A Secure and Effective Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks

Dawei Zhao · Haipeng Peng · Lixiang Li · Yixian Yang

Abstract Recently, Mun et al. analyzed Wu et al.’s authentication scheme and proposed an enhanced anonymous authentication scheme for roaming service in global mobility networks. However, through careful analysis, we find that Mun et al.’s scheme is vulnerable to impersonation attacks and insider attacks, and cannot provide user friendliness, user’s anonymity, proper mutual authentication and local verification. To remedy these weaknesses, we propose a novel anonymous authentication scheme for roaming service in global mobility networks. Compared with previous related works, our scheme has many advantages. Firstly, the secure authenticity of the scheme is formally validated by an useful formal model called BAN logic. Secondly, the scheme enjoys many important security attributes including prevention of various attacks, user anonymity, no verification table, local password verification and so on. Thirdly, the scheme does not use timestamp, thus it avoids the clock synchronization problem. Further, the scheme contains the authentication and establishment of session key scheme when mobile user is located in his/her home network, therefore it is more practical and universal for global mobility networks. Finally, performance and cost analysis show our scheme is more suitable for low-power and resource limited mobile devices and thus availability for real implementation.

D. Zhao · H. Peng (✉) · L. Li · Y. Yang
Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
e-mail: penghaipeng@bupt.edu.cn

D. Zhao
e-mail: dwzhao@ymail.com

D. Zhao · H. Peng · L. Li · Y. Yang
National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China

D. Zhao
Shandong Provincial Key Laboratory of Computer Network, Shandong Computer Science Center, Jinan 250014, China
1 Introduction

Global mobility network (GLOMONET) [1] provides global roaming service that permits mobile user to use the services provided by his/her home agent (HA) in a foreign agent (FA). When a mobile user roams into a foreign network, mutual authentication must first be solved to prevent illegal use from accessing services and to ensure that mobile users are connected to a trusted networks. A strong user authentication scheme in GLOMONET should satisfy the following requirements: (1) user anonymity; (2) low communication cost and computation complexity; (3) single registration; (4) update session key periodically; (5) user friendly; (6) no password/verifier table; (7) update password securely and freely; (8) prevention of fraud; (9) prevention of replay attack; (10) security; and (11) providing the authentication scheme when a user is located in the home network. More details about these requirements can be found in [2].

In order to achieve secure and effective mutual authentication and privacy protection in GLOMONET, many authentication protocols have been proposed [2–24]. In 2004, Zhu and Ma [3] proposed an authentication scheme with anonymity for wireless environments. In Zhu and Ma’s scheme, mobile users only do symmetric encryption and decryption, and only one round of message exchange is needed between the mobile user and the visited. Therefore, this scheme is high security and computational efficiency. However, Zhu and Ma’s scheme was later found that it cannot achieve mutual authentication and perfect backward secrecy, and is vulnerable to the forgery attack [4]. In 2006, Lee et al. [4] proposed an enhanced anonymous authentication scheme which not only achieve Zhu-Ma scheme’s advantages but also enhances their security by withstanding the security weaknesses. In addition, the efficiency of Lee et al’s scheme is higher than that of the Zhu-Ma scheme. But Chang et al. [5] and Wu et al. [6] found that Lee et al.’s scheme also cannot achieve user’anonymity, and an attacker who has registered as a user of an HA can obtain the identity of other users as long as they registered at the same HA. After that, in 2011, Li et al. [2] pointed out that Wu et al.’s scheme [6] is unlikely to provide user’s anonymity due to an inherent design weakness and also vulnerable to replay and impersonation attacks. Then they constructed a strong user authentication scheme with smart cards for wireless communications which enjoys both computation and communication efficiency as compared to some well-known authentication schemes. However, this scheme was later found that it lacks of user friendliness, and cannot provide user’s anonymity and unfairness in key agreement [7].

Recently, Mun et al. [8] reanalyzed Wu et al.’ [6] authentication scheme, they point out that Wu et al.’s scheme also fails to achieve user’s anonymity and perfect forward secrecy, and discloses of legitimate user’s password. Then they proposed an enhanced anonymous authentication scheme for roaming service in global mobility networks which has the following advantages:

1. It can provide several security properties such as providing perfect forward secrecy and preventing disclosure of users password.
2. It is more efficient regarding performance compared with some previous known schemes that use public key cryptosystem with certificates.
3. It does not use timestamps, thus it is not required to synchronize the time.
However, through careful analysis, we find that Mun et al.’s scheme is vulnerable to impersonation attacks and insider attacks, and cannot provide user friendliness, user’s anonymity, proper mutual authentication and local verification. To overcome these weaknesses, in this paper we propose a novel anonymous authentication scheme for roaming service in global mobility networks. The proposed scheme not only enjoys many important security attributes including prevention of various attacks, user anonymity, no verification table, local password verification and so on, but also its secure authenticity is formally validated by an useful formal model called BAN logic. The scheme does not use timestamp, thus it avoids the clock synchronization problem. And the scheme provides the authentication and establishment of session key scheme when mobile user is located in his/her home network, therefore it is more practical and universal for global mobility networks. Additionally, the performance and cost analysis also show our scheme is more suitable for low-power and resource limited mobile devices and thus availability for real implementation.

The remainder of this paper is organized as follows. Section 2 provides some basic knowledge. In Sect. 3, we review Mun et al.’s scheme and Sect. 4 shows the security weaknesses of Mun et al.’s scheme. A novel user authentication scheme is proposed in Sect. 5. In Sect. 6, we analyze the security of our proposed scheme. Next, we compare the functionality and performance of our proposed scheme and make comparisons with other related schemes in Sect. 7. Finally, in Sect. 8 we make some conclusions.

2 Preliminaries

In this section, we briefly introduce the elliptic curve cryptosystem, some related mathematical assumptions and BAN logic.

2.1 Elliptic Curve Cryptosystem

Compared with other public key cryptography, elliptic curve cryptosystem (ECC) has significant advantages like smaller key sizes, faster computation. It has been widely used in several cryptographic schemes of wireless network environment to provide desired level of security and computational efficiency.

Let $E_p(a, b)$ be a set of elliptic curve points over the prime field $E_p$, defined by the non-singular elliptic curve equation: $y^2 \mod p = (x^3 + ax + b) \mod p$ with $a, b \in F_p$ and $(4a^3 + 27b^2) \mod p \neq 0$. The additive elliptic curve group defined as $G_p = \{(x, y) : x, y \in F_p \text{ and } (x, y) \in E_p(a, b)\} \cup O$, where the point $O$ is known as “point at infinity”. The scalar multiplication on the cyclic group $G_p$ defined as $k \cdot P = P + P + \cdots + P$ for $n$ times, where $n \cdot P = O$ for smallest integer $n > 0$. More details about elliptic curve group properties can be found in [25–27].

2.2 Related Mathematical Assumptions

To illustrate the security of our proposed scheme, we present some important computational problems [26] over the elliptic curve group which are frequently used to design secure cryptographic schemes.

(1) Computational discrete logarithm (CDL) problem: Given $R = x \cdot P$, where $P, R \in G_p$.

It is easy to calculate $R$ given $x$ and $P$, but it is hard to determine $x$ given $P$ and $R$. 

