Hindawi
Security and Communication Networks
Volume 2021, Article ID 9463606, 10 pages
https://doi.org/10.1155/2021/9463606

Research Article

A Certificateless Pairing-Free Authentication Scheme for Unmanned Aerial Vehicle Networks

Jingyi Li,[1] Yujue Wang,[2] Yong Ding,[1,3] Wanqing Wu,[4] Chunhai Li,[5] and Huiyong Wang[6]

[1]*Guangxi Key Laboratory of Cryptography and Information Security, School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, China*
[2]*Hangzhou Innovation Institute, Beihang University, Hangzhou, China*
[3]*Cyberspace Security Research Center, Pengcheng Laboratory, Shenzhen, China*
[4]*School of Cyber Security and Computer, Hebei University, Baoding, China*
[5]*School of Information and Communication, Guilin University of Electronic Technology, Guilin, China*
[6]*School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin, China*

Correspondence should be addressed to Yong Ding; stone_dingy@126.com

Received 11 June 2021; Revised 4 August 2021; Accepted 14 August 2021; Published 11 September 2021

Academic Editor: Anjia Yang

Copyright © 2021 Jingyi Li et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In unmanned aerial vehicle networks (UAVNs), unmanned aerial vehicles with restricted computing and communication capabilities can perform tasks in collaborative manner. However, communications in UAVN confront many security issues, for example, malicious entities may launch impersonate attacks. In UAVN, the command center (CMC) needs to perform mutual authentication with unmanned aerial vehicles in clusters. The aggregator (AGT) can verify the authenticity of authentication request from CMC; then, the attested authentication request is broadcasted to the reconnaissance unmanned aerial vehicle (UAV) in the same cluster. The authentication responses from UAVs can be verified and aggregated by AGT before being sent to CMC for validation. Also, existing solutions cannot resist malicious key generation center (KGC). To address these issues, this paper proposes a pairing-free authentication scheme (CLAS) for UAVNs based on the certificateless signature technology, which supports batch verification at both AGT and CMC sides so that the verification efficiency can be improved greatly. Security analysis shows that our CLAS scheme can guarantee the unforgeability for (attested) authentication request and (aggregate) responses in all phases. Performance analysis indicates that our CLAS scheme enjoys practical efficiency.

1. Introduction

Unmanned aerial vehicles in UAVN have been widely used in many civilian and military fields, for example, data collection, communication relay, and military electronic reconnaissance [1]. Unmanned aerial vehicles can be classified into three categories according to the working mode, namely, unmanned aerial vehicles under the control of a remote operator, under the supervision of a remote supervisor, and without an operator and supervisor. UAVNs can be deployed in mesh topology or multistar topology [2]. With the mesh topology, all unmanned aerial vehicles are connected to CMC directly, where all communication between unmanned aerial vehicles and CMC may cause network congestion. Although with the mesh topology, each unmanned aerial vehicle can communicate with each other, it is hard to be expanded and controlled [3]. With the multistar topology, each unmanned aerial vehicle is connected to CMC; thus, any illegal requests or responses in UAVNs can be easily detected.

However, when deployed in an open communication environment, the UAVN system confronts many security issues [4, 5]. Due to multiple connections among unmanned aerial vehicles, a malicious entity may control some unmanned aerial vehicle or launch impersonate attacks. Thus, it is important to enforce a secure and efficient authentication mechanism in UAVNs [6, 7]. Recently, Wang et al. [8] proposed an identity-based authentication scheme, which

did not consider the verification mechanisms at the AGT side for validating the real sources of the authentication request from CMC and responses from UAVs. Li et al. [9] designed an identity-based aggregate authentication framework in bilinear groups, where the private keys of UAVs are generated by KGC. Thus, malicious KGC may launch attacks by sending illegal authentication request to AGTs and UAVs.

1.1. Our Contributions. To address the abovementioned issues, this paper proposes a certificateless pairing-free aggregate authentication scheme (CLAS) for UAVNs. In CLAS, KGC is responsible for generating partial private keys for all entities including CMC, AGTs, and UAVs. Each AGT acts as the cluster head of some cluster and plays the role of an intermediate between CMC and UAVs in the respective cluster. Each authentication request from CMC can be validated by AGT, which is then attested and broadcasted to UAVs in its administrative domain. A verification process can be run by each UAV so that the true source of the (forwarded) authentication request can be validated. AGT can aggregate all responses of UAVs in its administrative cluster before performing verification procedure in batch. Then, the response of AGT is further combined with the aggregated responses of UAVs, which can be validated by CMC in batch to complete the authentication process.

This paper describes a concrete CLAS construction based on the certificateless signature technology. Security analysis shows that our CLAS construction can protect malicious entity from forging the authentication request and responses of others and can resist against the malicious KGC. Performance comparison shows that our CLAS construction enjoys better computational efficiency compared with Wang et al.'s scheme [8] and Li et al.'s scheme [9].

1.2. Related Works. Taking advantages of recent advancement and development in information and communication technology, unmanned aerial vehicles have been employed to perform some special tasks in real-world applications [10]. In [11], Islam and Shin proposed a blockchain-based solution for safe healthcare, which uses the unmanned aerial vehicle (UAV) to collect health data (HD) from users. Liu et al. [1] presented a detailed survey on the opportunities and challenges of IoE supported by unmanned aerial vehicles. Jiang et al. [12] proposed a trust-based energy efficient data collection with the unmanned aerial vehicle (TEEDC-UAV) scheme, which can prolong lifetime in a trusted way. In the TEEDC-UAV scheme, an ant colony-based unmanned aerial vehicle (UAV) trajectory optimization algorithm was proposed, which constituted the most data anchor points in the working field with the shortest trajectory possible. In view of the untrusted broadcast features and wireless transmission of UAV networks, a novel privacy-preserving secure spectrum trading and sharing scheme based on blockchain technology is proposed in [13].

