Hindawi
Security and Communication Networks
Volume 2018, Article ID 8470949, 9 pages
https://doi.org/10.1155/2018/8470949

Research Article

Attribute-Based Anonymous Handover Authentication Protocol for Wireless Networks

Yongbin Zeng,[1] **Hui Guang**,[2] **and Guangsong Li**[1]

[1]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China*
[2]*Physical Education College of Zhengzhou University, Zhengzhou 450044, China*

Correspondence should be addressed to Guangsong Li; lgsok@163.com

Received 8 January 2018; Accepted 27 February 2018; Published 18 April 2018

Academic Editor: Petros Nicopolitidis

Mobile wireless networks are widely used in our daily lives. Seamless handover occurs frequently and how to guarantee security and efficiency during handover procedure is a major challenge. A handover authentication protocol with nice properties can achieve goals. Protocols proposed in recent years more or less have some security vulnerability. In this paper, we outline security requirements for handover authentication protocols and then propose an anonymous protocol based on a new attribute-based signature scheme. The proposed protocol realizes conditional privacy preserving, user revocation, and session key update as well as mutual authentication and anonymity. Besides, it achieves fine-grained access control due to attributes representing real identity. What is more, experiment shows the proposed protocol has a superior performance.

1. Introduction

Nowadays, due to the wide use of mobile smart devices (e.g., PDA, smart phone pad, laptop PC, and vehicle) in our daily lives, we can enjoy Internet access services through mobile wireless networks such as mobile telecommunication networks, WLANs, and vehicular ad hoc networks. As a result, mobile wireless networks attract a lot of attention from both academia and industry [1–3]. Mobile nodes (MNs), access points (APs), and an authentication server (AS) are major entities in mobile wireless networks. Different types of entities have distinct features. For example, MNs have limited storage, computation, and communication capabilities; meanwhile APs have relatively formidable resources. MNs could move from one place to another one while APs have a limited geographical coverage. As a consequence, the handover occurs frequently. It needs an efficient security handover protocol when the handover occurs. An essential goal of the handover protocol is authentication. It aims to guarantee only valid MNs could access wireless networks and prevent illegal access request from adversaries. Mutual authentication is a basic requirement which a handover authentication protocol should meet. What is more, users' privacy, such as ID information and location information, should be protected, so that anonymity is of importance in handover process. An anonymous handover authentication protocol could meet this requirement.

Regardless of the technology implementation details, a typical handover authentication scenario is indicated in Figure 1. An MN registers to AS firstly, then it could connect to an AP for accessing the network. Assume an MN, say MN_i, enters in the geography coverage of a new access point AP_j from current one AP_{j-1}, handover authentication protocol should be executed by MN_i and AP_j. If it is performed successfully, AP_j can recognize whether MN_i is a legal user. Only if MN_i is legal will AP_j accept its access request. At the same time, a session key for protecting subsequent communication should be established between AP_j and MN_i.

To design an anonymous handover authentication protocol is a hot issue for researchers. Generally, efficiency, security, and privacy should be considered carefully. First, an anonymous handover authentication protocol should have lightweight computation cost, especially on the MN side because of its limited resources. Further, the protocol should achieve good security such as data confidentiality and integrity for openness of wireless communication. At last, an anonymous handover authentication protocol should protect

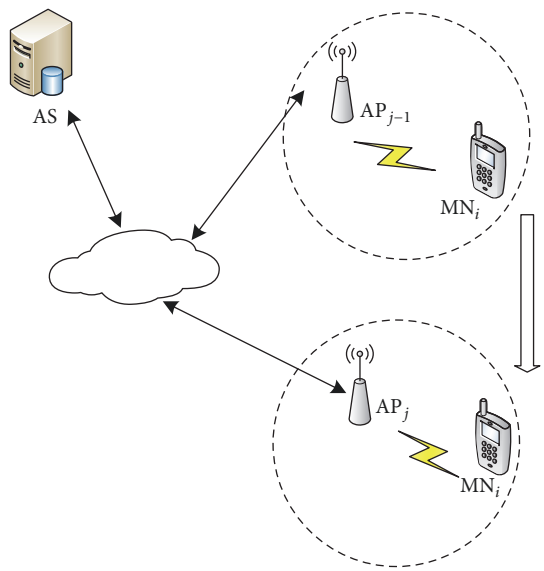

Figure 1: A typical scenario of handover.

users' privacy in case of serious crime caused by the leakage of private information.

Attribute-based signature (ABS) is a type of public key signature. Different from ID-based public key signature, in attribute-based signature, each user is tagged with a set of attributions. Attributes only expose group characteristics and hide individual characteristics which can provide anonymity. Introducing ABS to handover authentication protocols is an innovative idea for it can address the anonymity issue. However, designing an attribute-based handover authentication also presents some challenges because of computation complexity of common ABS. The ABS scheme usually involves lots of pairing operation which is a type of cryptographic operation with high computation complexity. Only ABS with low computation complexity is suitable for handover authentication protocols in wireless networks.

1.1. Related Works. Protocols with cryptographic technology are very suitable for handover authentication goal. In recent years, a lot of authentication protocols [4–7] were proposed for access control in various networks. In particular, ID-based public key cryptography (PKC) protocols are common in the latest proposed protocols. But some proposed protocols are not satisfactory. Wang et al. [8] figured out the roots of the identified failures in existing schemes. They are inherently unable to achieve key compromise impersonation resistance for authentication protocols in which the authentication server also acts as the registration center. He et al. [9] proposed a handover authentication protocol called PairHand, which utilized ID-based PKC based on the bilinear pairing. Authors claimed PairHand had a better performance compared with previous protocols. However, He et al. [10] pointed out that PairHand had a risk of key compromise for an adversary could extract a private key from intercepted traffic. Although an improvement had been presented in [10], Yeo et al. [11] declared the new scheme also suffered from the compromised key problem. What a pity, Yeo et al. did not address this issue. Later, Tsai et al. [12] gave a security-enhanced handover authentication protocol.

Later, an efficient attack [13] was given to show the vulnerability in PairHand [9] and the authors proposed an improved protocol also based on bilinear paring. At the same time, He et al. [14] did some improvement to enhance He et al.'s protocol [9]. Note that He et al. [15] and Liu et al. [16] independently presented two efficient handover authentication protocols without involving bilinear paring and map-to-point operation.

Due to the computation complexity of bilinear pairing and map-to-point operation, to design handover authentication protocols without them is an attractive job. Some handover authentication protocols [17–20] using Elliptic Curve Cryptography (ECC) could achieve the security goal with smaller key length. Li et al. [17] proposed a protocol using ECC. Meanwhile Chaudhry et al. [18] pointed out that Li et al.'s protocol suffered from impersonation attack and gave an enhanced security protocol. Xie et al. [19] also presented the vulnerability in [17] and then proposed an improved handover authentication protocol to address it. Yang et al. [20] presented a handover authentication protocol using ECC to strengthen security too.

Privacy protection requires handover authentication protocols to achieve anonymity. Some privacy-preserving protocols take advantage of pseudonyms to achieve anonymity [9–11, 17]. This type of method requires MNs to store a number of pseudonyms so that they can represent the true identifier to ensure privacy. Another type of method is using the group signature to provide anonymity [21]. In this way, any group member could produce a valid signature without involving private identity information. Therefore APs could verify the signature but could not determine which member did the signature. However, schemes based on the group signature usually have higher computation cost. Recently, attribute-based encryption was utilized to secure authentication [22]. However, the authors did not present concrete attribute-based encryption scheme and did not consider the high computation cost of common ABE scheme. Protocols with attribute-based encryption may not be suitable for confined devices in mobile wireless networks.

1.2. Our Contributions. To achieve security and efficiency as well as anonymity, we apply attribute-based signature to handover authentication protocols. We propose an attribute-based authentication protocol with light computation cost on the MN side. Compared with ID-based authentication protocols, attribute-based authentication protocols have a nice advantage due to their natural anonymity feature. To be specific, the major contributions of this paper are as follows.

Firstly, we propose an ABS scheme with low computation complexity and give the security proof for it. Different from other ABS schemes, our ABS scheme is lightweight so that it is fit for handover authentication protocols in wireless networks.

Secondly, we design a new handover authentication protocol based on our new lightweight ABS scheme. The new protocol meets requirements on security and efficiency. What is more, it provides anonymity inherently.

Finally, we present detailed security analysis and performance analysis of our new protocol to demonstrate that it achieves security and efficiency indeed.

1.3. Organization. The rest of the paper is organized as follows. We introduce some preliminaries used in this paper in Section 2. In Section 3, we describe our designed ABS scheme in detail and give its security proof. An attribute-based handover authentication protocol is proposed in Section 4. Security analysis and performance evaluation are given in Section 5. In Section 6, we conclude the whole paper.

2. Preliminaries

2.1. Bilinear Pairings and Computational Assumptions. Let G, G_T be cyclic groups of prime order p and g be a generator of G. A map $e : G \times G \to G_T$ is a bilinear pairing if it satisfies the following properties: (1) being bilinear: $e(g^a, g^b) = e(g, g)^{ab}$, where $a, b \in Z_p^*$; (2) nondegeneracy: $e(g, g) \neq 1_{G_T}$; (3) computability: there is an efficient algorithm to compute $e(g, h)$ for any $g, h \in G$.

It is well known that the following problems are hard for no probabilistic polynomial time algorithm can solve them.

Discrete Logarithm (DL) Problem. Given $g^x \in G$ with an unknown integer $x \in Z_p^*$, the DL problem is computing x in polynomial time.

Computational Diffie-Hellman (CDH) Problem. Given g^x, $g^y \in G$, the goal of CDH problem is computing g^{xy}, where x, y are two unknown integers in Z_p^*.

The CDH assumption means there is no probabilistic polynomial time algorithm that can solve the CDH problem with nonnegligible probability.

2.2. Security Requirements. For wireless communication, an adversary could control the communication channel between the MN and the AP. To ensure security, handover authentication protocol should meet the following security requirements [12, 14, 15].

(1) Mutual authentication: to guarantee only a legal MN and AP could communicate in the wireless network, the protocol should provide mutual confirmation of the MN's and AP's legitimacy.

(2) Session key establishment: the MN and AP should establish a unique random session key which guarantees confidentiality and integrity of the communication session.

(3) User anonymity and nontraceability: to protect the user's privacy, except for AS, no one include the AP could extract MN's identity or link any messages to the same user through intercepted messages.

(4) Provision of user revocation: service to the MN should be terminated once it comes to the expiration time.

(5) Updating session key periodically: in order to ensure strong security, when MN always accesses the Internet through the same AP, the session key needs to be updated periodically. This technique could reduce the risk due to a compromised session key.

(6) Attack resistance: due to the open environment of mobile wireless networks, a handover authentication protocol should prevent common attacks such as the replay attack, the impersonation attack, and the man-in-the-middle attack.