Table 1 Notations of BAN logic

| Notation | Description |
|----------|-------------|
| \( \mathcal{P} \models \mathcal{X} \) | The principal \( \mathcal{P} \) believes the statement \( \mathcal{X} \), or \( \mathcal{P} \) would be entitled to believe \( \mathcal{X} \). |
| \( \#(\mathcal{X}) \) | The formula \( \mathcal{X} \) is fresh. |
| \( \mathcal{P} \Rightarrow \mathcal{X} \) | The principal \( \mathcal{P} \) has jurisdiction over the statement \( \mathcal{X} \). |
| \( \mathcal{P} \prec \mathcal{X} \) | The principal \( \mathcal{P} \) sees the statement \( \mathcal{X} \). |
| \( \mathcal{P} \models \neg \mathcal{X} \) | The principal \( \mathcal{P} \) once said the statement \( \mathcal{X} \). |
| \( \langle \mathcal{X} \rangle_{\mathcal{Y}} \) | The formula \( \mathcal{X} \) combined with the formula \( \mathcal{Y} \). |
| \( \{ \mathcal{X} \}_{\mathcal{K}} \) | The formula \( \mathcal{X} \) encrypted under the key \( \mathcal{K} \). |
| \( \mathcal{P} \xleftarrow{\mathcal{K}} \mathcal{Q} \) | The principals \( \mathcal{P} \) and \( \mathcal{Q} \) may use the shared key \( \mathcal{K} \) to communicate. |
| \( \xrightarrow{\mathcal{K}} \mathcal{P} \) | The principals \( \mathcal{P} \) has \( \mathcal{K} \) as a public key, and the inverse of \( \mathcal{K} \) is \( \mathcal{K}^{-1} \). |
| \( \mathcal{P} \xrightarrow{\mathcal{X}} \mathcal{Q} \) | The formula \( \mathcal{X} \) is a secret known only to \( \mathcal{P} \) and \( \mathcal{Q} \). |

2.3 BAN Logic

BAN logic [28] is a useful formal model which can be used to analyze the security of various types of network protocol [5, 18, 29, 30]. Some notations of BAN logic are shown in Table 1, and logical postulates of BAN logic which will be used in the proof of our proposed scheme are described as follows.

(1) **Message-meaning rule.**

For shared keys, if principal \( \mathcal{P} \) believes he/she shares the secret key \( \mathcal{K} \) with \( \mathcal{Q} \), and \( \mathcal{P} \) sees the statement \( \mathcal{X} \) is encrypted under \( \mathcal{K} \). Then \( \mathcal{P} \) believes that \( \mathcal{Q} \) once said \( \mathcal{X} \):

\[
\begin{align*}
\mathcal{P} \models \mathcal{P} \xleftarrow{\mathcal{K}} \mathcal{Q}, \mathcal{P} \prec \langle \mathcal{X} \rangle_{\mathcal{K}} \\
\mathcal{P} \models \mathcal{Q} \models \neg \mathcal{X}.
\end{align*}
\]

For public keys, if principal \( \mathcal{P} \) believes \( \mathcal{K} \) is the public-private key pair of \( \mathcal{Q} \), and \( \mathcal{P} \) sees the statement \( \mathcal{X} \) is signatured by \( \mathcal{K}^{-1} \). Then \( \mathcal{P} \) believes that \( \mathcal{Q} \) once said \( \mathcal{X} \):

\[
\begin{align*}
\mathcal{P} \models \mathcal{K}, \mathcal{P} \prec \langle \mathcal{X} \rangle_{\mathcal{K}^{-1}} \\
\mathcal{P} \models \mathcal{Q} \models \neg \mathcal{X}.
\end{align*}
\]

(2) **Nonce-verification rule**

If principal \( \mathcal{P} \) believes \( \mathcal{X} \) is fresh and \( \mathcal{P} \) believes \( \mathcal{Q} \) once said \( \mathcal{X} \), then \( \mathcal{P} \) believes that \( \mathcal{Q} \) believes \( \mathcal{X} \):

\[
\begin{align*}
\mathcal{P} \models \#(\mathcal{X}), \mathcal{P} \models \mathcal{Q} \models \neg \mathcal{X} \\
\mathcal{P} \models \mathcal{Q} \models \mathcal{X}.
\end{align*}
\]

(3) **Jurisdiction rule**

If principal \( \mathcal{P} \) believes that \( \mathcal{Q} \) has jurisdiction over \( \mathcal{X} \) and \( \mathcal{P} \) believes that \( \mathcal{Q} \) believes \( \mathcal{X} \), then \( \mathcal{P} \) believes \( \mathcal{X} \):

\[
\begin{align*}
\mathcal{P} \models \#(\mathcal{X}), \mathcal{P} \models \mathcal{Q} \models \neg \mathcal{X} \\
\mathcal{P} \models \mathcal{Q} \models \mathcal{X}.
\end{align*}
\]
### Table 2 Notations used in Mun et al.’s scheme

| Notation | Description |
|----------|-------------|
| $MU, FA, HA$ | Mobile User, Foreign Agent, Home Agent. |
| $PW_X$ | Password of an entity $X$. |
| $ID_X$ | Identity of an entity $X$. |
| $h(\cdot)$ | A one-way hash function. |
| $NX$ | Number used only once (Random number) generated by an entity $X$. |
| $\|\|$ | Concatenation operation. |
| $\oplus$ | XOR operation. |
| $f_K$ | MAC generation function by using the key $K$. |
| $K_{XY}$ | Session key between entity $X$ and $Y$. |

\[
P \equiv Q \Rightarrow X, \quad P \equiv Q \equiv X \\
\frac{P \equiv X}{P \equiv X}
\]

(4) *Freshness-conjunctenation rule*

If principal $P$ believes $X$ is fresh, then $P$ believes $(X, Y)$ is fresh:

\[
P \equiv #(X) \Rightarrow P \equiv #(X, Y)
\]

### 3 Review of Mun et al.’s Scheme

In this section, we briefly review the Mun et al.’s scheme [8]. There are three phases in their scheme: registration phase, authentication and establishment of session key phase, and update session key phase. Three entities are involved: $MU$ is a mobile user, $FA$ is the agent of the foreign network, and $HA$ is the home agent of the mobile user $MU$. Table 2 lists some notations used in Mun et al.’s scheme.

#### 3.1 Registration Phase

When a mobile user $MU$ wants to become a legal client to access the services, $MU$ needs to register himself/herself to his/her home agent $HA$. The handshake between $MU$ and $HA$ is depicted in Fig. 1.

![Registration phase of Mun et al.’s scheme](image_url)
Fig. 2 Authentication and establishment of session key phase of Mun et al.’s scheme

Step R1: MU sends his/her identity ID_MU and a random number N_MU to HA.
Step R2: HA generates a random number N_HA and computes PW_MU = h(N_MU || N_HA) and r_MU = h(ID_MU || PW_MU) ⊕ ID_HA.
Step R3: HA sends r_MU, PW_MU, N_HA, ID_HA, and h(·) to MU through a secure channel.

3.2 Authentication and Establishment of Session Key Phase

When roaming into a foreign network FA, MU needs to verify the validity of FA and proves to FA that he is a legitimate user. The authentication and establishment of session key phase which used to solve the above issue in Mun et al.’s scheme is shown in Fig. 2.

Step A1: MU submits ID_HA, N_HA and r_MU to FA.
Step A2: FA stores the received message from MU for further communications and generates a random number N_FA. Then, FA sends ID_FA, N_FA and r_MU to HA.
Step A3: After receiving the message sent from FA, HA computes r_MU’ = h(ID_MU || PW_MU) ⊕ ID_HA and compares it with the received r_MU. If they are not equal, HA considers MU as illegal user and terminates this procedure. Otherwise, HA can authenticate MU. Next, HA computes P_HA = h(PW_MU || N_FA) and S_HA = h(ID_FA || N_FA) ⊕ r_MU ⊕ P_HA. Then, HA sends the computed S_HA and P_HA to FA.
Step A4: When receiving S_HA and P_HA sent from HA, FA computes S_HA’ = h(ID_FA || N_FA) ⊕ r_MU ⊕ P_HA. Then, FA verifies whether S_HA’ equals the received S_HA. If the result is not correct, the procedure is terminated. Next, FA computes S_FA =
A Secure and Effective Anonymous Authentication

3.3 Update Session Key Phase

**MU** and **FA** need to renew session key for security reasons if user is always within a same **FA**. When **MU** visits **FA** at the i\(^{\text{th}}\) session, the following process is conducted to authenticate **FA**:

**Step U1**: **MU** selects a new random number \(b_i\), computes \(b_i P\) \((i = 1, 2, \ldots, n)\), and sends \(b_i P\) to **FA**.

**Step U2**: **FA** selects a new random number \(a_i\) and computes \(a_i P\) \((i = 1, 2, \ldots, n)\). Then **FA** generates a new session key \(K_{MF_i} = h(a_i b_i P)\), and then computes \(S_{MF_i} = f_{K_{MF_i}}(a_i b_i P || a_{i-1} b_{i-1} P)\). After that, **FA** sends \(a_i P\) and \(S_{MF_i}\) to **MU**.

**Step U3**: **MU** computes session key \(K_{MF_i} = h(a_i b_i P)\) by using the received \(a_i P\). **MU** computes \(S'_{MF_i} = f_{K_{MF_i}}(a_i b_i P || a_{i-1} b_{i-1} P)\). Then, **MU** checks whether \(S'_{MF_i} = S_{MF_i}\). If they are equal, the new session key \(K_{MF_i} = h(a_i b_i P)\) is established between **MU** and **FA**.

Procedure of update session key phase is depicted in Fig. 3.

4 Weaknesses of Mun et al.’s Scheme

Recently, Kim and Kwak [19] pointed out that Mun et al.’s scheme [8] cannot withstand replay attacks and man-in-the-middle attacks. Through careful analysis, in this section we show that Mun et al.’s scheme is also vulnerable to impersonation attacks and insider attacks,
and cannot provide user friendliness, user’s anonymity, proper mutual authentication and local verification.

4.1 Impersonation Attacks

4.1.1 MU Impersonation Attacks

In Mun et al.’s scheme, an attacker can masquerade as a user MU to cheating any foreign agent FA’ and MU’s HA if he/she has intercepted a valid login request message \( \{ID_{HA}, N_{HA}, r_{MU}\} \) of MU. First, the attacker generates a random number \( N'_{HA} \) and sends \( \{ID_{HA}, N'_{HA}, r_{MU}'\} \) to FA’. Since \( ID_{HA} \) and \( r_{MU} \) are the real home agent and correct personal information of MU respectively, the login request message can pass the validation of HA. Furthermore, HA will notify the FA’ that the attacker who is masquerading as the user MU is a legitimate user. Therefore, the attacker can further establish a session key with FA’ and access the services provided by FA’.

4.1.2 FA Impersonation Attacks

In the authentication and establishment of session key phase of Mun et al.’s scheme, it can be found that the HA only authenticates the MU by verifying the received \( r_{MU} \) but do not make any authentication to the FA. At the same time, there is no secret information of FA in the message \( \{ID_{FA}, N_{FA}, r_{MU}\} \) sent from FA to MU’s HA. Thus an attacker can masquerade as a foreign agent FA to cheating any user MU’ and MU’’s HA. For example, if the attacker intercepts a login request message \( \{ID_{HA}, N_{HA}, r_{MU}'\} \) sent from MU’ to FA, the attacker can generate a random number \( N_{FA} \) and send \( \{ID_{FA}, N_{FA}, r_{MU}'\} \) to HA by masquerading as FA. Since \( r_{MU}' \) is the correct personal information of MU’ and there is no identity authentication process of HA to FA. Therefore, the message \( \{ID_{HA}, N_{HA}, r_{MU}'\} \) can pass the authentication of HA. At the same time, since the authentication of MU’ to FA is completely dependent on HA, the FA will pass the authentication of MU’. Therefore, the attacker who is masquerading as the FA can establish a session key with MU’ and tricks MU’ successfully.

4.1.3 HA Impersonation Attacks

In the authentication and establishment of session key phase of Mun et al.’s scheme, the FA authenticates MU and HA by verifying whether \( S'_{HA} = S_{HA} \). However, there is a security vulnerability in this step such that an attacker can masquerade as a home agent to help any agent pass the authentication of a FA and access the services provided by FA. It is assumed that B is a agent who wants to access the services provided by FA and A is an attacker who masquerades as B’s home agent HA to help B pass the authentication of FA.

First, B freely chooses two numbers \( N' \) and \( r' \), and submits \( \{ID_{HA}, N', r'\} \) to FA. Then FA generates a random number \( N_{FA} \) and sends the message \( \{ID_{FA}, N_{FA}, r'\} \) to HA. Right now, A intercepts this message, freely chooses a number \( P' \), and computes \( S_{HA} = h(ID_{FA}||N_{FA}) \oplus r' \oplus P' \). Then, A sends the computed \( S_{HA} \) and \( P' \) to FA. When receiving \( S_{HA} \) and \( P' \) sent from A who is masquerading as the HA, FA computes \( S'_{HA} = h(ID_{FA}||N_{FA}) \oplus r' \oplus P' \). Obviously, the \( S'_{HA} \) equals the received \( S_{HA} \). Next, FA computes \( S_{FA} = h(S_{HA}||N_{FA}||N') \), selects random number \( a \), and computes \( aP \). After that, FA sends \( \{S_{FA}, aP, P_{FA} = (S_{HA}||ID_{FA}||N_{FA})\} \) to B. At this point, B does not need to verify the \( S_{FA} \), but directly chooses a random number \( b \) and computes \( K_{MF} = h(abP) \) and
$S_{MF} = f_{K_{MF}}(N_{FA}||bP)$. Then $B$ sends $bP$ and $S_{MF}$ to $FA$. After receiving $\{bP, S_{MF}\}$ sent from $B$, $FA$ computes $K_{MF} = h(abP)$ and $S'_{MF} = f_{K_{MF}}(N_{FA}||bP)$. Obviously, there is $S'_{MF} = S_{MF}$. $FA$ thus authenticates $B$. By the above method, with the assistance of $A$, $B$ establishes the session key $K_{MF} = h(abP)$ with $FA$ and can access the services provided by $FA$.

4.2 Insider Attacks

In the registration phase, $MU$ sends $ID_{MU}$ and a random number $N_{MU}$ to $HA$. Then $HA$ generates a random number $N_{HA}$, computes $PW_{MU} = h(N_{MU}||N_{HA})$ and $r_{MU} = h(ID_{MU}||PW_{MU}) \oplus ID_{HA}$, and sends $\{r_{MU}, PW_{MU}, N_{HA}, ID_{HA}, h(\cdot)\}$ to $MU$ through a secure channel. It is obvious that the $HA$ knows all the secret information of $MU$ so that $HA$ can impersonate $MU$ to do anything. Therefore, Mun et al.’s scheme is vulnerable to the insider attack.

4.3 Lack of User Friendliness

User friendliness means that the proposed authentication scheme should be easily used by users. However, in the registration phase of Mun et al.’s scheme, the home agent $HA$ sends the information $\{r_{MU}, PW_{MU}, N_{HA}, ID_{HA}, h(\cdot)\}$ to the user $MU$ without using smart card. So that $MU$ needs to remember and enter so much information in the authentication and establishment of session key phase. Therefore, Mun et al.’s scheme is actually infeasible and unrealistic.

4.4 Lack of User’s Anonymity

In the second phase of Mun et al.’s scheme, $MU$ sends $r_{MU}$ to $FA$ instead of his/her real identity $ID_{MU}$. Thus the authors claimed that their scheme achieves the user’s anonymity. However, in each login message $\{ID_{HA}, N_{HA}, r_{MU}\}$ of $MU$, the contents of $N_{HA}$ and $r_{MU}$ are always unchanged. Any attacker could easily trace $MU$ according to $N_{HA}$ and $r_{MU}$ and thus the user’s anonymity cannot achieved.

4.5 Lack of Proper Mutual Authentication

In Mun et al.’s scheme, the $HA$ does not maintain any verification table. Thus after receiving the message $\{ID_{FA}, N_{FA}, r_{MU}\}$ sent from $FA$, $HA$ cannot recognize which user launched the authentication request to $FA$. So $HA$ cannot computes $r'_{MU}$ and checks it with the received $r_{MU}$. On the other hand, even if $HA$ can compute $r'_{MU}$ and check whether $r'_{MU} = r_{MU}$, it only means $HA$ authenticates the legality of $MU$. However, it is found that $HA$ do not make any authentication to the $FA$. Therefore, Mun et al.’s scheme cannot provide proper mutual authentication.

4.6 Lack of Local Verification

In the authentication and establishment of session key phase of Mun et al.’s scheme, the $MU$ directly enters and sends the login message to $FA$. Note that the smart terminal of $MU$ does not verify the entered information correctly or not. Therefore, even if the $MU$ enters the login message incorrectly by mistake or an attacker sends an forged message, the authentication phase still continue in their scheme. This obviously results to cause unnecessarily having extra communication and computational costs.
Table 3 Notations used in the proposed scheme

| Notation | Description |
|----------|-------------|
| $MU, FA, HA$ | Mobile user, Foreign agent, Home agent |
| $P$ | A point of the additive elliptic curve group $G_P$ |
| $PW_X$ | Password of an entity $X$ |
| $ID_X$ | Identity of an entity $X$ |
| $a, A$ | Random number generated by $MU$, $A = aP$ |
| $b, B$ | Random number generated by $FA$, $B = bP$ |
| $c, C$ | Random number generated by $HA$, $C = cP$ |
| $h(\cdot)$ | A one-way hash function |
| $Cert_X$ | Certificate of an entity $X$ |
| $PX$ | Public key of $X$ |
| $SX$ | Private key of $X$ |
| $EK[\cdot]/DK[\cdot]$ | Symmetric encryption/decryption using key $K$ |
| $EK[\cdot]/DK[\cdot]$ | Asymmetric encryption/decryption using key $K$ |
| $SK$ | Secret session key shared between $MU$ and $FA$ |
| $\|$ | Concatenation operation |
| $\oplus$ | XOR operation |

5 The Proposed Scheme

In this section, we propose a novel anonymous authentication scheme for roaming service in global mobility networks using elliptic curve cryptosystem to not only protect the scheme from security breaches, but also emphasize the efficient features. In addition to including the general registration phase, authentication and establishment of session key phase and update session key phase, our scheme also contains the update password phase and authentication and establishment of session key scheme when a mobile user is located in his/her home network. Therefore it is more practical and universal for global mobility networks. Table 3 lists some notations used in our proposed scheme.

5.1 Registration Phase

When a mobile user $MU$ wants to become a legal client to access the services, $MU$ needs to register himself/herself to his/her home agent $HA$.

**Step R1:** $MU$ freely chooses his/her identity $ID_{MU}$ and password $PW_{MU}$, and generates a random number $N_{MU}$. Then $MU$ submits $ID_{MU}$ and $h(PW_{MU} \| N_{MU})$ to $HA$ for registration via a secure channel.

**Step R2:** When receiving the message $ID_{MU}$ and $h(PW_{MU} \| N_{MU})$, $HA$ computes $Q = h(ID_{MU} \| y) \oplus h(PW_{MU} \| N_{MU})$ and $H = h(ID_{MU} \| h(PW_{MU} \| N_{MU}))$, where $y$ is a secret number of $HA$. Then $HA$ stores the message $\{Q, H, C = cP, ID_{HA}\}$ in a smart card and submits the smart card to $MU$ through a secure channel.

**Step R3:** After receiving the smart card, $MU$ enters $N_{MU}$ into the smart card. Finally, $MU$’s smart card contains parameters $\{Q, H, C, ID_{HA}, N_{MU}\}$.

The details of user registration phase are shown in Fig. 4.
5.2 Authentication and Establishment of Session Key Phase

When roaming into a foreign network FA, MU needs to verify the validity of FA and proves to FA that he is a legitimate user. The authentication and establishment of session key phase which used to solve the above issue in our proposed scheme is described as follows:

**Step A1:** MU inserts his/her smart card into the smart card reader, and inputs identity $ID_{MU}$ and password $PW_{MU}$. Then the smart card computes $H^* = h(ID_{MU} \parallel h(PW_{MU} \parallel N_{MU}))$, and checks whether $H^* = H$. If they are equal, it means $MU$ is a legitimate user. Otherwise the smart card aborts the session.

Next, the smart card generates a random numbers $a$, and computes $A = aP$, $R_{AC} = aC, N = Q \oplus h(PW_{MU} \parallel N_{MU}), ID_{DMU} = ID_{MU} \oplus h(R_{AC})$ and $V_1 = h(N \parallel R_{AC} \parallel ID_{HA} \parallel A \parallel C)$. Then the smart card sends the request message $\{A, ID_{DMU}, C, V_1, ID_{HA}\}$ to FA over a public channel.

**Step A2:** After receiving the message $\{A, ID_{DMU}, C, V_1, ID_{HA}\}, FA$ generates a random numbers $b$, and computes $B = bP, R_{BC} = bC$, $W_2 = E_{R_{BC}}[A, B, Cert_{FA}, V_1, ID_{DMU}]$ and $V_2 = E_{SFA}[h(A, B, Cert_{FA}, V_1, ID_{DMU})]$. Here, $S_{FA}$ is the private key of $FA$, and $Cert_{FA}$ is $FA$’s certificate. Then $FA$ sends $\{B, W_2, V_2\}$ to $HA$.

**Step A3:** When receiving $\{B, W_2, V_2\}, HA$ first computes $R_{BC} = cB$ and decrypts $D_{R_{BC}}[W_2]$ to reveal $A, B, Cert_{FA}, V_1$ and $ID_{DMU}$. Then, $HA$ verifies the FA’s signature $V_2$ by using the FA’s certificate $Cert_{FA}$. If they are valid, FA is authenticated. After that, $HA$ computes $R_{AC} = cA, ID_{MU} = ID_{DMU} \oplus h(R_{AC})$ and $V_1^* = h(h(ID_{MU} || y) || R_{AC} || ID_{HA} || A \parallel C)$. Then $HA$ checks whether $V_1^* = V_1$. If they are equal, $MU$ is authenticated by $HA$. Next, $HA$ generates a random number $d$ and computes $D = dP, G_{MU} = dB \oplus R_{AC}, W_1 = h(h(ID_{MU} || y) \parallel dB \parallel A \parallel D \parallel ID_{FA} \parallel ID_{HA}), W_3 = E_{R_{BC}}[ID_{FA}, Cert_{FA}, G_{MU}, dA, A, B, D, W_1]$ and $V_3 = E_{SHA}[h(ID_{FA}, Cert_{HA}, G_{MU}, dA, A, B, D, W_1)]$. At last, $HA$ sends $\{W_3, V_3\}$ to $FA$.

**Step A4:** $FA$ decrypts $D_{R_{BC}}[W_3]$ to reveal $ID_{FA}, Cert_{HA}, G_{MU}, dA, A, B, D$ and $W_1$. Then, $FA$ verifies the $HA$’s signature $V_3$ by using the $HA$’s certificate $Cert_{HA}$. If it is valid, $HA$ is authenticated which also means that $HA$ claimed $MU$ is a legitimate user. After that, $FA$ computes the common session key $SK = h(bdA)$ and $W_4 = E_{SK}[W_1, D, ID_{FA}]$, and sends $\{G_{MU}, W_4\}$ to $MU$.

**Step A5:** After receiving the message $\{G_{MU}, W_4\}, MU$ computes $dB = G_{MU} \oplus R_{AC}$ and $SK = h(adB)$, and decrypts $D_{SK}[W_4]$ to reveal $W_1, D, ID_{FA}$. Then $MU$...
computes $W_1^* = h(N \| dB \| A \| D \| ID_{FA} \| ID_{HA})$ and checks whether $W_1^* = W_1$. If they are equal, $FA$ and $HA$ are all authenticated by $MU$. Then $MU$ confirms the common session key is $SK = h(adB)$. After that, $MU$ computes $Auth = h(W_1 \| adB)$ and sends it to $FA$.

**Step A6:** After receiving the message $\{Auth\}$, $FA$ computes $Auth^* = h(W_1 \| bdA)$ and compares it with the received $Auth$. If they are equal, $FA$ confirms the common session key with $MU$ is $SK = h(bdA)$.

The authentication and establishment of session key phase is depicted in Fig. 5.

### 5.3 Update Session Key Phase

$MU$ and $FA$ need to renew session key for security reasons if user is always within a same $FA$. When $MU$ visits $FA$ at the $i$th session, the following process is conducted to authenticate $FA$:

**Step U1:** $MU$ selects a new random number $a_i$, computes $a_iD$, and sends $a_iD$ to $FA$.

**Step U2:** $FA$ selects a new random number $b_i$ and computes $b_iD$. Then $FA$ generates a new session key $SK_i = h(b_ia_iD)$, and then computes $S_i = h(b_ia_iD \| SK_{i-1})$. After that, $FA$ sends $b_iD$ and $S_i$ to $MU$.

**Step U3:** $MU$ computes $S'_i = h(a_ib_iD \| SK_{i-1})$ and checks whether $S'_i = S_i$. If they are not equal, $MU$ aborts the session. Otherwise, $MU$ computes the new session key $SK_i = h(a_ib_iD)$.

The details of update session key phase of the proposed scheme are shown in Fig. 6.

### 5.4 Update Password Phase

This phase is invoked whenever $MU$ wants to change his password $PW_{MU}$ to a new password $PW_{new \_MU}$. There is no need for a secure channel for password change, and it can be finished without communicating with his/her $HA$.

1. $MU$ inserts his/her smart card into the smart card reader, and inputs identity $ID_{MU}$ and password $PW_{MU}$. Then the smart card computes $H^* = h(ID_{MU} \| h(PW_{MU} \| NM_{MU}))$, and checks whether $H^* = H$. If they are not equal, the smart card rejects the password change request. Otherwise, $MU$ inputs a new password $PW_{new \_MU}$ and a new random number $x_{new \_MU}$.

2. The smart card computes $Q^{new \_MU} = Q \oplus h(PW_{MU} \| NM_{MU}) \oplus h(PW_{new \_MU} \| x_{new \_MU})$ and $H^{new \_MU} = h(ID_{MU} \| h(PW_{new \_MU} \| x_{new \_MU}))$. Then, the smart card replaces $Q$, $H$ and $NM_{MU}$ with $Q^{new \_MU}$, $H^{new \_MU}$ and $x^{new \_MU}$ to finish the password change phase.

### 5.5 Authentication and Establishment of Session Key Scheme When a Mobile User is Located in His/Her Home Network

Corresponding to the authentication and establishment of session key phase when a mobile user is located in a foreign network, in this subsection we propose an authentication and establishment of session key scheme for that when a mobile user is located in his/her home network. The detail processes are described as follows and depicted in Fig. 7.

**Step A1:** $MU$ inserts his/her smart card into the smart card reader, and inputs identity $ID_{MU}$ and password $PW_{MU}$. Then the smart card computes $H^* = h(ID_{MU} \| h(PW_{MU} \| NM_{MU}))$, and checks whether $H^* = H$. If they are equal,
Compute $H^* = h(ID_{MU} \| h(PW_{MU} \| N_{MU}))$.

Check $H^* = H$.

Generate random number $a$,

Compute: $A = aP, \quad R_{AC} = aC,$

$N = Q \oplus h(PW_{MU} \| N_{MU}),$

$DID_{MU} = ID_{MU} \oplus h(R_{AC}),$

$V_1 = h(N \| R_{AC} \| ID_{HA} \| A \| C), \quad \{A, DID_{MU}, C, V_1, ID_{HA}\}$

Generate random number $b$,

Compute: $B = bP, \quad R_{MC} = bC,$

$W_2 = E_{k_a}[A, B, Cert_{FA}, V_1, DID_{MU}],$

$V_2 = E_{k_a}(h(A, B, Cert_{FA}, V_1, DID_{MU})). \quad \{B, W_2, V_2\}$

Compute: $R_{MC} = cB,$

$D_{k_a}[W_2] \rightarrow A, B, Cert_{FA}, V_1, DID_{MU}.$

Verify signature $V_2$.

If $V_2$ is valid, $FA$ is authenticated.

Compute: $R_{AC} = cA, \quad ID_{MU} = DID_{MU} \oplus h(R_{AC}),$

$V_1^* = h(h(ID_{MU} \| y) \| R_{AC} \| ID_{HA} \| A \| C).$

Check $V_1^* = V_1$.

If they are equal, $MU$ is authenticated.

Generate random number $d$,

Compute: $D = dP, \quad G_{MU} = dB \oplus R_{AC},$

$W_1 = h(h(ID_{MU} \| y) \| dB \| D \| ID_{FA} \| ID_{HA}),$

$W_1 = E_{k_a}[ID_{FA}, Cert_{HA}, G_{MU}, dA, A, B, D, W_1],$

$V_3 = E_{k_a}(h(ID_{FA}, Cert_{HA}, G_{MU}, dA, A, B, D, W_1)). \quad \{W_3, V_3\}$

$D_{k_a}[W_3] \rightarrow ID_{FA}, Cert_{HA}, G_{MU}, dA, A, B, D, W_3,$

Verify signature $V_3$.

If $V_3$ is valid, $HA$ and $MU$ is authenticated.

Compute: $SK = h(bdA), \quad W_i = E_{k_a}[W_1, D, ID_{FA}].$

Compute: $b = G_{MU} \oplus R_{AC}, \quad SK = h(adB),$

$D_{k_a}[W_4] \rightarrow W_4, D, ID_{FA},$

Compare $W_4$ with $W'_4 = h(N \| dB \| D \| ID_{FA} \| ID_{HA}).$

If they are equal, $FA$ and $HA$ are authenticated, $MU$’s session key is $SK$.

Compute: $Auth = h(W_4 \| adB)$.

Compare $Auth$ with $Auth' = h(W_4 \| bdA),$

If they are equal, $FA$ confirms the session key is $SK$.

Fig. 5 Authentication and establishment of session key phase of the proposed scheme

it means $MU$ is a legitimate user. Otherwise the smart card aborts the session.

Next, the smart card generates a random numbers $a$, and computes $A = aP, \quad R_{AC} = aC, \quad N = Q \oplus h(PW_{MU} \| N_{MU}), \quad DID_{MU} = ID_{MU} \oplus h(R_{AC})$ and
\[ V_1 = h(N \| R_{AC} \| ID_{HA} \| A \| C) \] and then the smart card sends the request message \[ \{ A, D_{ID_{MU}}, C, V_1, ID_{HA} \} \] to HA over a public channel.

**Step A2:** After receiving the message \[ \{ A, D_{ID_{MU}}, C, V_1, ID_{HA} \} \], HA first computes \[ R_{AC} = cA \] and \[ ID_{MU} = D_{ID_{MU}} \oplus h(R_{AC}) \] and \[ V_1^* = h(h(ID_{MU} \| y) \| ID_{MU} \| A \| C) \]. Then HA checks whether \[ V_1^* = V_1 \]. If they are equal, MU is authenticated by HA. Next, HA generates a random number \( d \), and computes
$D = dP$ and $W_1 = h(h(ID_MU \| y) \| A \| C \| D \| ID_HA)$. At last, $HA$ computes the session key $SK = h(dA)$ and sends $\{D, W_1, ID_HA\}$ to $MU$.

**Step A3:** When receiving the message $\{D, W_1, ID_HA\}$, $MU$ computes $W_2^* = h(N \| A \| C \| D \| ID_HA)$ and checks whether $W_2^* = W_1$. If they are equal, $HA$ is authenticated by $MU$. Then $MU$ establishes the common session key $SK = h(aD)$.

### 6 Security Analysis of the Proposed Scheme

In this section, we show that the proposed scheme can withstand all possible security attacks, and then demonstrate the validity of our protocol using the BAN logic.

#### 6.1 Withstanding Possible Attacks

**Proposition 1** The proposed scheme can provide user’s anonymity.

**Proof** In our proposed scheme, the mobile user $MU$ sends the login request message $\{A, DID_MU, C, V_1, ID_HA\}$ to $FA$, where $DID_MU = ID_MU \oplus h(aC)$ is used to protect the real identity $ID_MU$ of $MU$. Based on the CDL problem, any attacker cannot obtain the random number $a$ form $A$ and thus cannot retrieve $ID_MU$ from $DID_MU$. At the same time, the attacker cannot trace the moving history and current location of $MU$ according to the login request message since $A$, $DID_MU$ and $V_1$ are dynamically changed in different login request messages of $MU$. Therefore, the proposed scheme can provide user’s anonymity.

**Proposition 2** The proposed scheme can prevent impersonation attack.

**Proof** Our proposed scheme can efficiently prevent impersonation attacks by considering the following scenarios:

1. Any attacker cannot impersonate $MU$ to cheat $FA$ and $HA$. In the proposed scheme, whether $MU$ is located in a foreign network or in his/her home network, the $HA$ authenticates $MU$ by verifying the computed $V_1^* = h(h(ID_MU \| y) \| R_{AC} \| ID_HA \| A \| C)$ with the received $V_1 = h(N \| R_{AC} \| ID_HA \| A \| C)$. Since the attacker does not possess $MU$’s password $PW_{MU}$, he/she cannot compute the correct $N = Q \oplus h(PW_{MU} \| NMU)$ and thus cannot cheat $HA$ by forging a login request message. At the same time, since $a$ is a one-time random number and only possessed by $MU$, $V_1$ is dynamically changed in each login request message. Therefore, the attacker cannot cheat the $HA$ by replaying a previous login request message. Beside, when $MU$ is located in a foreign network, the authentication of $FA$ to $MU$ is completely dependent on the authentication of $HA$ to $MU$. If an attacker cannot successfully cheat $HA$ by masquerading as $MU$, he/she cannot cheat $FA$ successfully.

2. Any attacker cannot impersonate $FA$ to cheat $HA$ and $MU$. In the proposed scheme, the $HA$ authenticates $FA$ by checking whether $DP_F \{V_2\}$ equals $h(A, B, V_1, DID_MU)$, where $V_2$ is $FA$’s digital signature. Obviously, the attacker cannot compute the correct $FA$’s digital signature without knowing $FA$’s private key $S_F$. Therefore, the attacker cannot cheat $HA$ successfully by masquerading as $FA$. At the same time, the authentication of $MU$ to $FA$ is completely dependent on the authentication of $HA$ to $FA$. If an attacker cannot successfully cheat $HA$ by masquerading as $FA$, he/she cannot cheat $MU$ successfully.

3. Any attacker cannot impersonate $HA$ to cheat $FA$ and $MU$. In the proposed scheme, the $FA$ authenticates $HA$ by checking whether $DP_H \{V_3\}$ equals $h(Cert_HA, W_1)$, where
V3 is HA’s digital signature. Obviously, the attacker cannot compute the correct HA’s digital signature without knowing HA’s private key $S_H$. Therefore, the attacker cannot cheat FA successfully by masquerading as HA. Besides, the MU authenticates HA by verifying the computed $W_1^* = h(N||dB||A||D||ID_FA||ID_HA)$ with the received $W_1 = h(h(ID_MU||y)||dB||A||D||ID_FA||ID_HA)$. Since any attacker cannot compute the correct $W_1$ without knowing $ID_MU$ and $y$, the attacker cannot cheat MU successfully.

**Proposition 3** The proposed scheme can withstand the replay attack.

*Proof* An attacker might replay an old login request message $[A, ID_MU, C, V_1, ID_HA]$ to FA and receive the message $[G_MU, W_4]$ from FA. However, the attacker still cannot compute the correct session key $SK = h(abdP)$ since he/she cannot derive the secret information $a$ form $A = aP$ based on the security of CDL problem. Thus, the proposed scheme can prevent the replay attack.

**Proposition 4** The proposed scheme meets the security requirement for perfect forward secrecy.

*Proof* Perfect forward secrecy means that even if an attacker compromises all the passwords of the entities of the system, he/her still cannot compromise the session key. In the proposed scheme, the session key $SK = h(abdP)$ is generated by three one-time random numbers $a$, $b$, and $d$ in each session. These three one-time random numbers are only held by the MU, FA and HA respectively, and cannot be retrieved from $A = aP$, $B = bP$, $D = dP$, $R_{AC} = aC = cA$ and $R_{BC} = bC = cB$ based on the security of CDL and CDH problem. Thus, even if an adversary obtains all the passwords of the entities, previous session keys and all the transmitted messages, he/her still cannot compromise other session key. Hence, the proposed scheme achieves perfect forward secrecy.

**Proposition 5** Our scheme can resist off-line password guessing attack with smart card security breach.

*Proof* In the proposed scheme, it is assume that if a smart card is stolen, physical protection methods cannot prevent malicious attackers to get the stored secure elements. At the same time, attacker can access to a big dictionary of words that likely includes user’s password and intercept the communications between the user and agents.

It is assumed that an attacker has obtained the information $\{Q, H, C, ID_HA, N_MU\}$ from the stolen MU’s smart card and has intercepted a previous full transmitted messages $[A, ID_MU, C, V_1, ID_HA, B, W_2, V_2, W_3, V_3, G_MU, W_4]$. In the proposed scheme, MU’s password only makes two appearances as $H = h(ID_MU||h(PW_MU||N_MU))$ and $V_1 = h((Q \oplus h(PW_MU||N_MU))||aC||ID_HA||A ||C)$. Obviously, the attacker cannot launch an off-line password guessing attack without knowing the $ID_MU$ and $a$. Since it has been demonstrated that our scheme can provide user anonymity and $a$ is MU’s secret random number, the proposed scheme can resist off-line password guessing attack with smart card security breach.

**Proposition 6** The proposed scheme can withstand insider attack.

*Proof* If an insider of the home agent HA has obtained a user MU’s password $PW_MU$, he/she can impersonate as MU to access any foreign agent. In the registration phase of the proposed scheme, MU sends identity $ID_MU$ and $h(PW_MU||N_MU)$ to HA. Thus, the insider cannot derive $PW_MU$ without $N_MU$. Besides, in the password change phase, MU
can change his/her default password $PW_{MU}$ without the assistance of his/her $HA$. Therefore the insider has no chance to obtain $MU$’s password, our scheme can withstand the insider attack.

**Proposition 7** There is no verification table in the proposed scheme.

**Proof** In the proposed scheme, it is obvious that the user, the foreign agent and the home agent do not maintain any verification table.

**Proposition 8** The proposed scheme can provide local password verification.

**Proof** In the proposed scheme, smart card checks the validity of $MU$’s identity $ID_{MU}$ and password $PW_{MU}$ before logging into $FA$. Since the attacker cannot compute the correct $H$ without the knowledge of $ID_{MU}$ and $PW_{MU}$ to pass the verification equation $H^* = H$, thus our scheme can avoid the unauthorized accessing by the local password verification.

### 6.2 Authentication Proof Based on BAN Logic

The general analytic procedures of BAN logic contains four phases: idealization of the protocol, making assumption, setting goal and analysis of the protocol. In this section, we will use the BAN logic to proof the validity of our protocol.

1. The messages of the protocol are transformed to the idealized form as shown below:

   $m_1.\ MU \rightarrow HA: \langle A, ID_{HA} \rangle h(ID_{MU} \| y)$
   $m_2.\ FA \rightarrow HA: \langle B \rangle_{SFA}$
   $m_3.\ HA \rightarrow MU: \langle A, B, ID_{FA}, MU \leftrightarrow FA \rangle h(ID_{MU} \| y)$
   $m_4.\ HA \rightarrow FA: \langle A, B, MU \leftrightarrow FA \rangle_{SH_A}$
   $m_5.\ FA \rightarrow MU: \langle A, B, MU \leftrightarrow FA \rangle_{SK}$
   $m_6.\ MU \rightarrow FA: \langle A, B, MU \leftrightarrow FA \rangle_{SK}$

2. In order to analyze the proposed protocol, we make the following assumptions:

   A1: $MU \equiv \#(B)$;
   A2: $FA \equiv \#(A)$;
   A3: $HA \equiv \#(A)$;
   A4: $HA \equiv \#(B)$;

   The above four assumptions are made since we have demonstrated that our protocol can withstand the replay attack.

   A5: $MU \equiv HA \Rightarrow MU \leftrightarrow FA$;
   A6: $FA \equiv HA \Rightarrow MU \leftrightarrow FA$;
   A7: $HA \equiv MU \Rightarrow A$;
   A8: $HA \equiv FA \Rightarrow B$;
   A9: $HA \equiv MU \Rightarrow ID_{MU}$;
   A10: $MU \equiv MU \leftrightarrow FA$;
   A11: $HA \equiv MU \leftrightarrow HA$;
   A12: $FA \equiv FA$;
   A13: $HA \equiv FA$;

3. In order to provide proper mutual authentication and the agreement of session key, our proposed protocol must satisfy the following goals:

   Goal1: $MU \equiv MU \leftrightarrow FA$;
Goal2: $MU \equiv FA \equiv MU \xleftarrow{SK} FA$;
Goal3: $FA \equiv MU \xleftarrow{SK} FA$;
Goal4: $FA \equiv MU \equiv MU \xleftarrow{SK} FA$;

(4) We analyze the idealized form of the proposed protocol according to the rules and assumptions of BAN logic. The main steps are shown as follows:

According to the message $m_1$, we could get

Statement1: $HA \leftarrow \langle A, ID_{HA} \rangle_{h(ID_{MU}||y)}$.
By Statement1 and A11, we apply the message-meaning rule to derive

Statement2: $HA \equiv FA \sim \langle A, ID_{HA} \rangle$.
By Statement2 and A3, we apply the nonce-verification rule and freshness-conjunctenation rule to derive

Statement3: $HA \equiv FA \equiv \langle A, ID_{HA} \rangle$.

According to the message $m_2$, we could get

Statement4: $HA \leftarrow \langle B \rangle_{SFA}$.
By Statement4 and A13, we apply the message-meaning rule to derive

Statement5: $HA \equiv FA \sim \langle B \rangle$.
By Statement5 and A4, we apply the nonce-verification rule to derive

Statement6: $HA \equiv FA \equiv \langle B \rangle$.

According to the message $m_3$, we could get

Statement7: $MU \leftarrow \langle A, B, MU \xleftarrow{dB} FA \rangle_{h(ID_{MU}||y)}$.
By Statement7 and A10, we apply the message-meaning rule to derive

Statement8: $MU \equiv HA \sim \langle A, B, MU \xleftarrow{dB} FA \rangle$.
By Statement8 and A1, we apply the nonce-verification rule and freshness-conjunctenation rule to derive

Statement9: $MU \equiv HA \equiv \langle A, B, MU \xleftarrow{dB} FA \rangle$.
By Statement9 and A5, we apply the jurisdiction rule to derive

Statement10: $MU \equiv \langle MU \xleftarrow{dB} FA \rangle$.
According to $SK = h(adB) = h(abdP)$, we could get

Statement11: $MU \equiv \langle MU \xleftarrow{SK} FA \rangle$. (Goal1)

According to the message $m_4$, we could get

Statement12: $FA \leftarrow \langle A, B, MU \xleftarrow{dA} FA \rangle_{SFA}$.
By Statement12 and A12, we apply the message-meaning rule to derive

Statement13: $FA \equiv HA \sim \langle A, B, MU \xleftarrow{dA} FA \rangle$.
By Statement13 and A2, we apply the nonce-verification rule and freshness-conjunctenation rule to derive

Statement14: $FA \equiv HA \equiv \langle A, B, MU \xleftarrow{dA} FA \rangle$.
By Statement14 and A6, we apply the jurisdiction rule to derive

Statement15: $FA \equiv \langle MU \xleftarrow{dA} FA \rangle$.
According to $SK = h(bdA) = h(abdP)$, we could get

Statement16: $FA \equiv \langle MU \xleftarrow{SK} FA \rangle$. (Goal2)

According to the message $m_5$, we could get

Statement17: $MU \leftarrow \langle A, B, MU \xleftarrow{SK} FA \rangle_{SK}$.
By Statement17, we apply the message-meaning rule to derive

Statement18: $MU \equiv FA \sim \langle A, B, MU \xleftarrow{SK} FA \rangle$. 

© Springer
Table 4  Communication cost comparison of our scheme and other schemes

|                         | Our scheme | He et al. [18] | Li et al. [7] | Mun et al. [8] | Chang et al. [5] |
|-------------------------|------------|----------------|---------------|----------------|------------------|
| Communication (bits)    | 5056       | 3072           | 8224          | 4192           | 1952             |
| Communication (rounds)  | 5          | 5              | 4             | 5              | 8                |

The bit-length of different parameter: \(xP: 1024\), \(g^x \mod p: 1024\), identity \(ID_x: 160\), time: 128, random number: 128, hash function \(h(x): 160\), encryption/decryption: 1024

By Statement18 and A1, we apply the nonce-verification rule and freshness-conjunctatenation rule to derive

Statement19: \(MU \equiv FA \equiv (A, B, MU \xleftrightarrow{SK} FA)\).

By Statement19, we break the conjunctions to produce

Statement20: \(MU \equiv FA \equiv (MU \xleftrightarrow{SK} FA)\). \hspace{1cm} (Goal3)

According to the message \(m_6\), we could get

Statement21: \(FA \leftarrow (A, B, MU \xleftrightarrow{SK} FA)_{SK}\).

By Statement21, we apply the message-meaning rule to derive

Statement22: \(FA \equiv MU \sim (A, B, MU \xleftrightarrow{SK} FA)\).

By Statement22 and A2, we apply the nonce-verification rule and freshness-conjunctatenation rule to derive

Statement23: \(FA \equiv MU \equiv (A, B, MU \xleftrightarrow{SK} FA)\).

By Statement23, we break the conjunctions to produce

Statement24: \(FA \equiv MU \equiv (MU \xleftrightarrow{SK} FA)\). \hspace{1cm} (Goal4)

Therefore, according to Goal1, Goal2, Goal3 and Goal4, we proved that our protocol establishes a secure session key between \(MU\) and \(FA\). Moreover, we also proved that \(MU\) and \(FA\) can authenticate each other using our protocol.

7 Performance Comparison and Functionality Analysis

In this section, we compares the performance and functionality of our proposed scheme with some previously schemes. It is well-known that most of the mobile devices have limited energy resources and computing capability. Hence, one of the most important issues in wireless networks is power consumption caused by communication and computation. In fact, the communication cost in the GLOMONET is higher than computation cost in terms of power consumption. In Table 4, we list the numbers of the message exchanges in the login, authentication and session key establish phases of our scheme and some related previous schemes. And the bit-length of communication of the mobile client in these phases is also shown since the foreign agent and home agent are regarded as powerful devices. Table 5 shows the computational cost of our proposed scheme and some other related protocols. Here we mainly focus on the total computational cost of three phases including login phase, authentication phase and session key establish phase because these phases are the principal part of an authentication scheme. And the computational cost showed is just the on-line computational cost, some pre-computations are not included. In general, our proposed scheme spends relatively few or almost the same communication and computational cost compared with some other schemes, especially for the mobile devices.
Table 5  Computational cost comparison of our scheme and other schemes

|                | MU   | FA   | HA   |
|----------------|------|------|------|
| Our scheme     | $3A+7H+1Mu+1D$ | $2H+2Mu+2E+1D+1G+1V$ | $2A+4H+3Mu+1E+1D+1G+1V$ |
| He et al. [2]  | $5A+10H+1E+1D$ | $2H+1E+1Da+1G+1V$   | $2A+3H+2D+1Ea+1G+1V$   |
| Li-Lee [7]     | $4A+2H+1Mo+3E+1D$ | $1H+3Mo+2E+2D+1G+1V$ | $2A+3H+3Mo+1E+3D+1G+1V$ |
| Mun et al. [8] | $2A+4H+1Mu+1E$ | $2A+3H+1Mu+1E$      | $3A+3H$                |

Note A: XOR operation, $H$: hash operation, $Mo$: modular exponentiation, $Mu$: point scalar multiplication, $E$: Symmetric encryption $E_K[·]$, $D$: Symmetric decryption $D_K[·]$, $Ea$: Asymmetric encryption $E_K{h(·)}$, $Da$: Asymmetric decryption $D_K{h(·)}$, $G$: Signature generation $E_K{h(·)}$, $V$: Signature verification $D_K{h(·)}$.

Table 6  Functionality comparison between the related schemes and our scheme

| Functionality                                | Our scheme | Wu et al. [6] | Chang et al. [5] | He et al. [2] | He et al. [9] | Mun et al. [8] | Liet al. [7] |
|----------------------------------------------|------------|---------------|------------------|---------------|---------------|----------------|---------------|
| User’s anonymity                             | Yes        | No            | No               | No            | No            | No             | Yes           |
| Proper mutual authentication                 | Yes        | No            | Yes              | Yes           | No            | No             | Yes           |
| Resist MU impersonation attack                | Yes        | No            | Yes              | Yes           | No            | No             | Yes           |
| Resist FA impersonation attack                | Yes        | No            | Yes              | Yes           | No            | No             | Yes           |
| Resist HA impersonation attack                | Yes        | Yes           | Yes              | Yes           | Yes           | No             | Yes           |
| Resist replay attack                         | Yes        | No            | Yes              | Yes           | No            | No             | No            |
| Perfect forward secrecy                      | Yes        | No            | No               | No            | No            | Yes            | Yes           |
| Resist off-line password guessing attack      | Yes        | No            | No               | Yes           | No            | Yes            | Yes           |
| Resist insider attack                        | Yes        | No            | No               | Yes           | No            | No             | Yes           |
| No verification table                        | Yes        | Yes           | No               | Yes           | No            | Yes            | Yes           |
| Local password verification                  | Yes        | No            | No               | Yes           | No            | Yes            | Yes           |
| Correct password change                      | Yes        | No            | No               | Yes           | No            | No             | Yes           |
| Provide the authentication scheme when user is located in his/her home network | Yes        | No            | No               | Yes           | No            | No             | No            |

Table 6 lists the functionality comparisons among our proposed scheme and other related schemes. It is obviously that our scheme has many excellent features and is more secure than other related schemes.

8 Conclusion

In this paper, we show that the recently proposed Mun et al.’s authentication scheme for roaming service cannot provide user friendliness, user’s anonymity, proper mutual authentication
and local verification and also vulnerable to impersonation attacks and insider attacks. In order to overcome the weaknesses of Mun et al.’s scheme, we propose a novel anonymous authentication scheme for roaming service in global mobility networks. Security and performance analysis show the proposed scheme is more suitable for the low-power and resource-limited mobile devices, and is secure against various attacks and has many excellent features.

Acknowledgments This paper was supported by the National Natural Science Foundation of China (Grant Nos. 61170269, 61121061), the China Postdoctoral Science Foundation Funded Project (Grant No. 2013MS540070), the Beijing Higher Education Young Elite Teacher Project (Grant No. YETP0449), and the Asia Foresight Program under NSFC Grant (Grant No. 61161140320).

References

1. Suzuki, S., & Nakada, K. (1997). An authentication technique based on distributed security management for the global mobility network. IEEE Journal Selected Areas in Communications, 15(8), 1608–1617.
2. He, D., Ma, M., Zhang, Y., Chen, C., & Bu, J. (2011). A strong user authentication scheme with smart cards for wireless communications. Computer Communications, 34(3), 367–374.
3. Zhu, J., & Ma, J. (2004). A new authentication scheme with anonymity for wireless environments. IEEE Transactions on Consumer Electronics, 51(1), 230–234.
4. Lee, C., Hwang, M., & Liao, I. (2006). Security enhancement on a new authentication scheme with anonymity for wireless environments. IEEE Transactions on Industrial Electronics, 53(5), 1683–1686.
5. Chang, C., Lee, C., & Chiu, Y. (2009). Enhanced authentication scheme with anonymity for roaming service in global networks. Computer Communications, 32(4), 611–618.
6. Wu, C., Lee, W., & Tsaur, W. (2008). A secure authentication scheme with anonymity for wireless communications. IEEE Communications Letters, 12(10), 722–723.
7. Li, C., & Lee, C. (2012). A novel user authentication and privacy preserving scheme with smart cards for wireless communications. Mathematical and Computer Modelling, 55(1–2), 35–44.
8. Mun, H., Han, K., Lee, Y., Yeun, C., & Choi, H. (2012). Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. Mathematical and Computer Modelling, 55(1–2), 214–222.
9. He, D., Chan, S., Chen, C., Bu, J., & