An Aggregate Authentication Framework for Unmanned Aerial Vehicle Cluster Network

Jingyi Li[1], Meng Zhao[1], Yong Ding[1,2,*], Dennis Y. W. Liu[3], Yujue Wang[1], Hai Liang[1]
1. Guangxi Key Laboratory of Cryptography and Information Security, School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, China
2. Cyberspace Security Research Center, Pengcheng Laboratory, Shenzhen, China
3. Department of Computing, The Hong Kong Polytechnic University, Hong Kong, China
E-mail: stone_dingy@126.com

***Abstract*—The unmanned aerial vehicle technology has achieved rapid development in recent years. In order to ensure the authenticity and reliability of information transmission in unmanned aerial vehicle cluster network (UAVCN), it is necessary to require unmanned aerial vehicles and control center (COC) to perform mutual authentication process. The authentication request issued by COC should be attested and forwarded by aggregators (AGE) to reconnaissance unmanned aerial vehicles (RAV) in respective cluster, due to the short-distance communication capabilities of RAVs. Moreover, the responses from RAVs are also aggregated and forwarded by their respective administrative AGE to COC. To address the security issues in such authentication scenario, this paper proposes an authentication framework for UAVCN based on the identity-based aggregate signature technology. Security analysis shows that our method offers unforgeability for (attested) authentication request and (aggregate) responses, and performance analysis demonstrates the practicality of our construction.**

***Index Terms*—Unmanned aerial vehicle, cluster network, authentication, aggregate signature, batch verification**

I. Introduction

With the rapid development of communication technology, the unmanned aerial vehicle technology has been widely used in military electronic reconnaissance, rescue and other civilian fields [1]. Although the unmanned aerial vehicle technology has advantages of low costs and strong ability to cope with complex environments, single unmanned aerial vehicle only has limited capabilities of computation and communication and can only perform restrict tasks in real world applications, for example, working within short-distance communication range. Since UAVCN allows multiple unmanned aerial vehicles to collaboratively perform complex tasks remotely, it can greatly extends the capability of a single unmanned aerial vehicle [2]. Therefore, UAVCN is a promising direction for the development of unmanned aerial vehicle technology.

The participants in UAVCN can work in a combination manner of centralized and distributed control, with real-time and frequent information exchange. With the centralized control method, the information transmission and interaction among all RAVs are realized through a unique COC. Whereas with the distributed control method, all RAVs are not only allowed to communicate with the COC, but also allowed to achieve mutual communication without the help from COC. To carry out a task, COC is able to send out a request, so that RAVs can respond accordingly by returning the collected data and their own status information for COC to make further classification and analysis.

However, UAVCN confronts some security issues in the open communication environment [3]. External entity may impersonate COC to send out control instructions to RAVs [4], for example, to terminate or interfere with the current task. Similarly, the response of RAV may also be forged to provide wrong or disturbing information to COC. Thus, it is necessary for the entities in UAVCN to implement effective authentication mechanism to realize secure communication. Recently, Wang et al. [5] proposed an identity-based authentication method, which allows COC to aggregate authenticate the real identity of RAVs. Note that their proposal [5] did not consider the security issues in forwarding authentication request and response by AGE, that is, RAVs cannot verify whether the authentication request is forwarded by their legitimate administrative AGE in the cluster, and there lacks a mechanism for AGE to validate the real source of responses from RAVs.

A. Our contributions

To address the above mentioned issues, this paper proposes an aggregate authentication system (AAS) for UAVCN. In AAS, each AGE serves as the cluster head and intermediator between COC and RAVs in respective cluster. Each AGE is able to validate the authentication request from COC, and forward the attested request to the administrated RAVs. Each RAV can run the verification procedure to confirm the real source and forwarding source of the authentication request. All responses of RAVs can be aggregated and verified by their administrative AGE in the cluster, which are further combined with the response of AGE and provided to COC for completing authentication.

This paper presents a concrete AAS construction in bilinear groups based on the identity-based aggregate signature. Security analysis shows that our construction can prevent malicious entities from forging the authentication request and responses, that is, the (attested) authentication request by COC/AGE and (aggregate) responses by RAVs/AGE are unforgeable by

other entities. The experiments are conducted on our AAS construction, which show that each procedure enjoys high performance, especially in generating authentication request and response, while the performance of response aggregation depends on the number of RAVs in the cluster.

B. Related works

With the advantages of rapid and easy deployment, unmanned aerial vehicles have been adopted in various real world applications [6]. In [7], Turgut and Gursoy studied the signal-to-interference-plus-noise ratio for the cellular networks constructed from unmanned aerial vehicles. In [8], unmanned aerial vehicles are employed to construct a wireless sensor network for detecting the locations of endangered species in wild areas. Jiang et al. [9] presented a trustworthy and energy efficient scheme for large-scale sensing data collection with unmanned aerial vehicles. The similar autonomous data collection problem in wireless sensor networks is also investigated in [10]. Li, Li and Chen [11] designed a flying Ad-Hoc network based on unmanned aerial vehicles, and proposed a framework with the focus on the effective mission planning and network connectivity for these vehicles.