3. A High Efficiency ABS Scheme

Different from ID-based signature scheme taking identity to generate the public key, attribute-based signature scheme utilizes attributes to produce the public key. It has a nice property that an adversary could not determine the identity according to user's attributes. Attributes refer to some features a user may have, such as gender, job, and privilege. Let the universal set of attributes be $Att = \{att_1, att_2, \ldots, att_n\}$ and for each att_i its value set be $S_i = \{v_{i,1}, v_{i,2}, \ldots, v_{i,n_i}\}$, where $|S_i| = n_i$. A user's attribute list is denoted as $L = [l_1, l_2, \ldots, l_n]$, and the access structure is denoted as $W = [w_1, w_2, \ldots, w_n]$, where $w_i, l_i \in S_i$. There are 4 algorithms in our proposed ABS scheme.

ABS.Setup. The AS takes a security parameter τ with universal attribute set Att and outputs system public parameters *params* and master key *mk*.

ABS.KeyGen. Upon receiving a register request with an attribute list L, the AS runs the algorithm to generate a secret key sk_L with input L, *params*, and sends sk_L to the user securely.

ABS.Sign. To sign a message *msg*, the signer runs this algorithm with input *msg*, W, sk_L and returns the signature σ.

ABS.Verify. To verify a signature, the verifier runs the algorithm with *msg*, W, and σ and outputs "reject" or "accept" according to the validity of the signature.

3.1. Security Model. Similar to security against existential forgery on adaptively chosen message attacks, we define the security model through a game between a challenger B and an attacker A. The game is defined below.

Setup. The challenger B runs the *ABS.Setup* algorithm and outputs *params* and *mk*. The challenger keeps *mk* secret and sends *params* to A.

Query. A makes a series of queries to B adaptively, and B responses in the following way.

(i) Key Query. Attacker A issues this query to acquire private key sk_L related to attribute list L. B runs *ABS.KeyGen* algorithm with input (L, *params*) and sends the output sk_L to A.

(ii) Signing Query. When A issues a signing query with a message msg, access structure W, B runs $ABS.Sign$ algorithm and returns a signature σ to A.

Forgery. A outputs a tuple $(msg^*, L^*, W^*, \sigma^*)$.

If the following conditions hold, an attack is successful:

(1) $ABS.Verify(msg^*, W^*, \sigma^*) = accept$.

(2) A does not issue the key query on L^*.

(3) A does not issue the signing query on (msg^*, W^*).

The probability of a successful attack is defined as A's advantage Adv_A.

Definition 1. An attribute-based signature is existentially unforgeable against adaptive chosen message if there is no probabilistic polynomial time adversary that has a nonnegligible advantage in the game.

3.2. Construction. ABS.Setup(τ, Att). The AS chooses two cyclic groups G, G_T of prime order p with a bilinear map $e : G \times G \to G_T$, random numbers $\alpha \in Z_p^*$, $g_1 = g^\alpha$, $g_2 \in G$, where g is a generator of G and sets the value $Y_1 = e(g_1, g_2)$, $Y_2 = e(g, g_2)$. Then AS randomly selects $u' \in Z_p^*, m' \in G$, a k-length vector $\overline{\gamma} = (u_i)$ with elements chosen at random from Z_p^*, and a k-length vector $\overline{\eta} = (m_i)$ with elements chosen at random from G. So the public parameters set is

$$params = \left\{p, g, g_0, g_1, g_2, u', m', Y_1, Y_2, \overline{\gamma}, \overline{\eta}, H\right\}, \quad (1)$$

where g_0 is a generator of G_T and H is a secure hash function $H : \{0,1\}^* \to \{0,1\}^k$. The master private key is α.

ABS.KeyGen(L, params). A user sends its attribute list L and identity information ID to register at the AS. The AS computes a k-bit string $v = H(L)$. Let v_i denote the ith bit of v and V be a subset of $\{1, 2, \ldots, k\}$, where $V = \{i \mid v_i = 1\}$. Then the AS randomly chooses a number $t \in Z_p^*$ and computes $\lambda = u' + \sum_{i \in V} u_i$, $d_0 = g_2^\alpha \cdot g_2^{\lambda t}$, $d_1 = Y_2^t$. Note that if $\lambda t + \alpha = 0 \bmod p$, the AS selects a new t. Finally, the AS sends the generated private key $sk_L = (d_0, d_1)$ to the user. For security, the user can verify whether the following equation holds: $e(g, d_0) = Y_1 \cdot d_1^\lambda$.

ABS.Sign(msg,W, sk$_L$). If the user's attribute list L satisfies the access structure, a message msg is signed by the user with its private key $sk_L = (d_0, d_1)$ as follows. The user computes a k-bit string $y = H(msg)$. let y_i denote the ith bits of y and M be a subset of $\{1, 2, \ldots, k\}$, where $M = \{i \mid y_i = 1\}$. Then the signer selects random numbers $t', s \in Z_p^*$, and computes

$$\begin{aligned} \sigma_1 &= d_0 \cdot g_2^{\lambda \cdot t'} \cdot \left(m' \cdot \prod_{i \in M} m_i\right)^s, \\ \sigma_2 &= g^s, \\ \sigma_3 &= d_1^{t'}, \end{aligned} \quad (2)$$

where $\lambda = u' + \sum_{i \in V} u_i$. So the signature of msg is $\sigma = (\sigma_1, \sigma_2, \sigma_3)$.

ABS.Verify(msg, W, σ). The verifier computes a k-bit string $q = H(W)$. Let q_i denote the ith bit of q and Q be a subset of $\{1, 2, \ldots, k\}$, where $Q = \{i \mid q_i = 1\}$. Then verifier computes $\lambda' = u' + \sum_{i \in Q} u_i$ and checks whether the following equation holds:

$$e(g, \sigma_1) = Y_1 \cdot \sigma_3^{\lambda'} \cdot e\left(\sigma_2, m' \prod_{i \in M} m_i\right). \quad (3)$$

If it holds, the verifier outputs "accept"; namely, the signature is valid. Otherwise, the verifier outputs "reject"; namely, the signature is illegal.

