SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

May 2017, Vol. 60 052104:1–052104:17
doi: 10.1007/s11432-016-0161-2

Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation

Debiao HE[1,2*], Ding WANG[3], Qi XIE[4] & Kefei CHEN[4]

[1]*State Key Laboratory of Software Engineering, Computer School, Wuhan University, Wuhan* 430072*, China;*
[2]*State Key Laboratory of Cryptology, Beijing* 100878*, China;*
[3]*School of Electronics Engineering and Computer Science, Peking University, Beijing* 100871*, China;*
[4]*Hangzhou Key Laboratory of Cryptography and Network Security,*
Hangzhou Normal University, Hangzhou 311121*, China*

Received March 9, 2016; accepted June 3, 2016; published online November 14, 2016

Abstract With the development of the wireless communication technology and the popularity of mobile devices, the mobile wireless network (MWN) has been widely used in our daily life. Through the access point (AP), users could access the Internet anytime and anywhere using their mobile devices. Therefore, MWNs can bring much convenience to us. Due to the limitation of AP's coverage, the seamless handover frequently occurs in practical applications. How to guarantee the user's privacy and security and identify the real identity when he/she brings harm to the system becomes very challenging. To achieve such goals, many anonymous handover authentication (AHA) protocols have been proposed in the last several years. However, most of them have high computation costs because mobile nodes need to carry out the bilinear pairing operations or the hash-to-point operations. Besides, most of them cannot satisfy some critical requirements, such as non-traceability and perfect forward secrecy. In this paper, we first outline the security requirements of AHA protocols, and then propose a new AHA protocol to eliminate weaknesses existing in previous AHA protocols. Based on the hardness of two famous mathematical problems, we demonstrate that the proposed AHA protocol is secure against different kinds of attacks and can meet a variety of security requirements. It can be seen from the details of implementations that the proposed AHA protocol also has much less computation cost than three latest AHA protocols.

Keywords mobile wireless network, handover authentication, anonymity, conditional privacy preservation, provable security

Citation He D B, Wang D, Xie Q, et al. Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation. Sci China Inf Sci, 2017, 60(5): 052104, doi: 10.1007/s11432-016-0161-2

1 Introduction

With the popularity of mobile devices in our daily life, we would like to process more and more transactions using mobile applications installed in mobile devices through the mobile wireless network (MWN). Subsequently, MWNs attract a lot of attention from both academia and industry [1, 2]. The MWN consists of a number of mobile nodes (MNs), a lot of access points (APs) and an authentication server (AS),

* Corresponding author (email: hedebiao@163.com)

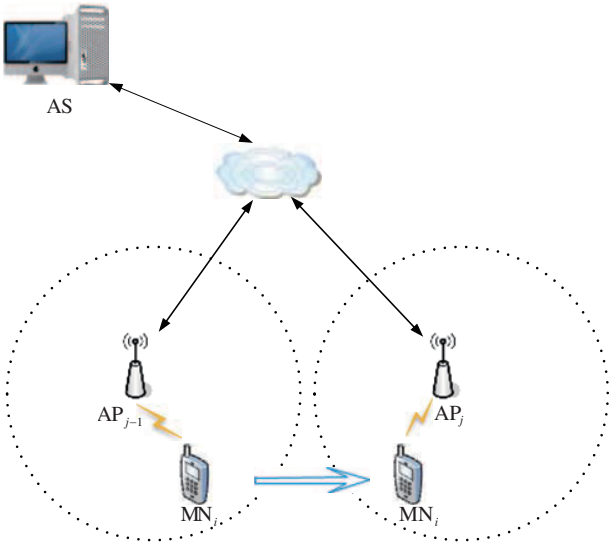

Figure 1 (Color online) A typical scenario of handover.

where MNs (such as mobile phones and laptops) have limited resources (such as storage, computation and communication capabilities) [3–5] and APs have powerful resources.

Because of the movement of MNs and the limited geographical coverage of APs, the handover occurs frequently when we enjoy services provided by MWNs. To guarantee only registered MNs access MWNs and stop illegal access from the adversaries, some security tools are required urgently to implement secure handover. The anonymous handover authentication (AHA) protocol is very suitable for achieving this goal because it could get mutual authentication between MN and AP and produce a session key for secure communication between them [6, 7]. Regardless of the details of implementation, a typical scenario of the handover is demonstrated in Figure 1.

Assume the ith mobile node MN_i leaves the geographical coverage of the current access point AP_{j-1} and enters in the geographical coverage of the new access point AP_j. In this scenario, the AHA protocol should be executed by MN_i and AP_j. If the handover authentication between them is executed successfully, MN_i is allowed to access MWNs through AP_j, at the same time they generate a new session key to protect their private communication in wireless channel; otherwise, AP_j rejects MN_i's access request.

To design an efficient and secure AHA protocol for MWN, three challenges should be considered carefully. First, the AHA protocol should have lightweight computation and communication costs at the side of the mobile side because it has limited computation and communication capabilities. Second, the AHA protocol should have high security level because the openness of wireless communication results in more various attacks. At last, the AHA protocol should provide privacy protection because the leakage of privacy information may result in serious crimes. To ensure secure communication in MWNs, many AHA protocols have been put forward in the last several years.

1.1 Related work

AHA protocol can be implemented using the traditional public key cryptography (TPKC) based on the public key infrastructure (PKI) [8]. Choi and Jung [9] proposed an AHA protocol using TPKC for MWNs. Later, several AHA protocols using TPKC were proposed to improve performance [10–12]. In those AHA protocols [9–12], each participant has a certificate to bind its identity and public key, where the certificate is produced by a trusted third party called the certificate authority (CA). However, those AHA protocols suffer from the following three weaknesses: (1) CA has to put extra effort to store, maintain and update those certificates. The task becomes more and more difficult with the increase of participants' number. (2) MN and AP have to verify the validity of the other party's certificate. This results in great increase of MN and AP's computation cost. (3) MN and AP transmit their certificates to each other in the process of handover authentication. This results in great increase of MN and AP's communication cost.

To solve above problems, a lot of AHA protocols using the identity-based public key cryptography were proposed in the last several years. The identities of MN and AP in those protocols [13–21] are their public keys and the corresponding private keys are generated by AS according to their identities. Therefore, no certificate is needed in such protocols. He et al. [13] proposed the first AHA protocol for MWNs using the identity-based public key cryptography. Compared with previous protocols, He et al.'s AHA protocol has much better performance. However, He et al. found that their AHA protocol suffers from the key compromised problem, i.e., the adversary could extract MN's private key using the intercepted message [14]. They also proposed a simple countermeasure to solve the serious problem. Unfortunately, Yeo et al. [15] pointed out that He et al.'s improved AHA protocol [14] still suffers from the key compromised problem. However, Yeo et al. did not give any countermeasure to address the problem.

Li et al. [19] presented an efficient AHA protocol using the elliptic curve cryptography (ECC). Unfortunately, Xie et al. [20] pointed out that Li et al.'s AHA protocol is not secure against the impersonation attack. To address the serious security weakness, Xie et al. proposed an improved AHA protocol using ECC. Later, Fu et al. [21] presented a new AHA protocol to stop the malicious server extracting the user's identity. However, the three AHA protocols [19–21] do not support batch verification and are not suitable for practical applications.

To improve security, Tsai et al. [16] proposed a new AHA protocol using the bilinear pairing. Wang and Hu [17] proposed a valid attack to show that He et al.'s protocol [14] suffers from the key compromised problem. To enhance security, Wang and Hu [17] also presented an improved AHA protocol. Recently, we also proposed a new attack again He et al.'s AHA protocol to show their protocol suffers from the key compromised problem and proposed an improved AHA protocol to enhance security [18].

Although the above AHA protocols [13–18] can address problems existing in traditional AHA protocols, they still have the following weaknesses: (1) The performance of those protocols is not satisfactory because some very complicated operations (such as bilinear pairing operation) are carried out by the mobile nodes. (2) The security of those protocols is not strong enough because the adversary can retrieve all previous session keys once he has got MN or AP's private key. (3) A very large storage space is needed by the user's mobile device because multiple pseudo-identities and corresponding private keys should be stored to ensure the user's anonymity. (4) The adversary can track the user's behavior according to the constant pseudo-identity used in the process of handover authentication.

1.2 Our contribution

To solve problems existing in previous AHA protocols based on identity-based public key cryptography, we propose a new AHA protocol with provable security. Compared with related AHA protocols, the proposed AHA protocol has much less computation cost at MN's side and has better security attributes at the cost of increasing communication cost slightly. To be specific, the major contributions of this paper are threefold.

- First, we outline the security requirements of the AHA protocol for MWNs, and propose a new AHA protocol for MWNs with batch verification.
- Second, we present a detailed security analysis of the proposed AHA protocol to demonstrate that it is secure and can meet security requirements.
- Finally, we present an analysis of the computation cost of the proposed AHA protocol and related AHA protocols to demonstrate that it has better performance.

1.3 Organization of the paper

The remainder content of this paper is summarized as below. We present the background of the bilinear pairing, network model, and security and function requirements in Section 2. The proposed AHA protocol is presented in Section 3. We present the security analysis and the performance evaluation of the proposed AHA protocol in Sections 4 and 5 respectively. We make the conclusion in Section 6.

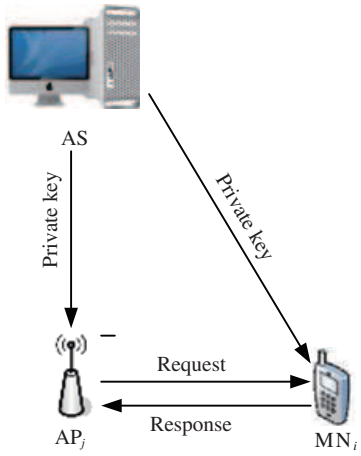

Figure 2 (Color online) The network model.

2 Preliminaries

2.1 Bilinear pairing

Let G_1 be an additive group with the prime order q and a generator P. Let G_2 be a multiplicative group with the same order. We say a map $e : G_1 \times G_1 \to G_2$ is a bilinear pairing if it satisfies the following three conditions:

(1) **Bilinear.** For any two random elements $Q, R \in G_1$ and any two random elements $a, b \in Z_q^*$, we have $e(a \cdot Q, b \cdot R) = e(Q, R)^{a \cdot b}$.

(2) **Non-degeneracy.** There is an element $Q \in G_1$ such that $e(Q, Q) \neq 1_{G_2}$.

(3) **Computability.** For any two random elements $Q, R \in G_1$, $e(Q, R)$ can be calculated efficiently.

It is well known that no probabilistic polynomial time algorithm can solve the following mathematical problems.

Discrete logarith (DL) problem. Given $x \cdot P \in G_1$ ($g^x \in G_2$), the task of the DL problem is computing $x \in Z_q^*$, where x is an unknown number.

Computational Diffie-Hellman (CDH) problem. Given $x \cdot P, y \cdot P \in G_1$ ($g^x, g^y \in G_2$), the task of the CDH problem is computing $x \cdot y \cdot P \in G_1$ ($g^{x \cdot y} \in G_2$), where $x, y \in Z_q^*$ are two unknown numbers.

