificates and identities cannot be bound, and malicious nodes can impersonate other nodes to join the network at will. In addition, the inconsistency of the certificate chain of each node also leads to authentication failure, and the certificate repository management and maintenance costs of the nodes increase with the expansion of the network scale. This is difficult to achieve for resource-constrained UAV nodes.

Certificate-less public key passwords [10] are an improvement on identity ID-based public key passwords, and [11–14] combined threshold cryptography with certificate-less public key passwords in the MANET authentication model. However, the security of the system master key relies on the absolute security and reliability of the distributed server, and in addition, there is a risk of man-in-the-middle attacks during key negotiation. Most of the schemes in the above literature use bilinear pairing, which provides good security, but their high operational complexity results in these schemes not being lightweight; key distribution mostly requires the establishment of a secure channel. Ad hoc, highly dynamic UAV networks cannot be provided.

Blockchain-based decentralized authentication uses the tamper-evident and traceable nature of the blockchain to store information such as identity and public key. The process of authentication traverses the blockchain to query the certificate, then checks whether the public key belongs to its declared identity, and finally sends a challenge message to determine whether the other party holds a matching private key by verifying the digital signature. [15] proposed authentication and key management mechanisms to achieve security of heterogeneous drones through the combination of transaction chain and blockchain, but the scheme requires that the drones as cluster head must have sufficient resources and act as the full node role of the blockchain, so there is still the risk of local single point of failure, which cannot guarantee the security of the full node of the cluster head itself, and the nonstop growth of the blockchain shared ledger makes the section face problems such as "storage bloat" and reduced authentication efficiency.

Researchers [16, 17] used blockchain technology to improve the public key infrastructure (PKI) authentication technology. Distributed PKI authentication is implemented to avoid the problems of single point of failure and certificate transparency in traditional PKI, and to effectively address the inefficiency of using the method of traversing the blockchain to query certificate authentication and the increasing storage overhead as the size of the blockchain grows. By combining blockchain and dynamic accumulator, a blockchain PKI model that can update certificates in bulk is constructed, thus improving the efficiency of authentication. The model can efficiently add, revoke, and renew user certificates. However, the consensus of the blockchain until the transaction is on the chain confirms that the authentication is successful, which makes the latency of a single authentication, as well as the computational and communication overheads insufficient to meet the requirements of mission drone networks in terms of real-time and low energy consumption. [18] Color green addressed this paradox by proposing a novel semipermitted blockchain framework that balances decentralization and efficiency, making the system scalable and efficient at the same time. A randomly selected public node joins the committee to execute the protocol to protect the block, but separates transaction execution from the protocol, thus reducing protocol waiting time and allowing lightweight nodes to participate, but the public node requires high resources.

The combination of blockchain technology and cryptographic accumulator technology has been used to solve the authentication problem of distributed network systems, and there have been many research results at home and abroad. The accumulator, first proposed by Benaloh and de Mare [19], is a compact representation of an arbitrarily large set that can be used to prove claims of membership or non-membership in the underlying set. The protocol in [20] used RSA accumulators to combine large states into a short commitment to design stateless blockchains where the verifier only needs to store block headers, greatly reducing the need for disk and RAM, reducing the storage overhead of the verifier, and linearly increasing system throughput. [21] provides cryptographic accumulator universal composable (UC) processing using two weaker accumulators, constructing the accumulator in a modular fashion and extending the anonymous credential system to support revocation using the results of the UC accumulator. Libert and Yung in [22–24] vector commitments give

Table 1: Classification and comparison of authentication methods.

Method	Papers	Overhead and shortcomings
Threshold secret sharing	[3, 5, 6]	High computational and communication overheads; unable to defend against black hole attacks launched by malicious nodes with powerful resources.
Certificate chain	[7–9]	High storage and communication overheads; there are key escrow issues and risk of impersonation attacks. Inconsistencies in the certificate chain across nodes lead to authentication failures. As the size of the network increases, the cost of managing and maintaining the certificate store increases.
Certificate-less public key	[10–13]	High computational and communication overheads; man-in-the-middle attack risk during key negotiation, key distribution mostly requires establishment of secure channels.
Traditional blockchain	[15–17]	High storage and computational overheads, "storage explosion," inefficient consensus, and limited system scale.
Stateless blockchain	[21–24]	Storage overhead very low; nodes are dynamically added and removed, resulting in frequent recalculations of the accumulator.

commitments to ordered sequences that satisfy positional binding; i.e., an adversary algorithm should not open a commitment for two different values at the same position. The commitment string and the open witness are short, and their size is independent of the vector length. [20] applies unknown-order group batch processing techniques to cryptographic accumulators and vector commitments to develop techniques for noninteractive aggregated membership proofs that are verified by a constant number of group operations and provide size invariant bulk nonmembership proofs for a large number of elements. Using these new accumulator and vector commitment constructs to design stateless blockchains where nodes require only a constant number of stores to participate in consensus. [25] proposed vector commitments with subvector openings that allow a commitment vector to be opened at a set of locations with an opening size that is independent of the length of the vector and the number of open locations. On its basis, [23] proposed incremental aggregation to design an algorithm that generates openings quickly by preprocessing and then to implement subvector commitments. VMware research and the Ethereum team [24] propose aggregatable subvector commitment (aSVC) schemes that can aggregate multiple proofs into a small subvector proof. The approach of aSVC obtaining a stateless payment cryptocurrency has very low communication and computational overhead. However, the above authentication methods complete consensus on a fixed number of nodes and all suffer from accumulator recalculation when nodes leave or join. The joining and leaving of drone nodes in a UAV network are frequent, and there is interference from Byzantine nodes with legitimate identities, which the above parties cannot handle. Table 1 summarizes the above authentication methods.

The authentication methods described above cannot be applied to lightweight, dynamic, and time-varying node trustworthiness for UAV networks. How to build a dynamic UAV trustworthy platform based on stateless blockchain to provide fast mutual authentication between UAVs is the main research objective of this paper.

3. System Models

UAV networks in complex and unknown mission environments are inherently Byzantine distributed systems with time-varying trustworthiness. The purpose of the lightweight authentication blockchain system is to monitor the trustworthiness of drone nodes during a mission and to provide a global platform for rapid mutual authentication between nodes. In traditional blockchains, transactions need to complete consensus and update the blockchain across the network before they can be authenticated successfully, which makes the authentication efficiency, and the computation and communication overhead insufficient to meet the requirements of UAV networks in terms of real-time and low energy consumption. The stateless authentication blockchain provided in this paper periodically performs data consensus on the local trustworthy state records of nodes, which are generated by monitoring the forwarding behavior of neighboring nodes, and then performs decision consensus on the data consensus results, i.e., aggregatable identity vector commitment based on the global trustworthiness of nodes. Its lightweight nature is reflected in the fact that only the decision consensus result is kept, and the new blocks added to the blockchain are blockheads of fixed size, without the need to keep intermediate historical state data; thus, its storage is controlled.

3.1. Network Model. In the mission preparation phase, the system authorizes the registration server as the authoritative control center in the initialization phase of the system, which initializes the security environment parameters of the mission. The UAV nodes and the created blocks of the blockchain register the UAV identity, calculate the identity vector commitment, and select the authoritative UAV node for the task execution phase. The proof-of-authority consensus mechanism (POA) is used to broadcast the created block to all the mission UAV nodes on the chain for reaching a consensus.

The system network model is divided into a network model for the mission preparation phase and a network model for the mission execution period based on the process of the mission (Figure 1). In the mission preparation phase, the UAV swarms and the registration server form a wireless network with the registration server as the authorization center in a secure environment. All nodes deploy blockchain client programs, and the registration server acts as a trusted authority to initialize the security environment parameters of the UAV mission network. The registration server acts as a

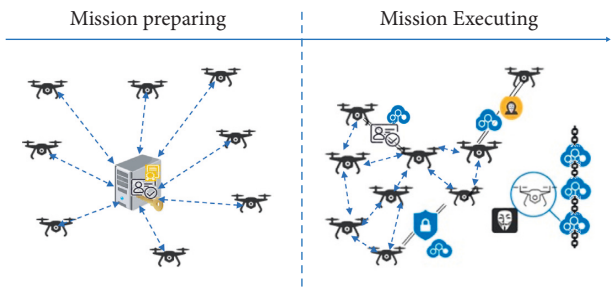

Figure 1: Mission-based UAV network model.

trusted authority to initialize the security environment parameters of the UAV mission network, register the identity of the UAV, assign public and private keys, establish the genesis block, and build the blockchain network system with the proof-of-authority consensus mechanism. The registration server does not participate in the mission execution, and the network after the mission starts is a self-organized network of autonomous UAV nodes that forward data in a multi-hop manner. The blockchain system supervises the flight dynamics and forwarding behavior of the network nodes in real time to maintain the effective operation of the mission network.

3.2. Threat Model. The ultimate goal of a mission-oriented UAV network is to complete time-sensitive missions, and any factor that affects the proper achievement of the mission can be considered a threat to the UAV network.

(i) Environmental threats: The UAV network mission execution environment is complex and variable, it may be the scene of distress and rescue, or it may be the enemy-occupied area of the battlefield, the UAV network may suffer physical interference, or even be directly damaged and affect the performance of the overall network, and the network system should have the ability to sense the nodes leaving the network in a timely manner and cancel the identity of the lost network members; at the same time, the additional network members can be quickly authenticated into the network. The network system should have the ability to sense when a node has left the network, to cancel the identity of lost network members, and to quickly authenticate additional network members to the network to ensure the network's ability to perform its mission.

(ii) Malicious nodes: Malicious nodes include external unauthorized malicious nodes and compromised nodes. Malicious nodes can launch impersonation attacks, black hole attacks, and DOS attacks, and can also conspire to conduct wormhole attacks. Compromised nodes with legitimate identities can be more damaging to the network by launching internal attacks. Therefore, in addition to authentication, the drone network should also have the ability to detect untrustworthy nodes and isolate compromised nodes from the network in a timely manner.