Hooper et al. [12] identified the zero-day vulnerabilities of commercial WiFi-based Parrot Bebop unmanned aerial vehicles under the denial of service and buffer-overflow attacks, and proposed a security framework to mitigate these security risks. Podhradsky, Coopmans and Hoffer [13] addressed the communications security for open-source unmanned aerial vehicles by implementing an encrypted Radio Control link, to prevent them from disturbing operation or control by malicious users. To protect the security and privacy of user's sensitive information carried by commercial unmanned aerial vehicles, Yoon et al. [14] designed an encrypted communication channel supporting source authentication. He, Chan and Guizani [15] showed some low-cost implementations of GPS spoofing attacks and WiFi attacks against unmanned aerial vehicles, and suggested some security countermeasures.

Liu, Qian and Hu [16] designed an authentication mechanism for the large-scale swarm system constructed from unmanned aerial vehicles, ground stations and relay stations, which allows the swarm to generate random labels to resist infiltrating attacks. Fu et al. [17] investigated the robustness and accuracy issues in collaborative task allocation for multiple unmanned aerial vehicles, where the intrusion detection technology was employed to resist the potential network attacks. Mao, Hu and Qi [18] noticed that existing key management protocols are not efficient and scalable in supporting unmanned aerial vehicle applications, and proposed a group key management protocol based on a secret sharing scheme from the Chinese Remainder theorem.

Boneh et al. [19] proposed an aggregate signature scheme in bilinear groups, where many signatures for different messages from different users can be aggregated into a single signature. It is especially useful in reducing the information size when realizing secure communication. Gentry and Ramzan [20] presented identity-based aggregate signature schemes, which do not require the verifier to maintain the public keys of signers. Lu and Wang [21] proposed an identity-based aggregate signature scheme under the discrete logarithm assumption, which is employed to aggregate the signatures of multiple sensor nodes before being sent to the base station for verifying their authenticity. Zhang et al. [22] developed a distributed aggregate authentication protocol based on the multiple trusted authority one-time identity-based aggregate signature for vehicular ad hoc networks, which allows a vehicle to batch verify the received multiple messages and their signatures.

C. Paper organization

The remainder of this paper is organized as follows. Section II describes the system architecture, security requirements, and the procedures in AAS. Section III covers the preliminaries on bilinear pairing and Computational Diffie-Hellman assumption. A concrete AAS construction is presented in Section IV, followed by its security and efficiency analysis in Section V. Finally, Section VI concludes the paper.

II. System architecture and security requirements

This section formalizes the architecture of AAS and summarizes its security requirements.

A. System architecture

As shown in Fig. 1, an AAS system consists of three types of entities, namely, a control center (COC) for unmanned aerial vehicles, many reconnaissance unmanned aerial vehicles (RAVs), and many aggregators (AGE). COC is a trusted entity with powerful computation and communication capabilities. It is responsible for producing public parameters to initialize the AAS system and issuing private keys for all RAVs and AGEs. Each AGE with medium-range communication capabilities manages a cluster of RAVs, whereas RAVs only have limited communication capabilities for short distances. Thus, AGE serves as a relay device for the communication between COC and the administrated RAVs of such AGE.

To secure AAS applications, COC needs to perform mutual authentication with RAVs before collecting information with the help of them. COC initializes the authentication process by broadcasting authentication request, so that AGEs are able to validate and forward it to its administrated RAVs. Each RAV can verify the real source and the forward process of the authentication request before responding. The responses of RAVs in the administrative domain can be validated by AGE in a batch, and then sends the aggregated response to COC for completing the authentication. The aggregated response is an aggregation on all responses of AGE and its administrated RAVs, so that all of them can be authenticated by COC in a batch to improve the verification performance.

B. Security requirements

An AAS system must satisfy the following security requirements.

Authenticity of COC: In a round of authentication, all AGEs and RAVs should be able to verify the real source of the

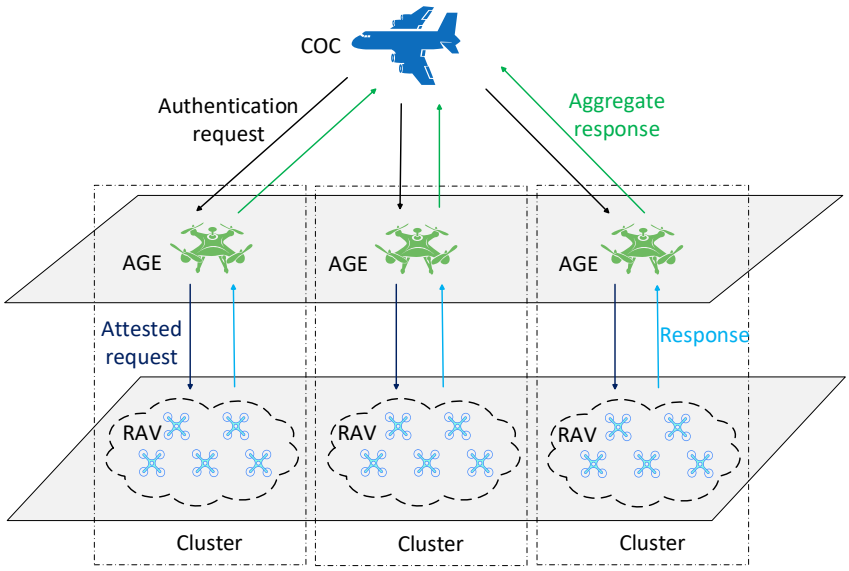

Fig. 1. AAS model for UAVCN.

authentication request. That is, any malicious entity cannot impersonate COC to forge an authentication request without being detected.

