Hindawi
Security and Communication Networks
Volume 2018, Article ID 5289383, 9 pages
https://doi.org/10.1155/2018/5289383

Research Article

Asynchronous Group Authentication Based on Geometric Approach

Hong Wang,[1,2] **Jianhua Li**,[1] **Feng Zhu**,[2] **and Zhe Wang**[1,2]

[1]*Information and Navigation College, Air Force Engineering University, Xi'an 710077, China*
[2]*Information and Communication College, National University of Defense Technology, Xi'an 710106, China*

Correspondence should be addressed to Hong Wang; whongger2017@163.com

Received 24 April 2018; Revised 15 October 2018; Accepted 25 October 2018; Published 5 December 2018

Academic Editor: Roberto Di Pietro

Individual authentication in air warfare is used to check whether a single participant is a legal member of the predefined group but not determine all participants at one time. An asynchronous (m, t, n) group authentication protocol is proposed based on multidimensional sphere reconstruction theorem of space analytic geometry without making any computational assumption, where m is the number of participants, t is threshold value, and n is the number of members. The proposed protocol can determine whether all participants belong to the predefined group at one time, which is applicable to batch verification prior to individual authentication. The center's coordinate of $(t-1)$-dimensional sphere is treated as the shared secret and the coordinate of the point on the surface of the sphere, multiplied by a random blind factor, is issued to all members as their tokens. If m participants can reconstruct the shared secret by utilizing their tokens, indicate that there is not any invalid participant, otherwise perform individual authentication. Analyses show the proposed scheme can not only rule out the illegal outsider but also resist up to $t-1$ group member conspiring to forge a valid token for an outsider. In addition, compared with other schemes the proposed scheme is more applicable for air warfare network, with light-weight computation, flexible distribution, and high information rate.

1. Introduction

In these days group oriented security become more and more important in air warfare. Take aeronautical communication network for an example, it is composed of various airborne weapons within a large scope by wireless. Airborne platforms share warfare information and interact with each other by aeronautical communication network. In the case the information which includes current position, condition and task, etc., is confidential, each airborne member would rather drop out the network than its confidential information is leaked [1, 2]. Hence every airborne platform should be assured that all members in the network are valid before transmitting confidential information.

Group authentication is one of the most important security services in many kinds of networks. Unlike traditional individual authentication group authentication verifies multiple signatures altogether at once and reduces verification time. Nowadays there are some proposed group authentication schemes which can authenticate all network members at one time. Concerning the basic theory group authentications fall into two categories: based on public key system and not based on public key system. In group authentication based on public key system [3–7], each member makes the individual signature by its private key and delivers its own signature to the aggregator, who is the selected one of group members. After receiving other signatures the aggregator compresses all signatures by the aggregate algorithms. The verifier can process multiple authentications at one time and make the batch verification of the security features, such as the integrity, traceability, and validity of messages. But it always includes complex computation, such as bilinear pairing and exponentiation, which need more computing efforts compared with symmetric cryptographic algorithms [8, 9]. Simultaneously there are also some group authentication schemes which are not based on public key system but some lightweight computation. For example, Harn [10] proposed a lightweight group authentication mechanism by using a preshared secret [11] in 2013. In the scheme the group manager is responsible for registering all group members. During registration the

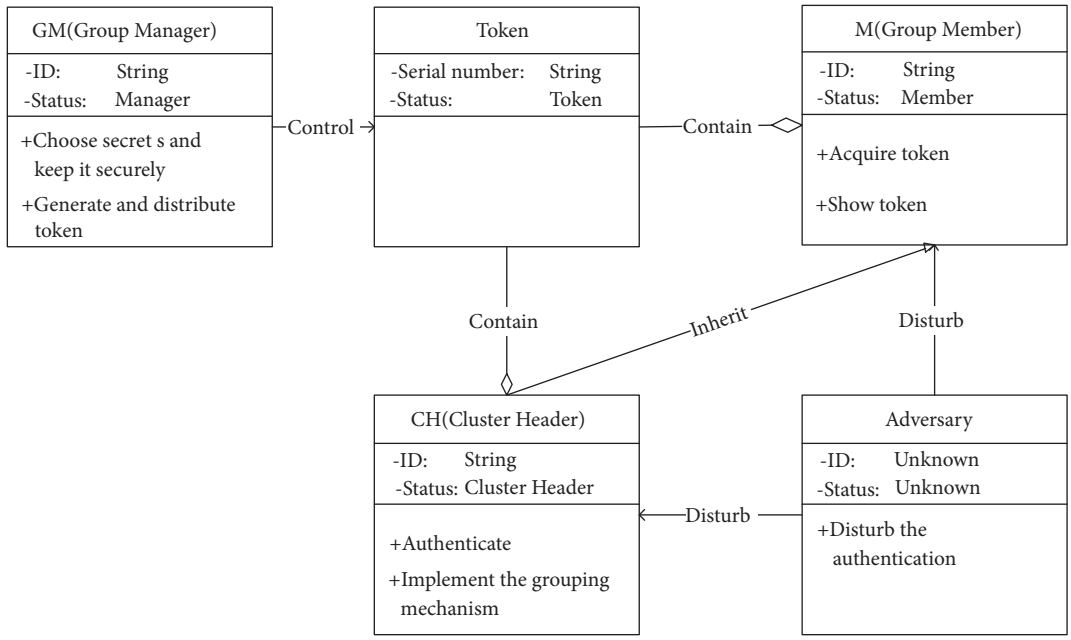

Figure 1: The class diagram of entities in the communication network.

group manager uses Shamir's secret sharing scheme to issue a private token to each group member. Subsequently all users participating in the group shall reconstruct the preshared secret. When reconstruction is successful it proves that nodes of a network must be valid and belong to a group. Otherwise there must be one or more invalid users among the participants and further authentication, such as individual authentication and batch identification, should be executed. Generally the group authentication based on secret reconstruction contains less computation overhead compared with public key based one; hence it is more suitable for airborne platform than public-key-based one when concerning fast and reliable authentication requirement in air warfare.

In Harn's scheme the notion of t-threshold, m-user and n-group was introduced and 3 schemes based on Shamir's (t,n)-threshold secret sharing was proposed. In asynchronous (t, m, n) group authentication scheme, k polynomials was used to generate k tokens for each group member and m $(m \geqslant t)$ participants are allowed to show the tokens asynchronously. Accept while the participants can reconstruct the secret, reject otherwise. The amount of participants must be known as a prior in order to reconstruct the secret, but in air warfare the amount is difficult to be known precisely and even not fixed. It require k polynomials and k is restricted by $kt > n - 1$. So it is not efficient and flexible enough. Based on the Lagrange interpolation theory Li et al. [14] proposed group authentication in 2016, and there also exists the same problem as Harn's scheme. Miao et al. [12] developed the group authentication based on Chinese Residue Theorem, but it is one-time authentication since the secret is no longer a secret once it has been recovered. Ji et al. [15] suggested another asynchronous (t, m, n) group authentication scheme based on threshold secret sharing theory in 2016. Before authentication it is assumed that every member has a predistributed randomized component (RC for short) which ensures that all the member's tokens are correlative, but a new token could not be deduced by coalition attacks. Nevertheless it is hard to meet that the amount of participants is a prerequisite knowledge for group authentication. He et al. [13] improved Ji's scheme and proposed another (t, m, n) group authentication scheme in which invalid members could be identified if group authentication fails. In He's scheme one trusted center; i.e., authentication server which is responsible for identification of bad member is needed. But it is hard to deploy a fixed and trusted center in air warfare.

Considering the characteristics of air warfare we give the asynchronous group authentication scheme which is applicable to the decentralized and asynchronous communication environment based on secret sharing theory. Meanwhile networking frequently in air warfare requires that the secret can be reused in our scheme. The remainder of this paper is organized as follows. In Section 2, we introduce the system model, authentication procedure and hypothesis of this scheme. In Section 3 we propose our asynchronous group authentication scheme based on geometric approach, followed by its security proof and performance analysis in Sections 4 and 5, respectively. In the end we draw our conclusion in Section 6.

2. Model and Hypothesis

In this section we formalize the system model and identify authentication procedure.

2.1. System Model

2.1.1. Entities. In terms of group authentication there are 4 types of entities in proposed scheme, the group manager (GM for short), group members, cluster header and some adversaries, as shown in Figure 1.

(a)GM: It is the coordinator of the scheme, which is trusted by all group members and responsible for the setup and distributing a secret share to each member by predeployed secure channel. Generally ground-based command site plays the role of GM and is assumed that it is not easy to be assaulted.

(b)Group members: All of the members possess the valid token. Group members belong to a predefined group and obtain the subsecret from GM in advance. The token which derives from the subsecret is deemed as the certificate of group member.

(c)Cluster Header: It is one of the group members who verify the tokens.

(d)Adversaries: There are 2 types of adversaries described as follows, including Insiders and Outsiders.

2.1.2. Adversary Model. In complicated air electromagnetic environment the network participants could be the members who have a valid token, or others who have no valid token. So there are 2 types of adversaries.

(a)Insiders: An insider is a legal member who obtains a valid token from GM but may band with other participants to forge a valid token for an illegal participant. It is assumed that there exist at most $t-2$ insiders in our scheme.

(b)Outsiders: An outsider does not belong to the predefined group and does not have a valid token. During networking authentication an outsider may eavesdrop information exchanged within group members, likely derive a valid token, and pretend to be a legal group member.

2.2. Authentication Procedure. Group authentication consists of three steps, i.e. setup, the generation of token and batch verification.

(a)Setup: GM generates some system parameters, selects a proper secret value S, and makes the shadow of S such as the hash value of S, publicly known.

(b)Generation of tokens: GM computes the subsecret and token for each group member, denoted as $U = \{U_1, U_2, \cdots, U_n\}$, and distributes them to each group member securely.

(c)Batch verification: all participants show their tokens, then reconstruct a secret S' and compare the hash value of S' with the one of S, and thus verify whether all participants are legal simultaneously.

3. Our Scheme Based on Geometric Approach

We propose a group authentication scheme based on the threshold secret sharing theory. Geometric theory brings inspiration and productivity to the secret sharing scheme. Blakley [16] proposed a threshold secret sharing scheme based on projective geometry theory early in 1979. Later, some literatures suggest the similar schemes based on analytical geometric theory sequentially. Our proposed scheme is based on multidimensional sphere reconstruction theory. Next we reveal and examine the theorem that four points determinate a sphere and give our group authentication scheme, followed by analysis of correctness.