(iii) Selfish nodes: Due to their own reduced energy, nodes only receive information and do not forward it out of self-protection. Such uncooperative zombie nodes, although they do not initiate harmful attacks, exist in the network and generate ineffective communication, wasting energy and reducing the overall performance of the network. The system should also have the ability to identify and mark them for isolation.

3.3. Blockchain Model. The solution recommended in this paper implements local mutual authentication of UAV network nodes using a stateless authentication blockchain. The initialization of the blockchain is done in a secure environment. The mission starts with all UAV network nodes having the same Genesis block, which contains an identity vector commitment, an authenticated smart contract, and a specified set of authorized nodes. The consensus process takes place in the authorized node group, with the number of authorized nodes set based on the network size. The authorized nodes are responsible for detecting the flight status of the drone nodes, such as whether they leave the network. All nodes send to the authorized nodes the local trust assessment of neighboring nodes generated during the consensus cycle. Similar to the node trustworthiness monitoring method (WatchDog) proposed in [26], monitor the forwarding behavior of neighboring nodes to assess their trustworthiness. The consensus cycle is set according to the network size, but consensus is initiated when two conditions occur during the consensus cycle: (i) an authorized node finds a record below the trustworthiness threshold in the collected local trustworthiness assessment dataset; (ii) an authorized node does not receive a response from a particular drone node several times in a row, and this number exceeds the threshold set by the system.

The consensus process consists of a data consensus and a decision consensus. The data consensus consists of a local trustworthiness assessment generated by all nodes during the consensus cycle, and the status records of the UAV flights detected by the authorized nodes (whether they respond or not). Data consensus results in each authorized node having an identical subset of status records. A decision consensus is performed on the results of the data consensus to determine the global trustworthiness of the nodes, elect a new set of authorized nodes, and update the triple identity vector commitment. The results of the above decision consensus are recorded in a new block, a fixed size block header to be exact, and the drone network continues to work under the management of the new authorized node group after the blockchain has been synchronized and updated. In the meantime, historical state data used for data consensus can be discarded after decision consensus, and the blockchain grows only the block head that holds the decision consensus result at a time, avoiding the creation of a "storage explosion."

The consensus process is generated periodically, and the group of authorized nodes for consensus in each period is dynamically generated according to the consensus result of

the decision, which is a dynamic polycentric proof-of-authority consensus mechanism (DPOTA), as shown in Figure 2, where the UAV network is reorganized by new blocks added to the blockchain, triple identity vector commitment, node cancellation determined by dynamic aggregation, and isolation. The stateless blockchain UAV network guarantees network trustworthiness and provides fast mutual authentication between nodes.

4. Recommended Scheme

In this section, we explain the stateless blockchain authentication system supporting DPOTA consensus mechanism, and our approach solves or alleviates the conflict between UAV networks with resource constraints in storage, computation, energy, and bandwidth and high requirements in dynamism, real time, and security during mission execution. Figure 3 shows the operation of the mission-oriented UAV network stateless blockchain light authentication certification by timeline.

The mission-oriented stateless blockchain authentication system for UAV networks consists of two phases and four roles. In the mission preparation phase, the UAV network operates in a secure network environment, including a trusted third party, a registration server (RS), and a UAV to be registered (UAV); in the mission execution phase, it works in a nonsecure network state, including a stateless blockchain trusted platform and a blockchain UAV node (BUAV), and throughout the mission, the UAV network security is performed by the registration server and the blockchain together.

At the beginning of the mission, a blockchain client program is deployed for the registration server and the candidate UAVs participating in the mission to initialize the UAV network in a secure environment with the registration server as the center. The registration server constructs the UAV network mission-related security environment parameters based on the hyperelliptic curve public key cryptosystem [27] (HECC), receives UAV registration requests, generates public and private keys and identity IDs, and builds the identity vector. The vector commitment is calculated based on the identity vector, and the identity witness of the corresponding UAV is generated at the same time. Subsequently, trust authorization committee members are randomly selected, node trust vectors are initialized, and creation blocks are constructed. After completing the initialization, the registration server broadcasts the Genesis block to all registered UAVs to build the blockchain system of the UAV network.

4.1. System Initialization. In the mission preparation phase, the network environment is secure and the registration server is authorized as the control center to complete the initialization of the stateless blockchain system. The mission-oriented UAV network system is initialized, including the initialization of the registration server, the initialization of the UAV, and the initialization of the blockchain. Table 2 lists the main authentication-related global symbol.

Registration server initialization: First, the hyperelliptic curve $\mathrm{HE}(F_p)$ is customized for the system, where $p \in \mathrm{HE}(F_p)$ is its basis, the large prime q is its order, $q \neq p$, and q is not divisible by $p-1$. Then, set the one-way hash functions by equation (1), where $G_1 \subseteq (C, F_q)$ is the Abelian cyclic additive group on the hyperelliptic curve, generating the element $P \in G_1$.

$$\begin{aligned} H_1 &= (0,1)^* \longrightarrow Z_q^*, \\ H_2 &= (0,1)^* \longrightarrow G_1^*. \end{aligned} \tag{1}$$

Randomly select $k \in Z_q^*$ as the private key of the registration server and $P_k = kP$ as its public key. The public cryptographic parameters, $\{q, G_1, P, P_k, H_1, H_2\}$, are stored in the registration server only as important security environment parameters for the current mission.

UAV initialization: The UAV provides hardware-related information such as MAC and IP address, and applies for identity registration with $\{U \| U_{\mathrm{mac}} \| \mathrm{IP}\}$ as a request to the registration server, which is not involved in the mission execution. The registration server generates the private key $d \in Z_q^*$ and the corresponding public key $U = d \cdot P$ for the UAV. The public security parameters, $\{q, G_1, P, P_k, H_1, H_2\}$, are built into the associated smart contract in binary form, which is deployed to the Genesis block by the registration server. Based on the UAV identity request $\{U \| U_{\mathrm{mac}} \| \mathrm{IP}\}$, the registration server key $k \in Z_q^*$ is used to sign the requested UAV, and the registration smart contract generates the UAV node identity and assigns the initial value of trust to each node, with the identity ID calculated by equation (2). The final registration server assigns the public and private keys of the UAV, the identity ID, and the creation block to the corresponding UAV nodes.

$$\mathrm{ID}_i = H_2\left(H_1\left(U_i \| \mathrm{ID}_i \| \mathrm{IP}\right) \| \mathrm{Sign}_{\mathrm{reg}}^{k}\left(U_i \| \mathrm{ID}_i \| \mathrm{IP}\right)\right). \tag{2}$$

Stateless blockchain initialization: During the mission preparation phase, the network environment of the registration server is secure and the setup $(1^\lambda, 1^N)$ function is run to establish vector committed common reference parameters (crs), which are built into the smart contract associated with the creation of the block in binary form. Since the registration server does not participate in the task network, the crs of the UAV network are hidden during the mission execution phase and no adversary algorithm can use the crs to fake the related information. The structure of the Genesis block is shown in Figure 4, which mainly includes the registered UAV identity vector commitment, the consensus committee member list, the UAV trust value vector, and the smart contracts related to registration, deregistration, trust management, and authentication. The UAV identity registration contract (SC_IDReg) is invoked only at the registration server. The hyperelliptic curve cryptosystem is used to sign UAV requests and generate unique UAV ID. The order of UAV registration forms the order of positions in the identity vector, and values in the trust vector are assigned in this order. The number of registered UAVs can be much larger than the number of UAVs for mission execution.

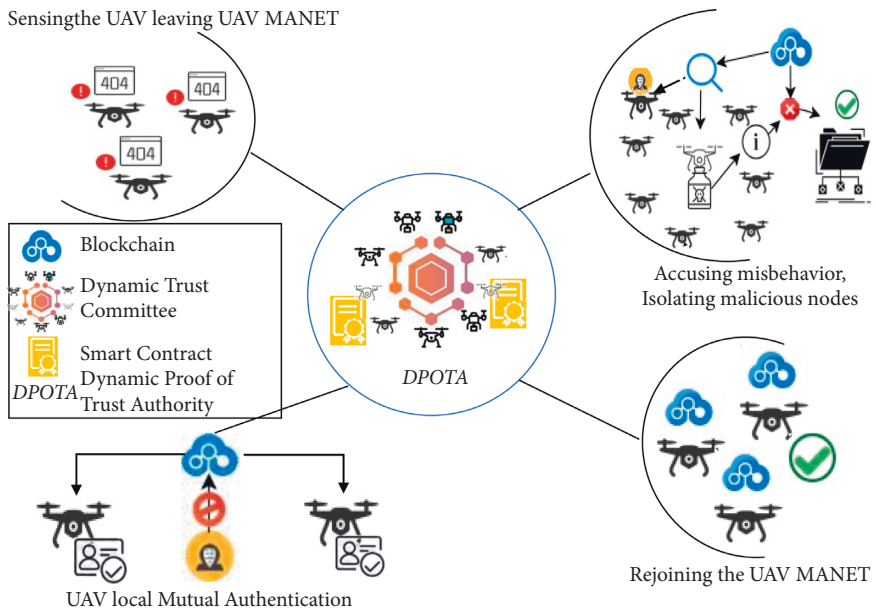

Figure 2: Stateless authentication blockchain model during mission execution.