3.3. Security Analysis. We analyze the security of above proposed ABS scheme according to the security model defined in Section 3.1.

Lemma 2. *If there is an adversary that makes at most q_e, q_s queries for key query and signing query, respectively, and breaks the proposed signature scheme with nonnegligible probability ε, then there exists a challenger that can solve the CDH problem with advantage*

$$\varepsilon' \geq \frac{\varepsilon}{16(q_e + q_s) q_s (k+1)^2}. \quad (4)$$

Proof. Suppose A is an adversary that wins the attack game with advantage ε. We construct an algorithm B to act as a challenger for the adversary. Suppose B is given a CDH instance (g, g^a, g^b), where g is a generator of a cyclic group G of order p and B does not know a, b. In order to compute g^{ab}, the simulation communication is as follows.

Setup. Let $l_v = 2(q_e + q_s)$, $l_y = 2q_s$, and B randomly selects $k_v \in Z_{l_v}$, $k_y \in Z_{l_y}$, $0 \leq k_v, k_y \leq k$. And for given q_e, q_s, k, B ensures $l_v(k+1) < p$, $l_y(k+1) < p$. Then B randomly chooses numbers $x' \in Z_{l_v}$, $z' \in Z_{l_y}$, $\omega' \in Z_p$ and k-length vectors $X = (x_i)$, $Z = (z_i)$, $\Phi = (\omega_i)$, where $x_i \in Z_{l_v}$, $z_i \in Z_{l_y}$, $\omega_i \in Z_p$. 3 functions are defined as follows:

$$\begin{aligned} F(v) &= x' + \sum_{i \in V} x_i - l_v k_v, \\ K(y) &= z' + \sum_{i \in M} z_i - l_y k_y, \\ L(y) &= \omega' + \sum_{i \in M} w_i. \end{aligned} \quad (5)$$

Finally B calculates system parameters as follows:

$$\begin{aligned} g_1 &= g^a, \\ g_2 &= g^b, \\ u' &= -l_v k_v + x', \\ u_i &= x_i, \quad 1 \leq i \leq k, \\ m' &= g_2^{-l_y \cdot k_y + z'} + g^{\omega'} x', \\ m_i &= g_2^{z_i} + g^{\omega_i}, \quad 1 \leq i \leq k, \end{aligned} \quad (6)$$

so

$$\begin{aligned} g_2^{\alpha} &= g_2^{a} = g^{ab}, \\ u' + \sum_{i \in V} u_i &= F(v), \\ m' \prod_{j \in M} m_j &= g_2^{K(y)} g^{L(y)}. \end{aligned} \tag{7}$$

Query. Algorithm B acts as a challenger to communicate with an adversary A as follows.

(i) Key Query. On receiving a key query on attribute list L, B could generate related private key if $F(v) \neq 0 \bmod p$, although B does not know the master key. B randomly selects $t \in Z_p$ and calculates

$$sk_L = (d_0, d_1) = \left(g_1^{-1} (g g_2)^{t\lambda}, e\left(g g_2, g^t g_1^{-1/\lambda}\right)\right), \tag{8}$$

where $\lambda = u' + \sum_{i \in V} u_i$. Then B sends sk_L to A and A could verify it. For an attacker, the above private key and the one generated by a true challenger are undistinguishable, because

$$sk_L = (d_0, d_1) = \left(g_2^{a} g_2^{\lambda t'}, Y_2^{t'} \right), \tag{9}$$

where

$$t' = \left(1 + \frac{1}{b}\right)\left(t - \frac{a}{F(v)}\right). \tag{10}$$

If $F(v) = 0 \bmod p$, B will abort.

In order to calculate probability simply, we set $F(v) \neq 0 \bmod l_v$ as the condition of generating valid private key. This is reasonable because $F(v) \neq 0 \bmod l_v$ indicates $F(v) \neq 0 \bmod p$, due to $0 \leq l_v(k+1) < p$, $0 \leq k_v \leq k$.

Signing Query. When A issues a signing query on (msg, W), if $K(y) \neq 0 \bmod p$, B chooses $s, t \in Z_p$ randomly and calculates

$$\begin{aligned} \sigma &= (\sigma_1, \sigma_2, \sigma_3) \\ &= \left(g_2^{t\lambda'} g_1^{-L(y)/K(y)} \left(m' \prod_{j \in M} m_j \right)^{s}, g^{s} g_1^{-1/K(y)}, Y_2^{t} \right) \\ &= \left(g_2^{t\lambda'} g_2^{\alpha} \left(m' \prod_{j \in M} m_j \right)^{s'}, g^{s'}, Y_2^{t} \right), \end{aligned} \tag{11}$$

$$\text{where } s' = s - \frac{a}{K(y)}.$$

B Sends σ to A, and A could verify the validity of the signature. Of course, for attacker A, the signature generated by B is undistinguishable from the one generated by a true challenger.

If $K(y) = 0 \bmod p$, B will abort. Similar to key query, we set $K(y) \neq 0 \bmod l_y$ as the condition of generating a valid signature.