Modified bilinear inverse Diffie-Hellman with k values (k-mBIDH) problem [22]**.** Given $P, y \cdot P \in G_1, z \cdot P \in G_1$, $\alpha_1, \alpha_2, \ldots, \alpha_k \in Z_q^*$, $\frac{1}{y+\alpha_1} \cdot P, \frac{1}{y+\alpha_2} \cdot P, \ldots, \frac{1}{y+\alpha_k} \cdot P$, the task of the k-mBIDH problem is computing $e(P, P)^{\frac{z}{y+\alpha}}$ for some $\alpha \notin \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$.

2.2 Network model

We consider the network model shown in Figure 2 for an AHA protocol for MWNs. There are three participants in the network model: the authentication server AS, the ith mobile node MN$_i$ and the jth access point AP$_j$.

AS. It denotes a trusted third party and is responsible for generating system parameters and private keys of MN$_i$ and AP$_j$.

MN$_i$. It denotes a mobile device equipped with wireless communication module, through which the user could access MWNs wirelessly.

AP$_j$. It denotes an access point connected to the Internet, through which MN$_i$ could access MWNs and enjoy a lot of services.

In the system setup phase, AS generates the systems parameters and the private keys of MN$_i$ and AP$_j$ according to their identities. Then, MN$_i$ and AP$_j$ can authenticate the other participant and shared a session key using their private keys.

2.3 Security requirements

The adversary in MWNs is able to control the communication channel between MN_i and AP_j easily because they exchange messages wirelessly [5, 23, 24]. To guarantee secure communication, the AHA protocol should be able to satisfy some security and function attributes and withstand various attacks. Based on previous work, we summarize that a AHA protocol should meet the following security requirements [12, 13, 16–18].

(1) **Mutual authentication.** To guarantee only authorized users could access Internet services through MWNs, a AHA protocol should provide mutual authentication between MN_i and AP_j.

(2) **User anonymity.** To protect the user's privacy, a AHA protocol should be able to provide user anonymity, i.e., the adversary including the malicious access point cannot extract MN_i's real identity through intercepted messages.

(3) **Non-traceability.** To protect the user's location privacy, a AHA protocol should be able to provide non-traceability, i.e., the adversary including the malicious access point cannot trace MN_i's behavior.

(4) **Conditional privacy preservation.** To punish the user when he/she brings some harm to MWNs, a AHA protocol should be able to provide conditional privacy preservation, i.e., only the authentication server can extract MN_i's real identity.

(5) **Session key establishment.** To share private key for secure communication, a AHA protocol should be able to provide session key establishment, i.e., a session key is generated between MN_i and AP_j after executing the protocol.

(6) **Perfect forward secrecy.** To protect the security of the session key, a AHA protocol should be able to provide perfect forward secrecy, i.e., the adversary cannot extract the session key produced in previous session even he/she gets both private keys of MN_i and AP_j.

(7) **Attack resistance.** Due to the open environment, the handover authentication protocol is susceptible to various attacks such as the impersonation attack, the replay attack, the modification attack, the stolen verifier table attack and the man-in-the-middle attack [25–29]. To ensure secure communication in MWNs, it is required that a handover authentication protocol should be able to withstand those aforementioned attacks.

3 The proposed anonymous handover authentication protocol

Based on He et al.'s authentication protocol for multi-server architectures [30] and Shim's authentication protocol for vehicular sensor networks [31], we construct a new AHA protocol for MWNs to address problems existing in previous AHA protocols.

There are three participants in the proposed AHA protocol, i.e., a mobile node MN_i, an access point AP_j and the authentication server AS. The proposed AHA protocol consists of five phases: the system initialization phase, the mobile node registration phase, the access point registration phase, the handover authentication phase and the batch verification phase. The details of those phases are presented as follows.

3.1 System initialization phase

In this phase, AS produces the system parameters and the system private key. The following steps are carried out in this phase.

(1) AS selects a large prime number q, an additive group G_1 with the order q and a multiplicative group G_2 with the same order.

(2) AS selects two generator P, Q of the group G_1, a bilinear pairing $e : G_1 \times G_1 \to G_2$ and computes $g = e(P, P)$.

(3) AS selects two random numbers $x, y \in Z_q^*$, computes $P_X = x \cdot P, P_Y = y \cdot P$ and sets $\{P_X, P_Y\}$ as the system public key.

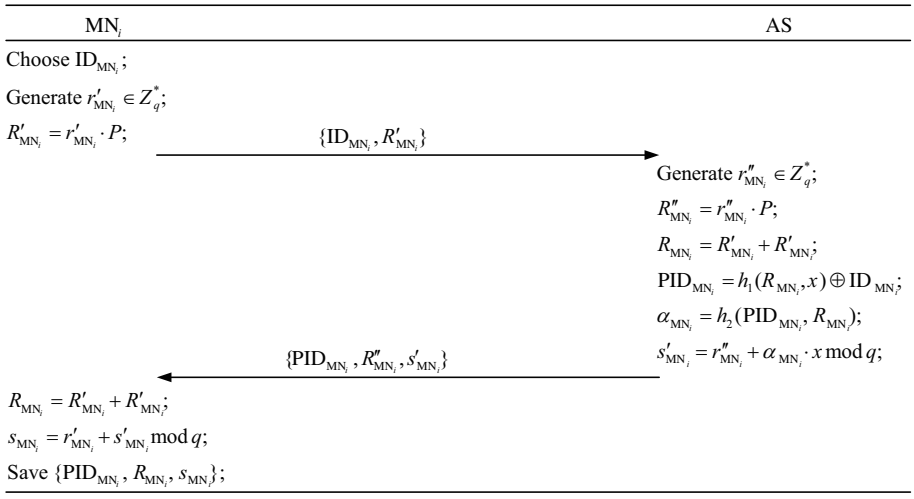

Figure 3 Mobile node registration phase.

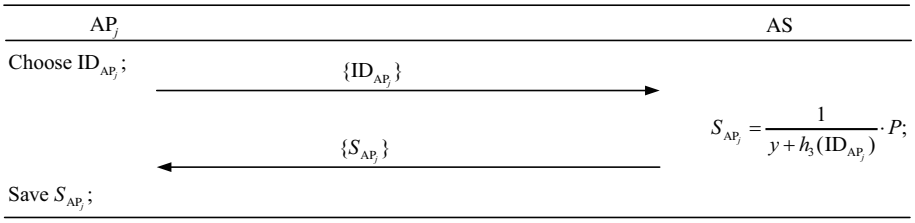

Figure 4 Access point registration phase.

(4) AS selects seven secure hash functions $\hat{h}, h_1, \ldots, h_6$, where $\hat{h} : \{0,1\} \to \{0,1\}^l$ and $h_i : \{0,1\} \to Z_q^*(i = 1, \ldots, 6)$.

(5) AS publishes the system parameters $\{q, G_1, G_2, P, Q, g, P_X, P_Y, H, \hat{h}, h_1, \ldots, h_6\}$ and saves the system private key $\{x, y\}$ securely.

3.2 Mobile node registration phase

In this phase, MN_i with the identity $\mathrm{ID}_{\mathrm{MN}_i}$ registers in AS to get its private key. Figure 3 shows the steps which should be executed in this phase.

(1) MN_i picks its identity $\mathrm{ID}_{\mathrm{MN}_i}$, chooses a random number $r'_{\mathrm{MN}_i} \in Z_q^*$, computes $R'_{\mathrm{MN}_i} = r'_{\mathrm{MN}_i} \cdot P$ and sends $\{\mathrm{ID}_{\mathrm{MN}_i}, R'_{\mathrm{MN}_i}\}$ identity to AS.

(2) AS picks a random number $r''_{\mathrm{MN}_i} \in Z_q^*$ and computes $R''_{\mathrm{MN}_i} = r''_{\mathrm{MN}_i} \cdot P$, $R_{\mathrm{MN}_i} = R'_{\mathrm{MN}_i} + R''_{\mathrm{MN}_i}$, $\mathrm{PID}_{\mathrm{MN}_i} = h_1(R_{\mathrm{MN}_i}, x) \oplus \mathrm{ID}_{\mathrm{MN}_i}$, $\alpha_{\mathrm{MN}_i} = h_2(\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i})$ and $s'_{\mathrm{MN}_i} = r''_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i} \cdot x \bmod q$. At last, AS sends $\{\mathrm{PID}_{\mathrm{MN}_i}, R''_{\mathrm{MN}_i}, s'_{\mathrm{MN}_i}\}$ to MN_i through a secure channel.

(3) MN_i computes $R_{\mathrm{MN}_i} = R'_{\mathrm{MN}_i} + R''_{\mathrm{MN}_i}$, $s_{\mathrm{MN}_i} = r'_{\mathrm{MN}_i} + s'_{\mathrm{MN}_i} \bmod q$ and saves $\{\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, s_{\mathrm{MN}_i}\}$ secretly.

3.3 Access point registration phase

In this phase, AP_j with the identity $\mathrm{ID}_{\mathrm{AP}_j}$ registers in AS to get its private key. Figure 4 shows the steps which should be executed in this phase.

(1) AP_j sends its identity $\mathrm{ID}_{\mathrm{AP}_j}$ to AS.

(2) AS computes $S_{\mathrm{AP}_j} = \frac{1}{y + h_3(\mathrm{ID}_{\mathrm{AP}_j})} \cdot P$. At last, AS sends $\{S_{\mathrm{AP}_j}\}$ to AP_j through a secure channel.

(3) AP_j keeps $\{S_{\mathrm{AP}_j}\}$ secretly.

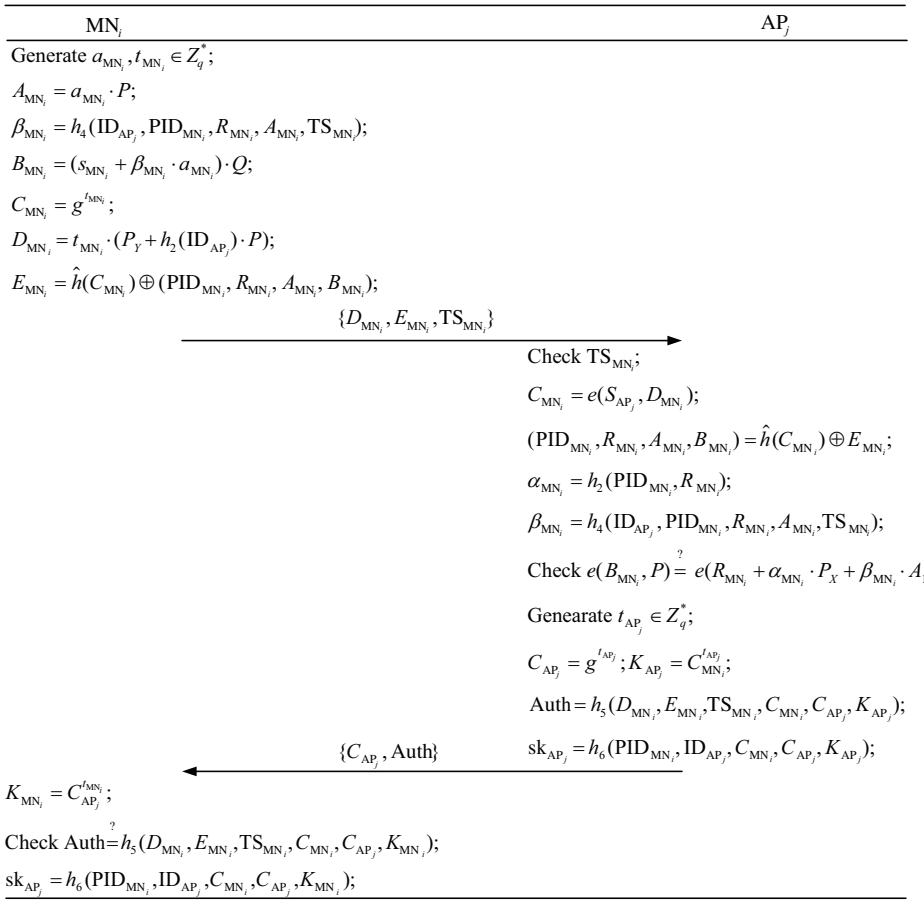

Figure 5 Handover authentication phase.