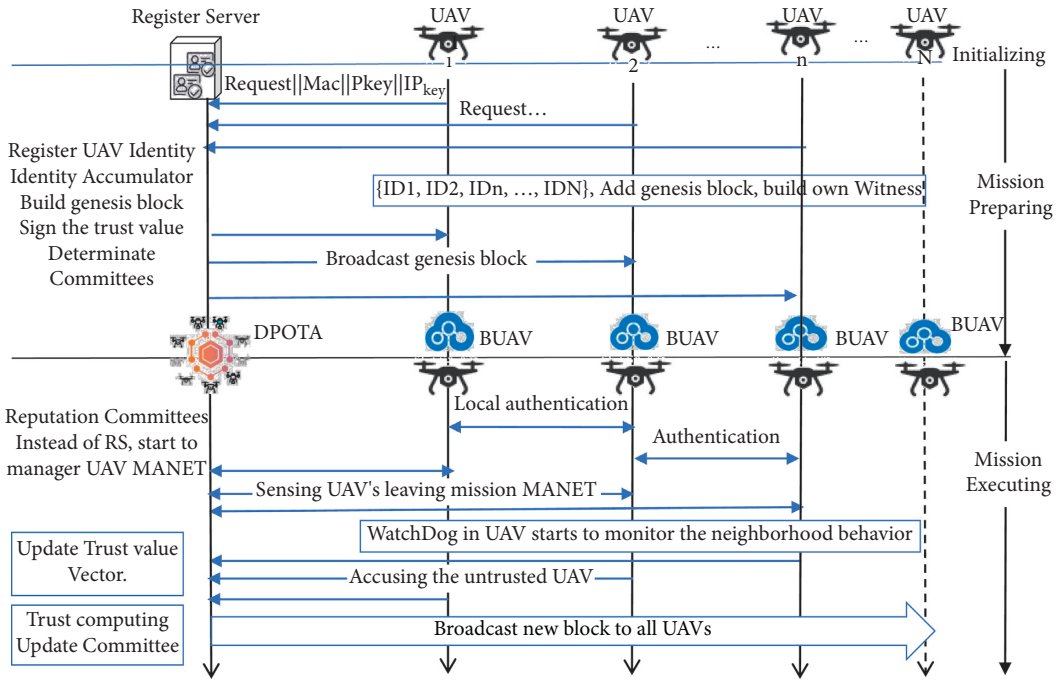

Figure 3: Mission-oriented UAV network blockchain workflow.

In the registration server, the smart contract, vector commitment accumulator (SC_VCCom), completes the registration of UAVs, generates identity witnesses, and builds vector commitments for all registered UAVs. After determining the UAVs to participate in the mission execution, t UAVs are randomly selected (t is set by the system in advance according to the application requirements) and their identity information key-value pairs, {ID: Pubkey, IPaddress}, are used to construct the initial list of trusted authorized members. These t UAVs are used as the blockchain consensus committee members in the first round of the mission execution phase.

Table 2: Global symbol.

Symbol	Description
ID_i	The i-th UAV identifier
W_i	The i-th UAV witness
C_{ID}	Identity vector commitment
$\widehat{W}$	Witness aggregation
$\widehat{W'}$	Aggregation of removed witnesses
G_1	The Abelian cyclic additive group of the hyperelliptic curve
$\overrightarrow{ID}$	UAV network node identity vector
$\overrightarrow{W}$	UAV network node witness vector

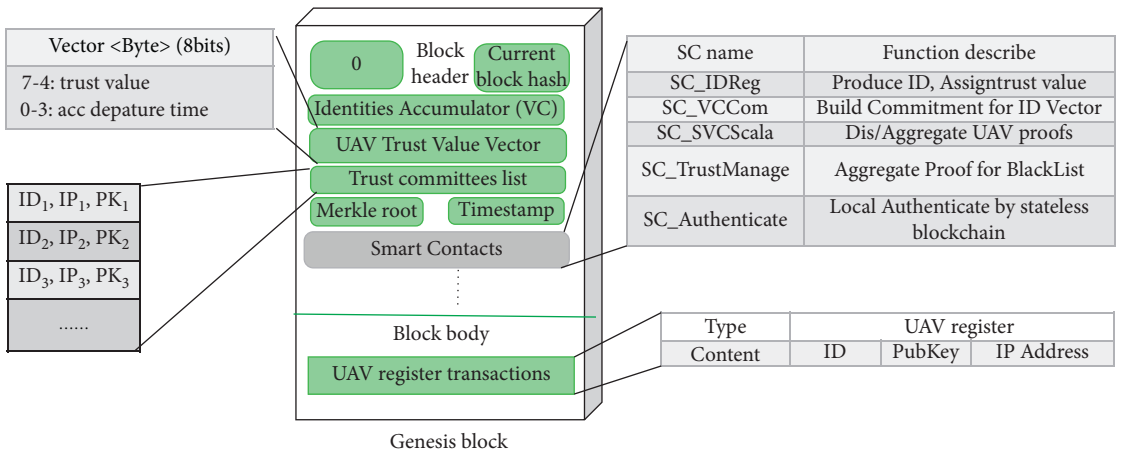

Figure 4: Stateless blockchain genesis block structure.

Input: Security parameters λ, UAV number N, UAVs request.
Output: Nodes' ID vector commitment, C_{ID} trust value vector.

In Register Server:
#Received all UAVs' requests
$\overrightarrow{\mathrm{ID}} = \{0\}$; TrustList = {0};
crs = Setup $(1^{\lambda}, 1^{N})$;
for i in N**do**# UAV nodes
  MySign = $\mathrm{Sign}^{k}_{\mathrm{reg}}(U_i \| \mathrm{MAC}_i \| \mathrm{IP})$
  $\mathrm{ID}_i = H_2(H_1(U_i \| \mathrm{MAC}_i \| \mathrm{IP}) \| \mathrm{MySign})$
  $\overrightarrow{\mathrm{ID}}$.Append$(\mathrm{ID}_i)$;
  TrustList.Append(trustvalue);
end for
#Get the all registered UAVs identities:
$\#\left\{\overrightarrow{\mathrm{ID}} = \{\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_i, \ldots, \mathrm{ID}_N\}\right\}$
$C_{\mathrm{ID}} \longleftarrow$ Commit$(\overrightarrow{\mathrm{ID}}, r)$, #$r$ is randomnal;
#Randomly selects 5 UAVs from n UAVs as the trusted committee
IninilizeTrustList( )
for all UAV nodes:
for uav_i in length of $\overrightarrow{\mathrm{ID}}$. **do**
  $W_i \longleftarrow$ Prove$(i, \overrightarrow{\mathrm{ID}}, k)$, # k is randomnal;
  Send $(\overrightarrow{\mathrm{ID}}.\mathrm{ID}_i, W_i)$
end for
#When receive genesis_block from register sever
if current_block is constructed correctly **then**
  block_chain.append(genesis_block);
else
  Abort Genesis block;
end if

Algorithm 1: UAV registers/builds the stateless blockchain.

The identity vector is generated in the registration server $\overrightarrow{\mathrm{ID}} = \{\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_i, \ldots, \mathrm{ID}_N\}, i \in \{1, 2, 3, \ldots, N\}$, combined with a random number to compute the identity vector commitment of the UAV, C_{ID}, and the identity witness vector $\overrightarrow{W} = \{W_1, W_2, \ldots, W_3, \ldots, W_N\}$. The registration server constructs the Genesis block and synchronizes it to all registered UAVs. The registered UAVs obtain their own IDs and identity witness to initialize the mission-oriented UAV network blockchain system. Please refer to Algorithm 1.

4.2. Triple Vector Commitment Stateless Blockchain. In the mission execution phase, the network environment is complex and insecure; with the possibility of external network attacks, nodes leaving the network, and nodes being compromised, the stateless blockchain serves as a global trust platform to manage the mission UAV network.

Dynamic multicenter proof-of-authority consensus protocol: When a new block is created, the current authoritative nodes randomly select the consensus committee members for the next round based on the blockchain trust

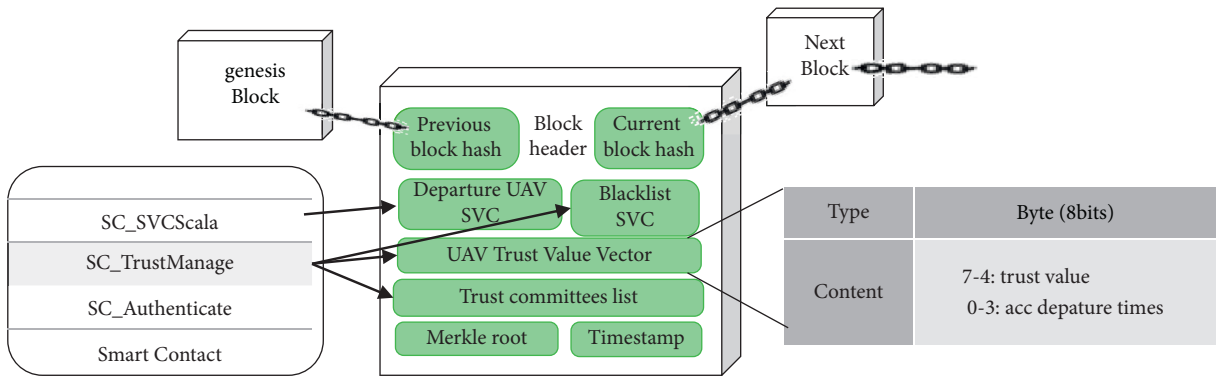

Figure 5: Stateless blockchain structure diagram.

vector. This makes it difficult for adversaries to ascertain the target to attack Through a smart contract related to trust management, the consensus committee members respond to the flight status of the drones and handle reports of abnormal behaviors when nodes forward data. The consensus mechanism is triggered directly when the aggregatable deregistration subvector or blacklist subvector of consensus nodes changes to ensure the trustworthiness and validity of participating members in the mission-oriented UAV network.

Figure 5 represents the structure of a new block added to the stateless blockchain, a fixed size block header that holds the results of each cycle of decision consensus, containing subvector witness aggregation, subvector witness aggregation for nodes leaving the network, subvector witness aggregation for untrustworthy nodes, and a dynamically changing vector of trust values for all nodes. The system sets the blockchain consensus period according to the network size and specific environment, and the historical state data used for data consensus need not be on the chain. Consensus committee members call the smart contract SC_SVCScala to perform dynamic aggregation of drone member witness and call the smart contract SC_TrustManage to modify the trust vector value of the drone. After the decision consensus, if any drone's trust value is below a certain threshold, its witness will be aggregated into the malicious node blacklist subvector; the witness of a drone that does not respond to the authorized node detection with a test greater than a set value will be aggregated into the revocation subvector. The number of authorized node groups is relatively small, and the PBFT consensus algorithm can be used for data consensus.

Identity vector commitment: Mission-oriented UAV networks operate in unknown and complex mission environments. The mission process is exposed to multiple risks, such as environmental factors causing nodes to leave the network, or compromise of internal nodes due to malicious attacks, and selfish behavior of nodes protecting their own resources. The UAV network needs to sense the dynamic changes in the validity and trustworthiness of UAV nodes in a timely manner. Rapid response to the deregistration, restoration, or isolation of abnormal nodes is necessary to maintain the overall performance of the network and ensure the reliability of mission execution. The proposed triple identity vector commitment mechanism avoids costly recalculation of the generic cryptographic accumulator due to changes in membership status and only requires reclassification of the changing UAV identity proofs. The key functions of the proposed scheme are shown below:

(1) $\text{crs} \leftarrow \text{Setup}(1^{\lambda}, 1^{N})$, output public parameter crs, supported vector length N, (crs include public parameters of the security environment of this mission network, providing implicit input for other algorithms, including adversary algorithms, and UAV network applications need hidden processing).

(2) $C_{\text{ID}} \leftarrow \text{Commit}(\overrightarrow{\text{ID}}, r)$, input vector $\overrightarrow{\text{ID}}$ and random number r, output vector of commitment C_{ID}.

(3) $\overrightarrow{W_i} \leftarrow \text{Prove}(i, \overrightarrow{\text{ID}}, r)$, generating witness of the existence of the corresponding element at position $i \in [N]$ in the $\overrightarrow{\text{ID}}$ vector.

(4) $\widehat{W} \leftarrow \text{Aggregate}(C_{\text{ID}}, \overrightarrow{\text{ID}}[S], \{W_i : i \in S\})$, given the set of positions $S \subset [N]$ of the elements of the vector to be aggregated, has been witnessed accordingly $W_i : i \in S$, and outputs aggregation $\widehat{W}$: $|\widehat{W}| = |W_i|$.

(5) $\widehat{W'} \leftarrow \text{Disaggregate}(\widehat{W}, \overrightarrow{\text{ID}}[S'], \{W_j : i \in S\}')$, unmake the corresponding witness in the set $S' \subset [N]$ from the aggregated $\widehat{W}$.

(6) $b \leftarrow \text{Verify}(C_{\text{ID}}, \overrightarrow{\text{ID}}[S], \widehat{W})$ verifies whether the commitment C_{ID} contains the corresponding subvector, $\overrightarrow{\text{ID}}[S]$, in the location set S by aggregating the witness $\widehat{W}$, and $b = 1$ indicates that the corresponding identity ID is legitimate.

In the mission preparation phase, the legal information of all nodes' ID witness is compressed into the identity vector commitment, and the UAV is assigned the identity ID_i in the registration phase, as well as the witness W_i that proves its existence in the commitment C. The first layer of vector commitment, $C_{\text{ID}} \leftarrow \text{Commit}(\overrightarrow{\text{ID}}, r)$, is created by the registration server and saved in the Genesis block. UAVs that become members of the consensus committee initiate the UAV flight state sensing module, which aggregates the identity witness of UAVs that have left the network to the revocation subvector commitment (the second layer vector commitment). During the mission execution phase, when the

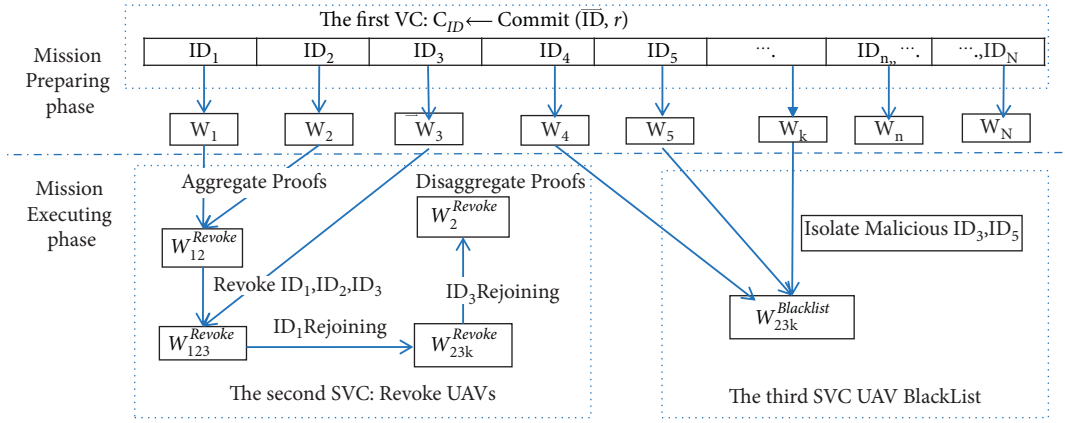

Figure 6: UAV network triple authentication vector commitment.

UAV forwards data, its built-in monitoring module WatchDog [12] reports the bad behaviors of neighboring nodes to authorized nodes. The smart contract related to trust management of the blockchain system determines whether to aggregate the identity witness of the questioned nodes to the blacklist subvector (the third layer vector commitment) based on their trustworthiness. As shown in Figure 6, when a UAV launches a communication request, the received UAV verifies whether it is in the identity vector commitment in turn, then detects whether its witness is in the blacklist subcommitment, otherwise detects whether its witness is in the revocation subvector commitment, and finally decides whether to de-aggregate the witness of the UAV from the revocation subvector, and de-aggregation means that the UAV rejoins the network. This ensures that the UAVs participating in the mission network are valid and trusted.

4.3. Identity Revocation Subvector Commitment. During the execution of the mission, the UAV leaves the network actively due to the mission need or the UAV leaves the network passively due to failure, attack, and other reasons, as well as the flight obstacle that causes the UAV to temporarily leave the network; the members of the blockchain trust authority committee in each period activates the UAV flight state sensing module, sensing UAV leaving, and dynamically aggregate the corresponding UAV according to the received UAV leaving event transactions of the witness and update the cancellation identity subvector commitment, indicating the identity of the node corresponding to the revocation witness from the task network, as shown in Figure 6, UAV ID1, ID2, ID3 at due to the loss of connection state; the smart contract SC_SVCScala invokes the aggregation function module to establish or update the dual identity commitment as follows.

$$S = 1, 2, 3,$$
$$W_{123}^{\text{Revoke}} \longleftarrow \text{Aggregate}\left(C_{\text{ID}}, \text{ID}[S], \{W_i\}, i \in S.\right) \tag{3}$$

When the once departed UAV returns to the mission network, if UAV ID3 requests network communication, its identity is verified as legitimate in the first layer vector commitment, it is determined not to be a compromised node after verification in the third layer subvector commitment, and the associated smart contract then updates its second layer identity deregistration subvector commitment as follows.

$$S' = 1, 2,$$
$$W_{12}^{\text{Revoke}} \longleftarrow \text{Disaggregate}\left(W_{123}, \text{ID}[S'], \{W_j\}, j \in S'.\right) \tag{4}$$

De-aggregation with identity subvector commitment adapts to network scalability and reduces invalid communication. Revocation aggregation refers to the algorithm 2, where actively departing UAVs send departure transactions to the current authority committee; meanwhile, the authority committee members periodically sense all current trusted members of the UAV network. If no response is received for more than two periods, the unresponsive UAVs are set to leave the network state. The authority committee members in the current cycle accumulate the departure time, update the trust vector in the blockchain, and reach consensus on whether the UAV leaves the network by voting. The high four bits of the UAV trust value vector in the block structure are the trust value of the UAV, and the low four bits are the cumulative value of the time the UAV is off the network.

4.4. Untrustworthy Node Identity Subvector Commitment. To secure the entire UAV network and prevent malicious nodes from causing unbearable malicious damage to the entire network system, the triple identity subvector promises an irrecoverable revocation mechanism for malicious drone node identities. The objective is to discover and isolate the malicious nodes from the mission UAV network in the shortest possible time. The trustworthiness of the UAV nodes involved in the mission execution is guaranteed. This paper focuses on stateless local lightweight authentication based on vector commitment, node trustworthiness control refers to WatchDog algorithm to identify whether neighboring nodes are abnormal by nodes monitoring their neighboring nodes to forward packets, and the detailed process refers to [28].

The trust level saved by the UAV trust vector in the latest block is an important reference standard when selecting new

authority members in the periodic consensus. If the trust value of UAV ID_4, ID_5, ID_i is less than the threshold value set by the system, a triple identity subvector aggregation, and malicious node blacklist, an irreversible identity witness aggregation is established or updated, and the smart contract invokes the following functional module to achieve it.

$$\begin{aligned} &S = 4, 5, k, \\ &W_{45}^{\text{Blacklist}} \longleftarrow \text{Aggregate}\left(C, \text{ID}[S], \{W_i : i \in S\}\right). \end{aligned} \tag{5}$$

Triple subvector commitment: Identity witness of a node whose identity is legitimate but not trusted can be classified as a third layer of blacklisted subvector commitment. During this period, a new block is created by a bookkeeper elected by the committee and the new block is multicast with updated trust vectors and blacklisted subvector commitments to UAVs that the blockchain confirms are valid. When a UAV initiates a communication request, the UAV that receives the request first performs the first layer of vector commitment verification to determine whether the identity of the requesting node is legitimate and again verifies that its identity is trustworthy. All the verification is done locally without traversing the blockchain to query. The details are described in Algorithm 3.

4.5. Local Two-Way Authentication of UAV Node. Two-way authentication process: The identity vector commitment ensures the infeasibility of forgery attacks, man-in-the-middle attacks; timestamp mechanism ensures that reentry attack requests are directly abandoned, circumventing the formation of broadcast storms; at the same time, the random number r is generated by the initiating request node, then signed by the receiver, and sent back to the requester, confirming that it is a response to the requester's request, while the information replied by other receivers is directly rejected. The authentication protocol in the recommended scheme, whether it is a replay attack of the legitimate identity of the compromised node, or a replay attack of the external malicious node after eavesdropping, can be effectively circumvented.