Authenticity of RAV: For the responses from RAVs in the same administrative domain of some AGE, both COC and such AGE should be able to verify their authenticity. That is, any malicious entity cannot forge a valid response of some RAV.

Authenticity of AGE: For the attested authentication request of some AGE, all RAVs in its administrative domain should be able to verify its authenticity. Also, COC should be able to validate the authenticity of the response from AGE. That is, any malicious entity cannot forge valid forwarded authentication request and response of some AGE.

A *correct* AAS construction should satisfy the following conditions: If all entities faithfully follow the authentication procedures, then

1) the authentication request generated by COC can be successfully validated by all AGEs;
2) the attested authentication request by AGE can be successfully validated by RAVs in the same cluster;
3) the response of RAVs can be validated by AGE in the same cluster;
4) the aggregate response can be successfully validated by COC.

III. Preliminaries

This section summarizes the preliminaries of our AAS construction, such as bilinear pairing and complexity assumption.

Suppose $(G_1, +)$ and $(G_2, \cdot)$ are additive and multiplicative cyclic groups with prime order q, respectively. The mapping $e : G_1 \times G_1 \to G_2$ is bilinear if the following properties are satisfied:

1) Bilinearity: For all $P, Q, R \in G_1$ and $a, b \in Z_q^*$, both
$$e(aP, bP) = e(P, P)^{ab}$$
and
$$e(P + Q, R) = e(P, R) \cdot e(Q, R)$$
hold.
2) Non-degeneracy: $e(P, P) \neq 1$.
3) Computability: $e(P, Q)$ can be computed efficiently in polynomial time for all $P, Q \in G_1$.

Computational Diffie-Hellman Assumption (CDH) Let $G_1 = \langle P \rangle$ be an additive cyclic group with prime order q. Given a tuple (P, aP, bP) for some random values $a, b \in_R Z_q^*$, any probabilistic polynomial time algorithm ξ would have negligible probability in computing $(ab)P \in G_1$.

IV. AAS Construction

This section describes a concrete AAS construction in bilinear groups. A running procedure of our AAS construction is shown in Fig. 2.

A. System setup

On input a security parameter l, COC chooses two cyclic groups $(G_1, +)$ and $(G_2, \cdot)$ of prime order q, and defines a bilinear map $e : G_1 \times G_1 \to G_2$, where P is a generator of G_1. COC selects four cryptographic hash functions $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \to G_1$, $H_3 : \{0,1\}^* \to G_1$ and $H_4 : \{0,1\}^* \to Z_q^*$. COC randomly chooses $h_1, h_2 \in Z_q^*$, and computes

$$X_1 = h_1 P$$

and

$$X_2 = h_2 P$$

Thus, the system parameter is $param = (q, P, G_1, G_2, e, H_1, H_2, H_3, H_4, X_1, X_2)$ and the private key of COC is (h_1, h_2).

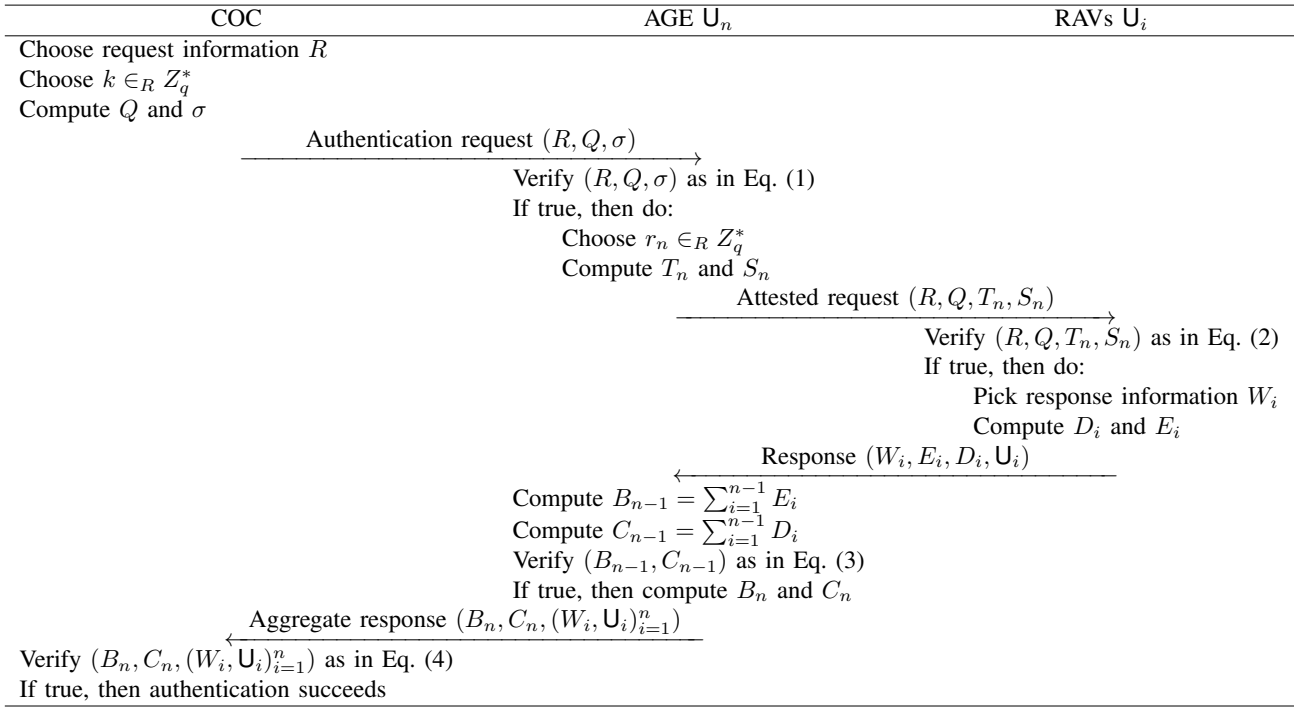

Fig. 2. A procedure of authentication in our AAS construction

B. Key generation for unmanned aerial vehicles

Let U_i be an unmanned aerial vehicle in the AAS system. For ease of representation, let U_n be an AGE and $\mathsf{U}_1, \cdots, \mathsf{U}_{n-1}$ be RAVs in the administration domain of U_n. For each RAV U_i $(i = 1, 2, \cdots, n-1)$, COC computes

$$Y_{i,j} = H_1(\mathsf{U}_i \| \mathsf{U}_n \| j)$$

and

$$f_{i,j} = h_1 Y_{i,j}$$

where $j \in \{0, 1\}$. Thus, the private key $(f_{i,0}, f_{i,1})$ is given to RAV U_i.

For AGE U_n, COC computes

$$Y_{n,j} = H_1(\mathsf{U}_n \| j)$$

and

$$f_{n,j} = h_1 Y_{n,j}$$

where $j \in \{0, 1\}$. Thus, the private key $(f_{n,0}, f_{n,1})$ is given to AGE U_n.

C. Authentication request

COC initiates the authentication procedure with unmanned aerial vehicles by sending a request to AGEs. Let R denote the request information chosen by COC. COC randomly picks $k \in Z_q^*$, and computes

$$Q = kP$$

and

$$\sigma = h_2 H_2(R \| Q)$$

COC sends out the authentication request (R, Q, σ).

D. Request forwarding

Upon receiving the request (R, Q, σ) from COC, each AGE U_n validates its authenticity by checking the following equality

$$e(\sigma, P) \stackrel{?}{=} e\left(H_2(R \| Q), X_2\right) \tag{1}$$

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

$$T_n = r_n P$$

and

$$S_n = \sigma + f_{n,0} + r_n H_3(R \| Q \| \mathsf{U}_n \| T_n)$$

At last, AGE U_n broadcasts the tuple of attested authentication request (R, Q, T_n, S_n) to all RAVs U_i $(i = 1, 2, \cdots, n-1)$ in its administrative domain.

E. RAV response

Once received (R, Q, T_n, S_n) from AGE U_n, each RAV U_i $(i = 1, 2, \cdots, n-1)$ verifies its authenticity by checking the following equality

$$\begin{aligned} e(S_n, P) \stackrel{?}{=} & e(H_1(\mathsf{U}_n \| 0), X_1) \cdot e(H_2(R \| Q), X_2) \\ & \cdot e(H_3(R \| Q \| \mathsf{U}_n \| T_n), T_n) \end{aligned} \tag{2}$$

If it holds, then RAV U_i accepts the authentication request from COC, otherwise terminates. Let W_i denote the response

information chosen by U_i. RAV U_i randomly picks $d_i \in Z_q^*$, computes

$$\begin{aligned}\delta &= H_2(R\|Q)\\ D_i &= d_iP\\ E_i &= d_i\delta + f_{i,0} + H_4(W_i\|\mathsf{U}_i\|R\|Q)f_{i,1}\end{aligned}$$

then sends the response tuple $(W_i, E_i, D_i, \mathsf{U}_i)$ to AGE U_n.

F. AGE aggregation

Once received the response tuples $\{W_i, E_i, D_i, \mathsf{U}_i\}_{i=1}^{n-1}$ from the controlled RAVs U_i $(i = 1, 2, \cdots, n-1)$, AGE U_n computes

$$\begin{aligned}\delta &= H_2(R\|Q)\\ B_{n-1} &= \sum_{i=1}^{n-1} E_i\\ C_{n-1} &= \sum_{i=1}^{n-1} D_i\end{aligned}$$

AGE U_n verifies the authenticity of the received the response tuples in a batch by checking the following equality

$$e(B_{n-1}, P) \stackrel{?}{=} e(\delta, C_{n-1}) \cdot e(\theta, X_1) \tag{3}$$

where

$$\theta = \sum_{i=1}^{n-1} H_1(\mathsf{U}_i\|\mathsf{U}_n\|0) + \sum_{i=1}^{n-1} H_4(W_i\|\mathsf{U}_i\|R\|Q)H_1(\mathsf{U}_i\|\mathsf{U}_n\|1)$$

If it holds, then all response tuples of U_i $(i = 1, 2, \cdots, n-1)$ are valid, otherwise U_n validates each response tuple in individual to find the invalid one. AGE U_n generates a response information W_n, randomly picks $d_n \in Z_q^*$, and computes

$$B_n = B_{n-1} + (d_n\delta + f_{n,0} + H_4(W_n\|\mathsf{U}_n\|R\|Q)f_{n,1})$$

and

$$C_n = C_{n-1} + d_nP$$

Then AGE U_n sends the aggregate response tuple $(B_n, C_n, (W_1, \mathsf{U}_1), \cdots, (W_n, \mathsf{U}_n))$ to COC.

G. COC verification

Once received the aggregate response tuple $(B_n, C_n, (W_1, \mathsf{U}_1), \cdots, (W_n, \mathsf{U}_n))$ from AGE U_n, COC validates its authenticity by checking the following equality

$$e(B_n, P) \stackrel{?}{=} e(H_2(R\|Q), C_n)e(\vartheta, X_1) \tag{4}$$

where

$$\begin{aligned}\vartheta = &\sum_{i=1}^{n-1} H_1(\mathsf{U}_i\|\mathsf{U}_n\|0) + \sum_{i=1}^{n-1} H_4(W_i\|\mathsf{U}_i\|R\|Q)H_1(\mathsf{U}_i\|\mathsf{U}_n\|1)\\ &+ H_1(\mathsf{U}_n\|0) + H_4(W_n\|\mathsf{U}_n\|R\|Q)H_1(\mathsf{U}_n\|1)\end{aligned}$$

If it holds, then AGE U_n and RAVs U_i $(i = 1, 2, \cdots, n-1)$ are all accepted as legitimate.

Theorem 1: The proposed AAS construction is correct.

Proof 1: To prove the correctness of the above proposed AAS construction, it is only necessary to prove that all equalities in (1)-(4) are satisfied.

1) For the authentication request (R, Q, σ) generated by COC, equality (1) satisfies as follows

$$e(\sigma, P) = e(h_2H_2(R\|Q), P) = e\left(H_2(R\|Q), X_2\right)$$

2) For the attested authentication request (R, Q, T_n, S_n) from AGE U_n, equality (2) satisfies as follows

$$\begin{aligned}&e(S_n, P)\\ &= e(\sigma, P)e(f_{n,0}, P)e(r_nH_3(R\|Q\|\mathsf{U}_n\|T_n), P))\\ &= e(\sigma, P)e(h_1H_1(\mathsf{U}_n\|0), P)e(H_3(R\|Q\|\mathsf{U}_n\|T_n), r_nP)\\ &= e(H_1(\mathsf{U}_n\|0), X_1) \cdot e(H_2(R\|Q), X_2)\\ &\qquad \cdot e(H_3(R\|Q\|\mathsf{U}_n\|T_n), T_n)\end{aligned}$$

3) For the response tuples $\{E_i, D_i, \mathsf{U}_i\}_{i=1}^{n-1}$ from the controlled RAVs U_i $(i = 1, 2, \cdots, n-1)$, equality (3) holds as follows

$$\begin{aligned}&e(B_{n-1}, P)\\ &\quad = e\left(\sum_{i=1}^{n-1} d_i\delta, P\right)\\ &\qquad \cdot e\left(\sum_{i=1}^{n-1} f_{i,0} + \sum_{i=1}^{n-1} H_4(W_i\|\mathsf{U}_i\|R\|Q)f_{i,1}, P\right)\\ &\quad = e\left(\delta, \sum_{i=1}^{n-1} d_iP\right)e(h_1\theta, P)\\ &\quad = e(\delta, C_{n-1}) \cdot e\left(\theta, X_1\right)\end{aligned}$$

4) For the aggregate response tuple $(B_n, C_n, (W_1, \mathsf{U}_1), \cdots, (W_n, \mathsf{U}_n))$ from AGE U_n, equality (4) holds as follows

$$\begin{aligned}&e(B_n, P)\\ &= e(B_{n-1}, P) \cdot e(d_n\delta + f_{n,0} + H_4(W_n\|\mathsf{U}_n\|R\|Q)f_{n,1}, P)\\ &= e(\delta, C_{n-1}) \cdot e\left(\theta, X_1\right) \cdot e(\delta, d_nP)\\ &\quad \cdot e(H_1(\mathsf{U}_n\|0) + H_4(W_n\|\mathsf{U}_n\|R\|Q)H_1(\mathsf{U}_n\|1), h_1P)\\ &= e(\delta, C_{n-1} + d_nP)\\ &\quad \cdot e(\theta + H_1(\mathsf{U}_n\|0) + H_4(W_n\|\mathsf{U}_n\|R\|Q)H_1(\mathsf{U}_n\|1), X_1)\\ &= e(H_2(R\|Q), C_n)e\left(\vartheta, X_1\right)\end{aligned}$$

V. Analysis

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

A. Security analysis

Theorem 2: Suppose the CDH assumption holds in bilinear group G_1. The proposed AAS construction can guarantee the authenticity of COC in producing authentication request.