Forgery. Finally, if B does not abort during above queries, the adversary outputs a forgery $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*)$ on message msg^*, access structure W^* with a probability ε. Here we assume $\sigma_1^* = g_2^{a} g_2^{\lambda t^*} \cdot (m' \prod_{j \in M} m_j)^{s^*}$, $\sigma_2^* = g^{s^*}$, $\sigma_3^* = Y_2^{t^*}$, and A does not issue a signing query on msg^* and key query on L^* which satisfies W^*. If $K(y^*) \neq 0 \bmod p$ or $F(v^*) \neq 0 \bmod p$, B will abort. If $K(y^*) = 0 \bmod p$ and $F(v^*) = 0 \bmod p$, B computes and outputs

$$\frac{\sigma_1^*}{(\sigma_2^*)^{L(y^*)}} = \frac{g_2^{a + t^* \lambda} \cdot \left(m' \prod_{j \in M} m_j\right)^{s^*}}{g^{L(y^*) s^*}} = g_2^{a} = g^{ab}, \tag{12}$$

which is the solution to the given CDH problem.

We analyze the probability of B outputting the solution to CDH problem, namely, B not aborting. For the case without aborting, we require that all key queries will have $F(v) \neq 0 \bmod p$, and all signing queries will have $K(y) \neq 0 \bmod p$ and that $K(y^*) = 0 \bmod p$ and $F(v^*) = 0 \bmod p$ in forgery.

For convenience, we will define the events A_i, A^*, B_i, B^* as follows:

A_i: $F(v_i) \neq 0 \bmod l_v$, with $i = 1, 2, \ldots, q_e$;

A^*: $F(v^*) = 0 \bmod p$;

B_i: $K(y_i) \neq 0 \bmod l_y$, with $i = 1, 2, \ldots, q_s$;

B^*: $K(y^*) = 0 \bmod p$.

So the probability of B not aborting is

$$\Pr(\text{not\_abort}) = \Pr\left(\bigcap_{i=1}^{q_e+q_s} A_i \wedge A^* \wedge \bigcap_{i=1}^{q_e} B_i \wedge B^* \right). \tag{13}$$

We have

$$\begin{aligned} \Pr(A^*) &= \Pr\left(F(v^*) = 0 \bmod p \wedge F(v^*) = 0 \bmod l_v\right) \\ &= \Pr\left(F(v^*) = 0 \bmod l_v\right) \\ &\quad \cdot \Pr\left(F(v^*) = 0 \bmod p \mid F(v^*) = 0 \bmod l_v\right) \\ &= \frac{1}{l_v (k+1)}, \end{aligned} \tag{14}$$

$$\Pr\left(\bigcap_{i=1}^{q_e+q_s} A_i \right) = \Pr\left(1 - \bigcup_{i=1}^{q_e+q_s} \overline{A_i} \right) \geq 1 - \frac{q_e + q_s}{l_v}. \tag{15}$$

Due to $l_v = 2(q_e + q_s)$, we have

$$\Pr\left(\bigcap_{i=1}^{q_e+q_s} A_i \wedge A^* \right) \geq \frac{1}{4(q_e + q_s)(k+1)}. \tag{16}$$

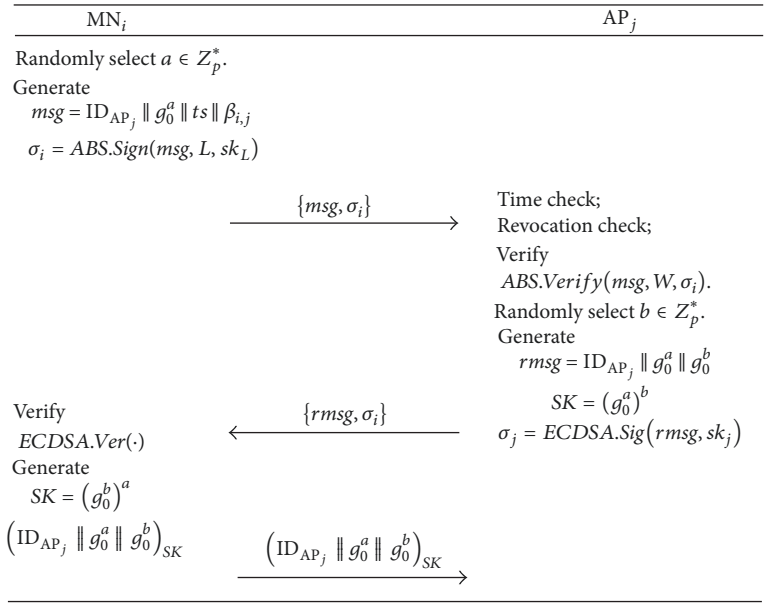

Figure 2: Handover authentication procedure.

Similarly, we have $\Pr(\bigcap_{i=1}^{q_s} B_i \wedge B^*) \geq 1/4q_s(k+1)$, so that the probability of B not aborting is

$$\begin{aligned}\Pr(\text{not\_abort}) &= \Pr\left(\bigcap_{i=1}^{q_e+q_s} A_i \wedge A^* \wedge \bigcap_{i=1}^{q_e} B_i \wedge B^*\right) \\ &= \Pr\left(\bigcap_{i=1}^{q_e+q_s} A_i \wedge A^*\right) \\ &\quad \wedge \Pr\left(\bigcap_{i=1}^{q_s} B_i \wedge B^*\right) \\ &\geq \frac{1}{16(q_e+q_s)q_s(k+1)^2}.\end{aligned} \tag{17}$$

In general, if simulation does not abort and an attacker breaks the proposed signature scheme with nonnegligible probability ε, then B could give a solution to CDH problem with the probability ε', where

$$\varepsilon' \geq \frac{\varepsilon}{16(q_e+q_s)q_s(k+1)^2}. \tag{18}$$

□

So we have the following theorem.