Figure 7 shows an authentication process between two nodes of the task-oriented UAV network. The UAV ID_A broadcasts an authentication request, and the UAV ID_B receives the request, verifies the legitimacy of ID_A through the authentication smart contract of the local blockchain, determines the legitimacy of its identity through triple subvector commitment, detects the timestamp, and filters the replay request. After the verification is passed, ID_B sends a response to ID_A, and ID_A also verifies the legitimacy of ID_B. After passing the verification, it stops receiving the response information sent by other nodes, establishes the session key, encrypts the sent data, and sends it directly to ID_B, completing one-time transmission, where t_{A_R} is the request timestamp, t_B is the response timestamp, $r \leftarrow Z_n^*$ is the random number generated when ID_A requests, $\text{sign}(SK_A(r \| t_A)$ is the signature when UAV ID_A requests, $\text{sign}(SK_B(r \| t_B)$ is the signature when UAV ID_B responds, SK_A/PK_A, SK_B/PK_B are the public and private keys of UAV ID_A and ID_B, respectively, and W_A, W_B are the respective identity witnesses.

5. System Analysis

5.1. Authentication Correctness. Symbol explanation: The UAV network node identity vector $\overrightarrow{\text{ID}} = (\text{ID}_1, \text{ID}_2, \ldots, \text{ID}_N)$, $\overrightarrow{\text{ID}}[S] = (\text{ID}_i, i \in S)$ denotes the identity subvector represented by the ordinal number in the UAV identity set S. Using $\text{ID}[-i]$ to represent $\text{ID}[N] \setminus i$ denotes the removal of the unmanned node corresponding to position i from the identity vector. n is an integer and using $[N]$ to represent the set$\{1, 2, \ldots, N\}$. Algebraic group model means that the group elements of the adversary output cannot be created arbitrarily, but must be obtained by group computation based on the group elements. If the adversary algorithm is given group elements $X_1, X_2, \ldots, X_N \in G_1$, then each adversary algorithm outputs group elements:

$$\begin{aligned} &Z \in G_1, Z = \prod_{i=1}^{N} X_i^{Z_i}, \\ &Z_1, \ldots, Z_N \in \mathbb{Z}_p. \end{aligned} \tag{6}$$

Security assumption: Let G_1, G_2 be cyclic additive groups and G_T be cyclic multiplicative groups, both of order prime q. G_1, G_2, G_T is based on the hyperelliptic curve public key cryptosystem and satisfies the nondegenerate bilinear pairing:

$$e: G_1 \times G_2 \longrightarrow G_T. \tag{7}$$

$g_1, g_2, g_T := e(g_1, g_2)$ then are G_1, G_2, G_T generating elements, respectively. It is difficult to solve the l-wBDHE (weak bilinear Diffie–Hellman exponent problem) in the group of bilinear pairings; i.e., the probability expressed by the following equation can be neglected.

$$\begin{aligned} &\Pr\left[\left(\begin{matrix} \forall \alpha \leftarrow \mathbb{Z}_p \\ g_1^{\alpha^1}, g_1^{\alpha^2}, \ldots, g_1^{\alpha^N}, g_1^{\alpha^{N+2}}, \ldots, g_1^{\alpha^{3N}}, g_2^{\alpha^1}, g_2^{\alpha^2}, \ldots, g_2^{\alpha^N} \end{matrix}\right) : g_1^{\alpha^{N+1}}\right] \\ &= \text{negl}(\lambda), \end{aligned} \tag{8}$$

where $\alpha \leftarrow \mathbb{Z}_p$ is the secret value, no one knows after the initial generation of public parameters, the public parameters are taken from the group G_1 with $2N - 1$ values except $g_1^{\alpha(N+1)}$, and N values are taken in G_2 by calculating the values in G_T:

$$\begin{aligned} g_T^{\alpha^{(N+1)}} &= e\left(g_1^{\alpha^1}, g_2^{\alpha^1}\right) \\ &= e(g_1, g_2)^{\alpha^{(N+1)}}. \end{aligned} \tag{9}$$

Stateless verification: Establish the commitment, vector $\overrightarrow{\text{ID}} = (\text{ID}_1, \text{ID}_2, \ldots, \text{ID}_N) \in \mathbb{Z}_p^N$, and compute the commitment:

$$C_{\text{ID}} = g_1^{\sum_{i=1}^{N} ID_i \alpha^i}. \tag{10}$$

Input: Identity vector commitment, C_{ID}, related UAV ID, aggregation flag.
Output: Aggregation of the uncontacted UAVs' proof.

```
# assign committee members, monitoring all UAVs' fly status.
W^revoke = 0; Monitor_period = 5 s;
#counter: detect if UAV is online.
timeout_count = 0;
TimeoutList = 0;
# mission executing phase, crs are hardcode;
thread_monitor_leaving_Event( ) #monitoring start.
while 1 do
    #activating leaving UAV request
    Receive(ActiveleavingMsg)
    #calculating uncontacted times
    ModifyTimeoutlist( )
    if Aggregation Flag then
        W_S^Revoke ⟵ Aggregate(C, ID[S], W_i), i ∈ S
    else
        W_{S,S'}^Revoke ⟵ Disaggregate(W_123, ID[S'], W_j), j ∈ S'
    end if
end while
while aggregation flag is true do
    iftimeout_court++ > Monitor_periodthen
        blockchain.Broadcast_Send(online_hello)
        timeout_court = 0;
    end if
end while
#current turn expired,
In the header of committee:
blockchain.create(newblock)
blockchain.append(newblock)
blockchain.broadcast(newblock)
In UAV nodes:
for uav_i in length of ID⃗ do
    #when receiving new block from authority committee
    if new_block is constructed correctly then
        block_chain.append(newblock)
    else
        abort new block
    end if
end for
```

Algorithm 2: Second subvector commitment build/update.

Generate witness and member ID_i existence evidence establishment:

$$W_i = g_1^{\sum_{j\neq i} ID_j \alpha^{N+1-i+j}} = \left(\frac{C_{\mathrm{ID}}}{g_1^{\mathrm{ID}_i \alpha^i}}\right)^{\alpha^{N+1-i}}. \tag{11}$$

Member verification, based on commitment C and witness W_i verification, is

$$e\left(C_{\mathrm{ID}}, g_2^{\alpha^{N+1-i}}\right) = e\left(W_i, g_2\right) \cdot g_T^{\mathrm{ID}_i \alpha^{N+1}}. \tag{12}$$

5.2. Security Analysis. The timeliness of mission-oriented UAV networks is the biggest feature that distinguishes them from other self-organized networks. The security configuration of network nodes, such as public and private keys, and identity IDs, is generated by the mission and expires with the completion of the mission. Therefore, physical attacks such as capture and cloning are not considered, but they must have the ability to resist unauthorized access, eavesdropping, impersonation, replay, and man-in-the-middle attacks. Since the registration server that keeps the system master key does not participate in the task execution, there is no possibility of generating legitimate malicious nodes due to the master key leakage during the mission, the generation of vector commitment and witness are also completed in the task preparation stage, and the vector commitment cryptographic accumulator has conflict-free and strong unidirectionality, so the success probability of active attackers forging witnesses by constructing false member sets is negligible.

Resistance to eavesdropping attacks: Communication between UAVs in a UAV network begins with two-way authentication, and after authentication is passed, a session key is negotiated to encrypt the information for

Input: Identities VC, C_{ID}, related uav ID.
Output: Aggregation of the uncontacted UAVs' proof.
In UAV node:
$W^{Blacklist} = 0$;
watchCycle = 10 s, ObserveCounter = 0;
#watchdog in UAV observes neighbors' behaviors,
#uavs locally analysis
#send the misbehavior to the current committee.
while 1 **do**
    AnalysisObserveData ( );
    ifObserveCounter + + > watchCycle**then**
        #create untrust transaction
        SendMisBehavor (ID, behaviorType);
        ObserveCounter = 0;
    end if
end while
In Committee members:
#In current turn the committee receives the tip-offs
VoteforalluntrustedTransaction ( );
if the uav with its trust value less than 0 or current turn expired **then**
    blockchain.create (newblock)
    ckchain.append (newblock)
    ckchain.broadcast (newblock)
end if
In UAV nodes:
for uav_i in length of $\overrightarrow{ID}$. **do**
    if current_block is constructed correctly **then**
        block_chain.append (genesis_block)
    else
        abort Genesis block
    end if
end for

Algorithm 3: Third subvector commitment.

transmission. Eavesdropping attacks alone do not cause degradation of the performance of the UAV network in the mission.

Resisting man-in-the-middle attacks: Active tampering attacks that can be launched by the man-in-the-middle role through eavesdropping attacks are rejected outright because the identity and identity witness of the vector commitment cannot be forged and the identity of the man-in-the-middle node cannot be verified by the authentication smart contract because it is not registered in the stateless blockchain. Man-in-the-middle attacks do not pose a threat to the UAV network.

Resistant to replay attacks, for replay attacks after eavesdropping, the UAV network generates a large amount of invalid communication, which will seriously affect the performance of the network. There are three main methods to resist replay attacks, timestamp, execution sequence number, and random number to ensure the freshness of requests, but execution sequence number and random number methods need to save historical data and require consensus of all nodes, which is unaffordable for lightweight drones, so this paper recommends the stateless lightweight blockchain authentication method, which uses a timestamp plus a random number side for two-way authentication to identify replay attacks, reject malicious forwarding, and avoid unnecessary communication interference.

5.3. Efficacy Analysis. In this paper, we recommend a lightweight authentication scheme based on the hyperelliptic curve cryptosystem, which has a shorter key length compared to RSA and elliptic curve cryptosystem at the same security level, and its dot product operation is faster than the bilinear pair operation. It is concluded from the [29] that the relative computational cost of the bilinear [30] pair operation is about several twenty times that of the elliptic curve dot product operation; therefore, the elliptic curve dot product algorithm is more efficient and more suitable for UAV networks with limited arithmetic power. Transferring, drones run the stateless blockchain system as full nodes, and the dynamic trust authorization proof consensus mechanism ensures the security and trustworthiness of the UAV network in each round of generating new blocks. Each authentication process record is not used as a blockchain transaction to mark whether the nodes within the drone network are valid and trustworthy in the current round by recording the dynamically aggregated identity witness subvector change values into new blocks. This not only

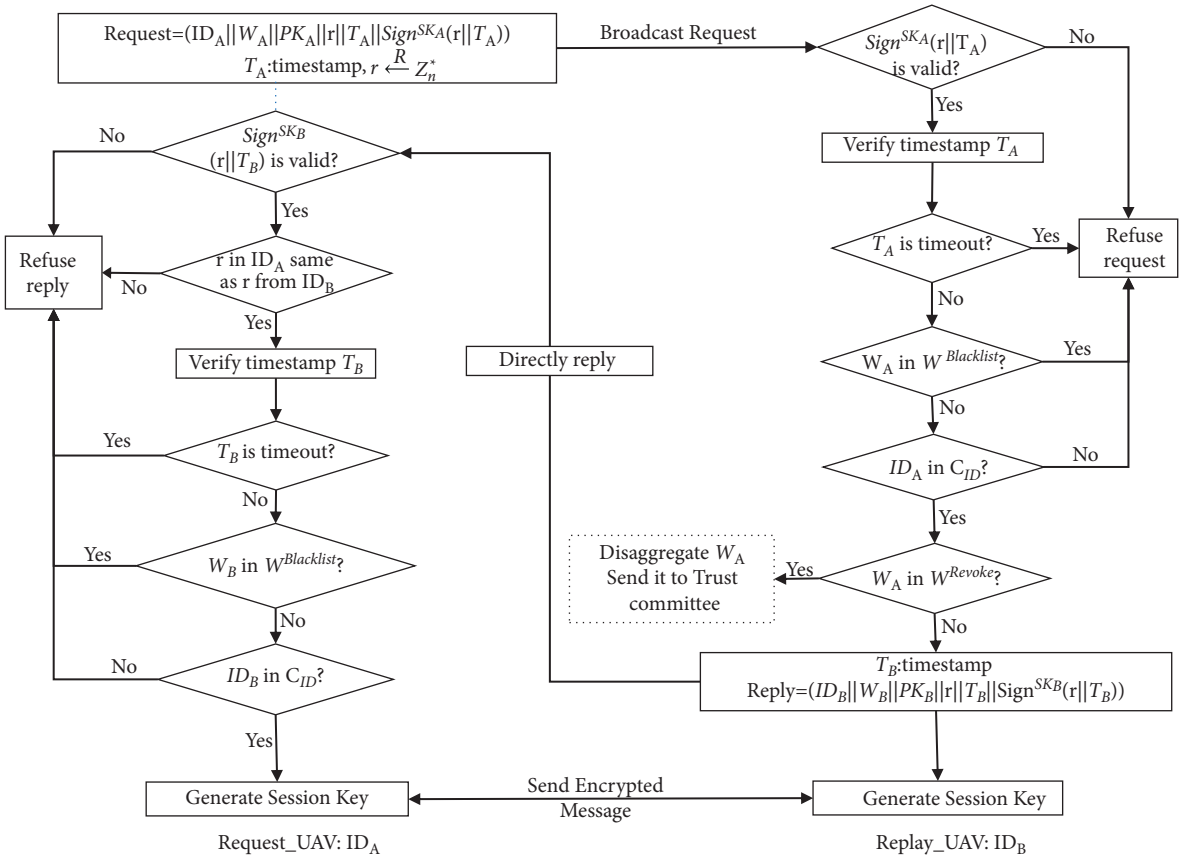

Figure 7: Communication process of the mutual authentication.

eliminates the "storage bloat" problem, but also reduces the single-step authentication time complexity from $O(n)$ to $O(\log n)$ and space complexity from $O(n)$ to $O(1)$ compared to stateful blockchain (historical state shared ledger), where no traversal of state records is required to query for authentication, but instead local authentication is performed in a proof manner. In the next section, experimental simulations and results analysis are presented in detail to effectively reduce the speed of UAV network energy consumption.

6. Experimental Simulation and Result Analysis

6.1. QualNet Network Simulation. The QualNet Simulator, developed by Scalable Networks Technologies (SNT), is software to help with network design, operation, and management. The QualNet Simulator simulates the network behavior and performance of thousands of nodes and is a comprehensive suite of tools for simulating large wireless or wired networks. The simulation experiment scenario for the proposed solution is described in Table 3. The scenario was developed by comparing the single-step authentication latency of the UAV nodes at different network sizes, the energy consumption rate of the UAV network for a fixed period of time at a specified size, the computational effort of the UAV network in the presence of different numbers of malicious nodes at a specified time (200 s), and the fixed size of the UAV network with different malicious nodes to measure the performance superiority of the stateless block authentication scheme with triple vector commitment recommended in this paper relative to the following schemes.

Scheme I [4]: relies on remote direct anonymous authentication over mobile communication link connections such as 4G: remote DAA.

Scheme II [5]: Threshold key sharing scheme.

Scheme III [18]: BlockchainPKI, a public blockchain authentication scheme for certificate tokens.

Scheme IV [25]: The stateless BlockchainVC with cryptographic accumulator.

6.2. Analysis of Experimental Results of UAV Network Simulation. Single-step authentication latency: The authentication latency is tested at the node movement speed of 10 m/s and different scales. The time required for the UAV to initiate an authentication request and obtain access or start communication after verification is passed as shown in Figure 8. In Scheme I, the UAV connects to a trusted third entity through a remote network for direct anonymous authentication, and the latency continues to increase as the number of nodes increases because all nodes share the mobile communication connection center. Scheme II increases with the size of the network and the time to collect the key share to recover the master key to ensure the security threshold value increases. In Scheme III, with blockchain certificate token authentication, the query time and

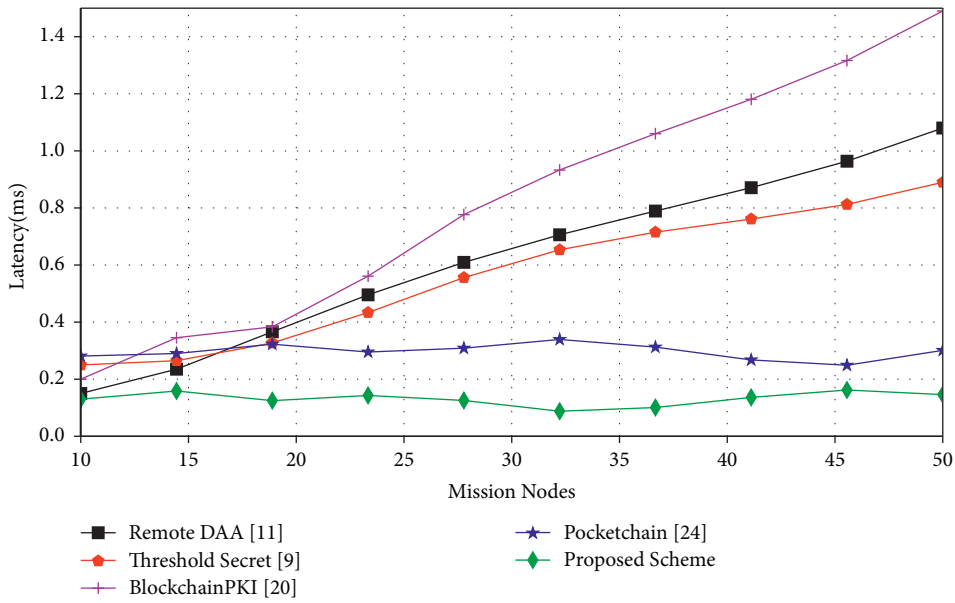

Figure 8: Single authentication latency of UAV networks at different sizes.

Table 3: Parameters related to the UAV network simulation scenario.

UAV network topology	Planar structure
Simulation area size	1000 m × 1000 m × 100 m
UAV flight speed	0, 5, 10, 15, 20, 25
Number of multicenter authorized nodes	5, 10, 15, 20
UAV node dwell time	2 s
Simulation time	800 s
Total number of UAV nodes	50
Number of lost UAV sorties triggering new blocks	2, 5, 8
Number of malicious UAV nodes	0, 5, 10, 20
New block round time (s)	10, 20

consensus time grow rapidly with the number of outgoing blockchain certificates and the increase in the size of participating network nodes. Constructing a stateless blockchain with the cryptographic accumulator approach in Scheme IV, the time for authentication is theoretically constant in magnitude, but fluctuates in time due to recalculation of accumulation values and network member witnesses caused by UAVs entering and leaving the network. The recommended method does not update computation by triple vector commitment and only changes some of the member witness aggregation to other subvectors into a promise, and the authentication delay fluctuation is small.

The rate of energy consumption of the UAV network: The consumption of the mission UAV network energy is directly related to the UAV range, and reducing the consumption rate of energy usage is the key to mission completion. Figure 9 shows the simulation test of five scenarios; in the time of 800 s, 50 UAV network, the presence of 20 malicious nodes, and the implementation of replay attack case, observe the rate of energy decline; in Scheme III due to the consensus algorithm of proof of workload, energy consumption is the fastest, about 400 s of time simulation energy is consumed; Scheme I requires remote communication, shared channel resource competition, and the interference from replay attacks; the energy consumption also decreases quickly and eventually ends around 500 s; and because the UAV moves in a random wandering manner, resulting in frequent access to the network by the UAV, leading to an increase in the computation of the update of Scheme IV, the energy decreases significantly at a later stage. Recommended scheme. The recommended scheme because they are all local authentication, no consensus, and better resistance to replay attacks, knowledge in maintaining the network trustworthy is the DPOTA consensus protocol cycle, processing can be aggregated subvector commitment operations, energy consumption is small, energy consumption is also the slowest, increasing the overall working time of the UAV network.