3.1. Multi-Dimensional Sphere Reconstruction Theory. Every three triangle vertexes can determine a circle in a plane. And the center of the circle is the outside center of the triangle. Namely, every three points that do not lie on a straight line can determine a circle in a plane. Let (x_1, y_1),(x_2, y_2) and (x_3, y_3) be the coordinators of three triangle vertexes. Suppose that the equation of circle is

$$(x-a)^2 + (y-b)^2 = r^2 \tag{1}$$

Now let us substitute its coordinates into (1) and then get

$$\begin{aligned}(x_1-a)^2 + (y_1-b)^2 &= (x_2-a)^2 + (y_2-b)^2 \\ &= (x_3-a)^2 + (y_3-b)^2\end{aligned} \tag{2}$$

Simplify (2) further to

$$\begin{aligned}A_1 a + B_1 b &= C_1 \\ A_2 a + B_2 b &= C_2\end{aligned} \tag{3}$$

where $A_1 = 2(x_2 - x_1), B_1 = 2(y_2 - y_1), C_1 = x_2^2 + y_2^2 - x_1^2 - y_1^2$, $A_2 = 2(x_3 - x_2), B_2 = 2(y_3 - y_2), C_2 = x_3^2 + y_3^2 - x_2^2 - y_2^2$, and thus

$$\begin{aligned}a &= \frac{\begin{vmatrix} C_1 & B_1 \\ C_2 & B_2 \end{vmatrix}}{\begin{vmatrix} A_1 & B_1 \\ A_2 & B_2 \end{vmatrix}}, \\ b &= \frac{\begin{vmatrix} A_1 & C_1 \\ A_2 & C_2 \end{vmatrix}}{\begin{vmatrix} A_1 & B_1 \\ A_2 & B_2 \end{vmatrix}}\end{aligned} \tag{4}$$

Choose a point (a, b) of the plane and a random number r as the center and the radius of the circle respectively. The point (a, b) of the plane is considered as the secret to be shared. Select n points of the circle arbitrarily and distribute the coordinates of n points to n users as the subsecrets of them, respectively. Therefore, it is a $(3, n)$ threshold secret sharing scheme; at least 3 users show the subsecrets synchronously and reconstruct the circle and the secret (a, b) is recovered.

When the reconstruction theory of three-dimensional circle is extended to $(t-1)$-dimensional space, t arbitrary points that do not lie on the same $(t-2)$-dimensional space could determine the sphere of $(t-1)$-dimensional space. The equation of the sphere is denoted as

$$\begin{aligned}&\sum_{i=1}^{t-1} (x_i - a_i)^2 = R, \quad (R > 0) \\ \text{or } &\sum_{i=1}^{t-1} x_i^2 - 2a_1 x_1 - \cdots - 2a_{t-1} x_{t-1} + d = 0\end{aligned} \tag{5}$$

where $d = \sum_{i=1}^{t-1} a_i^2 - R$.

Similarly, the center $(a_1, a_2, \cdots, a_{t-1})$ of sphere is deemed as the secret to be shared. Select n points of the circle arbitrarily and distribute the coordinates of n points to n users as the subsecrets of them, respectively. Therefore, it is a (t, n) threshold secret sharing scheme; at least t users show the subsecrets synchronously and reconstruct the circle, and the secret $(a_1, a_2, \cdots, a_{t-1})$ is recovered.

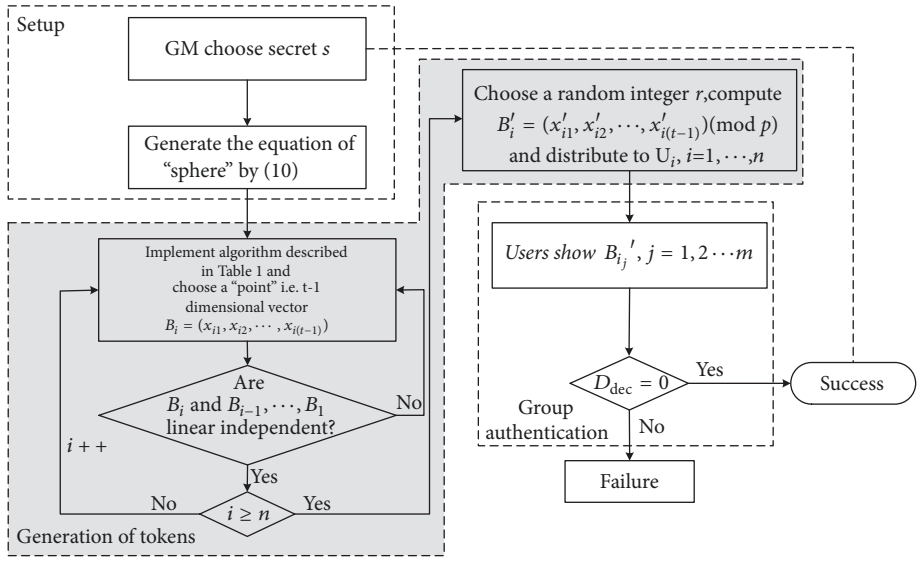

Figure 2: The detailed process diagram of asynchronous group authentication.

Theorem 1 (see [17]). *If t points $A_1(y_{11}, y_{12}, \cdots, y_{1(t-1)})$, $A_2(y_{21}, y_{22}, \cdots, y_{2(t-1)}) \ldots A_t(y_{t1}, y_{t2}, \cdots, y_{t(t-1)})$ do not lie in the common (t-2)-dimensional space, then they can uniquely determine a sphere, described as (5), in (t-1)-dimensional space uniquely, where*

$$a_i = \frac{D_i}{2D}, \quad i = 1, 2, \cdots, t-1 \tag{6}$$

$$R = \frac{D_t}{D} + \sum_{i=1}^{t-1} a_i^2 \tag{7}$$

$$D = \begin{vmatrix} y_{11} & \cdots & y_{1(i-1)} & y_{1i} & y_{1(i+1)} & \cdots & y_{1(t-1)} & 1 \\ y_{21} & \cdots & y_{2(i-1)} & y_{2i} & y_{2(i+1)} & \cdots & y_{2(t-1)} & 1 \\ \vdots & \cdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ y_{t1} & \cdots & y_{t(i-1)} & y_{ti} & y_{t(i+1)} & \cdots & y_{t(t-1)} & 1 \end{vmatrix} \neq 0 \tag{8}$$