For the Internet of Drones (IoD) infrastructure, Cho et al. [14] proposed a framework called SENTINEL (Secure and Efficient autheNTIcation for uNmanned aErial vehicLes). Khanh et al. [15] presented a safe and effective authentication mechanism suitable for the dynamic environment of the unmanned aerial vehicle. In order to solve the information security problem of unmanned aerial vehicle ad-hoc network communication, Sun et al. [2] introduced an efficient and energy-saving distributed network architecture based on clustering stratification. Owing to the unreliable wireless channel and high-dynamic topology of Unmanned Aerial Vehicles Ad-Hoc Network (UAANET), the loss of some certain group key broadcast messages by nodes occurs frequently. Therefore, Li et al. [16] proposed a mutual-healing group key distribution scheme based on the blockchain. Yang et al. [17] investigated degradation-of-QoS attacks in vehicular ad hoc networks, where the attacker is able to relay the authentication exchanges but cannot relay the service afterwards. In [18], Gope et al. proposed a novel anonymous authentication scheme for RFID-enabled UAV applications using Physically Unclonable Functions (PUF).

Al-Riyami et al. [19] first introduced and made concrete the concept of certificateless public key cryptography (CL-PKC), a model for the use of public key cryptography which avoids the inherent escrow of identity-based cryptography. Baek et al. [20] considered a relaxation of the original model of CLPKE and proposed a new CLPKE scheme that does not depend on the bilinear pairings. In order to ensure security for interactions between these smart things, Yeh et al. [21] presented a certificateless signature scheme for smart objects in IoT-based pervasive computing environments. Jia et al. [22] made an improvement on the scheme of Yeh et al.'s certificateless signature scheme; they presented an improved scheme and demonstrated its unforgeability against super-adversaries in the random oracle model. Zhao et al. [23] presented an advanced efficient CLAS scheme with elliptic curve cryptography for the IoV environment. Furthermore, their scheme used pseudonyms in communications to prevent vehicles from revealing their identity. Shu et al. [24] presented a certificateless aggregate signature scheme for blockchain-based MCPS, which can realize the authentication of related medical staffs, medical equipment, and medical apps, ensure the integrity of medical records, and support the secure storage and sharing of medical information.

1.3. Paper Organization. The structure of this paper is organized as follows. In Section 2, we introduce the system architecture and system requirements for CLAS. A concrete CLAS construction is presented in Section 3, followed by its security and efficiency analysis in Section 4. Finally, Section 5 concludes the paper.

2. System Architecture and Requirements

This section formalizes the architecture of CLAS and summarizes its system requirements.

2.1. System Architecture. As shown in Figure 1, there are four types of entities in a CLAS system, namely, key generation center (KGC), command center (CMC), reconnaissance

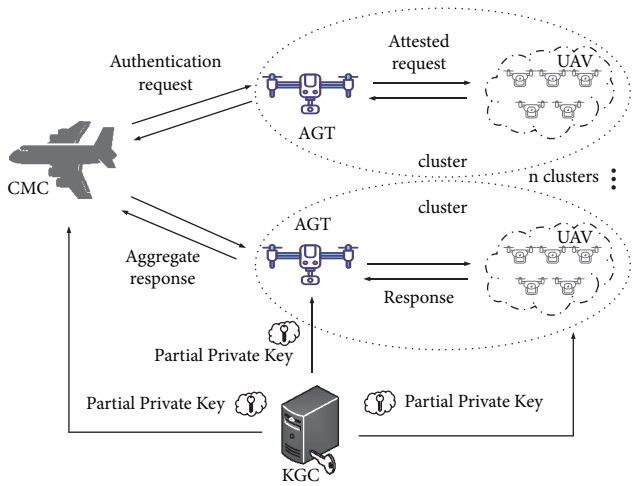

Figure 1: CLAS model for UAVNs.

unmanned aerial vehicles (UAVs), and aggregators (AGTs). KGC is assumed to be fully trusted by all the entities, which is responsible for initializing the CLAS system by generating system public parameters and producing partial private keys for all entities in UAVNs. After system initialization, CMC performs the mutual authentication process with unmanned aerial vehicles before assigning tasks. CMC initializes the authentication process so that AGT can validate, attest, and broadcast authentication request to its administrated UAVs.

As the intermediary between CMC and UAV, AGT has the computing and communication capabilities to manage its UAV cluster. UAV only has limited short-distance communication capability; thus, its communication with CMC is performed via the AGT in the cluster. Before responding to the authentication request of CMC, each UAV can verify its true source and the attested request. The responses of UAVs in the same cluster can be validated by AGT in batch. Then, the response of AGT can be further combined with that of UAVs so that the aggregated response is sent to CMC for validation.

2.2. System Requirements. Similar to [25], we define two types of adversaries for the CLAS system, namely, Type-I adversary and Type-II adversary. A Type-I adversary acts as an outsider who can replace the public keys of CMC, AGT, and UAV but cannot access the master secret key, whereas a Type-II adversary acts as the KGC that can access the master secret key but cannot replace the public keys of CMC, AGT, and UAV. A CLAS system must satisfy the following system requirements.

Unforgeability of authentication request: in the authentication process, for the authentication request generated by CMC, it should be guaranteed that it is existentially unforgeable against Type-I adversary. That is, any entity cannot launch attacks by impersonating CMC to forge an authentication request.

Unforgeability of attested request: for the attested authentication request of AGT, it should be guaranteed that it is existentially unforgeable against Type-I adversary. That is, any entity cannot launch attacks by impersonating AGT to forge an attested authentication request.

Unforgeability of response: for the responses from UAVs in its administrative cluster of AGT, it should be guaranteed that it is existentially unforgeable against Type-I adversary. That is, any entity cannot launch attacks by impersonating some UAV to forge a response.

Unforgeability of aggregate response: for the attested authentication request of some AGT, it should be guaranteed that it is existentially unforgeable against Type-I adversary. That is, any entity cannot launch attacks by impersonating AGT to forge an aggregate response.

Resistance against malicious KGC: for the whole authentication procedure, it should be guaranteed that it is existentially unforgeable against Type-II adversary. That is, malicious KGC cannot forge a valid signature of CMC, AGT, or UAV.

A *correct* CLAS construction should satisfy the following conditions:

(1) For the partial private key sent by KGC, it can be successfully verified by respective entity including CMC, AGTs, and UAVs

(2) For the authentication request generated by CMC, it can be successfully validated by AGTs

(3) For the attested authentication request forwarded by AGT, it can be successfully validated by UAVs in the same cluster

(4) For the responses of UAVs, they can be validated by AGT in the same cluster

(5) For the aggregate response from AGT, it can be successfully validated by CMC

3. CLAS Construction

This section describes our concrete CLAS construction. The authentication process in UAVNs is shown in Figure 2.

The Discrete Logarithm Assumption in Elliptic Curve (ECDLP): let G be an elliptic curve group with prime order q. Given P and $Q \in G$, any probabilistic polynomial time algorithm ξ would have negligible probability in computing $x \in Z_q^*$ such that $Q = xP$.

3.1. System Setup. On inputting a security parameter $l \in Z^+$, KGC chooses an additive group G with prime order q on some elliptic curve, where P is a generator of G. Then, KGC chooses $b \in Z_q^*$ randomly and computes

$$B = bP. \tag{1}$$

KGC continues to choose four collision-resistant hash functions $H_i: \{0,1\}^* \longrightarrow Z_q^*$ for $i = 1, 2, 3,$ and 4. Finally, KGC publishes the system parameters

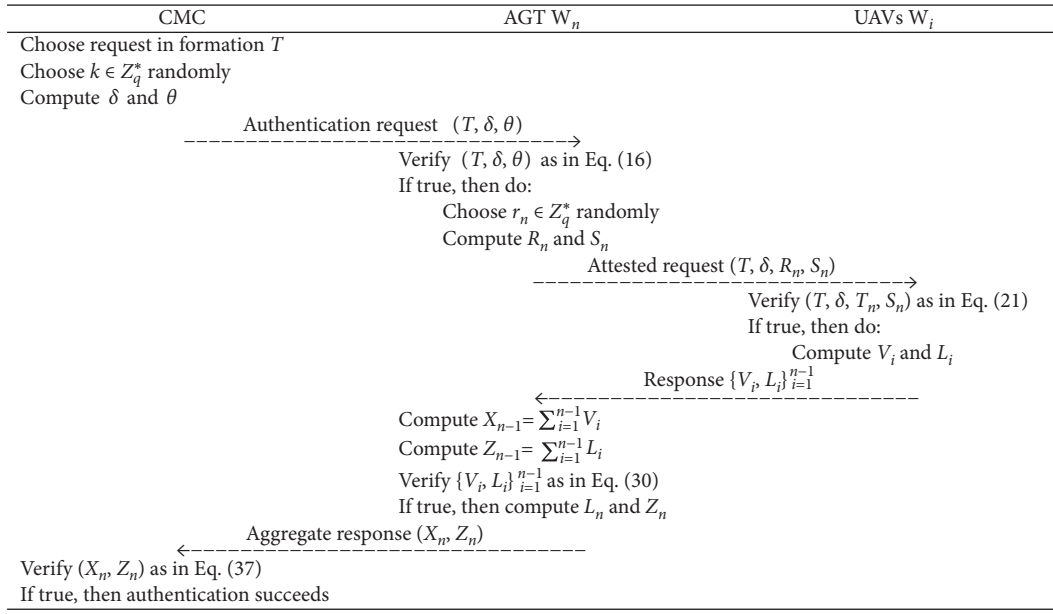

Figure 2: A procedure of authentication in our CLAS construction.

params = $(q, G, P, H_1, H_2, H_3, H_4, B)$ and keeps the master secret key msk = b secret.

3.2. Key Generation for CMC. KGC sets the partial private key for the control center as follows. KGC chooses a random number $e \in Z_q^*$ and computes

$$A = eP, \tag{2}$$

$$a = e + bH_1(\mathrm{CMC} \| A \| B) \mathrm{mod} q. \tag{3}$$

Then, KGC sends the partial private key (a, A) to CMC through a secure channel. CMC can validate the partial private key as follows:

$$aP \stackrel{?}{=} A + H_1(\mathrm{CMC} \| A \| B)B. \tag{4}$$

CMC sets a secret value and generates its public key PK_c and private key SK_c as follows. CMC chooses a random number $s \in Z_q^*$ and computes

$$F = sP, \tag{5}$$

$$M = A + H_2(CMC \| F)F. \tag{6}$$

Then, CMC sets $PK_c = (A, M)$ and $SK_c = (a, s)$.

3.3. Key Generation for Unmanned Aerial Vehicles. Let W_i be an unmanned aerial vehicle. For the ease of representation, let W_n be an AGT and $W_1, \ldots, W_{n-1}$ be UAVs in the administration domain of W_n. KGC sets a partial private key for unmanned aerial vehicles as follows.