Computational cost under different numbers of malicious nodes: The test conditions are set up with a drone network size of 50 drones, running for 100 seconds, with different numbers of malicious nodes in the network, initiating the same communication task, and comparing the computational cost required for the five authentication schemes. As shown in Figure 10, Scheme III has insignificant changes because the computational overhead is mainly

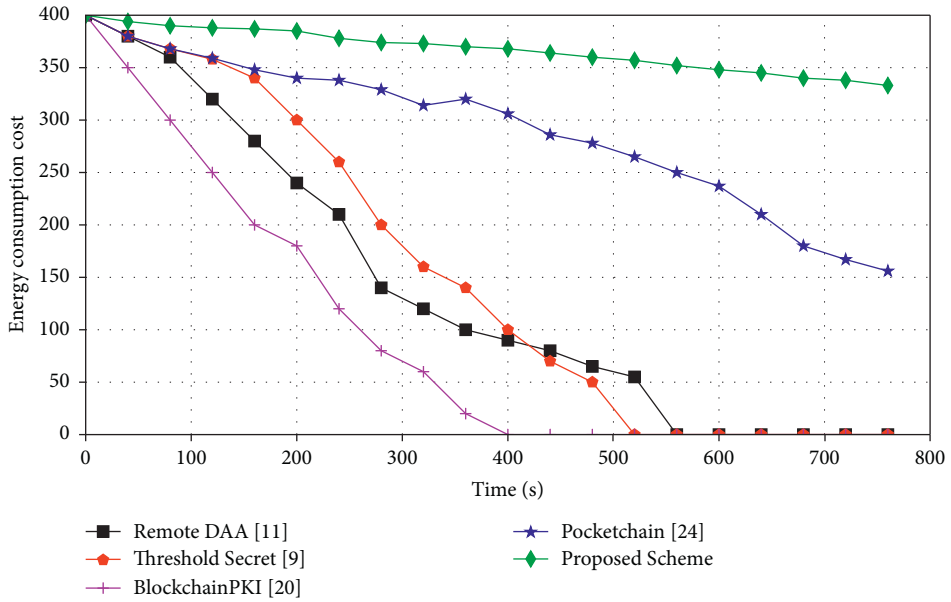

Figure 9: UAV network energy consumption rate.

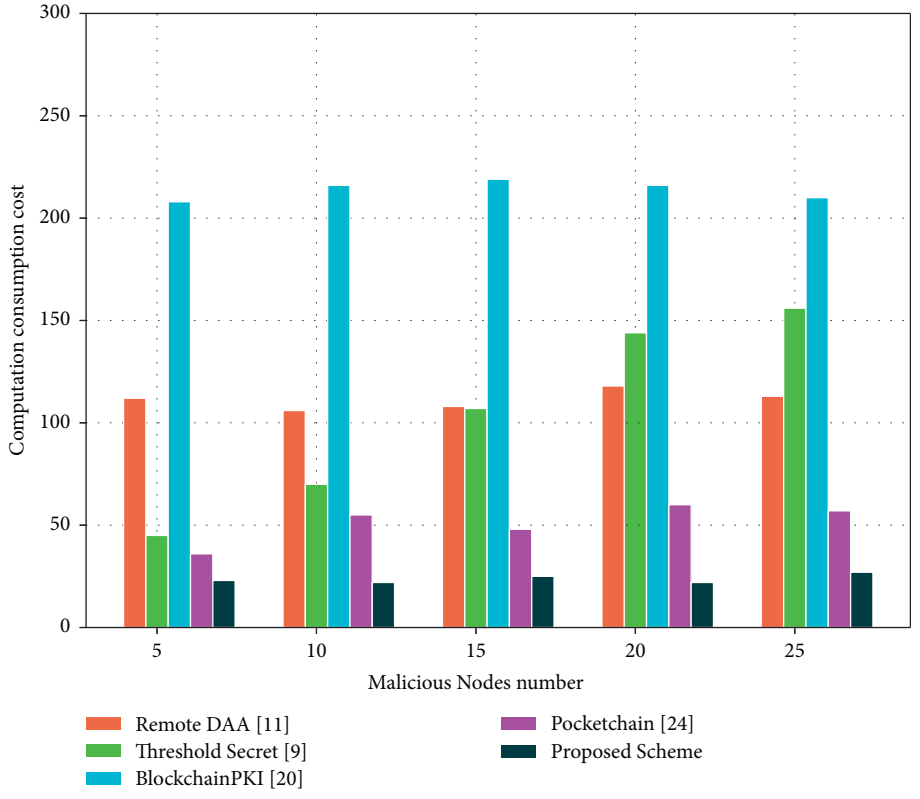

Figure 10: Computational cost with the different malicious nodes.

derived from the consensus overhead caused by the scale of the nodes due to the qualities of the traditional blockchain itself to prevent double-splash attacks; Scheme I, which relies on a remote third-party trusted entity to provide authentication, can resist replay attacks, and the computational overhead is basically unchanged; Scheme II has a rapid increase in computational overhead when the number of malicious nodes increases, as there is no effective defense given by the certificate center or blockchain platform. The computational overhead of Scheme IV also increases gradually because of the increase in malicious nodes, which increases the frequency of recalculating the cumulative value and updating the identity witness of its system.

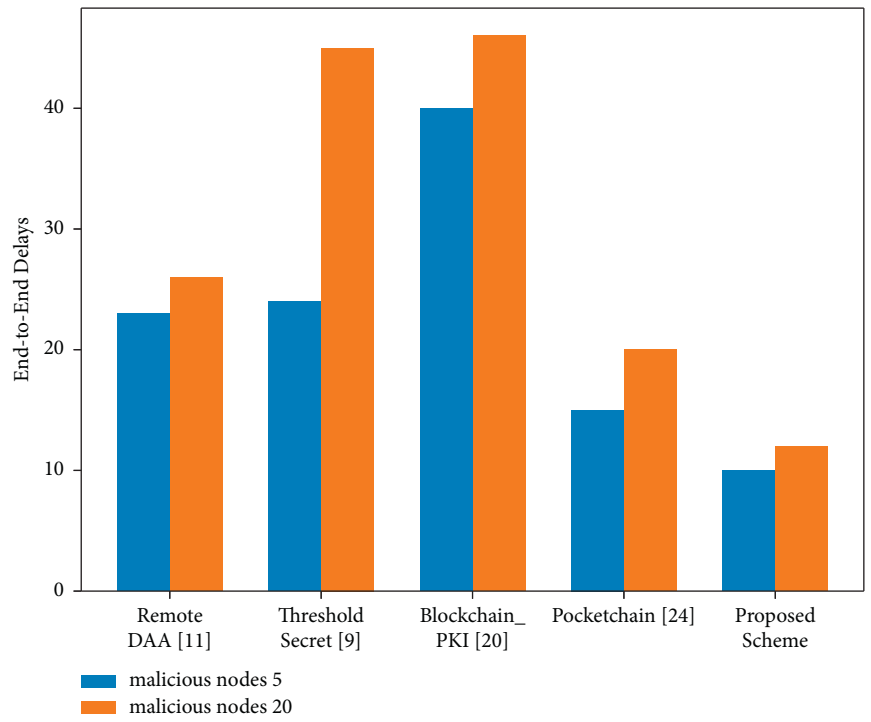

Figure 11: End-to-end transmission delay in the presence of malicious nodes.

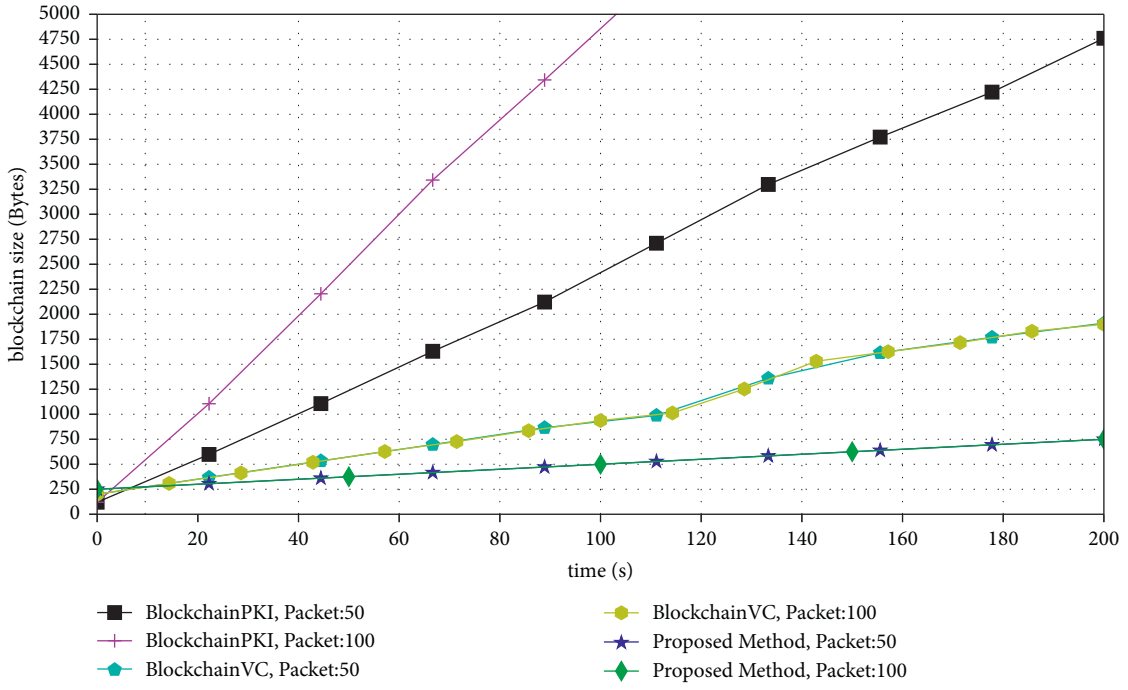

Figure 12: Comparison of storage growth of different blockchains in UAV networks.

End-to-end transmission latency under different numbers of malicious nodes: The test conditions are set with a drone network size of 50 drones and the presence of 5 malicious nodes and 20 malicious nodes in the network. The end-to-end communication latency of the five authentication schemes is compared, as shown in Figure 11. Scheme III, the interference of replay attacks by malicious nodes on end-to-end transmission, is negligible due to the traditional blockchain with the feature of preventing replay attacks, and the inefficient consensus leads to its high time consumption. Scheme I, which relies on remote third-party trusted entities to provide authentication, can resist replay attacks, and end-to-end latency makes no difference in these two cases. In Scheme II, when the number of malicious nodes increases, its end-to-end

transmission latency is severely affected due to the absence of effective defense given by certificate centers or blockchain platforms; Scheme IV, because the increase of malicious nodes leads to the change of effective nodes in the network, which increases the computation of commitment and witness updates, thus affecting the end-to-end transmission latency; Recommended scenario, due to local two-way authentication and effective defense against malicious nodes, the end-to-end changes in transmission latency are minimal.