Proof 2: In the authentication request (R, Q, σ) generated by COC, the element σ can be seen as a BLS signature [23] on $R\|Q$. According to [23, Theorem 3.2], the BLS signature is existentially unforgeable under adaptive chosen-message attacks, assuming the CDH assumption holds in bilinear group

G_1. Thus, any attacker is unable to forge a valid authentication request of COC without knowing its private key.

Theorem 3: Suppose the CDH assumption holds in bilinear group G_1. The proposed AAS construction can guarantee the authenticity of AGE in producing attested authentication request.

Proof 3: In the attested authentication request (R, Q, T_n, S_n) by AGE U_n, the element S_n combines the authentication request element σ and $f_{n,0}+r_nH_3(R\|Q\|\mathsf{U}_n\|T_n)$. Notice that $f_{n,0} + r_nH_3(R\|Q\|\mathsf{U}_n\|T_n)$ and T_n can be seen as an individual signature in producing identity-based multisignature [20] on $R\|Q\|\mathsf{U}_n$. According to [20, Theorem 1], their identity-based multisignature scheme is existentially unforgeable under adaptive chosen-message attacks, assuming the CDH assumption holds in bilinear group G_1. Thus, any attacker is unable to forge a valid individual signature of AGE U_n on $R\|Q\|\mathsf{U}_n$ without knowing its private key, which means the authenticity of AGE can be guaranteed in the attested authentication request.

Theorem 4: Suppose the CDH assumption holds in bilinear group G_1. The proposed AAS construction can guarantee the authenticity of RAV in producing authentication response.

Proof 4: For the response tuple (W_i, E_i, D_i) by RAV U_i, it can be seen as an individual signature on W_i in producing identity-based aggregate signature [20, Sect. 5]. According to [20, Theorem 2], their identity-based aggregate scheme is existentially unforgeable under adaptive chosen-message attacks, assuming the CDH assumption holds in bilinear group G_1. Thus, any attacker is unable to forge a valid individual signature of RAV U_i on W_i without knowing its private key.

Theorem 5: Suppose the CDH assumption holds in bilinear group G_1. The proposed AAS construction can guarantee the authenticity of AGE in producing aggregate authentication response.

Proof 5: For the aggregate response tuple $(B_n, C_n, (W_1, \mathsf{U}_1), \cdots, (W_n, \mathsf{U}_n))$ from AGE U_n, (B_n, C_n) can be seen as the aggregate signature [20, Sect. 5] on n individual responses $W_1, W_2, \cdots, W_n$. Note that $R\|Q$ can serve as the common value w in Gentry and Ramzan's identity-based aggregate signature scheme [20]. According to [20, Theorem 2], their scheme is existentially unforgeable under adaptive chosen-message attacks, assuming the CDH assumption holds in bilinear group G_1. Thus, any attacker is unable to forge a valid aggregate signature of AGE U_n on responses $W_1, W_2, \cdots, W_n$ without knowing its private key, which means the authenticity of AGE can be guaranteed in the aggregate authentication response.

B. Functional comparison

In [5], Wang et al. proposed an identity-based aggregate authentication scheme for UAVCN in bilinear groups. All RAVs can communicate with COC with the help of their respective AGE in the cluster, to carry out mutual authentication process. However, no security mechanism is considered in their scheme at the side of AGE. Specifically, there is no attestation mechanism for AGE to attest the authentication request of COC, before forwarding it to RAVs in its administrative domain. Also, when aggregating the individual responses from its controlled RAVs, the authenticity of these responses are not validated. Whereas in our AAS construction, both these mechanisms are provided to enhance the security of authentication in UAVCN. The detailed comparison on the functionalities between Wang et al.'s proposal [5] and our AAS construction is summarized in Table I.

C. Experimental performance

We conducted the experiments of our AAS system 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) i5-4210M CPU @ 2.60GHz and 4GB 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_1 is 512 bits.

The performance of the procedures such as system setup (Setup), key generation for RAV (RAVkgen) and AGE (AGEkgen), authentication request generation (REQgen) and attestation (REQfwd), and RAV response (RAVresp) are shown in Fig. 3, respectively. The setup procedure is run once to initialize the whole AAS system, which evaluation performance depends on the computation of X_1 and X_2, and can be completed in roughly 30 msec. For the key generation procedure of RAV and AGE, the only difference lies in the input to H_1. Thus, the key generation for a RAV and an AGE take the some time, i.e., about 85 msec in the experiments.