$$D_i = \begin{vmatrix} y_{11} & \cdots & y_{1(i-1)} & \sum_{i=1}^{t-1} y_{1i}^2 & y_{1(i+1)} & \cdots & y_{1(t-1)} & 1 \\ y_{21} & \cdots & y_{2(i-1)} & \sum_{i=1}^{t-1} y_{2i}^2 & y_{2(i+1)} & \cdots & y_{2(t-1)} & 1 \\ \vdots & \cdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ y_{t1} & \cdots & y_{t(i-1)} & \sum_{i=1}^{t-1} y_{ti}^2 & y_{t(i+1)} & \cdots & y_{t(t-1)} & 1 \end{vmatrix} \tag{9}$$

Theorem 2 (see [18]). *If there is an odd prime p, such that $p = 3(\mathrm{mod}\ 4)$, any integer $z \in [0, p)$ could be expressed as a modulo sum of square of k integers; i.e., while z and p are known, there is a solution for $z = w_1^2 + w_2^2 + \cdots + w_k^2 (\mathrm{mod}\, p)$.*

3.2. Asynchronous Group Authentication. The asynchronous group authentication contains three steps: setup, generation of tokens and batch verification, as shown in Figure 2.

(1)Setup. GM chooses an odd prime $p = 3(\mathrm{mod}\ 4)$, secret vertex $S = \{s_1, s_2 \cdots s_{t-1}\}$, and $c \in_R (0, p)$. Compute

$$\begin{aligned} a_1 &= s_1 + c \,(\mathrm{mod}\, p) \\ a_2 &= s_2 + c \,(\mathrm{mod}\, p) \\ &\cdots \\ a_{t-2} &= s_{t-2} + c \,(\mathrm{mod}\, p) \\ a_{t-1} &= c \,(\mathrm{mod}\, p) \\ R &= s_{t-1} + c \,(\mathrm{mod}\, p) \end{aligned} \tag{10}$$

Let $\Omega : \sum_{j=1}^{t-1} (x_j - a_j)^2 = R(\mathrm{mod}\, p)$ be the equation of sphere in (t-1)-dimensional space.

(2)Generation of Tokens. (i)GM runs the algorithm described in Table 1 and generates $B_i = (x_{i1}, x_{i2}, \cdots, x_{i(t-1)})$, where $i = 1, 2 \cdots n$, for each user $U = \{U_1, U_2, \cdots, U_n\}$.

(ii)Choose a random integer $r \in_R (0, p), (r, p) = 1$, and then compute

$$\begin{aligned} B_i' &= \left(x_{i1}', x_{i2}', \cdots, x_{i(t-1)}'\right) (\mathrm{mod}\, p) \\ &= \left(rx_{i1}, rx_{i2}, \cdots, rx_{i(t-1)}\right) (\mathrm{mod}\, p), \quad i = 1, 2 \cdots n. \end{aligned} \tag{11}$$

B_i' is regarded as token and distributed to U_i, $i = 1, 2 \cdots n$.

(3)Batch Verification. While $m (t < m < n)$ participants $U_{I_m} = \{U_{i_1}, U_{i_2}, \cdots, U_{i_m}\}$ show tokens $B_{i_j}{}'$, $j = 1, 2 \cdots m$, each participant collects all the tokens and computes

Table 1: Choose an arbitrary point in a sphere Ω.

Input: $\Omega : \sum_{j=1}^{t-1}(x_j - a_j)^2 = R$; Output: $(t-1)$-dimensional points $B_i = (x_{i1}, x_{i2}, \cdots, x_{i(t-1)})$ in Ω
(1) Choose $x_{i1}, x_{i2}, \ldots\ldots x_{i(t-3)}$ in $(0, p)$ randomly;
(2) Compute $d_{i1} = x_{i1} - a_1 (\mathrm{mod} p)$, $d_{i2} = x_{i2} - a_2 (\mathrm{mod} p) \ldots\ldots d_{i(t-3)} = x_{i(t-3)} - a_{t-3} (\mathrm{mod} p)$;
(3) Compute $e_{ij} = d_{ij}^2 (\mathrm{mod} p)$, $j = 1, 2, \cdots, t-3$;
(4) Choose $d_{i(t-2)} \in (0, p)$, then compute $e_{i(t-2)} = d_{i(t-2)}^2 (\mathrm{mod} p)$;
(5) Compute $e'_{i(t-1)} = R - \sum_{j=1}^{t-2} e_{ij} (\mathrm{mod} p)$, $d_{i(t-1)} = (e'_{i(t-1)})^{(p+1)/4} (\mathrm{mod} p)$;
(6) Compute $e_{i(t-1)} = d_{i(t-1)}^2 (\mathrm{mod} p)$;
(7) If $e_{t-2} + e_{t-1} \neq R - \sum_{j=1}^{t-3} e_j (\mathrm{mod} p)$, then return 4;
(8) $x_{i(t-2)} = d_{i(t-2)} + a_{t-2} (\mathrm{mod} p)$, $x_{i(t-1)} = d_{i(t-1)} + a_{t-1} (\mathrm{mod} p)$
(9) Output $B_i = (x_{i1}, x_{i2}, \cdots, x_{i(t-1)})$

$$D_{\mathrm{dec}} = \begin{vmatrix} \sum_{j=1}^{t-1} x'^{\,2}_{i_1 j} & x'_{i_1 1} & x'_{i_1 2} & \cdots & x'_{i_1 (t-1)} & 1 \\ \sum_{j=1}^{t-1} x'^{\,2}_{i_2 j} & x'_{i_2 1} & x'_{i_2 2} & \cdots & x'_{i_2 (t-1)} & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sum_{j=1}^{t-1} x'^{\,2}_{i_t j} & x'_{i_t 1} & x'_{i_t 2} & \cdots & x'_{i_t (t-1)} & 1 \\ \sum_{j=1}^{t-1} z_j^2 & z_1 & z_2 & \cdots & z_{t-1} & 1 \end{vmatrix} \tag{12}$$

where $(z_1, z_2, \cdots, z_{t-1})$ is substituted by ${B_{i_j}}'$, $j = t+1, t+2, \cdots, m$. If all $\mathrm{D_{dec}} = 0$ is true for $j = t+1, t+2 \cdots m$, then all participants are legal; otherwise there is at least one illegal participant, identifying the illegal participants is next to do.

3.3. Analysis of Correctness. Lemma Linear equations

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1,n-1}x_{n-1} + a_{1,n} &= 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2,n-1}x_{n-1} + a_{2,n} &= 0 \\ \cdots & \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{n,n-1}x_{n-1} + a_{n,n} &= 0 \end{aligned} \tag{13}$$

have a solution if and only if

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = 0 \tag{14}$$

Proof. If the system of linear equations (13) has a solution, thus the rank of its coefficient matrix C equals the one of augmented matrix A, where

$$C = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,n-1} \\ a_{21} & a_{22} & \cdots & a_{2,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{n,n-1} \end{pmatrix},$$
$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,n-1} & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2,n-1} & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{n,n-1} & a_{nn} \end{pmatrix}, \tag{15}$$

i.e., Rank(C)=Rank(A).

Since Rank(A)$\leq n-1$, Rank(C) $\leq n-1$. So $|A| = 0$, (14) is true.

Moreover, if (14) is true, i.e., column vectors are linear dependent, $(a_{1n}, a_{2n}, \cdots, a_{nn})^T$ could be expressed as linear combination of $(a_{11}, a_{21}, \cdots, a_{n1})^T \ldots (a_{1,n-1}, a_{2,n-1}, \cdots, a_{n,n-1})^T$; i.e., (13) have a solution. □

Theorem 3. *If t vector* $B_i = (x_{i1}, x_{i2}, \cdots, x_{i(t-1)}) (\mathrm{mod} p)$, $(i = 1, 2, \cdots, t)$, *is linear independent in* $(t-1)$*-dimensional space, then the equation of sphere that the t vectors determine is*

$$\begin{vmatrix} \sum_{j=1}^{t-1} x_{1j}^2 & x_{11} & x_{12} & \cdots & x_{1(t-1)} & 1 \\ \sum_{j=1}^{t-1} x_{2j}^2 & x_{21} & x_{22} & \cdots & x_{2(t-1)} & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sum_{j=1}^{t-1} x_{tj}^2 & x_{t1} & x_{t2} & \cdots & x_{t(t-1)} & 1 \\ \sum_{j=1}^{t-1} z_j^2 & z_1 & z_2 & \cdots & z_{t-1} & 1 \end{vmatrix} = 0 \tag{16}$$

Proof. Suppose that (5) is the sphere equation to be determined. Since $B_i = (x_{i1}, x_{i2}, \cdots, x_{i(t-1)}) (\mathrm{mod} p)$, $(i = 1, 2, \cdots, t)$, lie on the sphere, then $A_i : \sum_{k=1}^{t-1} x_{ik}^2 - 2a_1 x_{i1} - \cdots - 2a_{t-1} x_{i,t-1} + d = 0$, $j = 1, 2, \cdots, t$. After variable substitution (5) is transformed into $\sum_{i=1}^{t-1} z_i^2 - 2a_1 z_1 - \cdots - 2a_{t-1} z_{t-1} + d = 0$.

While $a_1 \cdots a_{t-1}$ and d are regarded as the unknown variables, thus

$$\begin{gathered}
\sum_{k=1}^{t-1} x_{1k}^2 - 2a_1 x_{11} - \cdots - 2a_{t-1} x_{1,t-1} + d = 0 \\
\sum_{k=1}^{t-1} x_{2k}^2 - 2a_1 x_{21} - \cdots - 2a_{t-1} x_{2,t-1} + d = 0 \\
\cdots \\
\sum_{k=1}^{t-1} x_{t-1,k}^2 - 2a_1 x_{t-1,1} - \cdots - 2a_{t-1} x_{t-1,t-1} + d = 0 \\
\sum_{i=1}^{t-1} z_i^2 - 2a_1 z_1 - \cdots - 2a_{t-1} z_{t-1} + d = 0
\end{gathered} \tag{17}$$

Equations (17) have a solution if and only if the determinant (16) is true by referring to Lemma, so the equation of the sphere that $B_i = (x_{i1}, x_{i2}, \cdots, x_{i(t-1)}) (\mathrm{mod} p)$, $(i = 1, 2, \cdots, t)$, lie on is (16).

According to the characteristics of determinant (16) takes on the following form:

$$\begin{vmatrix}
\sum_{j=1}^{t-1} \left(rx_{1j}\right)^2 & rx_{11} & rx_{12} & \cdots & rx_{1(t-1)} & 1 \\
\sum_{j=1}^{t-1} \left(rx_{2j}\right)^2 & rx_{21} & rx_{22} & \cdots & rx_{2(t-1)} & 1 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\sum_{j=1}^{t-1} \left(rx_{tj}\right)^2 & rx_{t1} & rx_{t2} & \cdots & rx_{t(t-1)} & 1 \\
\sum_{j=1}^{t-1} \left(rz_j\right)^2 & rz_1 & rz_2 & \cdots & rz_{t-1} & 1
\end{vmatrix} = 0 \tag{18}$$

Namely,

$$\begin{vmatrix}
\sum_{j=1}^{t-1} {x'_{1j}}^2 & x'_{11} & x'_{12} & \cdots & x'_{1,(t-1)} & 1 \\
\sum_{j=1}^{t-1} {x'_{2j}}^2 & x'_{21} & x'_{22} & \cdots & x'_{2,(t-1)} & 1 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\sum_{j=1}^{t-1} {x'_{tj}}^2 & x'_{t1} & x'_{t2} & \cdots & x'_{t,(t-1)} & 1 \\
\sum_{j=1}^{t-1} \left(rz_j\right)^2 & rz_1 & rz_2 & \cdots & rz_{t-1} & 1
\end{vmatrix} = 0 \tag{19}$$

When $B'_i = (x'_{i1}, x'_{i2}, \cdots, x'_{i(t-1)}) (\mathrm{mod} p) = (rx_{i1}, rx_{i2}, \cdots, rx_{i(t-1)}) (\mathrm{mod} p)$, $i = 1, 2 \cdots n$, lie on the sphere Ω, (17) is true. □

4. Security Analyses

As mentioned previously, there exist two attacks against group authentication. One is from Insider, the other is from Outsider. In our scheme some Insiders attempt to reconstruct the predefined secret successfully by using their own tokens, thus they may generate a new token for an invalid member. However, it is impossible for some Insiders to derive the secret from their own tokens according to sphere reconstruction theory, and so the scheme is secure even if some legal members are compromised; see the following Theorem 4 for details. On the other hand, an Outsider may intercept a valid token by eavesdropping on the private channel successfully. It is also impossible for an Outsider to replay the used token since blind factor is changed frequently, for details see Theorem 5.

4.1. Coalition Attack Resistance. Assume that less than $t - 1$ legal members may attack the scheme together as previous hypothesis. But there exist $t - 2$ members who are likely to attack jointly and try to reconstruct the shared secret. It is out of the question to reconstruct a predefined sphere in $t - 1$ dimensional space by using $t - 2$ points on the sphere, so the coalition attack is ineffective by $t - 2$ members correspondingly.

Theorem 4. *Less than $t - 1$ legal members cannot get the secret $S = \{s_1, s_2 \cdots s_{t-1}\}$, i.e., the center's coordinate of $t - 1$ dimensional sphere.*

Proof. Let $t - 2$ participants' tokens be $B'_i = rB_i = (rx_{i1}, rx_{i2}, \cdots, rx_{i(t-1)}) = (x'_{i1}, x'_{i2}, \cdots, x'_{i(t-1)}) (\mathrm{mod} p)$, where $i = 1, 2 \cdots t - 2$, $B_i = (x_{i1}, x_{i2}, \cdots, x_{i(t-1)})$, r is a random number which plays the role of blinding B_i. The attacker could not derive B_i from B'_i unless the large integer factorization problem is feasible to be solved. Additionally $t - 2$ vectors are insufficient to determine the $(t - 1)$-dimensional sphere. The proof is by contradiction. Suppose it is true that $t - 2$ vectors are enough to determine the $(t - 1)$-dimensional sphere. Without lose of generality, let the vectors be denoted as $B_1, B_2 \cdots B_{t-2}$ determining a sphere Ω_1. Besides pick other two points W and V which are not on the sphere Ω_1. Due to Theorem 1, by $B_1, B_2 \cdots B_{t-2}$, W and V, another sphere, called as Ω_2, is determined. Clearly $\Omega_1 \neq \Omega_2$, since $W \notin \Omega_1$ and $V \notin \Omega_1$, but $W \in \Omega_2$ and $V \in \Omega_2$. Consequently by $B_1, B_2 \cdots B_{t-2}$ two different spheres are determined. If it did, it would be in contradiction with the above supposition of $B_1, B_2 \cdots B_{t-2}$ uniquely determining a sphere of $(t - 1)$-dimension. Therefore the sphere is not recovered by less than $t - 1$ legal members, nor is the secret correspondingly. □

4.2. Replay Attack Resistance. After legal participants showing the invalid tokens asynchronously, the Outsider may acquire the token which is to be reused illegally next. In our scheme blind factor concealing the token is beneficial to resist against the replay attack.

Theorem 5. *An Outsider cannot pass the group authentication by reusing the other token.*

Proof. Assume that U'_{i_1}'s token is leaked of the participants, $U'_{I_m} = \{U'_{i_1}, U'_{i_2}, \cdots, U'_{i_m}\}$ $(t < m < n)$. U'_{i_1}'s token is denoted as $B_{i_1}{}' = (x'_{i_1 1}, x'_{i_1 2}, \cdots, x'_{i_1(t-1)})(\mathrm{mod}p) = (rx_{i_1 1}, rx_{i_1 2}, \cdots, rx_{i_1(t-1)})(\mathrm{mod}p)$ which is to be replayed. But GM has updated all online tokens before next group authentication, so all tokens become $B_{i_j}{}'' = (x''_{i_j 1}, x''_{i_j 2}, \cdots, x''_{i_j(t-1)})(\mathrm{mod}p) = (r' x_{i_j 1}, r' x_{i_j 2}, \cdots, r' x_{i_j(t-1)})(\mathrm{mod}p)$, $j = 1, 2 \cdots n$. The replay attacker fakes U'_{i_1} by reusing $B_{i_1}{}'$ in a new authentication protocol. After substituting these values into determinant (16), we get

$$\begin{vmatrix} \sum_{j=1}^{t-1} x'^{\,2}_{1j} & x'_{11} & x'_{12} & \cdots & x'_{1,(t-1)} & 1 \\ \sum_{j=1}^{t-1} x''^{\,2}_{2j} & x''_{21} & x''_{22} & \cdots & x''_{2,(t-1)} & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sum_{j=1}^{t-1} x''^{2}_{tj} & x''_{t1} & x''_{t2} & \cdots & x''_{t,(t-1)} & 1 \\ \sum_{j=1}^{t-1} x''^{\,2}_{t+1,j} & x''_{t+1,1} & x''_{t+1,2} & \cdots & x''_{t+1,t-1} & 1 \end{vmatrix} \tag{20}$$

$$= \begin{vmatrix} \sum_{j=1}^{t-1} \left(rx_{1j}\right)^2 & rx_{11} & rx_{12} & \cdots & rx_{1,(t-1)} & 1 \\ \sum_{j=1}^{t-1} \left(r' x_{2j}\right)^2 & r' x_{21} & r' x_{22} & \cdots & r' x_{2,(t-1)} & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sum_{j=1}^{t-1} \left(r' x_{tj}\right)^2 & r' x_{t1} & r' x_{t2} & \cdots & r' x_{t,(t-1)} & 1 \\ \sum_{j=1}^{t-1} \left(r' x_{t+1,j}\right)^2 & r' x_{t+1,1} & r' x_{t+1,2} & \cdots & r' x_{t+1,t-1} & 1 \end{vmatrix}$$

There is any common factor in each row and column of determinant (20), so equation (16) is different from equation (20). The probability that $r = r'$ is $1/(p-1)$, where p is an odd prime, while $p \longrightarrow \infty$, $1/(p-1) \longrightarrow 0$. Consequently the probability that the reused token passes the new authentication is negligible. □

5. Performance Comparison and Analysis

The network environment in air warfare is complicated. Besides security requirement, efficiency is necessary for any group oriented authentication. The air tactical network has their inherent characteristics, such as high speed of aircrafts, poor stability of network topology, unpredictable discontinuity of communication link etc., which pose challenges for authentication. Considering these requirements our scheme has four contributions. Firstly our scheme can determine if there is any invalid participant in network by computing determinant (12) once, whose complexity is O(1). Secondly all participants are allowed to show their tokens asynchronously since blind factor hides the token. Thirdly GM serves for system setup and secret issuing, not online server. Any participant may act as the verifier since the network is deployed by distributed mode. Fourthly in the proposed scheme tokens generated by the GM initially can be used only to determine whether all participants are legal members, not to recover the secret. So the same secret can be employed for multiple authentications. In addition, any open token will not compromise the secrecy of uncovered secrets. Besides feasible practicability the proposed scheme provides some gains in efficiency, as batch verification of multiple participants is significantly faster than individual authentication, i.e.,"one-by-one" verification. The following is for details comparing with other authentication schemes.

5.1. Comparison with Individual Authentication. Individual authentication means that every two participants verify each other and any participant need verify other participants. Assume that 5 communications is necessary in each individual authentication, and it costs $5(m-1)!$ communications for m participants to finish individual authentications mutually. However, it costs only 2m communications for m participants to finish group authentication. One is for showing the token and the other is for issuing the decision. In terms of computation overhead our proposed group authentication scheme outperforms previously individual authentication. Individual authentication demands any participant to verify each of other participants, so the complexity is O(m), but our proposed group authentication scheme demands only one batch verification so as to determine whether there is any invalid participant. The complexity is O(1).

5.2. Comparison with Other Group Authentication. Our scheme is based on multidimensional sphere reconstruction theory instead of any mathematical hard problem. The computation overhead in our scheme is more lightweight, which contains neither bilinear pairing computation nor exponentiation, comparing with batch verification based on public key algorithm. Obviously our scheme mainly includes the calculation of high-order determinants which is associated with the number of participants. Concerning the efficiency of calculation Wiedemann [19] gave a probabilistic method whose complexity is $O((t+1)(w + (t+1)\log(t+1)))$ for the calculation of $t-1$ order determinant, where w represents the total of computation in Galios field. When m $(t < m < n)$ participants join the group authentication, the computation of $m-t$ determinants is demanded, so the complexity of our proposed scheme is $O((m-t)(t+1)(w + (t+1)\log(t+1)))$.

By contrast with other group authentication schemes based on the secret sharing theory our scheme shows better efficiency, parallelization and accuracy, as shown in Table 2. Harn's scheme made use of k different polynomials of degree $t-1$ to generate k tokens, the secret is magnified by k times and the information rate is $\rho = \log_2|S|/\log_2|K| < 1$, where S is the secret and K is the total of secret share. Besides the threshold t is restricted by the number of polynomials and the total of members, i.e., $kt > n-1$ in order to guarantee the security. For instance, if there are 1000 members and Harn's

Table 2: Comparison with other group authentication.

	Manage mode	Threshold restriction	Information rate	Basic theory
Literature[4]	Centralized	\	\	Public key algorithm
Literature[10]	Distributed	$kt > n - 1$	<1	Lagrange interpolation
Literature[12]	Distributed	$n > t$	1	Chinese remainder theorem
Literature[13]	Centralized	$n > t$	<1	Lagrange interpolation
Our scheme	Distributed	$n > t$	1	Sphere renconstruction

scheme uses polynomials of degree 2 to generate tokens, at least 500 polynomials are demanded, which means that each member hold at least 500 shares as the token, thus the scheme is too inefficient. Miao's scheme hide the secret shares by using blind factors which guarantee the asynchronism of token-showing, but the secret is not reused to next authentication once it is recovered. He's scheme consists of unified authentication, which ensure that there are not any invalid member of participants, and single authentication, which run individual verifications one by one when unified authentication fails. But a permanent online sever is required in He's scheme which does not apply to the de-centralized air warfare.

6. Conclusions and Future Work

We propose an asynchronous group authentication scheme based on space analytic geometry, which verifies if all participants belong to a predefined group at one time. Our scheme does depend on not any mathematical hard problem, but sphere reconstruction theorem of multidimension space. Each member has a unique share obtained from GM as the token. The token is a hidden coordinate, multiplied by a blind factor, of a point on $(t - 1)$ dimensional sphere, the center of which is the shared secret. While more than t participants show their tokens, we determine if participants are legal by verifying whether the shown token is on the $(t - 1)$ dimensional sphere. Analyses indicate that the proposed scheme can rule out fake outsider attackers and resist against coalition of insider attackers. In addition, compared with other schemes the proposed scheme is more applicable for air warfare network, with light-weight computation, flexible distribution, and high information rate.

The proposed scheme actually puts forward a general method to construct an asynchronous group authentication scheme based on space analytic geometry. The participants pass the group authentication if and only if everyone's token is valid. In our future work, we are about to address the problem of finding invalid efficiently when batch verification fails.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors acknowledge the support of the National Natural Science Foundation of China (nos. 61401499, 61174162).

References

[1] Y. X. Liang, G. Cheng, X. J. Guo et al., "Research progress on architecture and protocol stack of the airborne network," *Journal of Software*, vol. 27, no. 1, pp. 96–111, 2016.

[2] Y. Yu and NE Academy, "Research Progress of U.S. Military Forces' Battlefield Airborne Communication Node," *Telecommunication Engineering*, vol. 54, no. 6, pp. 56–63, 2014.

[3] C. Gentry and Z. Ramzan, "Identity-Based Aggregate Signatures," in *Proceedings of the International Conference on Theory and Practice of Public-Key Cryptography*, pp. 257–273, Springer-Verlag, 2006.

[4] L. Shen, J. Ma, X. Liu, F. Wei, and M. Miao, "A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 546–554, 2017.

[5] T. Iwasaki, N. Yanai, M. Inamura, and K. Iwamura, "Tightly-secure identity-based structured aggregate signature scheme under the computational diffie-hellman assumption," in *Proceedings of the 30th IEEE International Conference on Advanced Information Networking and Applications, AINA 2016*, pp. 669–676, Crans-Montana, Switzerland, March 2016.

[6] H. Chen, S. M. Wei, C. J. Zhu, and Y. Yang, "Secure certificateless aggregate signature scheme," *Journal of Software*, vol. 26, no. 5, pp. 1173–1180, 2015.

[7] Y. P. Li, H. H. Nie, Y. W. Zhou et al., "A novel and provably secure certificateless aggregate signature scheme," *Journal of Cryptologic Research*, vol. 2, no. 6, pp. 526–535, 2015.

[8] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 416–432, Springer, Berlin, Heidelberg, 2003.

[9] T. Yang, L. Kong, J. Hu et al., "Survey on aggregate signature and its applications," *Journal of Computer Research and Development*, vol. 49, no. s2, pp. 192–199, 2012.

[10] L. Harn, "Group authentication," *IEEE Transactions on Computers*, vol. 62, no. 9, pp. 1893–1898, 2013.

[11] L. Pang, *Research on Secret Sharing Technology And Its Application*, Xidian University, Xi'an, China, 2006.

[12] F. Miao, H. Jiang, Y. Ji, and Y. Xiong, "Asynchronous group authentication," *Journal of Electronics*, vol. 26, no. 4, pp. 820–826, 2017.

[13] X. He, F. Miao, and L. Fang, "(t,m,n)-AS Group Authentication Scheme Based on Secret Sharing," *Computer Engineering*, vol. 43, no. 3, pp. 1–6, 2017.

[14] S. Li, I. Doh, and K. Chae, "A group authentication scheme based on lagrange interpolation polynomial," in *Proceedings of the 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2016*, pp. 386–391, IEEE, Japan, July 2016.

[15] Y. Ji, F. Miao, and H. Jiang, "Simple asynchronous (t-m-n) group authentication," *Computer Engineering and Applications*, vol. 52, no. 15, pp. 8–12, 2016.

[16] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the AFIPS National Computer Conference (NCC '79)*, pp. 313–317, IEEE Computer Society, 1979.

[17] L. Ge and S. Tang, "Sharing multi-secret based on circle properties," in *Proceedings of the 2008 International Conference on Computational Intelligence and Security, CIS 2008*, pp. 340–344, IEEE Computer Society, China, December 2008.

[18] Z. Ke and Q. Sun, *Number Theory[M]*, pp. 109-110, High education press, Beijing, China, 2005.

[19] D. H. Wiedemann, "Solving sparse linear equations over finite fields," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 32, no. 1, pp. 54–62, 1986.