Consensus and storage: Blockchains are shared databases that keep growing along with consensus. Experiments are conducted to compare the storage requirements of drone networks under different blockchains. To satisfy comparability, the following experimental scenario is set up, where malicious nodes are not considered, the UAV network is well connected, the network size is 100 nodes, the running time is 200 seconds, the routing protocol is DSR, all nodes send data randomly every 5 seconds, and the size of data packets is fixed.

(1) Traditional blockchain based on a distributed PKI with a delegated proof of stake consensus algorithm (DPOS). Each time a packet is sent as a transaction, consensus is accomplished by a fixed number of 21 delegated nodes, with a provision to initiate consensus every 20 seconds.

(2) Stateless blockchain based on accumulator: same as above.

(3) Stateless authentication chain recommended in this paper: set the consensus cycle to 20 s, and the local trustworthiness assessment generated by monitoring the forwarding behavior of neighboring nodes on routing information and data packets as a data consensus transaction, again reaching consensus among the 21 authorized nodes selected dynamically in the cycle and completing consensus on the decision.

The experimental results are shown in Figure 12.

As with traditional blockchains, each of transaction data needs to be on the chain, and the new block after consensus is reached contains the transaction data within 20 s. As new blocks are created, the size of the blockchain keeps increasing, and the larger the transaction data package, the faster the blockchain grows.

Stateless blockchain based on cryptographic accumulator or vector commitment is to create new blocks with authentication results as transactions, and the new blocks reach consensus at delegated authorized nodes to finally confirm the authentication success. Its transactions are smaller than the authenticated data, but still have transaction blocks.

The recommended stateless authentication chain is with triple identity vector commitment, its consensus process contains data consensus and decision consensus, the local trust assessment of all nodes to their neighboring nodes in each cycle is the object of its number consensus, its ultimate purpose is to obtain decision results through statistical analysis of the results of data consensus, its decision results in fixed size, including updated triple vector commitment and new authorized node group, the size is not more than 50 bytes. The historical state data used for data consensus do not need to be saved.

At the same time, it is clear that the first two types of authentication are confirmed after the block consensus, then the blockchain is updated, and their authentication efficiency is equivalent to the consensus efficiency. The recommended solution, on the other hand, whose consensus aims to maintain the trustworthiness of the drone network, is authenticated locally by the nodes on that blockchain's trusted platform, which is fast and not limited by the size of the network.

7. Conclusions

In this paper, a scheme for lightweight mutual authentication of UAV network nodes is proposed. The recommended scheme is based on vector commitment to establish a stateless blockchain with a consensus mechanism of dynamic multicentric trust authorization proof to maintain the trustworthiness and effectiveness of participating nodes in the UAV network during mission execution in the scenario of dynamic changes in the size and agency of the mission network due to environmental factors and cyber attacks. According to the timeliness requirements of the mission network, a triple aggregatable subvector commitment mutual authentication protocol is designed to effectively resist counterfeit attacks, man-in-the-middle attacks, and replay attacks. Simulation experiments demonstrate that this scheme has better performance in terms of energy consumption, computational cost, single authentication latency, and end-to-end delay compared to current authentication methods that can run in mission-based UAV networks.

Data Availability

Due to the privacy of the data and sensitive information, it is not convenient to provide.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Key Research and Development Program of China (2019YFB2102002), in part by the National Natural Science Foundation of China (62176122 and 62001217), and in part by A3 Foresight Program of NSFC (62061146002).

References

[1] İ. Bekmezci, OK Sahingoz, and S Temel, "Flying ad-hoc networks (fanets): Flying Ad-Hoc Networks (FANETs): A survey survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, 2013.

[2] V. A. K. Singh K, *Threat Modeling for Multi-Uavs Adhoc Networks*, Tencon, Japan, 2017.

[3] K. Kurosawa, S. Obana, and W. Ogata, "Threshold secret sharing schemes," in *Proceedings of the Advances in Cryptology - CRYPTO '95, 15th Annual International Cryptology Conference*, vol. 963, pp. 410–423, Springer, Santa Barbara, CA, USA, 1995.

[4] L. Chen, S. Qian, M. Lim, and S. Wang, "An enhanced direct anonymous attestation scheme with mutual authentication for network-connected uav communication systems," *China Communications*, vol. 15, no. 5, pp. 61–76, 2018.

[5] A. Alomari, "Fully distributed certificate authority based on polynomial over elliptic curve for MANET," *International Journal of Networked and Distributed Computing*, vol. 2, no. 2, pp. 70–77, 2014.

[6] Y Seung and K Robin, "MOCA: mobile certificate authority for wireless Ad Hoc networks," 2004.

[7] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," in *Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT 2003)*, pp. 342–346, IEEE Computer Society, Orlando, FL, USA, January 2003.

[8] H. Deng, A. Mukherjee, and D. P. Agrawal, "Threshold and identity-based key management and authentication for wireless ad hoc networks," in *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)*, vol. 1, pp. 107–111, IEEE Computer Society, Las Vegas, NV, USA, April 2004.

[9] J. Chen, J. Ling, J. Ning, and J. Ding, "Identity-based signature schemes for multivariate public key cryptosystems," *The Computer Journal*, vol. 62, no. 8, pp. 1132–1147, 2019.

[10] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proceedings of the Advances in Cryptology - ASIACRYPT 2003, 9th International Conference on the Theory and Application of Cryptology and Information Security*, vol. 2894, pp. 452–473, Springer, Taipei, Taiwan, December 2003.

[11] J. Zheng, S. Xu, F. Zhao, D. Wang, and Y. Li, "A novel detective and self-organized certificateless key management scheme in mobile ad hoc networks," in *Proceedings of the IEEE International Conference on Granular Computing, GrC 2013*, pp. 443–448, IEEE Computer Society, Beijing, China, December 2013.

[12] Y. Zhao, Y. Hou, Y. Chen, S. Kumar, and F. Deng, "An efficient certificateless public key encryption with equality test toward internet of vehicles," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 5, 2022.

[13] E. Frimpong, R. Rabbaninejad, and A. Michalas, "Arrows in a quiver: a secure certificateless group key distribution protocol for drones," *IACR Cryptol. ePrint Arch.*, Virtual Event, November 2021.

[14] D. Mishra and S. Mukhopadhyay, "A certificateless authenticated key agreement protocol for digital rights management system," in *Proceedings of the Quality, Reliability, Security and Robustness in Heterogeneous Networks - 9th International Conference*, vol. 115, pp. 568–577, Springer, Greader Noida India, January 2013.

[15] Y. Tan, J. Liu, and N. Kato, "Blockchain-based key management for heterogeneous flying ad hoc network," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7629–7638, 2021.

[16] M. Toorani and C. Gehrmann, "A decentralized dynamic PKI based on blockchain," 2020, https://arxiv.org/abs/2012.15351.

[17] M. Y. Kubilay, M. S. Kiraz, and H. A. Mantar, "Certledger: a new PKI model with certificate transparency based on blockchain," *Computers & Security*, vol. 85, p. 1071, 2018.

[18] Q. T. Thai, J. Yim, and S. Kim, "A scalable semi-permissionless blockchain framework," in *Proceedings of the 2019 International Conference on Information and Communication Technology Convergence*, pp. 990–995, IEEE, Jeju Island, Republic of Korea, October 2019.

[19] J. C. Benaloh and M. de Mare, "One-way accumulators: a decentralized alternative to digital sinatures (extended abstract)," in *Proceedings of the Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques*, vol. 765, pp. 274–285, Springer, Lofthus, Norway, May 1993.

[20] D. Boneh, B. Bünz, and B. Fisch, "Batching techniques for accumulators with applications to iops and stateless blockchains," in *Proceedings of the Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference*, vol. 11692, pp. 561–586, Springer, Santa Barbara, CA, USA, August 2019.

[21] F. Baldimtsi, R. Canetti, and S. Yakoubov, "Universally composable accumulators," in *Proceedings of the Topics in Cryptology - CT-RSA 2020 - The Cryptographers' Track at the RSA Conference 2020*, vol. 12006, pp. 638–666, Springer, San Francisco, CA, USA, February 2020.

[22] D. Catalano and D. Fiore, "Vector commitments and their applications," in *Proceedings of the Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography*, vol. 7778, pp. 55–72, Springer, Nara, Japan, February 2013.

[23] M. Campanelli, D. Fiore, N. Greco, D. Kolonelos, and L. Nizzardo, "Vector commitment techniques and applications to verifiable decentralized storage," 2020, https://eprint.iacr.org/2020/149.

[24] A. Tomescu, I. Abraham, V. Buterin, J. Drake, D. Feist, and D. Khovratovich, "Aggregatable subvector commitments for stateless cryptocurrencies," in *Proceedings of the Security and Cryptography for Networks - 12th International Conference, SCN 2020*, vol. 12238, pp. 45–64, Springer, Amalfi, Italy, September 2020.

[25] R. W. F. Lai and G. Malavolta, "Subvector commitments with application to succinct arguments," in *Proceedings of the Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference*, A. Boldyreva and D. Micciancio, Eds., vol. 11692, pp. 530–560, Springer, Santa Barbara, CA, USA, August 2019.

[26] V. Keerthika and R. Suganthe, "Watchdog: reduce time delay for spreading selfish information in manet," in *Proceedings of the 2013 International Conference on Information Communication and Embedded Systems*, pp. 1104–1107, Chennai, India, 2013.

[27] U. Ali, M. Y. I. B. Idris, M. N. B. Ayub et al., "Rfid authentication scheme based on hyperelliptic curve signcryption," *IEEE Access*, vol. 9, Article ID 49942, 2021.

[28] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K.-K. R. Choo, "Homechain: a blockchain-based secure mutual authentication system for smart homes," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 818–829, 2020.

[29] Y. Liao, Y. Liu, Y. Liang, Y. Wu, and X. Nie, "Revisit of certificateless signature scheme used to remote authentication schemes for wireless body area networks," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2160–2168, 2020.

[30] F. Guo, Y. Mu, W. Susilo, H. Hsing, D. S. Wong, and V. Varadharajan, "Optimized identity-based encryption from bilinear pairing for lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 2, pp. 211–220, 2017.