For the authentication request generation procedure, its performance is mainly determined by two scalar multiplications in computing Q and σ, and a map-to-point hash evaluation H_2. As shown in Fig. 3, an authentication request can be produced in less than 70 msec. In forwarding a request, it should be first validated by AGE as shown in Equality (1), and then an attestation is attached using its private key. Notice that the validation requires AGE to perform two bilinear map evaluations. In the experiment, the overall computation time for forwarding a request by AGE is no more than 0.12 seconds. Before producing a response, each RAV needs to validate the authenticity of the received attested request as shown in Equality (2), which requires four bilinear map evaluations. Thus, each RAV would take roughly 0.2 seconds in running the response procedure.

In the response aggregation procedure, AGE needs to combine the elements $\{E_i, D_i\}$ from the received response tuples. Note that $(2n - 2)$ map-to-point hash evaluations on H_1 should also be performed in generating θ, before batch validating these responses as shown in Equality (3). In the experiments, several cases with different number of unmanned aerial vehicles are considered, i.e., $n = 10, 20, \cdots, 100$, which contains $(n-1)$ RAVs and one AGE. That is, $(n-1)$ response tuples from RAVs are aggregated and validated by their AGE, and further combined with the response tuple of AGE. The experiment results are depicted in Fig. 4, which show that the

TABLE I
COMPARISON

	Request verification	Request attestation	Aggregate verification by AGE	Aggregate verification by COC
Our scheme	√	√	√	√
Wang et al.'s scheme [5]	√	×	×	√

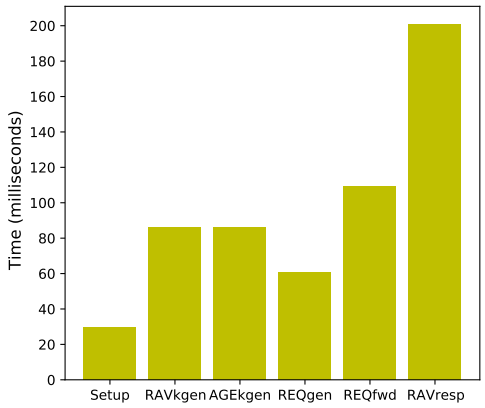

Fig. 3. Performance evaluation of the setup, key generation, request generation, forwarding and RAV response procedures

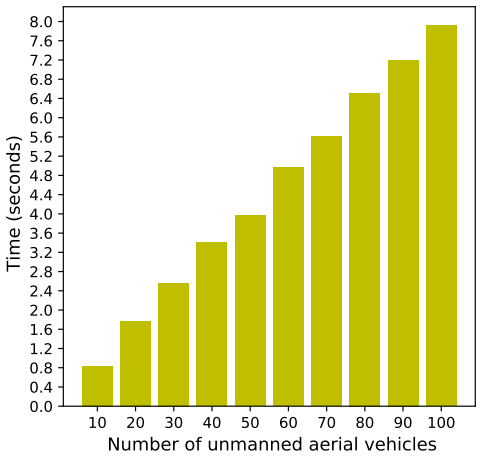

Fig. 5. Performance evaluation of the COC verification procedure

performance of this procedure is linearly determined by the number of unmanned aerial vehicles in each cluster.

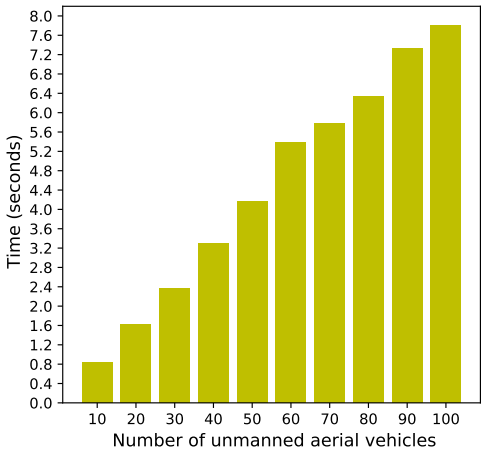

Fig. 4. Performance evaluation of the AGE aggregation procedure

Fig. 5 plots the performance of the COC verification procedure on the aggregate response from AGE of some cluster. Similar to Fig. 4, different cases with different number n of unmanned aerial vehicles in a cluster are considered, i.e., $n = 10, 20, \cdots, 100$. As shown in Equality (4), the verification requires COC to compute three bilinear maps. To calculate ϑ, COC needs to evaluate $2n$ map-to-point hashes on H_1. It can be seen that the performance of the COC verification procedure is also linearly determined by the number of unmanned aerial vehicles in each cluster.

VI. CONCLUSION

This paper considered the security issues in UAVCN and proposed an AAS construction in bilinear groups to realize mutual authentication between control center and unmanned aerial vehicles. COC initiates the authentication process, where the authentication request is attested and forwarded by aggregators in respective cluster to their controlled unmanned aerial vehicles. The responses from unmanned aerial vehicles can be aggregated by their aggregator of the same cluster, and then submitted to COC for verification on their authenticity. Security analysis showed that all (attested) authentication request and (aggregate) responses are unforgeable against malicious entities. Experimental analysis demonstrated that the proposed AAS construction is suitable to support unmanned aerial vehicles-assisted applications in real world.

ACKNOWLEDGMENT

This article is supported in part by the National Key R&D Program of China under projects 2020YFB1006004 and 2020YFB1006003, the National Natural Science Foundation of China under projects 61772150, 61862012 and 61962012, the Guangxi Key R&D Program under project AB17195025, the Guangxi Natural Science Foundation under grants 2018GXNSFDA281054, 2018GXNSFAA281232, 2019GXNSFFA245015, 2019GXNSFGA245004 and AD19245048, the Peng Cheng Laboratory Project of Guangdong Province PCL2018KP004, and the Innovation and Technology Support Programme of Innovation and Technology Fund of Hong Kong under Grant PRP/010/19FX.

REFERENCES

[1] M. Rodrigues, J. Amaro, F. S. Osório, and B. Kalinka. R. L. J. C., "Authentication methods for uav communication," in *2019 IEEE Symposium on Computers and Communications (ISCC)*, 2019, pp. 1210–1215.

[2] M. Rodrigues, D. F. Pigatto, and K. R. L. J. C. Branco, "Cloud-sphere: A security approach for connected unmanned aerial vehicles," in *2018 International Conference on Unmanned Aircraft Systems (ICUAS)*, 2018, pp. 769–778.

[3] C. Jiang, Y. Fang, P. Zhao, and J. Panneerselvam, "Intelligent uav identity authentication and safety supervision based on behavior modeling and prediction," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6652–6662, 2020.

[4] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in uav systems: Challenges and opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40–47, 2019.

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

[6] 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.

[7] E. Turgut and M. C. Gursoy, "Downlink analysis in unmanned aerial vehicle (uav) assisted cellular networks with clustered users," *IEEE Access*, vol. 6, pp. 36 313–36 324, 2018.

[8] J. Xu, G. Solmaz, R. Rahmatizadeh, D. Turgut, and L. Bölöni, "Animal monitoring with unmanned aerial vehicle-aided wireless sensor networks," in *2015 IEEE 40th Conference on Local Computer Networks (LCN)*, 2015, pp. 125–132.

[9] 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*, vol. n/a, no. n/a, p. e3942. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3942

[10] O. Bouhamed, H. Ghazzai, H. Besbes, and Y. Massoud, "A uav-assisted data collection for wireless sensor networks: Autonomous navigation and scheduling," *IEEE Access*, vol. 8, pp. 110 446–110 460, 2020.

[11] X. Li, J. Li, and J. Chen, "Effective cooperative uav searching using adaptive stgm mobility model in a fanet," in *2018 IEEE Intl Conf on Parallel Distributed Processing with Applications, Ubiquitous Computing Communications, Big Data Cloud Computing, Social Computing Networking, Sustainable Computing Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, 2018, pp. 295–301.

[12] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson, and W. Alexis, "Securing commercial wifi-based uavs from common security attacks," in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, 2016, pp. 1213–1218.

[13] M. Podhradsky, C. Coopmans, and N. Hoffer, "Improving communication security of open source uavs: Encrypting radio control link," in *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*, 2017, pp. 1153–1159.

[14] K. Yoon, D. Park, Y. Yim, K. Kim, S. K. Yang, and M. Robinson, "Security authentication system using encrypted channel on uav network," in *2017 First IEEE International Conference on Robotic Computing (IRC)*, 2017, pp. 393–398.

[15] D. He, S. Chan, and M. Guizani, "Communication security of unmanned aerial vehicles," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 134–139, 2017.

[16] L. Liu, H. Qian, and F. Hu, "Random label based security authentication mechanism for large-scale uav swarm," in *2019 IEEE Intl Conf on Parallel Distributed Processing with Applications, Big Data Cloud Computing, Sustainable Computing Communications, Social Computing Networking (ISPA/BDCloud/SocialCom/SustainCom)*, 2019, pp. 229–235.

[17] Z. Fu, Y. Mao, D. He, J. Yu, and G. Xie, "Secure multi-uav collaborative task allocation," *IEEE Access*, vol. 7, pp. 35 579–35 587, 2019.

[18] Q. Mao, F. Hu, and J. Qi, "Dynamic centered group key management for unmanned aerial vehicle networks with multibeam concurrent transmissions," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017, pp. 1–6.

[19] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, ser. Lecture Notes in Computer Science, vol. 2656. Springer, 2003, pp. 416–432.

[20] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," in *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings*, ser. Lecture Notes in Computer Science, vol. 3958. Springer, 2006, pp. 257–273.

[21] D. Lu and Y. Wang, "An identity-based aggregate signature scheme for wireless sensor network environmental monitoring," in *2019 6th International Conference on Systems and Informatics (ICSAI)*, 2019, pp. 1559–1564.

[22] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2017.

[23] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004. [Online]. Available: https://doi.org/10.1007/s00145-004-0314-9