Theorem 3. *The proposed attribute-based signature scheme is existence unforgeable against adaptive chosen message and attribute list attack under CDH assumption.*

4. The Proposed Handover Authentication Protocol

Based on our designed signature scheme, we propose a new handover authentication protocol. We consider that each AP has a signing/verification key pair (pk, sk) of a common digital signature scheme ECDSA [23]. To guarantee revocation check, we make some extension of the algorithm $ABS.KeyGen(\cdot)$ in Section 3. The AS also generates extra revocation information for the user. For interval index ts_j, the revocation information of the user is $\beta_j = \overline{H}_{rk}^j(\mathrm{ID})$, where rk is a random number selected for the user by AS and $\overline{H}_{rk}^j(\cdot)$ is a keyed hash chain.

In the following, we describe the protocol in detail. Assume the handover authentication protocol is carried out between MN_i and AP_j. According to the signature algorithm, MN_i acquires its private key sk_L and revocation information $\beta_{i,j}$ for each ts_j. The protocol is illustrated in Figure 2. And the notations used to describe the protocol are listed as follows.

(i) W: specified access structure

(ii) ts: timestamp

(iii) $\mathrm{ID}_{\mathrm{AP}_j}$: identity of AP_j

(iv) $\beta_{i,j}$: revocation information with time interval index ts_j for MN_i

(v) L: attribute list owned by MN

(vi) sk_L: MN's secret private key on attribute list L

(vii) a, b: random numbers in Z_p^*

(viii) σ_i, σ_j: digital signature of MN_i and AP_j, respectively

(ix) SK: session key.

(1) MN_i could obtain the access structure W from the beacon message from AP_j. If its attribute list satisfies the access structure, then MN_i firstly selects a random number $a \in Z_p^*$ and generates $\sigma_i = ABS.Sign(msg, L, sk_L)$, where $msg = \mathrm{ID}_{\mathrm{AP}_j} \| g_0^a \| ts \| \beta_{i,j}$. And then it sends $\{msg, \sigma_i\}$ to

AP_j. Here a timestamp ts is added for revocation check and replay attack prevention.

(2) After receiving the signature message $\{msg, \sigma_i\}$ from MN_i, AP_j checks the time ts to prevent replay attack and executes the revocation check (the details in Revocation). If it passes the above check, then AP_j verifies the signature. If the signature is invalid, AP_j rejects it; otherwise, AP_j selects a random number $b \in Z_p^*$ and computes $\sigma_j = ECDSA.Sig(rmsg, sk_j)$, where $rmsg = ID_{AP_j} \parallel g_0^a \parallel g_0^b$. Then AP_j sends $\{rmsg, \sigma_j\}$ back to MN_i. Finally, AP_j computes the session key $SK = (g_0^a)^b$ and erases the random number b from its memory.

(3) Upon receiving $\{rmsg, \sigma_j\}$, MN_i verifies σ_j according to $ECDSA.Ver(\cdot)$. If the algorithm returns 1, MN_i generates the session key $SK = (g_0^b)^a$ and erases the random number a from its memory. After that, MN_i generates $(ID_{AP_j} \parallel g_0^a \parallel g_0^b)_{SK}$ and then sends it to AP_j. Here $(X)_K$ refers to using a symmetric key K to encrypt a message X. After receiving the encrypted message, AP_j decrypts and verifies it with SK. If the message is valid, AP_j believes that they have established a session key SK; otherwise, it rejects the access request.

Session Key Update. When MN_i is always connecting to the same AP, assume their current session key is SK_j. They establish a new session key as follows. (1) MN_i chooses a random number $c \in Z_p^*$, computes $g_0^c, Aut_1 = H(SK_j \parallel g_0^c)$, and sends $\{g_0^c, Aut_1\}$ to the AP. (2) Upon receipt of $\{g_0^c, Aut_1\}$, the AP uses current to SK_j compute a verification code $Ver_1 = H(SK_j \parallel g_0^c)$ and compares it with Aut_1. If Ver_1 does not match Aut_1, the AP rejects session key update; otherwise, the AP concludes that the message is from MN_i. Then the AP randomly picks $d \in Z_p^*$, computes

$$g_0^d, SK_{j+1} = \left(g_0^c\right)^d,$$
$$Aut_2 = H\left(SK_{j+1}, g_0^c, g_0^d\right). \tag{19}$$

and erases d from its memory. Finally, AP transmits $\{g_0^d, Aut_2\}$ to MN_i. (3) Upon receiving the message from the AP, MN_i computes $SK'_{j+1} = (g_0^d)^c$, generates a verification code $Ver_2 = H(SK'_{j+1}, g_0^c, g_0^d)$, and compares it with Aut_2. If Ver_2 matches Aut_2, MN_i erases c from its memory and believes that they have established a new session key SK_{j+1}; otherwise, MN_i rejects session key update.

Revocation. The detailed revocation check is described as follows. (1) The AS generates a revocation list RL_j which consists of revocation information corresponding to ts_j and transmits it to every AP along with secret key rk_i corresponding to the revoked user. This can prevent the revoked user access to the network. (2) Upon acquiring RL_j, each AP updates $\beta_{i,j-1}$ as follows: for any $\beta_{i,j-1} \in RL_{j-1}$, $\beta_{i,j} = \overline{H}_{rk_i}(\beta_{i,j-1})$. Then AP stores both RL_{j-1} and RL_j in its database. (3) During the handover authentication procedure, upon receipt of $\{msg, \sigma_i\}$, the AP parses the revocation information $\beta_{i,j}$ and checks whether it is in the revocation list RL_j. If $\beta_{i,j}$ is in RL_j, the user is revoked. As a result, the handover request is rejected. Otherwise, the protocol performs next steps sequentially.

5. Security Analysis and Performance Evaluation

5.1. Security Analysis. We present the security analysis of the proposed protocol to check whether it achieves the security goal mentioned in Section 2.

Mutual Authentication. On one hand, AP authentication is ensured by the challenge-response pair $msg, ECDSA.Sig(rmsg, sk_j)$. Due to the security of digital signature, only AP_j that has sk_j can generate a valid signature on a fresh challenge g_0^a from MN_i. If the signature passes the verification $ECDSA.Ver(\cdot)$, it will demonstrate the AP is a trusted valid entity. On the other hand, the designed ABS scheme provides user authentication. Only the user that has the right key on right attribute list (satisfying the access structure) could generate the valid signature. In other words, a malicious node could neither impersonate a valid node nor pass the authentication. Therefore, the proposed protocol achieves mutual authentication.

Key Establishment. As described in protocol, MN_i and AP_j, respectively, use g_0^a and g_0^b to complete DH key establishment. On one hand, MN_i figures out $(g_0^b)^a$. On the other hand, AP_j figures out $(g_0^a)^b$. Obviously, $(g_0^b)^a = (g_0^a)^b$. As a result, both compute the session key $SK = g_0^{ab}$. Besides, any adversary could not calculate the secret session key due to the CDH problem.

User Anonymity and Nontraceability. Due to the outstanding property of attribute-based signature, the identity information is not contained in the transmitted message in the whole handover authentication procedure. So except for the AS, nobody could tell the identity of the user including the AP. In addition, the request message msg does not contain any specific privacy information of the MN except for the revocation information $\beta_{i,j}$. Since $\beta_{i,j}$ is a secure hash value, an adversary could not parse the identity of a user or trace the user. So user anonymity and nontraceability are guaranteed.

User Revocation. Once the revocation hash value $\beta_{i,j}$ of MN_i exists in the revocation list RL_j with ts_j, it will exist in the database in the future due to update technique of the AP. If $\beta_{i,j}$ exists in RL_j, it means MN_i is revoked since the time ts_j, and as a result the authentication fails.

Updating Session Key Periodically. As described in session key update phase, the MN and AP could establish a new session key successfully according to the current session key. In detail, The MN and AP leverage a new Diffie-Hellman key establishment procedure to generate a new session key. This is based on the hard DL problem and CDH problem. Once a new session key is established, the previous one is destroyed

Table 1: Security comparisons of four protocols.

	P1	P2	P3	P4	P5	P6
He et al.'s protocol [9]	No	No	No	No	Yes	No
He et al.'s protocol [14]	Yes	No	No	No	Yes	No
Xie et al.'s protocol [19]	Yes	No	No	No	Yes	No
Our protocol	Yes	Yes	Yes	Yes	Yes	Yes

P1, P2, P3, P4, P5, and P6 denote mutual authentication, user anonymity with nontraceability, session key update, conditional privacy preserving, session key establishment, and user revocation, respectively.

securely, so that adversaries could not reveal the new session key.

Besides, the protocol could prevent replay attack due to timestamp. It is important that only the AS could find the real identity of a user according to $\beta_{i,j} = \overline{H}_{rk_i}(\mathrm{ID}_i)$ since rk_i is selected for MN_i by the AS. So the protocol achieves conditional privacy preservation too.

For convenience, we let P1, P2, P3, P4, P5, and P6 denote mutual authentication, user anonymity with nontraceability, session key update, conditional privacy preserving, session key establishment, and user revocation, respectively. Security comparisons between our protocol and 3 other protocols are presented in Table 1. In general, our protocol meets all the security requirements in the table while the other 3 protocols more or less have some security vulnerability. All protocols could guarantee session key establishment but only ours adds the session key update technique. Except for our protocol, the other 3 protocols do not meet the requirements of conditional privacy preserving and user revocation. Moreover, they neither achieve user anonymity nor achieve nontraceability, so that our protocol has an obvious advantage of security.

Note that our protocol has a nice exclusive property that it can achieve fine-grained access control due to the attribute-based cryptography. For example, the AP can provide better service for specific users by indicating a required access structure, so that only the user with right attribute list can enjoy the service.

5.2. Performance Evaluation. Although signal transmission also affects handover delay, in view of high speed rate of WLAN and only 3 interaction messages involved in our proposed protocol, we only discuss the authentication latency determined by the time of computation cost. We compare the computation cost of our protocol with that of some other protocols. For more reasonable simulation, we cross-compile the Pair-Based Cryptography (PBC) Library (version pbc-0.5.14) so that related cryptographic operations could be performed on mobile devices. We let a smart phone (HUAWEI honor 5C) and a personal computer (Acer) act as a MN and an AP, respectively, and select the type A pairing in PBC library as the bilinear pairing. Device information is listed in Table 2 and Table 3 presents time consumption of different operations on MN and AP. Note that we ignore the light cryptographic operations such as general hash operations. But one type of hash operation, called map-to-point (denoted as MTP in Table 3) hash operation, is not a lightweight cryptographic operation. To some extent, its time consumption can be compared with the pairing operation. Table 4 gives the performance comparison between our protocol and related works, where the time data in parentheses is calculated on the basis of data in Table 3.

Table 2: Device configurations.

	Processor	Frequency	Memory	Operation system
HUAWEI	Kirin 650	2.0 GHz	2 GB	Android 6.0
Acer	Core I5 2430M	2.4 GHz	4 GB	Ubuntu 14.04

Table 3: Time consumption of different operations (in ms).

	BP	ME	ECSM	MTP
AP	3.778	0.465	3.180	7.254
MN	8.587	1.270	5.515	13.110

BP: bilinear pairing; ME: modular exponentiation; ECSM: elliptic curve scalar multiplication; MTP: map-to-point.

As presented, our protocol does not have much computation cost which means it is feasible. There is no heavy cryptographic operation, such as pairing and map-to-point operation, on the MN side. Our protocol has lower computation cost on both the MN side and AP side.