3.4 Handover authentication phase

In this phase, MN_i with the identity $\mathrm{ID}_{\mathrm{MN}_i}$ moves into the coverage of AP_j with the identity $\mathrm{ID}_{\mathrm{AP}_j}$, they will authenticate the other participant and produce a session key for secure communication between them. Figure 5 shows the steps which should be executed in this phase.

(1) MN_i selects two random numbers $a_{\mathrm{MN}_i}, t_{\mathrm{MN}_i} \in Z_q^*$ and computes $A_{\mathrm{MN}_i} = a_{\mathrm{MN}_i} \cdot P$, $\beta_{\mathrm{MN}_i} = h_4(\mathrm{ID}_{\mathrm{AP}_j}, \mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i})$, $B_{\mathrm{MN}_i} = (s_{\mathrm{MN}_i} + \beta_{\mathrm{MN}_i} \cdot a_{\mathrm{MN}_i}) \cdot Q$, $C_{\mathrm{MN}_i} = g^{t_{\mathrm{MN}_i}}$, $D_{\mathrm{MN}_i} = t_{\mathrm{MN}_i} \cdot (P_Y + h_3(\mathrm{ID}_{\mathrm{AP}_j}) \cdot P)$ and $E_{\mathrm{MN}_i} = \hat{h}(C_{\mathrm{MN}_i}) \oplus (\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, B_{\mathrm{MN}_i})$, where $\mathrm{TS}_{\mathrm{MN}_i}$ is the current timestamp. At last, MN sends the login message $\{D_{\mathrm{MN}_i}, E_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$ to AP_j.

(2) After receiving the login message $\{D_{\mathrm{MN}_i}, E_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$, AP checks if $\mathrm{TS}_{\mathrm{MN}_i}$ is fresh. If not, AP_j rejects the process; otherwise, AP_j computes $C_{\mathrm{MN}_i} = e(S_{\mathrm{AP}_j}, D_{\mathrm{MN}_i})$, $(\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, B_{\mathrm{MN}_i}) = \hat{h}(C_{\mathrm{MN}_i}) \oplus E_{\mathrm{MN}_i}$, $\alpha_{\mathrm{MN}_i} = h_1(\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i})$ and $\beta_{\mathrm{MN}_i} = h_4(\mathrm{ID}_{\mathrm{AP}_j}, \mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i})$. AP_j checks if $e(B_{\mathrm{MN}_i}, P)$ and $e(R_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i} \cdot P_X + \beta_{\mathrm{MN}_i} \cdot A_{\mathrm{MN}_i}, Q)$ are equal. If not, AP_j rejects the session; otherwise, AP_j selects a random number $t_{\mathrm{AP}_j} \in Z_q^*$ and computes $C_{\mathrm{AP}_j} = g^{t_{\mathrm{AP}_j}}$, $K_{\mathrm{AP}_j} = C_{\mathrm{MN}_i}^{t_{\mathrm{AP}_j}}$, $\mathrm{Auth} = h_5(D_{\mathrm{MN}_i}, E_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}, C_{\mathrm{MN}_i}, C_{\mathrm{AP}_j}, K_{\mathrm{AP}_j})$ and $\mathrm{sk}_{\mathrm{AP}_j} = h_6(\mathrm{PID}_{\mathrm{MN}_i}, \mathrm{ID}_{\mathrm{AP}_j}, C_{\mathrm{MN}_i}, C_{\mathrm{AP}_j}, K_{\mathrm{AP}_j})$. At last, AP_j sends $\{C_{\mathrm{AP}_j}, \mathrm{Auth}\}$ to MN_i.

(3) After receiving the response message $\{C_{\mathrm{AP}_j}, \mathrm{Auth}\}$, MN computes $K_{\mathrm{MN}_i} = C_{\mathrm{AP}_j}^{t_{\mathrm{MN}_i}}$ and checks if the equation $\mathrm{Auth} = h_5(D_{\mathrm{MN}_i}, E_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}, C_{\mathrm{MN}_i}, C_{\mathrm{AP}_j}, K_{\mathrm{MN}_i})$ holds. If not, AP_j rejects the process; otherwise, MN computes the session key $\mathrm{sk}_{\mathrm{MN}_i} = h_6(\mathrm{PID}_{\mathrm{MN}_i}, \mathrm{ID}_{\mathrm{AP}_j}, C_{\mathrm{MN}_i}, C_{\mathrm{AP}_j}, K_{\mathrm{MN}_i})$.

Due to $P_X = x \cdot P$, $P_Y = y \cdot P$, $R'_{\mathrm{MN}_i} = r'_{\mathrm{MN}_i} \cdot P$, $R''_{\mathrm{MN}_i} = r''_{\mathrm{MN}_i} \cdot P$, $R_{\mathrm{MN}_i} = R'_{\mathrm{MN}_i} + R''_{\mathrm{MN}_i}$, $s'_{\mathrm{MN}_i} = r''_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i} \cdot x \bmod q$, $s_{\mathrm{MN}_i} = r'_{\mathrm{MN}_i} + s'_{\mathrm{MN}_i} \bmod q$, $S_{\mathrm{AP}_j} = \frac{1}{y + h_3(\mathrm{ID}_{\mathrm{AP}_j})} \cdot P$, $A_{\mathrm{MN}_i} = a_{\mathrm{MN}_i} \cdot P$, $B_{\mathrm{MN}_i} = (s_{\mathrm{MN}_i} + \beta_{\mathrm{MN}_i} \cdot a_{\mathrm{MN}_i}) \cdot Q$, $C_{\mathrm{MN}_i} = g^{t_{\mathrm{MN}_i}}$, $D_{\mathrm{MN}_i} = t_{\mathrm{MN}_i} \cdot (P_Y + h_2(\mathrm{ID}_{\mathrm{AP}_j}) \cdot P)$ and $C_{\mathrm{AP}_j} = g^{t_{\mathrm{AP}_j}}$,

we can get the following three equations:

$$\begin{aligned} e(S_{\mathrm{AP}_j}, D_{\mathrm{MN}_i}) &= e\bigg(\frac{1}{y+h_3(\mathrm{ID}_{\mathrm{AP}_j})}\cdot P, t_{\mathrm{MN}_i}\cdot(P_Y + h_3(\mathrm{ID}_{\mathrm{AP}_j})\cdot P)\bigg) \\ &= e\bigg(\frac{1}{y+h_3(\mathrm{ID}_{\mathrm{AP}_j})}\cdot P, t_{\mathrm{MN}_i}\cdot(y\cdot P + h_3(\mathrm{ID}_{\mathrm{AP}_j})\cdot P)\bigg) \\ &= e(P,P)^{\frac{1}{y+h_2(\mathrm{ID}_{\mathrm{AP}_j})}\cdot t_{\mathrm{MN}_i}\cdot(y+h_3(\mathrm{ID}_{\mathrm{AP}_j}))} \\ &= g^{t_{\mathrm{MN}_i}} = C_{\mathrm{MN}_i}, \end{aligned} \tag{1}$$

$$\begin{aligned} e(B_{\mathrm{MN}_i}, P) &= e((s_{\mathrm{MN}_i} + \beta_{\mathrm{MN}_i}\cdot a_{\mathrm{MN}_i})\cdot Q, P) \\ &= e((s_{\mathrm{MN}_i} + \beta_{\mathrm{MN}_i}\cdot a_{\mathrm{MN}_i})\cdot P, Q) \\ &= e((r'_{\mathrm{MN}_i} + s'_{\mathrm{MN}_i} + \beta_{\mathrm{MN}_i}\cdot a_{\mathrm{MN}_i})\cdot P, Q) \\ &= e((r'_{\mathrm{MN}_i} + r''_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i}\cdot x + \beta_{\mathrm{MN}_i}\cdot a_{\mathrm{MN}_i})\cdot P, Q) \\ &= e(r'_{\mathrm{MN}_i}\cdot P + r''_{\mathrm{MN}_i}\cdot P + \alpha_{\mathrm{MN}_i}\cdot x\cdot P + \beta_{\mathrm{MN}_i}\cdot a_{\mathrm{MN}_i}\cdot P, Q) \\ &= e(R'_{\mathrm{MN}_i} + R''_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i}\cdot P_X + \beta_{\mathrm{MN}_i}\cdot A_{\mathrm{MN}_i}, Q) \\ &= e(R_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i}\cdot P_X + \beta_{\mathrm{MN}_i}\cdot A_{\mathrm{MN}_i}, Q), \end{aligned} \tag{2}$$

and

$$K_{\mathrm{AP}_j} = C_{\mathrm{MN}_i}^{t_{\mathrm{AP}_j}} = (g^{t_{\mathrm{MN}_i}})^{t_{\mathrm{AP}_j}} = (g^{t_{\mathrm{AP}_j}})^{t_{\mathrm{MN}_i}} = C_{\mathrm{AP}_j}^{t_{\mathrm{MN}_i}} = K_{\mathrm{MN}_i}. \tag{3}$$

According to the above equations, the validity of the proposed AHA protocol is analyzed correctly.

3.5 Batch verification phase

With the increase of mobile nodes' number, the access point AP_j will receive a lot of login messages simultaneously. To improve the performance, the proposed protocol is able to provide batch verification. Given n login messages $\{D_{\mathrm{MN}_i}, E_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$ $(i = 1, 2, \ldots, n)$, AP_j runs the following process to verify the valid of those login messages simultaneously.

(1) AP_j computes $C_{\mathrm{MN}_i} = e(S_{\mathrm{AP}_j}, D_{\mathrm{MN}_i})$, $(\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, B_{\mathrm{MN}_i}) = \hat{h}(C_{\mathrm{MN}_i}) \oplus E_{\mathrm{MN}_i}$, $\alpha_{\mathrm{MN}_i} = h_1(\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i})$ and $\beta_{\mathrm{MN}_i} = h_3(\mathrm{ID}_{\mathrm{AP}_j}, \mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i})$, where $i = 1, 2, \ldots, n$.

(2) AP_j checks if $e(\sum_{i=1}^n B_{\mathrm{MN}_i}, P)$ and $e(\sum_{i=1}^n R_{\mathrm{MN}_i} + (\sum_{i=1}^n \alpha_{\mathrm{MN}_i})\cdot P_X + \sum_{i=1}^n(\beta_{\mathrm{MN}_i}\cdot A_{\mathrm{MN}_i}), Q)$ are equal. If not, AP_j rejects the session.

Due to $P_X = x\cdot P$, $P_Y = y\cdot P$, $R'_{\mathrm{MN}_i} = r'_{\mathrm{MN}_i}\cdot P$, $R''_{\mathrm{MN}_i} = r''_{\mathrm{MN}_i}\cdot P$, $R_{\mathrm{MN}_i} = R'_{\mathrm{MN}_i} + R''_{\mathrm{MN}_i}$, $s'_{\mathrm{MN}_i} = r''_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i}\cdot x \bmod q$, $s_{\mathrm{MN}_i} = r'_{\mathrm{MN}_i} + s'_{\mathrm{MN}_i} \bmod q$, $S_{\mathrm{AP}_j} = \frac{1}{y+h_3(\mathrm{ID}_{\mathrm{AP}_j})}\cdot P$, $A_{\mathrm{MN}_i} = a_{\mathrm{MN}_i}\cdot P$, $B_{\mathrm{MN}_i} = (s_{\mathrm{MN}_i} + \beta_{\mathrm{MN}_i}\cdot a_{\mathrm{MN}_i})\cdot Q$, $C_{\mathrm{MN}_i} = g^{t_{\mathrm{MN}_i}}$, $D_{\mathrm{MN}_i} = t_{\mathrm{MN}_i}\cdot(P_Y + h_2(\mathrm{ID}_{\mathrm{AP}_j})\cdot P)$ and $C_{\mathrm{AP}_j} = g^{t_{\mathrm{AP}_j}}$, we can get the following equation:

$$\begin{aligned} e\bigg(\sum_{i=1}^n B_{\mathrm{MN}_i}, P\bigg) &= e\bigg(\sum_{i=1}^n((s_{\mathrm{MN}_i} + \beta_{\mathrm{MN}_i}\cdot a_{\mathrm{MN}_i})\cdot Q), P\bigg) = e\bigg(\sum_{i=1}^n((s_{\mathrm{MN}_i} + \beta_{\mathrm{MN}_i}\cdot a_{\mathrm{MN}_i})\cdot P), Q\bigg) \\ &= e\bigg(\sum_{i=1}^n((r'_{\mathrm{MN}_i} + s'_{\mathrm{MN}_i} + \beta_{\mathrm{MN}_i}\cdot a_{\mathrm{MN}_i})\cdot P), Q\bigg) \\ &= e\bigg(\sum_{i=1}^n((r'_{\mathrm{MN}_i} + r''_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i}\cdot x + \beta_{\mathrm{MN}_i}\cdot a_{\mathrm{MN}_i})\cdot P), Q\bigg) \\ &= e\bigg(\sum_{i=1}^n(r'_{\mathrm{MN}_i}\cdot P + r''_{\mathrm{MN}_i}\cdot P + \alpha_{\mathrm{MN}_i}\cdot x\cdot P + \beta_{\mathrm{MN}_i}\cdot a_{\mathrm{MN}_i}\cdot P), Q\bigg) \\ &= e\bigg(\sum_{i=1}^n(R'_{\mathrm{MN}_i} + R''_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i}\cdot P_X + \beta_{\mathrm{MN}_i}\cdot A_{\mathrm{MN}_i}), Q\bigg) \end{aligned}$$

$$
\begin{aligned}
&= e\Big(\sum_{i=1}^{n}(R_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i}\cdot P_X + \beta_{\mathrm{MN}_i}\cdot A_{\mathrm{MN}_i}), Q\Big)\\
&= e\Big(\sum_{i=1}^{n} R_{\mathrm{MN}_i} + \sum_{i=1}^{n}(\alpha_{\mathrm{MN}_i}\cdot P_X) + \sum_{i=1}^{n}(\beta_{\mathrm{MN}_i}\cdot A_{\mathrm{MN}_i}), Q\Big)\\
&= e\Big(\sum_{i=1}^{n} R_{\mathrm{MN}_i} + (\sum_{i=1}^{n}\alpha_{\mathrm{MN}_i})\cdot P_X + \sum_{i=1}^{n}(\beta_{\mathrm{MN}_i}\cdot A_{\mathrm{MN}_i}), Q\Big). \qquad (4)
\end{aligned}
$$

Therefore, the proposed AHA protocol is able to provide the function of batch verification.

4 Security analysis

In this section, the security analysis of our proposed AHA protocol for MWNs is presented. First, we present a security model for AHA protocols based on previous work. Second, we prove that our proposed AHA protocol is secure based on the hardness of two famous mathematical problems. Third, we show the proposed AHA protocol can satisfy security requirements listed in Section 2. At last, we present security comparisons among related AHA protocols.

4.1 Security model

Based on previous security models [22, 30], we define the security model for the proposed AHA protocol as below. There are two participants in the handover authentication phase of an AHA protocol: a mobile node $\mathrm{MN}_i \in$ MobileNode and an access point $\mathrm{AP}_j \in$ AccessPoint. Both MN_i and AP_j get from their secret keys from the authentication server AS. Let $\mathcal{A}$ and Π_{Γ}^{φ} be a probabilistic polynomial-time adversary and φth instance of a participant Γ respectively, where Γ is a mobile node or an access point. The security of an AHA protocol is defined by a game played between the adversary $\mathcal{A}$ and a simulator $\mathcal{S}$. The following queries will be made by the adversary in the game.

- $H(m)$. $\mathcal{S}$ maintains a list L_H consisting of tuples (m, R_m), where L_H is initialized empty. $\mathcal{S}$ first checks if a tuple (m, R_m) exists in the list L_H when he receives a query with the message m. If yes, $\mathcal{S}$ transmits R_m to $\mathcal{A}$; otherwise, $\mathcal{S}$ picks a random element $R_m \in G_1$, inserts (m, R_m) into the list L_H and returns R_m to $\mathcal{A}$.
- $h_i(m)$. $\mathcal{S}$ maintains a list L_{h_i} consisting of tuples (m, r_m), where L_{h_i} is initialized empty and $i = 1, 2, 3, 4$. $\mathcal{S}$ first checks whether a tuple (m, r_m) exists in the list L_{h_i} when he receives a query with the message m. If it exists, $\mathcal{S}$ returns r_m to $\mathcal{A}$; otherwise, $\mathcal{S}$ selects a random element $r_m \in Z_q^*$, inserts (m, r_m) into the list L_{h_i} and returns r_m to $\mathcal{A}$.
- CreateMN($\mathrm{ID}_{\mathrm{MN}_i}$). $\mathcal{S}$ generates MN_i's private key according to its identity $\mathrm{ID}_{\mathrm{MN}_i}$.
- CreateAP($\mathrm{ID}_{\mathrm{AP}_j}$). $\mathcal{S}$ generates AP_j's private key according to its identity $\mathrm{ID}_{\mathrm{AP}_j}$.
- Send($\Pi_{\Gamma}^{\varphi}, m$). $\mathcal{S}$ executes corresponding steps in the AHA protocol when it receives the message m and outputs corresponding message.
- Reveal(Π_{Γ}^{φ}). $\mathcal{S}$ transmits the session key produced in Π_{Γ}^{φ} to $\mathcal{A}$.
- CorruptMN($\mathrm{ID}_{\mathrm{MN}_i}$). $\mathcal{S}$ returns MN_i's private key to $\mathcal{A}$.
- CorruptAP($\mathrm{ID}_{\mathrm{AP}_j}$). $\mathcal{S}$ returns AP_j's private key to $\mathcal{A}$.
- Test(Π_{Γ}^{φ}). $\mathcal{S}$ flips a coin $b \in \{0, 1\}$. If $b = 1$, $\mathcal{S}$ outputs Π_{Γ}^{φ}'s session key; otherwise, $\mathcal{S}$ outputs a random number.

We say an adversary $\mathcal{A}$ can violate MN-to-AP (AP-to-MN) authentication of an AHA protocol Ψ if $\mathcal{A}$ can forage a legal request (response) message. Let $E_{\text{MN-to-AP}}$ and $E_{\text{AP-to-MN}}$ denote the events that $\mathcal{A}$ can violate MN-to-AP authentication and AP-to-MN authentication respectively. The advantage that the adversary can violate the authentication of the AHA protocol Ψ is defined as $\mathrm{Adv}_{\Psi}^{\mathrm{MA}}(\mathcal{A}) = \Pr[E_{\text{MN-to-AP}}] + \Pr[E_{\mathrm{AP-to-MN}}]$.

Definition 1 (MA-secure)**.** We say an AHA protocol Ψ is MA-secure if $\mathrm{Adv}_{\Psi}^{\mathrm{MA}}(\mathcal{A})$ is negligible for any a polynomial-time adversary $\mathcal{A}$.

The concatenation of all messages sent and received by the instance Γ^{φ} is called its session identification. We say the instance Γ^{φ} is accepted when it receives the final message and turns into some intended status. Besides, we say two instances MN_i^{φ} and AP_j^{ϕ} are partnered if all the following three conditions hold simultaneously: (1) MN_i^{φ} and AP_j^{ϕ} are accepted; (2) MN_i^{φ} and AP_j^{ϕ} have the same session identification; (3) MN_i^{φ} and AP_j^{ϕ} are the partner of the other party. We say an instance Γ^{φ} is fresh if all the following three conditions hold: (1) Γ^{φ} is accepted; (2) neither Γ^{φ} nor its partner is made a Reveal query; (3) neither Γ^{φ} nor its partner is made a Corrupt query.

Let $\mathrm{Succ}(\mathcal{A})$ denote the event that $\mathcal{A}$ could guess the coin b correctly. $\mathcal{A}$'s advantage against the indistinguishability of an AHA protocol is defined as $\mathrm{Adv}_{\Psi}^{\mathrm{AKE}}(\mathcal{A}) = |2 \cdot \Pr[\mathrm{Succ}(\mathcal{A})] - 1|$.

Definition 2 (AKE-secure)**.** We say that an AHA protocol Ψ for MWNs is AKE-secure if $\mathrm{Adv}_{\Psi}^{\mathrm{AKE}}(\mathcal{A})$ is negligible for any polynomial-time adversary.

4.2 Security theory

In this subsection, we analyze the security of the proposed AHA protocol for MWNs in the above security model. The following lemmas and theories are proposed to demonstrate that the proposed protocol is secure enough for practical applications.

Lemma 1. No adversary can violate the MN-to-AP authentication of the proposed AHA protocol if the CDH problem in G_1 is hard.

Proof. Suppose that the adversary $\mathcal{A}$ could violate the MN-to-AP authentication of the proposed AHA protocol with a non-negligible probability ϵ. We will demonstates a simulator $\mathcal{S}$ could solve the CDH problem in G_1 by running $\mathcal{A}$ as a subroutine.

Given an instance $(P, a \cdot P, b \cdot P)$ of the CDH problem, $\mathcal{S}$'s goal is to compute $a\dot{b}\dot{P}$. To realize the goal, $\mathcal{S}$ picks a random number $y \in Z_q^*$ and sets $P_X \leftarrow a \cdot P$, $Q \leftarrow b \cdot P$ and $P_Y \leftarrow y \cdot P$. $\mathcal{S}$ randomly selects $\mathrm{ID}_{\mathrm{MN}_I}$ and answers $\mathcal{A}$'s queries according to the following description.

• $\hat{h}(m)$. $\mathcal{S}$ maintains a list $L_{\hat{h}}$ initialized empty. Upon receiving the query with the message m, $\mathcal{S}$ verifies if (m, r) exists in $L_{\hat{h}}$. If yes, $\mathcal{S}$ transmits r to $\mathcal{A}$; otherwise, $\mathcal{S}$ randomly picks $r \in \{0,1\}^l$, stores (m, r) in $L_{\hat{h}}$ and transmits r to $\mathcal{A}$.

• $h_i(m_i)$. $\mathcal{S}$ maintains a list L_{h_i} initialized empty, where $i = 1, \ldots, 6$. Upon receiving the query with the message m_i, $\mathcal{S}$ checks if a tuple (m_i, r_i) exists in L_{h_i}. If yes, $\mathcal{S}$ transmits r_i to $\mathcal{A}$; otherwise, $\mathcal{S}$ randomly picks $r_i \in Z_q^*$, stores (m_i, r_i) in L_{h_i} and transmits r_i to $\mathcal{A}$.

• CreateMN($\mathrm{ID}_{\mathrm{MN}_i}$). $\mathcal{S}$ maintains a list L_{MN} initialized empty. Upon receiving the query with MN_i's identity $\mathrm{ID}_{\mathrm{MN}_i}$, $\mathcal{S}$ checks if a tuple $(\mathrm{ID}_{\mathrm{MN}_i}, \mathrm{PID}_{\mathrm{MN}_i}, r_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, s_{\mathrm{MN}_i})$ exists in L_{MN}. If yes, $\mathcal{S}$ transmits R_{MN_i} to $\mathcal{A}$; otherwise, $\mathcal{S}$ checks if $\mathrm{ID}_{\mathrm{MN}_i}$ and $\mathrm{ID}_{\mathrm{MN}_I}$ are equal. If yes, $\mathcal{S}$ randomly picks $r_{\mathrm{MN}_i}, \alpha_{\mathrm{MN}_i}, \mathrm{PID}_{\mathrm{MN}_i} \in Z_q^*$, computes $R_{\mathrm{MN}_i} = r_{\mathrm{MN}_i} \cdot P$, stores $(\mathrm{ID}_{\mathrm{MN}_i}, \mathrm{PID}_{\mathrm{MN}_i}, r_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, \perp)$ in L_{MN} and inserts $(\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, \alpha_{\mathrm{MN}_i})$ into L_{h_1}; otherwise, $\mathcal{S}$ randomly picks $s_{\mathrm{MN}_i}, \alpha_{\mathrm{MN}_i}, \mathrm{PID}_{\mathrm{MN}_i} \in Z_q^*$, computes $R_{\mathrm{MN}_i} = s_{\mathrm{MN}_i} \cdot P - \alpha_{\mathrm{MN}_i} \cdot P_X$, stores $(\mathrm{ID}_{\mathrm{MN}_i}, \mathrm{PID}_{\mathrm{MN}_i}, \perp, R_{\mathrm{MN}_i}, s_{\mathrm{MN}_i})$ in L_{MN} and inserts $(\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, \alpha_{\mathrm{MN}_i})$ into L_{h_1}. At last, $\mathcal{S}$ transmits R_{MN_i} to $\mathcal{A}$.

• CreateAP($\mathrm{ID}_{\mathrm{AP}_j}$). $\mathcal{S}$ maintains a list L_{AP} initialized empty. Upon receiving the query with AP_j's identity $\mathrm{ID}_{\mathrm{AP}_j}$, $\mathcal{S}$ checks if a tuple $(\mathrm{ID}_{\mathrm{AP}_j}, S_{\mathrm{AP}_j})$ exists in L_{AP}. If yes, $\mathcal{S}$ transmits $\mathrm{ID}_{\mathrm{AP}_j}$ to $\mathcal{A}$; otherwise, $\mathcal{S}$ randomly picks $r_{\mathrm{AP}_j} \in Z_q^*$ and computes $S_{\mathrm{AP}_j} = \frac{1}{y + r_{\mathrm{AP}_j}} \cdot P$. $\mathcal{S}$ stores $(\mathrm{ID}_{\mathrm{AP}_j}, S_{\mathrm{AP}_j})$ and $(\mathrm{ID}_{\mathrm{AP}_j}, r_{\mathrm{AP}_j})$ in L_{AP} and L_{h_2} separately.

• Send($\Pi_{\Gamma}^{\varphi}, m$). Upon receiving the query with the message m, $\mathcal{S}$ checks if Γ and MN_I are equal; If not, $\mathcal{S}$ acts based on the presentation of the proposed AHA protocol; otherwise ($\Gamma = \mathrm{MN}_I$), $\mathcal{S}$ checks if $m =$"start". If yes, $\mathcal{S}$ randomly picks $a_{\mathrm{MN}_i}, t_{\mathrm{MN}_i}, \beta_{\mathrm{MN}_i} \in Z_q^*$, computes $A_{\mathrm{MN}_i} = \beta_{\mathrm{MN}_i}^{-1}(a \cdot P - R_{\mathrm{MN}_i} - \alpha_{\mathrm{MN}_i} \cdot P_X)$, $B_{\mathrm{MN}_i} = a_{\mathrm{MN}_i} \cdot Q$, $C_{\mathrm{MN}_i} = g^{t_{\mathrm{MN}_i}}$, $D_{\mathrm{MN}_i} = t_{\mathrm{MN}_i} \cdot (P_Y + h_2(\mathrm{ID}_{\mathrm{AP}_j}) \cdot P)$ and $E_{\mathrm{MN}_i} = \hat{h}(C_{\mathrm{MN}_i}) \oplus (\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, B_{\mathrm{MN}_i})$. At last, $\mathcal{S}$ transmits $\{D_{\mathrm{MN}_i}, E_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$ to $\mathcal{A}$.

• Reveal(Π_{Γ}^{φ}). Upon receiving the query, $\mathcal{S}$ transmits the session key produced in Π_{Γ}^{φ} to $\mathcal{A}$.

• CorruptMN($\mathrm{ID}_{\mathrm{MN}_i}$). $\mathcal{S}$ checks if $\mathrm{ID}_{\mathrm{MN}_i}$ and $\mathrm{ID}_{\mathrm{MN}_I}$ are equal. If not, $\mathcal{S}$ looks up the list L_{MN} for the tuple $(\mathrm{ID}_{\mathrm{MN}_i}, \mathrm{PID}_{\mathrm{MN}_i}, r_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, s_{\mathrm{MN}_i})$ and transmits $(R_{\mathrm{MN}_i}, s_{\mathrm{MN}_i})$ to $\mathcal{A}$; otherwise, $\mathcal{S}$ aborts the game.

• CorruptAP($\mathrm{ID}_{\mathrm{AP}_j}$). $\mathcal{S}$ looks up the list L_{AP} for the tuple $(\mathrm{ID}_{\mathrm{AP}_j}, S_{\mathrm{AP}_j})$ and transmits S_{AP_j} to $\mathcal{A}$.

Finally, $\mathcal{A}$ outputs a legal message $\{D_{\mathrm{MN}_i}, E_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$ corresponding to the mobile node MN_i with the identity $\mathrm{ID}_{\mathrm{MN}_i}$. According to the forking lemma [32], $\mathcal{A}$ outputs another legal message $\{D_{\mathrm{MN}_i}, E'_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$ if different one hash function h_1 is used in the game. Due to the validity of the above two messages, we can get the following two equations:

$$e(B_{\mathrm{MN}_i}, P) = e(R_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i} \cdot P_X + \beta_{\mathrm{MN}_i} \cdot A_{\mathrm{MN}_i}, Q), \tag{5}$$

$$e(B'_{\mathrm{MN}_i}, P) = e(R_{\mathrm{MN}_i} + \alpha'_{\mathrm{MN}_i} \cdot P_X + \beta_{\mathrm{MN}_i} \cdot A_{\mathrm{MN}_i}, Q). \tag{6}$$

According to above two equations, we can get that

$$\begin{aligned} e(B_{\mathrm{MN}_i} - B'_{\mathrm{MN}_i}, P) &= \frac{e(B_{\mathrm{MN}_i}, P)}{e(B'_{\mathrm{MN}_i}, P)} = \frac{e(R_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i} \cdot P_X + \beta_{\mathrm{MN}_i} \cdot A_{\mathrm{MN}_i}, Q)}{e(R_{\mathrm{MN}_i} + \alpha'_{\mathrm{MN}_i} \cdot P_X + \beta_{\mathrm{MN}_i} \cdot A_{\mathrm{MN}_i}, Q)} \\ &= e((\alpha_{\mathrm{MN}_i} - \alpha'_{\mathrm{MN}_i}) \cdot P_X, Q) = e((\alpha_{\mathrm{MN}_i} - \alpha'_{\mathrm{MN}_i}) \cdot a \cdot P, b \cdot P) \\ &= e((\alpha_{\mathrm{MN}_i} - \alpha'_{\mathrm{MN}_i}) \cdot a \cdot b \cdot P, P). \end{aligned} \tag{7}$$

Then, $\mathcal{S}$ outputs $(\alpha_{\mathrm{MN}_i} - \alpha'_{\mathrm{MN}_i})^{-1} \cdot (B_{\mathrm{MN}_i} - B'_{\mathrm{MN}_i})$ as the answer of the given CDH problem. The probability that $\mathcal{S}$ can solve the CDH problem is elaborated as follows. Three events related to the probability are listed as below.

• E_1. $\mathcal{S}$ does not abort in CorruptMN-queries.
• E_2. $\mathrm{ID}_{\mathrm{MN}_I}$ and $\mathrm{ID}_{\mathrm{MN}_i}$ are equal.
• E_3. $\mathcal{A}$ produces a valid login message.

Let q_{h_1} and q_{c} be the numbers of h_1-queries and CorruptMN-queries respectively. We can get $\Pr[E_1] \geqslant (1-\frac{1}{q_{h_1}})^{q_{\mathrm{c}}}$, $\Pr[E_2|E_1] \geqslant \frac{1}{q_{h_1}}$ and $\Pr[E_3|E_1 \wedge E_2] \geqslant \epsilon$. Then, probability that $\mathcal{S}$ can solve the CDH problem is

$$\begin{aligned} \Pr[E_1 \wedge E_2 \wedge E_3] &= \Pr[E_3|E_1 \wedge E_2] \cdot \Pr[E_2|E_1] \cdot \Pr[E_1] \\ &\geqslant \left(1 - \frac{1}{q_{h_1}}\right)^{q_{\mathrm{c}}} \cdot \frac{1}{q_{h_1}} \cdot \epsilon = \frac{(1 - \frac{1}{q_{h_1}})^{q_{\mathrm{c}}}}{q_{h_1}} \cdot \epsilon. \end{aligned} \tag{8}$$

Due to the non-negligibility of ϵ, we can conclude that $\mathcal{S}$ is able to address the CDH problem with a non-negligible probability. This contradicts with the hardness of the CDH problem. Therefore, no adversary can violate the MN-to-AP authentication of the proposed AHA protocol.

Lemma 2. No adversary can violate the AP-to-MN authentication of the proposed AHA protocol if the k-mBIDH problem is hard.

Proof. Suppose that the adversary $\mathcal{A}$ could violate the AP-to-MN authentication of the proposed AHA protocol with a non-negligible probability ϵ. We will show that a simulator $\mathcal{S}$ could solve the k-mBIDH problem in G_1 by running $\mathcal{A}$ as a subroutine.

Given an instance $P, y \cdot P \in G_1, z \cdot P \in G_1, \alpha_1, \alpha_2, \ldots, \alpha_k \in Z_q^*, \frac{1}{y+\alpha_1} \cdot P, \frac{1}{y+\alpha_2} \cdot P, \ldots, \frac{1}{y+\alpha_k} \cdot P$ of the k-mBIDH problem, $\mathcal{S}$'s goal is to compute $e(P,P)^{\frac{z}{y+\alpha}}$ for some $\alpha \notin \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$. To realize the goal, $\mathcal{S}$ picks a random number $x \in Z_q^*$ and sets $P_X \leftarrow x \cdot P$ and $P_Y \leftarrow y \cdot P$. $\mathcal{S}$ selects $\mathrm{ID}_{\mathrm{AP}_J}$ as the challenge identity and answers $\hat{h}(m)$-query, $h_i(m_i)$-query $(i = 1, \ldots, 6)$ and Reveal-query as it does in the above lemma. $\mathcal{S}$ also answers other queries according to the following description.

• CreateMN($\mathrm{ID}_{\mathrm{MN}_i}$). $\mathcal{S}$ maintains a list L_{MN} initialized empty. Upon receiving the query with MN_i's identity $\mathrm{ID}_{\mathrm{MN}_i}$, $\mathcal{S}$ verifies if $(\mathrm{ID}_{\mathrm{MN}_i}, \mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, s_{\mathrm{MN}_i})$ exists in L_{MN}. If yes, $\mathcal{S}$ transmits R_{MN_i} to $\mathcal{A}$; otherwise, $\mathcal{S}$ picks a random number $r_{\mathrm{MN}_i} \in Z_q^*$ and computes $R_{\mathrm{MN}_i} = r_{\mathrm{MN}_i} \cdot P$, $\mathrm{PID}_{\mathrm{MN}_i} = h_1(R_{\mathrm{MN}_i}, x) \oplus \mathrm{ID}_{\mathrm{MN}_i}$, $\alpha_{\mathrm{MN}_i} = h_2(\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i})$ and $s_{\mathrm{MN}_i} = r_{\mathrm{MN}_i} + \alpha_{\mathrm{MN}_i} \cdot x \bmod q$. At last, $\mathcal{S}$ stores $(\mathrm{ID}_{\mathrm{MN}_i}, \mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, s_{\mathrm{MN}_i})$ in L_{MN} and transmits R_{MN_i} to $\mathcal{A}$.

• CreateAP($\mathrm{ID}_{\mathrm{AP}_j}$). $\mathcal{S}$ maintains a list L_{AP} initialized empty. Upon receiving the query with AP_j's identity $\mathrm{ID}_{\mathrm{AP}_j}$, $\mathcal{S}$ checks if a tuple $(\mathrm{ID}_{\mathrm{AP}_j}, \alpha_j, S_{\mathrm{AP}_j})$ exists in L_{AP}. If yes, $\mathcal{S}$ transmits $\mathrm{ID}_{\mathrm{AP}_j}$ to $\mathcal{A}$.

Otherwise, $\mathcal{S}$ checks if $\mathrm{ID}_{\mathrm{AP}_j}$ and $\mathrm{ID}_{\mathrm{AP}_J}$ are equal. If not, $\mathcal{S}$ randomly selects $\alpha_j \in \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ and stores $(\mathrm{ID}_{\mathrm{AP}_j}, \alpha_j, \frac{1}{y+\alpha_j} \cdot P)$ and $(\mathrm{ID}_{\mathrm{AP}_j}, \alpha_j)$ in L_{AP} and L_{h_3} respectively. Otherwise ($\mathrm{ID}_{\mathrm{AP}_j} = \mathrm{ID}_{\mathrm{AP}_J}$), $\mathcal{S}$ randomly selects $\alpha \notin \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$, and stores $(\mathrm{ID}_{\mathrm{AP}_J}, \alpha, \perp)$ and $(\mathrm{ID}_{\mathrm{AP}_J}, \alpha)$ in L_{AP} and L_{h_3} respectively.

• Send(Π_Γ^φ, m). Upon receiving the query with the message m, $\mathcal{S}$ checks if Γ and AP_J are equal; If yes, $\mathcal{S}$ aborts the game; otherwise, $\mathcal{S}$ checks if the equation $\mathrm{ID}_\Gamma = \mathrm{ID}_{\mathrm{MN}_i}$ holds and Γ's partner is AP_J. If not, $\mathcal{S}$ acts based on the presentation of our proposed AHA protocol; otherwise, $\mathcal{S}$ randomly picks $a_{\mathrm{MN}_i} \in Z_q^*$, $C_{\mathrm{MN}_i} \in \{0,1\}^l$ and sets $D_{\mathrm{MN}_i} \leftarrow z \cdot P$. $\mathcal{S}$ computes $A_{\mathrm{MN}_i} = a_{\mathrm{MN}_i} \cdot P$, $\beta_{\mathrm{MN}_i} = h_4(\mathrm{ID}_{\mathrm{AP}_j}, \mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i})$, $B_{\mathrm{MN}_i} = (s_{\mathrm{MN}_i} + \beta_{\mathrm{MN}_i} \cdot a_{\mathrm{MN}_i}) \cdot Q$ and $E_{\mathrm{MN}_i} = \hat{h}(C_{\mathrm{MN}_i}) \oplus (\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, B_{\mathrm{MN}_i})$. At last, $\mathcal{S}$ transmits the login message $\{D_{\mathrm{MN}_i}, E_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$ to $\mathcal{A}$.

• CorruptMN($\mathrm{ID}_{\mathrm{MN}_i}$). $\mathcal{S}$ looks up the list L_{MN} for the tuple $(\mathrm{ID}_{\mathrm{MN}_i}, \mathrm{PID}_{\mathrm{MN}_i}, r_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, s_{\mathrm{MN}_i})$ and transmits $(R_{\mathrm{MN}_i}, s_{\mathrm{MN}_i})$ to $\mathcal{A}$.

• CorruptAP($\mathrm{ID}_{\mathrm{AP}_j}$). $\mathcal{S}$ checks if $\mathrm{ID}_{\mathrm{AP}_j}$ and $\mathrm{ID}_{\mathrm{AP}_J}$ are equal. If yes, $\mathcal{S}$ aborts the game; otherwise, $\mathcal{S}$ looks up the list L_{AP} for the tuple $(\mathrm{ID}_{\mathrm{AP}_j}, S_{\mathrm{AP}_j})$ and transmits S_{AP_j} to $\mathcal{A}$;

Finally, $\mathcal{A}$ outputs a response message $\{C_{\mathrm{AP}_j}, \mathrm{Auth}\}$ corresponding to AP_j with the identity $\mathrm{ID}_{\mathrm{AP}_j}$. $\mathcal{S}$ randomly picks a tuple $(D_{\mathrm{MN}_i}, E_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}, C_{\mathrm{MN}_i}, C_{\mathrm{AP}_j}, K_{\mathrm{AP}_j}, \mathrm{Auth})$ in the list L_{h_5} and outputs $C_{\mathrm{MN}_i} = e(S_{\mathrm{AP}_j}, D_{\mathrm{MN}_i}) = e(\frac{1}{y+\alpha_j} \cdot P, z \cdot P) = e(P,P)^{\frac{z}{y+\alpha_j}}$ as the solution of the given k-mBIDH problem. The probability that $\mathcal{S}$ can solve the k-mBIDH problem is elaborated as follows. Three events related to the probability are listed as below:

• E_1. $\mathcal{S}$ does not abort in the CorruptMN-queries or Send-queires.

• E_2. $\mathrm{ID}_{\mathrm{AP}_J}$ and $\mathrm{ID}_{\mathrm{AP}_j}$ are equal.

• E_3. $\mathcal{A}$ outputs a legal login message.

Let q_{h_3}, q_{c} and q_{s} denote the numbers of h_3-queries, CorruptMN-queries and Send-queires respective. We can get $\Pr[E_1] \geqslant (1 - \frac{1}{q_{h_3}})^{q_{\mathrm{c}}+q_{\mathrm{s}}}$, $\Pr[E_2|E_1] \geqslant \frac{1}{q_{h_3}}$ and $\Pr[E_3|E_1 \wedge E_2] \geqslant \epsilon$. Then, probability that $\mathcal{S}$ can solve the k-mBIDH problem is

$$\begin{aligned}\Pr[E_1 \wedge E_2 \wedge E_3] &= \Pr[E_3|E_1 \wedge E_2] \cdot \Pr[E_2|E_1] \cdot \Pr[E_1] \\ &\geqslant \left(1 - \frac{1}{q_{h_3}}\right)^{q_{\mathrm{c}}+q_{\mathrm{s}}} \cdot \frac{1}{q_{h_3}} \cdot \epsilon = \frac{(1 - \frac{1}{q_{h_3}})^{q_{\mathrm{c}}+q_{\mathrm{s}}}}{q_{h_3}} \cdot \epsilon. \end{aligned} \tag{9}$$

Due to the non-negligibility of ϵ, we can conclude that $\mathcal{S}$ is able to address the k-mBIDH problem with a non-negligible probability. This contradicts with the hardness of the k-mBIDH problem. Therefore, no adversary can violate the AP-to-MN authentication of the proposed AHA protocol.

According to the above two lemmas, we can get the following theory for the security of the proposed AHA protocol.

Theorem 1. The proposed AHA protocol for MWNs is MA-secure if the CDH problem and k-mBIDH problem are hard.

We also have the following theory for the AKE-security of the proposed AHA protocol for MWNs.

Theorem 2. The proposed AHA protocol for MWNs is AKE-secure if the CDH problem is hard.

The proof of the theory is similar to Theory 2 in [30]. To save space, we will not present its details here.

4.3 Analysis of security and privacy

(1) **Mutual authentication.** Two Lemmas in this paper show that the adversary against the proposed AHA protocol cannot produce a valid login or response message. Then, MN_i and AP_j can authenticate the other party by checking the legality of received response message and login message respectively. Therefore, the proposed AHA protocol can support the mutual authentication.

(2) **User anonymity.** MN_i's pseudo-identity $\mathrm{PID}_{\mathrm{MN}_i} = h_1(R_{\mathrm{MN}_i}, x) \oplus \mathrm{ID}_{\mathrm{MN}_i}$ is transmitted to AP_j in the login message $\{D_{\mathrm{MN}_i}, E_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$. A malicious AP_j can extract $\mathrm{PID}_{\mathrm{MN}_i}$ by computing $C_{\mathrm{MN}_i} = e(S_{\mathrm{AP}_j}, D_{\mathrm{MN}_i})$ and $(\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, B_{\mathrm{MN}_i}) = \hat{h}(C_{\mathrm{MN}_i}) \oplus E_{\mathrm{MN}_i}$. However, it cannot extract

$\mathrm{ID}_{\mathrm{MN}_i}$ from $\mathrm{PID}_{\mathrm{MN}_i}$ because it does not know the system private key x. Moreover, a general adversary even cannot extract $\mathrm{PID}_{\mathrm{MN}_i}$ from E_{MN_i} because it does not have AP_j's private key S_{AP_j}. Therefore, the proposed AHA protocol can support the user anonymity.

(3) **Non-traceability.** The adversary can intercept the login message $\{D_{\mathrm{MN}_i}, E_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$. However, he/she cannot trace MN_i's behavior according to the intercepted message because MN_i generate new random numbers to avoid producing constant value. Therefore, the proposed AHA protocol can support the non-traceability.

(4) **Conditional privacy preservation.** The authentication server can extract MN_i's identity by computing $S_{\mathrm{AP}_j} = \frac{1}{y+h_3(\mathrm{ID}_{\mathrm{AP}_j})} \cdot P$, $C_{\mathrm{MN}_i} = e(S_{\mathrm{AP}_j}, D_{\mathrm{MN}_i})$, $(\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, B_{\mathrm{MN}_i}) = \hat{h}(C_{\mathrm{MN}_i}) \oplus E_{\mathrm{MN}_i}$ and $\mathrm{ID}_{\mathrm{MN}_i} = h_1(R_{\mathrm{MN}_i}, x) \oplus \mathrm{PID}_{\mathrm{MN}_i}$. Therefore, the proposed AHA protocol can support the conditional privacy preservation.

(5) **Session key establishment.** Based on the presentation of the proposed AHA protocol, both MN_i and AP_j produce a session key $h_6(\mathrm{PID}_{\mathrm{MN}_i}, \mathrm{ID}_{\mathrm{AP}_j}, C_{\mathrm{MN}_i}, C_{\mathrm{AP}_j}, g^{t_{\mathrm{MN}_i} \cdot t_{\mathrm{AP}_j}})$ after executing the protocol. Therefore, the proposed AHA protocol can support the session key establishment.

(6) **Perfect forward secrecy.** To get the session key $\mathrm{sk}_{\mathrm{MN}_i} = h_6(\mathrm{PID}_{\mathrm{MN}_i}, \mathrm{ID}_{\mathrm{AP}_j}, C_{\mathrm{MN}_i}, C_{\mathrm{AP}_j}, g^{t_{\mathrm{MN}_i} \cdot t_{\mathrm{AP}_j}})$ produced in a previous session, the adversary has to extract $g^{t_{\mathrm{MN}_i} \cdot t_{\mathrm{AP}_j}}$ from $g^{t_{\mathrm{MN}_i}}$ and $g^{t_{\mathrm{AP}_j}}$, i.e., he/she has to address the CDH problem. Because the CDH problem is hard, the proposed AHA protocol can support the perfect forward secrecy.

(7) **Scalability.** The authentication server can extract MN_i's real identity by computing $S_{\mathrm{AP}_j} = \frac{1}{y+h_3(\mathrm{ID}_{\mathrm{AP}_j})} \cdot P$, $C_{\mathrm{MN}_i} = e(S_{\mathrm{AP}_j}, D_{\mathrm{MN}_i})$, $(\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, B_{\mathrm{MN}_i}) = \hat{h}(C_{\mathrm{MN}_i}) \oplus E_{\mathrm{MN}_i}$ and $\mathrm{ID}_{\mathrm{MN}_i} = h_1(R_{\mathrm{MN}_i}, x) \oplus \mathrm{PID}_{\mathrm{MN}_i}$. The computation cost of the process does not increase with the growth of mobile notes. Therefore, the proposed AHA protocol can support the scalability.

(8) **Attack resistance.** We show that the proposed AHA protocol can withstand existing attacks. The analysis is presented as follows.

• **Impersonation attack.** Two Lemmas in this paper show that the adversary against the proposed AHA protocol cannot produce a valid login or response message. Then, no adversary can impersonate the mobile node or the access point. Therefore, the proposed AHA protocol can withstand the impersonation attack.

• **Replay attack.** The mobile node or the access point produce new random number t_{MN_i} and t_{AP_j} in each session and use them to produce a message authentication code or a digital signature. Then, any replay of previous messages can be detected by checking the freshness of received message. Therefore, the proposed AHA protocol can withstand the replay attack.

• **Modification attack.** A message authentication code or a digital signature is produced by MN_i and AP_j to ensure integrity of the message. Then, any malicious modification of the message can be detected by MN_i or AP_j. Therefore, the proposed AHA protocol can withstand the modification attack.

• **Stolen verifier table attack.** Based on the description, we know no verifier table is involved in the proposed AHA protocol. Therefore, the proposed AHA protocol can withstand the stolen verifier table attack.

• **Man-in-the-middle attack.** According to the above analysis, the mutual authentication can be achieved after the execution of the proposed AHA. Therefore, the proposed AHA protocol can withstand the man-in-the-middle attack.

4.4 Security comparisons

To show the security advantages of the proposed AHA protocol, we present security comparisons between the proposed AHA protocol and three latest AHA protocols [16–18]. Let $R-1$, $R-2$, $R-3$, $R-4$, $R-5$, $R-6$, $R-7$, and $R-8$ denote mutual authentication, user anonymity, non-traceability, conditional privacy preservation, session key establishment, perfect forward secrecy and attack resistance respectively. The security comparisons are listed in Table 1.

From Table 1, we can get that the previous three AHA protocols [16–18] can provide none of non-traceability, conditional privacy preservation and perfect forward secrecy. The proposed AHA protocol

Table 1 Security and function comparisons

	Tsai et al.'s protocol [16]	Wang and Hu's protocol [17]	He et al.'s protocol [18]	**The proposed protocol**
$R-1$	Yes	Yes	Yes	**Yes**
$R-2$	Yes	Yes	Yes	**Yes**
$R-3$	No	No	No	**Yes**
$R-4$	No	No	No	**Yes**
$R-5$	Yes	Yes	Yes	**Yes**
$R-6$	No	No	No	**Yes**
$R-7$	Yes	Yes	Yes	**Yes**

Table 2 The system configurations

	Processor	Frequency	Memory	Operating system
Samsung galaxy S5	Quad-core	2.45 GHz	2 GB	Android 4.4.2
Dell Inspiron 3647	I5-4460S	2.90 GHz	4 GB	Window 8

Table 3 The running time of related operations (ms)

	T_{BP}	T_{MTP}	T_{SM}	T_{PA}	T_{EXP}	T_{MUL}	T_H
Mobile node	32.713	33.582	13.405	0.081	2.249	0.008	0.056
Access point	5.427	5.493	2.165	0.013	0.339	0.001	0.007

can satisfy all seven security and function requirements. Therefore, the proposed AHA protocol is more secure than those three protocols.

5 Performance analysis

In this section, we analyze the performance of the proposed AHA protocol. We also compare its computation cost and communication cost with that of three latest AHA protocols [16–18].

The Ate pairing has been widely used in the identity-based public key cryptography. Therefore, we use it to evaluate the performance of the proposed AHA protocol and related AHA protocols. To achieve the convincing security, we use a Ate pairing e defined on a super singular elliptic curve $E(F_p)$, where $E(F_p)$ defined on the finite field F_p with order q and the size of p and q are 512 bits and 160 bits respectively.

5.1 Computation cost

We analyze and compare the computation costs of the proposed AHA protocol and related AHA protocols. For convenience, we define some notations about the running time. Let BP, MTP, SM, PA, EXP, MUL and GH denote the bilinear paring operation, the map-to-point hash operation in G_1, the scalar multiplication operation in G_1, the point addition operation in G_1, the exponentiation operation operation in G_2, the multiplication operation in G_2 and the general hash function operation.

We established an experiment platform using a mobile device and a personal computer, whose system configurations are listed in Table 2. We use the mobile device and the personal computer to simulate the mobile node and access point respectively and get the exact running time of those operations based on the MIRACL library. The running time is listed in Table 3 [30], where T_{ope} denotes the running time of the ope operation.

Based on the above implementation results, we analyze and compare the computation cost of related AHA protocols. The comparisons among related protocols are listed in Table 4, where n denotes the number of received login messages by the access point simultaneously.

MN_i in Tsai et al.'s AHA protocol [16] has to carry out one BP operation, one MTP operation, three SM operations, one PA operation and two GH operations. Therefore, MN_i's running time is $T_{\mathrm{BP}} + T_{\mathrm{MTP}} + 3 \cdot T_{\mathrm{SM}} + T_{\mathrm{PA}} + T_H = 32.713 + 33.582 + 3 \times 13.405 + 0.081 + 2 \times 0.056 = 106.703$ ms. AP_j in Tsai et al.'s AHA protocol [16] needs to execute $(n+2)$ BP operation, n MTP operations,

Table 4 The comparisons of computation cost (ms)

	Tsai et al.'s protocol [16]	Wang and Hu's protocol [17]	He et al.'s protocol [18]	The proposed protocol
Mobile node	106.703	106.703	93.298	58.479
Access point	$13.125 \cdot n + 10.828$	$13.112 \cdot n + 10.854$	$13.138 \cdot n + 16.242$	$12.694 \cdot n + 12.857$

n SM operations, $(2n-2)$ PA operation and $2n$ GH operations. Therefore, AP_j's running time is $(n+2) \cdot T_{\mathrm{BP}} + n \cdot T_{\mathrm{MTP}} + \mathrm{n} \cdot T_{\mathrm{SM}} + (2n-2) \cdot T_{\mathrm{PA}} + 2n \cdot T_H = (n+2) \cdot 5.427 + n \cdot 5.493 + n \cdot 2.165 + (2n-2) \cdot 0.013 + 2n \cdot 0.007 = (13.125 \cdot n + 10.828)$ ms.

MN_i in Wang and Hu's AHA protocol [17] needs to execute one BP operation, one MTP operation, three SM operations, one PA operation and two GH operations. Therefore, MN_i's running time is $T_{\mathrm{BP}} + T_{\mathrm{MTP}} + 3 \cdot T_{\mathrm{SM}} + T_{\mathrm{PA}} + T_H = 32.713 + 33.582 + 3 \times 13.405 + 0.081 + 2 \times 0.056 = 106.703$ ms. AP_j in Wang and Hu's AHA protocol [17] needs to execute $(n+2)$ BP operation, n MTP operations, n SM operations, n PA operation and $2n$ GH operations. Therefore, AP_j's running time is $(n+2) \cdot T_{\mathrm{BP}} + n \cdot T_{\mathrm{MTP}} + \mathrm{n} \cdot T_{\mathrm{SM}} + n \cdot T_{\mathrm{PA}} + 2n \cdot T_H = (n+2) \cdot 5.427 + n \cdot 5.493 + n \cdot 2.165 + n \cdot 0.013 + 2n \cdot 0.007 = (13.112 \cdot n + 10.854)$ ms.

MN_i in He et al.'s AHA protocol [18] needs to execute one BP operation, one MTP operation, two SM operations, one PA operation and two GH operations. Therefore, MN_i's running time is $T_{\mathrm{BP}} + T_{\mathrm{MTP}} + 2 \cdot T_{\mathrm{SM}} + T_{\mathrm{PA}} + T_H = 32.713 + 33.582 + 2 \times 13.405 + 0.081 + 2 \times 0.056 = 93.298$ ms. AP_j in He et al.'s AHA protocol [17] needs to execute $(n+3)$ BP operation, n MTP operations, n SM operations, $(3n-3)$ PA operation and $2n$ GH operations. Therefore, AP_j's running time is $(n+3) \cdot T_{\mathrm{BP}} + n \cdot T_{\mathrm{MTP}} + n \cdot T_{\mathrm{SM}} + (3n-3) \cdot T_{\mathrm{PA}} + 2n \cdot T_H = (n+3) \cdot 5.427 + n \cdot 5.493 + n \cdot 2.165 + (3n-3) \cdot 0.013 + 2n \cdot 0.007 = (13.138 \cdot n + 16.242)$ ms.

MN_i in the proposed AHA protocol [18] needs to execute four SM operations, one PA operation, two EXP operations and five GH operations. Therefore, MN_i's running time is $4 \cdot T_{\mathrm{SM}} + T_{\mathrm{PA}} + 2 \cdot T_{\mathrm{EXP}} + 5 \cdot T_H = 4 \times 13.405 + 0.081 + 2 \times 2.249 + 5 \times 0.056 = 58.479$ ms. AP_j in the proposed AHA protocol [17] needs to execute $(n+2)$ BP operation, $(n+1)$ SM operations, $(4n-2)$ PA operation, $2n$ EXP operations and $5n$ GH operations. Therefore, AP_j's running time is $(n+2) \cdot T_{\mathrm{BP}} + (n+1) \cdot T_{\mathrm{SM}} + (4n-2) \cdot T_{\mathrm{PA}} + 2n \cdot T_{\mathrm{EXP}} + 5n \cdot T_H = (n+2) \times 5.427 + (n+1) \cdot 2.165 + (4n-2) \cdot 0.081 + 2n \times 2.249 + 5n \times 0.056 = (12.694 \cdot n + 12.857)$ ms.

According to the above comparisons of computation cost, we know that the proposed AHA protocol has much less running time than three latest AHA protocols [16–18] in both sides of the mobile node and the access point.

5.2 Communication cost

In this subsection, we analyze and compare the communication costs of the proposed AHA protocol and three latest AHA protocols [16–18]. Because the size of p is 512 bits, then the size of an element in G_1 and G_2 is 1024 bits. Let the sizes of the general hash function's output, the length of the pseudo identity and the timestamp be 160 bits, 128 bits and 32 bits separately.

MN_i and AP_j in Tsai et al.'s AHA protocol [16] sends $\{\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, S_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$ and $\{\mathrm{PID}_{\mathrm{MN}_i}, \mathrm{Auth}\}$ to the other side, where $\mathrm{PID}_{\mathrm{MN}_i}$ is the pseudo identity, $R_{\mathrm{MN}_i}, S_{\mathrm{MN}_i}$ are two elements in G_1, $\mathrm{TS}_{\mathrm{MN}_i}$ is the current timestamp and Auth is an output of the general hash function. Therefore, the communication cost of Tsai et al.'s AHA protocol [16] is $128 + 1024 + 1024 + 32 + 128 + 160 = 2496$ bits.

MN_i and AP_j in Wang and Hu's AHA protocol [17] sends $\{\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, \sigma_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$ and $\{\mathrm{PID}_{\mathrm{MN}_i}, \mathrm{Auth}\}$ to the other side, where $\mathrm{PID}_{\mathrm{MN}_i}$ is the pseudo identity, $R_{\mathrm{MN}_i}, \sigma_{\mathrm{MN}_i}$ are two elements in G_1, $\mathrm{TS}_{\mathrm{MN}_i}$ is the current timestamp and Auth is an output of the general hash function. Therefore, the communication cost of Wang and Hu's AHA protocol [17] is $128 + 1024 + 1024 + 32 + 128 + 160 = 2496$ bits.

MN_i and AP_j in He et al.'s AHA protocol [18] sends $\{\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, S_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$ and $\{\mathrm{PID}_{\mathrm{MN}_i}, \mathrm{Auth}\}$ to the other side, where $\mathrm{PID}_{\mathrm{MN}_i}$ is the pseudo identity, $R_{\mathrm{MN}_i}, S_{\mathrm{MN}_i}$ are two elements in G_1, $\mathrm{TS}_{\mathrm{MN}_i}$ is the current timestamp and Auth is an output of the general hash function. Therefore, the

communication cost of He et al.'s AHA protocol [16, 18] is $128 + 1024 + 1024 + 32 + 128 + 160 = 2496$ bits.

MN_i and AP_j in the proposed AHA protocol sends $\{D_{\mathrm{MN}_i}, E_{\mathrm{MN}_i}, \mathrm{TS}_{\mathrm{MN}_i}\}$ and $\{C_{\mathrm{AP}_j}, \mathrm{Auth}\}$ to the other side, where $E_{\mathrm{MN}_i} = \hat{h}(C_{\mathrm{MN}_i}) \oplus (\mathrm{PID}_{\mathrm{MN}_i}, R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, B_{\mathrm{MN}_i})$, $R_{\mathrm{MN}_i}, A_{\mathrm{MN}_i}, B_{\mathrm{MN}_i}, D_{\mathrm{MN}_i}$ are four elements in G_1, C_{AP_j} is an element in G_2, $\mathrm{TS}_{\mathrm{MN}_i}$ is the current timestamp and Auth is an output of the general hash function. Therefore, the communication cost of the proposed AHA protocol [16, 18] is $128 + 1024 + 1024 + 1024 + 1024 + 32 + 1024 + 160 = 5440$ bits.

According to the above comparisons, we know that the proposed AHA protocol increases the communication cost. The reason for the increases is that AP_j in the proposed AHA protocol generates a random nonce and sends $C_{\mathrm{AP}_j} = g^{t_{\mathrm{AP}_j}}$ to MN_i for achieving the perfect forward secrecy. It is worthy to achieve the important security attribute at the cost of increasing computation cost only.

6 Conclusion

In this paper, we outline the security requirements of anonymous handover authentication protocol for MWNs, and propose a new protocol to address problems existing in previous protocols. Security analysis demonstrates that the proposed AHA protocol is secure against various attacks and can meet security requirements from practical applications. Concrete experiments on a concrete platform using the MIRACL library show that the proposed protocol has much less running time than three latest protocols [16–18]. It is still a pity that the proposed protocol has higher communication cost than those three protocols. How to reduce communication cost is our future work.

Acknowledgements The work of He D B was supported by National Natural Science Foundation of China (Grant Nos. 61572379, 61501333, U1536204), National High Technology Research and Development Program of China (863 Program) (Grant No. 2015AA016004), Open Foundation of the State Key Laboratory of Cryptology, and Natural Science Foundation of Hubei Province (Grant No. 2015CFB257). The work of Wang D was supported by National Natural Science Foundation of China (Grant No. 61472016). The work of Xie Q was supported by Natural Science Foundation of Zhejiang Province (Grant No. LZ12F02005), National Basic Research Program of China (973 Program) (Grant No. 2013CB834205), and National Natural Science Foundation of China (Grant Nos. 61133014, 61472114).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Zheng X, Chen Y, Wang H, et al. Neighborhood prediction based decentralized key management for mobile wireless networks. Wirel Netw, 2013, 19: 1387–1406
2 Tu H, Kumar N, He D, et al. An efficient password-based three-party authenticated multiple key exchange protocol for wireless mobile networks. J Supercomput, 2014, 70: 224–235
3 Jo H, Paik J, Lee D. Efficient privacy-preserving authentication in wireless mobile networks. IEEE Trans Mobile Comput, 2014, 13: 1469–1481
4 He D B, Zeadally S, Kumar N, et al. Anonymous authentication for wireless body area networks with provable security. IEEE Syst J, in press, doi: 10.1109/JSYST.2016.2544805
5 He D B, Kumar N, Shen H, et al. One-to-many authentication for access control in mobile pay-tv systems. Sci China Inf Sci, 2016, 59: 052108
6 Shen H, Li Z, Chen K. A scalable and mobility-resilient data search system for large-scale mobile wireless networks. IEEE Trans Parall Distrib Syst, 2014, 25: 1124–1134
7 Liang C, Yu F, Zhang X. Information-centric network function virtualization over 5G mobile wireless networks. IEEE Netw, 2015, 29: 68–74
8 Menezes A J, Oorschot P C, Vanstone S A. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996
9 Choi J, Jung S. A secure and efficient handover authentication based on light-weight diffe-hellman on mobile node in fmipv6. IEICE Trans Commun, 2008, 91: 605–608
10 Yang G, Huang Q, Wong D, et al. Universal authentication protocols for anonymous wireless communications. IEEE Trans Wirel Commun, 2010, 9: 168–174
11 He D, Bu J, Chan S, et al. Privacy-preserving universal authentication protocol for wireless communications. IEEE Trans Wirel Commun, 2011, 10: 431–436

12 He D, Bu J, Chan S, et al. Handauth: efficient handover authentication with conditional privacy for wireless networks. IEEE Trans Comput, 2013, 62: 616–622
13 He D, Chen C, Chan S, et al. Secure and efficient handover authentication based on bilinear pairing functions. IEEE Trans Wirel Commun, 2012, 11: 48–53
14 He D, Chen C, Chan S, et al. Analysis and improvement of a secure and efficient handover authentication for wireless networks. IEEE Commun Lett, 2012, 16: 1270–1273
15 Yeo S, Yap W, Liu J, et al. Comments on "analysis and improvement of a secure and efficient handover authentication based on bilinear pairing functions". IEEE Commun Lett, 2013, 17: 1521–1523
16 Tsai J, Lo N, Wu T. Secure handover authentication protocol based on bilinear pairings. Wirel Personal Commun, 2013, 73: 1037–1047
17 Wang W, Hu L. A secure and efficient handover authentication protocol for wireless networks. Sensors, 2014, 14: 11379–11394
18 He D, Khan M, Kumar N. A new handover authentication protocol based on bilinear pairing functions for wireless networks. Int J Ad Hoc Ubiquit Comput, 2015, 18: 67–74
19 Li G, Jiang Q, Wei F, et al. A new privacy-aware handover authentication scheme for wireless networks. Wirel Personal Commun, 2015, 80: 581–589
20 Xie Y, Wu L, Kumar N, et al. Analysis and improvement of a privacy-aware handover authentication scheme for wireless network. Wirel Personal Commun, doi: 10.1007/s11277-016-3352-3
21 Fu A M, Qin N Y, Wang Y L, et al. Nframe: a privacy-preserving with non-frameability handover authentication protocol based on (t, n) secret sharing for lte/lte-a networks. Wirel Netw, in press. doi: 10.1007/s11276-016-1277-0
22 Choi K Y, Hwang J Y, Lee D H, et al. Id-based authenticated key agreement for low-power mobile devices. In: Proceedings of the 10th Australasian Conference on Information Security and Privacy, Brisbane, 2005. 494–505
23 Huang X, Xiang Y, Bertino E, et al. Robust multi-factor authentication for fragile communications. IEEE Trans Depend Secure Comput, 2014, 11: 568–581
24 Huang X, Xiang Y, Chonka A, et al. A generic framework for three-factor authentication: preserving security and privacy in distributed systems. IEEE Trans Parall Distr Syst, 2011, 22: 1390–1397
25 Shen J, Tan H, Moh S, et al. Enhanced secure sensor association and key management in wireless body area networks. J Commun Netw, 2015, 17: 453–462
26 Xie S, Wang Y. Construction of tree network with limited delivery latency in homogeneous wireless sensor networks. Wirel Personal Commun, 2014, 78: 231–246
27 Wang D, He D, Wang P, et al. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Trans Depend Secure Comput, 2015, 12: 428–442
28 Wang D, Wang N, Wang P, et al. Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity. Inf Sci, 2015, 321: 162–178
29 Guo P, Wang J, Li B, et al. A variable threshold-value authentication architecture for wireless mesh networks. J Int Tech, 2014, 15: 929–936
30 He D, Zeadally S, Kumar N, et al. Efficient and anonymous mobile user authentication protocol using self-certied public key cryptography for multi-server architectures. IEEE Trans Inf Foren Secur, in press. doi: 10.1109/TIFS.2016.2573746
31 Shim K. Cpas: an efficient conditional privacy-preserving authentication scheme for sehicular sensor vetworks. IEEE Trans Veh Tech, 2012, 61: 1874–1883
32 Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. J Cryptol, 2000, 13: 361–396