KGC chooses a random number $d_i \in Z_q^*$ and computes

$$Y_i = d_i P, \tag{7}$$

$$y_i = d_i + bh_{1,i} \mathrm{mod} q, \tag{8}$$

where

$$h_{1,i} = H_1\left(W_i \| Y_i \| B\right). \tag{9}$$

Then, KGC sends the partial private key (y_i, Y_i) to W_i through a secure channel. The unmanned aerial vehicle W_i can validate the partial private key as follows:

$$y_i P \stackrel{?}{=} Y_i + h_{1,i}B. \tag{10}$$

The unmanned aerial vehicle W_i sets a secret value and generates its public key PK_i and private key SK_i as follows. W_i chooses a random number $c_i \in Z_q^*$ and computes

$$C_i = c_i P, \tag{11}$$

$$Q_i = Y_i + h_{2,i}C_i, \tag{12}$$

where

$$h_{2,i} = H_2\left(W_i \| C_i\right). \tag{13}$$

Then, the unmanned aerial vehicle W_i sets $PK_i = (Y_i, Q_i)$ and $SK_i = (y_i, c_i)$.

3.4. Authentication Request. Let $T \in \{0,1\}^*$ denote the request information chosen by CMC, which contains the timestamp. CMC randomly picks $k \in Z_q^*$ and computes

$$\delta = kP, \tag{14}$$

$$\theta = k + H_3\left(T \| \delta \| \mathrm{CMC} \| PK_c\right)\left(a + H_2(\mathrm{CMC} \| F)s\right) \mathrm{mod}\, q. \tag{15}$$

Then, CMC sends the authentication request (T, δ, θ) to AGTs.

3.5. Request Forwarding. After receiving the request (T, δ, θ) from CMC, each AGT W_n validates its authenticity by checking the following equality:

$$\theta P \stackrel{?}{=} \delta + H_3(T\|\delta\|\mathrm{CMC}\|PK_c)(M + H_1(\mathrm{CMC}\|A\|B)B). \tag{16}$$

If it holds, then AGT W_n accepts the authentication request from CMC, otherwise terminates. AGT W_n randomly chooses $r_n \in Z_q^*$ and computes

$$R_n = r_n P, \tag{17}$$

$$S_n = \theta + r_n + h_{4,n}(y_n + h_{2,n}c_n) \bmod q, \tag{18}$$

where

$$h_{4,n} = H_4(T\|\delta\|W_n\|PK_n\|R_n), \tag{19}$$

$$h_{2,n} = H_2(W_n\|C_n). \tag{20}$$

At last, AGT W_n broadcasts the tuple of attested authentication request (T, δ, R_n, S_n) to all UAVs $W_i\,(i = 1, 2, \ldots, n-1)$ in its administrative domain.

3.6. UAV Response. Once received (T, δ, R_n, S_n) from AGT W_n, each UAV $W_i\,(i = 1, 2, \ldots, n-1)$ verifies its authenticity by checking the following equality:

$$S_n P \stackrel{?}{=} \delta + R_n + h_{4,n}(Q_n + h_{1,n}B) + H_3(T\|\delta\|\mathrm{CMC}\|PK_c) \cdot (M + H_1(\mathrm{CMC}\|A\|)B), \tag{21}$$

where

$$h_{1,n} = H_1(W_n\|Y_n\|B), \tag{22}$$

$$h_{4,n} = H_4(T\|\delta\|W_n\|PK_n\|R_n). \tag{23}$$

If it holds, then UAV W_i accepts the authentication request from CMC, otherwise terminates. W_i randomly picks $f_i \in Z_q^*$ and computes

$$V_i = f_i P, \tag{24}$$

$$L_i = f_i + \widehat{h}_{4,i}(y_i + h_{2,i}c_i) \bmod q, \tag{25}$$

where

$$\widehat{h}_{4,i} = H_4(T\|\delta\|W_i\|PK_i\|V_i), \tag{26}$$

$$h_{2,i} = H_2(W_i\|C_i). \tag{27}$$

Then, UAV W_i sends the response tuple $\sigma_i = (V_i, L_i)$ to AGT W_n.

3.7. AGT Aggregation. Upon receiving the response tuples $\{V_i, L_i\}_{i=1}^{n-1}$ from the controlled UAVs $W_i\,(i = 1, 2, \ldots, n-1)$, AGT W_n computes

$$X_{n-1} = \sum_{i=1}^{n-1} V_i, \tag{28}$$

$$Z_{n-1} = \sum_{i=1}^{n-1} L_i \bmod q. \tag{29}$$

Then, AGT W_n verifies the authenticity of the received response tuples in a batch as follows:

$$Z_{n-1}P \stackrel{?}{=} X_{n-1} + \left(\sum_{i=1}^{n-1} \widehat{h}_{4,i}h_{1,i}\right)B + \sum_{i=1}^{n-1} \widehat{h}_{4,i}Q_i, \tag{30}$$

where

$$\widehat{h}_{4,i} = H_4(T\|\delta\|W_i\|PK_i\|V_i), \tag{31}$$

$$h_{1,i} = H_1(W_i\|Y_i\|B). \tag{32}$$

If it holds, then all response tuples of $W_i\,(i = 1, 2, \ldots, n-1)$ are valid; otherwise, W_n validates each response tuple in individual to find the invalid one. AGT W_n continues to pick a random element $f_n \in Z_q^*$ and compute

$$X_n = X_{n-1} + f_n P, \tag{33}$$

$$Z_n = Z_{n-1} + L_n \bmod q, \tag{34}$$

where

$$\begin{aligned} L_n &= f_n + \widehat{h}_{4,n}(y_n + h_{2,n}c_n) \bmod q, \\ \widehat{h}_{4,n} &= H_4(T\|\delta\|W_n\|PK_n\|f_n P), \end{aligned} \tag{35}$$

$$h_{2,n} = H_2(W_n\|C_n). \tag{36}$$

Then, AGT W_n sends the aggregate response (X_n, Z_n) to CMC.

3.8. CMC Verification. Once received the aggregate response (X_n, Z_n) from AGT W_n, CMC validates its authenticity by checking the following equality:

$$Z_n P \stackrel{?}{=} X_n + \left(\sum_{i=1}^{n} \widehat{h}_{4,i}h_{1,i}\right)B + \sum_{i=1}^{n} \widehat{h}_{4,i}Q_i, \tag{37}$$

where

$$\widehat{h}_{4,i} = H_4(T\|\delta\|W_i\|PK_i\|V_i), \tag{38}$$

$$h_{1,i} = H_1(W_i\|Y_i\|B). \tag{39}$$

If it holds, then AGT W_n and UAVs $W_i\,(i = 1, 2, \ldots, n-1)$ are all accepted as legitimate.

Theorem 1. *The proposed CLAS construction is correct.*

Proof 1. To prove the correctness of the proposed CLAS construction, it only needs to show that equalities (16), (21), (30), and (37) are satisfied.

(1) For the authentication request (T, δ, θ) generated by CMC, equality (16) satisfies as follows:

$$\begin{aligned}\theta P &= kP + H_3(T\|\delta\|\mathrm{CMC}\|K_c)(a + H_2(\mathrm{CMC}\|F)s)P \\ &= \delta + H_3(T\|\delta\|\mathrm{CMC}\|PK_c)(A + H_2(\mathrm{CMC}\|F)F \\ &\quad + H_1(\mathrm{CMC}\|A\|B)B) \\ &= \delta + H_3(T\|\delta\|\mathrm{CMC}\|PK_c)(M + H_1(\mathrm{CMC}\|A\|B)B).\end{aligned} \tag{40}$$

(2) For the attested authentication request (T, δ, R_n, S_n) from AGT W_n, equality (21) satisfies as follows:

$$\begin{aligned}S_nP &= \theta P + r_nP + h_{4,n}(y_i + h_{2,n}c_n)P \\ &= \delta + R_n + h_{4,n}(Q_n + h_{1,n}B) + H_3(T\|\delta\|\mathrm{CMC}\|PK_c)(M + H_1(\mathrm{CMC}\|A\|B)B).\end{aligned} \tag{41}$$

(3) For the response tuples $\{V_i, L_i\}_{i=1}^{n-1}$ from the controlled UAVs $W_i\,(i = 1, 2, \ldots, n-1)$, equality (30) holds as follows:

$$\begin{aligned}Z_{n-1}P &= \sum_{i=1}^{n-1} L_iP \\ &= \sum_{i=1}^{n-1}\left(f_iP + \widehat{h}_{4,i}(y_i + h_{2,i}c_i)P\right) \\ &= X_{n-1} + \sum_{i=1}^{n-1}\left(\widehat{h}_{4,i}(Y_i + h_{1,i}B + h_{2,i}C_i)\right) \\ &= X_{n-1} + \left(\sum_{i=1}^{n-1}\widehat{h}_{4,i}h_{1,i}\right)B + \sum_{i=1}^{n-1}\widehat{h}_{4,i}Q_i.\end{aligned} \tag{42}$$

(4) For the aggregate response tuple (V_n, L_n) from AGT W_n, equality (37) holds as follows:

$$\begin{aligned}Z_nP &= \sum_{i=1}^{n} L_iP \\ &= \sum_{i=1}^{n}\left(f_iP + \widehat{h}_{4,i}(y_i + h_{2,i}c_i)P\right) \\ &= X_n + \sum_{i=1}^{n}\left(\widehat{h}_{4,i}(Y_i + h_{1,i}B + h_{2,i}C_i)\right) \\ &= X_n + \left(\sum_{i=1}^{n}\widehat{h}_{4,i}h_{1,i}\right)B + \sum_{i=1}^{n}\widehat{h}_{4,i}Q_i.\end{aligned} \tag{43}$$

Thus, the proposed CLAS construction is correct.

4. System Analysis

This section analyzes the security and performance of the proposed CLAS construction.

4.1. Security Analysis

Theorem 2. *Assume that the ECDLP assumption holds in cyclic group G. The proposed CLAS construction can guarantee the unforgeability of the authentication request from CMC.*

Proof 2. In the authentication request (T, δ, θ) generated by CMC, the element θ is considered to be a certificateless signature of $T\|\delta\|\mathrm{CMC}\|PK_c$. It can be seen that θ can serve as the common signature v_i in Thumbur et al.'s scheme [26]. As proved in Theorem 1 in [26], their scheme is existentially unforgeable against Type-I adversary, which assumes that the ECDLP assumption holds in additive group G of elliptic curve points. Therefore, any attacker cannot forge a valid authentication request of CMC without knowing public key PK_c, which implies the unforgeability of the authentication request from CMC can be guaranteed.

Theorem 3. *Assume that the ECDLP assumption holds in cyclic group G. The proposed CLAS construction can guarantee the unforgeability of the attested authentication request from AGT.*

Proof 3. In the attested request (T, δ, R_n, S_n) generated by AGT, the element S_n is considered to be a certificateless signature on θ. It can be seen that S_n can serve as the common signature v_i in Thumbur et al.'s scheme [26]. As proved in Theorem 1 in [26], their scheme is existentially

unforgeable against Type-I adversary, which assumes that the ECDLP assumption holds in additive group G of elliptic curve points. Therefore, any attacker cannot forge a valid attested request or response of AGT without knowing public key PK_n, which implies the unforgeability of the attested authentication request from AGT can be guaranteed.

Theorem 4. *Assume that the ECDLP assumption holds in cyclic group G. The proposed CLAS construction can guarantee the unforgeability of the responses from UAVs.*

Proof 4. For the response tuple (V_i, L_i) generated by UAV W_i, it is considered to be a certificateless signature on $T\|\delta$. It can be seen that (V_i, L_i) can serve as the common signature v_i in Thumbur et al.'s scheme [26]. As proved in Theorem 1 in [26], their scheme is existentially unforgeable against Type-I adversary, which assumes that the ECDLP assumption holds in additive group G of elliptic curve points. Therefore, any attacker cannot forge a valid authentication response of UAV without knowing public key PK_i, which implies the unforgeability of the responses from UAVs can be guaranteed.

Theorem 5. *Assume that the ECDLP assumption holds in cyclic group G. The proposed CLAS construction can guarantee the unforgeability of the aggregate response from AGT.*

Proof 5. For the aggregate response tuple (X_n, Z_n) generated by CMC, it is considered as the aggregate signature on n individual responses. It can be seen that (X_n, Z_n) can serve as the common signature v_i in Thumbur et al.'s scheme [26]. As proved in Theorem 1 in [26], their scheme is existentially unforgeable against Type-I adversary, which assumes the ECDLP assumption holds in additive group G of elliptic curve points. Therefore, any attacker cannot forge a valid aggregate response of AGT without knowing public key PK_i, which implies the unforgeability of the aggregate response from AGT can be guaranteed.

Theorem 6. *Assume that the ECDLP assumption holds in cyclic group G. The proposed CLAS construction can be resistant to malicious KGC.*

Proof 6. For the partial private key (y_i, Y_i) generated by KGC, it is considered as a Schnorr signature [27] on W_i. It can be seen that (y_i, Y_i) can serve as the common signature D_i in [26]. As proved in Theorem 2 in [26], their scheme is existentially unforgeable against Type-II adversary, which assumes that the ECDLP assumption holds in additive group G of elliptic curve points. Therefore, any malicious KGC cannot forge valid partial private key of UAVs without knowing master secret key b; thus, the authenticity of KGC can be guaranteed in producing a partial private key.

4.2. Functional Comparison. Wang et al. [8] proposed an identity-based aggregate authentication scheme for UAVNs in bilinear groups. In [8], all UAVs are able to communicate with the CMC through their respective AGTs in the cluster, to perform valid authentication. There is no mechanism for AGT to validate the authenticity of CMC before forwarding authentication request to UAVs in its administrative domain. Furthermore, when individual responses are aggregated from UAVs in the respective cluster, the AGT does not verify the authenticity of those responses.

Li et al. [9] proposed an aggregate authentication scheme, where the above two mechanisms are introduced to enhance the security of authentication in UAVNs. Note that CMC may be malicious in generating keys for UAVs, which means their scheme cannot resistant against malicious KGC. While in our CLAS construction, the partial private key for UAVs are generated by KGC. The detailed comparison on the functionalities among Wang et al.'s proposal [8], Li et al.'s proposal [9], and our CLAS construction is summarized in Table 1.

4.3. Theoretical Comparison. Let T_{SM} be the time of one scalar point multiplication and T_{BP} be one bilinear pairing operation. For the key generation procedure, Wang et al.'s scheme [8] and Li et al.'s scheme [9] require n and $2n$ scalar point multiplications for n entities, respectively. In the request verification procedure, 2 bilinear pairing operations are both required in Wang et al.'s scheme [8] and Li et al.'s scheme [9]. For the aggregate verification by AGT procedure, Li et al.'s scheme [9] requires $(n-1)$ scalar point multiplications and 3 bilinear pairing operations. In the aggregate verification by CMC procedure, compared with Li et al.'s scheme [9], our scheme requires only $(n+2)$ scalar point multiplications. More details for comparsion on computation costs are summarized in Table 2.

4.4. Experimental Performance. To evaluate the computation cost of our CLAS construction, we conduct experiments using the Java Pairing-Based Cryptography Library (JPBC, http://gas.dia.unisa.it/projects/jpbc/), on a platform with Microsoft Windows 10 operating system, Intel(R) Core(TM) i5-6500 CPU @ 3.20 GHz, and 12 GB RAM. The elliptic curve is of Type A ($y^2 = x^3 + x$) such that q is a 160 bit prime, and the element size in group G is 512 bits.

The performance of the procedures of our CLAS construction is depicted in Figure 3, which are system setup (Setup), key generation (SUMkgen), authentication request generation (REQgen) and attestation (REQfwd), and RAV response (UAVresp). The SUMkgen stage consists of three algorithms, partial key generation for UAV (KGCkgen), key verification for UAV (UAVerify), and key generation for UAV (UAVkgen). The setup algorithm is used to initialize the CLAS system. We can see that the majority of the computation depends on B, which takes roughly 144 msec. The SUMkgen algorithm is used to generate public and private keys for UAVs, which efficiency depends on the UAVerify and the UAVkgen algorithms. Since the partial private key is generated by KGC, the time for UAVs to generate public and private keys is reduced, which is approximately 24 msec in experiments.

The REQgen algorithm can be run to generate authentication request. Its performance mainly depends on

Table 1: Functional comparison.

	Request verification	Request attestation	Aggregate verification		Resistant to malicious KGC
			By AGT	By CMC	
Our scheme	√	√	√	√	√
Li et al. [9]	√	√	√	√	×
Wang et al. [8]	√	×	×	√	×

Table 2: Theoretical comparison.

	Key generation	Request verification	Request attestation	Aggregate verification	
				By AGT	By CMC
Our scheme	$3nT_{SM}$	$3T_{SM}$	$1T_{SM}$	$(n+1)T_{SM}$	$(n+2)T_{SM}$
Li et al. [9]	$2nT_{SM}$	$2T_{BP}$	$2T_{SM}$	$(n-1)T_{SM} + 3T_{BP}$	$nT_{SM} + 3T_{BP}$
Wang et al. [8]	nT_{SM}	$2T_{BP}$	—	—	$nT_{SM} + 3T_{BP}$

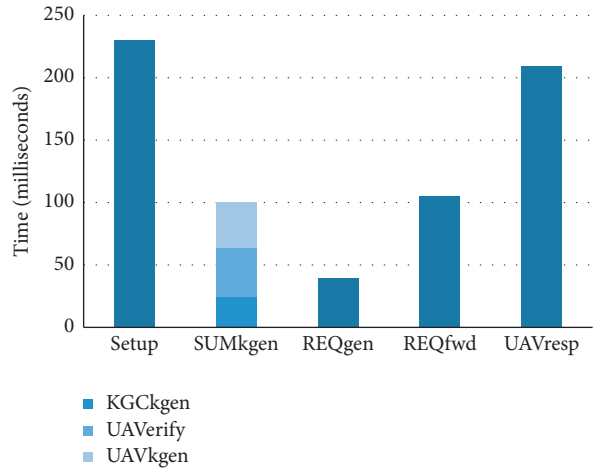

Figure 3: Performance evaluation of the setup, key generation, request generation, forwarding, and UAV response procedures.

the computation of δ, requiring one scalar point multiplication, whereas Wang et al.'s scheme [8] and Li et al.'s scheme [9] both cost two scalar point multiplications. As depicted in Figure 3, an authentication request is able to be transmitted in less than 24 msec. In the stage of REQfwd, before producing attested request, AGT verifies the authenticity of the authentication request from CMC by checking equality (16), which takes two scalar point multiplications. It requires AGT to forward the request in roughly 0.07 seconds. Before generating a response, each UAV validates the authenticity of the attested request received from its administrative AGT, requiring 5 scalar point multiplications. As a result, it takes about 0.15 seconds for each UAV to run the response procedure, while Li et al.'s scheme [9] requires more computational costs, i.e., 4 bilinear pairing operations.

In the response aggregation procedure, AGT needs to aggregate the elements $\{V_i, L_i\}$ in the received response tuples. It can be seen that prior to the batch verification of these responses, only $(n+1)$ scalar point multiplications are required in equality (30), as compared to Li et al.'scheme [9]. In the simulation, a variety of scenarios for the number of unmanned aerial vehicles are considered, that is, $n = 10, 20, \ldots, 100$, and the amount of UAVs consists of one AGT and $(n-1)$ UAVs. AGT aggregates and verifies $(n-1)$ response tuples of UAVs and further aggregates all the response tuples including its response. The experimental results are shown in Figure 4, which indicates a linear correlation between the computation time of this process and the number of unmanned aerial vehicles in a single cluster.

For the process of aggregating verification by CMC, Figure 5 shows the computation time that the CMC verifies the aggregate response from AGT for a single cluster. We also consider multiple cases where the number of unmanned aerial vehicles in a single cluster are $n = 10, 20, \ldots, 100$, respectively. As shown in equality (37), CMC is required to compute $(n+2)$ scalar point multiplications. It can be seen from Figure 5 that there is also a linear correlation between the computation time of this process and the number of unmanned aerial vehicles in a single cluster.

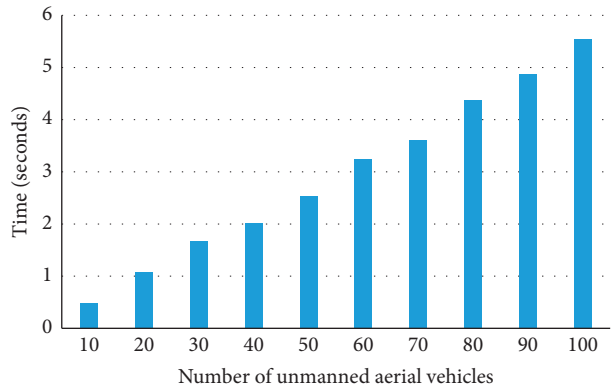

Figure 4: Performance evaluation of the AGT aggregation procedure.

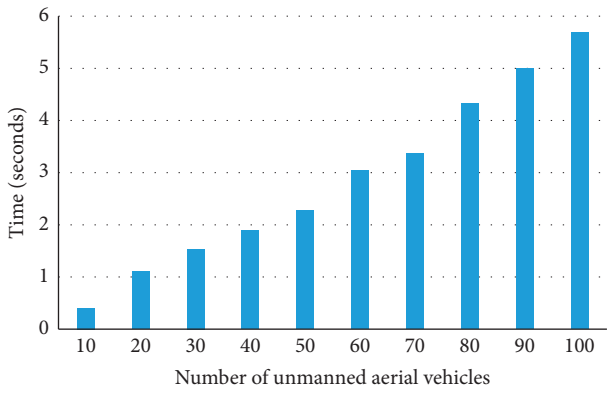

Figure 5: Performance evaluation of the CMC verification procedure.

5. Conclusion

To address the security problems in UAVNs, this paper proposed a CLAS construction without bilinear groups to realize efficient mutual authentication between control center and unmanned aerial vehicles. After the system is initialized, KGC produces the partial private key for each entity. CMC sends the authentication request to AGT; then, AGT forwards the attested request to UAVs in its administrative cluster. All response tuples of UAVs are validated by the cluster head AGT and then forwarded to CMC for further verificaton. Security analysis showed that our CLAS construction can not only provide unforgeability for (attested) authentication request and (aggregate) responses but also can resist malicious KGC. Experimental analysis demonstrated that the proposed CLAS construction enjoys practical performance.

Data Availability

No data were used to support the findings of this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This article was supported in part by the National Key R&D Program of China under project 2020YFB1006003, National Natural Science Foundation of China under projects 61772150, 61862012, and 61962012, Guangdong Key R&D Program under project 2020B0101090002, Guangxi Natural Science Foundation under grants 2018GXNSFDA281054, 2019GXNSFFA245015, and 2019GXNSFGA245004, Peng Cheng Laboratory Project of Guangdong Province under grant PCL2018KP004, and Innovation Project of Guangxi Graduate Education under grant YCSW2021176.

References

[1] Y. Liu, H.-N. Dai, Q. Wang, M. K. Shukla, and M. Imran, "Unmanned aerial vehicle for internet of everything: opportunities and challenges," *Computer Communications*, vol. 155, pp. 66–83, 2020.

[2] J. Sun, W. Wang, L. Kou et al., "A data authentication scheme for UAV ad hoc network communication," *The Journal of Supercomputing*, vol. 76, no. 6, pp. 4041–4056, 2020.

[3] M. Y. Arafat and S. Moh, "A survey on cluster-based routing protocols for unmanned aerial vehicle networks," *IEEE Access*, vol. 7, pp. 498–516, 2019.

[4] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: a survey," *Mobile Networks and Applications*, vol. 25, no. 1, pp. 95–101, 2020.

[5] R. Fotohi, E. Nazemi, and F. Shams Aliee, "An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks," *Vehicular Communications*, vol. 26, 2020 https://www.sciencedirect.com/science/article/pii/S2214209620300383, Article ID 100267.

[6] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: a survey," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, pp. 1–25, 2016.

[7] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the internet of drones: challenges and solutions," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 64–69, 2018.

[8] H. Wang, J. Li, C. Lai, and Z. Wang, "A provably secure aggregate authentication scheme for unmanned aerial vehicle cluster networks," *Peer-to-Peer Networking and Applications*, vol. 13, no. 1, pp. 53–63, 2020.

[9] J. Li, M. Zhao, Y. Ding, D. Y. W. Liu, Y. Wang, and H. Liang, "An aggregate authentication framework for unmanned aerial vehicle cluster network," in *Proceedings of the 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, pp. 1249–1256, Xiamen, China, December 2020.

[10] N. Mohamed, J. Al-Jaroodi, I. Jawhar, I. Ahmed, and F. Mohammed, "Unmanned aerial vehicles applications in future smart cities," *Technological Forecasting and Social Change*, vol. 153, 2020 https://www.sciencedirect.com/science/article/pii/S0040162517314968, Article ID 119293.

[11] A. Islam and S. Y. Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in internet of things," *Computers & Electrical Engineering*, vol. 84, 2020 https://www.sciencedirect.com/science/article/pii/S0045790620304821, Article ID 106627.

[12] B. Jiang, G. Huang, T. Wang, J. Gui, and X. Zhu, "Trust based energy efficient data collection with unmanned aerial vehicle in edge network," *Transactions on Emerging Telecommunications Technologies*, 2020, https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3942, Article ID e3942.

[13] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: an operator's perspective," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 451–466, 2020.

[14] G. Cho, J. Cho, S. Hyun, and H. Kim, "Sentinel: a secure and efficient authentication framework for unmanned aerial vehicles," *Applied Sciences*, vol. 10, no. 9, p. 3149, 2020.

[15] T. Duy Khanh, I. Komarov, Le Duy Don, R. Iureva, and S. Chuprov, "Tra: effective authentication mechanism for swarms of unmanned aerial vehicles," in *Proceedings of the 2020 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 1852–1858, Canberra, ACT, Australia, December 2020.

[16] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, and J. Ma, "Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11309–11322, 2019.

[17] A. Yang, J. Weng, N. Cheng, J. Ni, X. Lin, and X. Shen, "Deqos attack: degrading quality of service in vanets and its mitigation," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4834–4845, 2019.

[18] P. Gope, O. Millwood, and N. Saxena, "A provably secure authentication scheme for rfid-enabled UAV applications," *Computer Communications*, vol. 166, pp. 19–25, 2021.

[19] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proceedings of the International Cnference on the Theory and Application of Cryptology and Information Security*, pp. 452–473, Springer, Taipei, Taiwan, December 2003.

[20] J. Baek, R. Safavi-Naini, and W. Susilo, "Certificateless public key encryption without pairing," in *Proceedings of the International Conference on Information Security*, pp. 134–148, Springer, Singapore, Asia, September 2005.

[21] K.-H. Yeh, C. Su, K.-K. Raymond Choo, and W. Chiu, "A novel certificateless signature scheme for smart objects in the internet-of-things," *Sensors*, vol. 17, no. 5, https://www.mdpi.com/1424-8220/17/5/1001, 2017.

[22] X. Jia, D. He, Q. Liu, and K.-K. R. Choo, "An efficient provably-secure certificateless signature scheme for internet-of-things deployment," *Ad Hoc Networks*, vol. 71, pp. 78–87, 2018, https://www.sciencedirect.com/science/article/pii/S1570870518300015.

[23] Y. Zhao, Y. Hou, L. Wang, S. Kumari, M. Khurram Khan, and Hu Xiong, "An efficient certificateless aggregate signature scheme for the internet of vehicles," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 5, Article ID e3708, 2020.

[24] H. Shu, P. Qi, Y. Huang, F. Chen, D. Xie, and L. Sun, "An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems," *Sensors*, vol. 20, no. 5, p. 1521, 2020.

[25] Y.-C. Chen and R. Tso, "A survey on security of certificateless signature schemes," *IETE Technical Review*, vol. 33, no. 2, pp. 115–121, 2016.

[26] G. Thumbur, G. S. Rao, P. V. Reddy, N. B. Gayathri, and D. V. R. K. Reddy, "Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices," *IEEE Communications Letters*, vol. 24, no. 8, pp. 1641–1645, 2020.

[27] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.