6. Conclusions and Future works

In this paper, we summarize the security requirements a handover authentication protocol should meet. After reviewing previous ID-based protocols in recent years, we point out that they have some vulnerability to some extent. We design an ABS scheme based on which we present an anonymous handover authentication protocol. Security analysis demonstrates our proposed protocol meets various security requirements, especially inherent anonymity with attribute-based cryptography. What is more, concrete experiments on a smart phone and a personal computer show that our proposed protocol is practical in mobile wireless networks.

Our proposed protocol achieves user revocation property. Besides, attribute revocation could provide more flexible access control. If an attribute is revoked, the secret key corresponding to it is no longer valid. What a pity, to achieve attribute revocation, computation cost will be high. The new protocol does not involve this property. Therefore, our work focus is to achieve attribute revocation with light computation cost. Note that access structure in our proposed protocol is as simple as a single AND gate. It is also our future work to introduce more complex access structure into

Table 4: Evaluation of computation cost (in ms).

	MN	AP
He et al.'s protocol [9]	2MTP + BP + ECSM = 40.322	MTP + 3BP + ECSM = 21.768
He et al.'s protocol [14]	MTP + BP + 3ECSM = 38.242	MTP + 4BP = 22.366
Xie et al.'s protocol [19]	3ECSM = 16.545	6ECSM = 19.080
Our protocol	5ME + ECSM = 11.865	2ME + 2BP + ECSM = 11.666

authentication protocols in order to realize more fine-grained access control.

Conflicts of Interest

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

Acknowledgments

This work is supported by National Key Research Program of China (2016YFB0800101, 2016YF0800100) and Innovative Research Groups of the National Natural Science Foundation of China (Grant no. 61521003).

References

[1] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 28–35, 2015.

[2] A. Fu, G. Zhang, Y. Yu, and Z. Zhu, "A privacy preserving vertical handover authentication scheme for WiMAX-WiFi networks," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 9, pp. 3250–3265, 2014.

[3] A. Kumar and H. Om, "A Secure Seamless Handover Authentication Technique for Wireless LAN," in *Proceedings of the 14th International Conference on Information Technology, ICIT 2015*, pp. 43–47, India, December 2015.

[4] Q. Jiang, Z. Chen, B. Li, J. Shen, L. Yang, and J. Ma, "Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems," *Journal of Ambient Intelligence and Humanized Computing*.

[5] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[6] D. Wang and P. Wang, "Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound," *IEEE Transactions on Dependable and Secure Computing*, pp. 1-1.

[7] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, 2016.

[8] D. Wang, H. Cheng, D. He, and P. Wang, "On the Challenges in Designing Identity-Based Privacy-Preserving Authentication Schemes for Mobile Devices," *IEEE Systems Journal*, pp. 1–10.

[9] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 48–53, 2012.

[10] D. He, C. Chen, S. Chan, and J. Bu, "Analysis and improvement of a secure and efficient handover authentication for wireless networks," *IEEE Communications Letters*, vol. 16, no. 8, pp. 1270–1273, 2012.

[11] S. L. Yeo, W.-S. Yap, J. K. Liu, and M. Henricksen, "Comments on analysis and improvement of a secure and efficient handover authentication based on bilinear pairing functions," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1521–1523, 2013.

[12] J.-L. Tsai, N.-W. Lo, and T.-C. Wu, "Secure handover authentication protocol based on bilinear pairings," *Wireless Personal Communications*, vol. 73, no. 3, pp. 1037–1047, 2013.

[13] W. Wang and L. Hu, "A secure and effcient handover authentication protocol for wireless networks," *Sensors*, vol. 14, no. 7, pp. 11379–11394, 2014.

[14] D. He, M. K. Khan, and N. Kumar, "A new handover authentication protocol based on bilinear pairing functions for wireless networks," *International Journal of Ad Hoc & Ubiquitous Computing*, vol. 18, 2015.

[15] D. He, D. Wang, Q. Xie, and K. Chen, "Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation," *Science China Information Sciences*, vol. 60, no. 5, Article ID 052104, 2017.

[16] L. Liu, H. Quan, X. Liu, and Y. Zhang, "Lightweight handover authentication with location privacy-preserving in mobile wireless networks," *International Journal of Embedded Systems*, vol. 7, no. 3-4, pp. 280–288, 2015.

[17] G. Li, Q. Jiang, F. Wei, and C. Ma, "A New Privacy-Aware Handover Authentication Scheme for Wireless Networks," *Wireless Personal Communications*, vol. 80, no. 2, pp. 581–589, 2014.

[18] S. A. Chaudhry, M. S. Farash, H. Naqvi, S. H. Islam, and T. Shon, "A Robust and Efficient Privacy Aware Handover Authentication Scheme for Wireless Networks," *Wireless Personal Communications*, vol. 93, no. 2, pp. 311–335, 2017.

[19] Y. Xie, L. Wu, N. Kumar, and J. Shen, "Analysis and Improvement of a Privacy-Aware Handover Authentication Scheme for Wireless Network," *Wireless Personal Communications*, vol. 93, no. 2, pp. 523–541, 2017.

[20] X. Yang, X. Huang, and J. K. Liu, "Efficient handover authentication with user anonymity and untraceability for Mobile Cloud Computing," *Future Generation Computer Systems*, vol. 62, pp. 190–195, 2016.

[21] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," *IEEE Transactions on Wireless Communications*, vol. 10, no. 2, pp. 431–436, 2011.

[22] H. Kwon, D. Kim, C. Hahn, and J. Hur, "Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks," *Multimedia Tools and Applications*, vol. 76, no. 19, pp. 19507–19521, 2017.

[23] X. Ansi, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 1999.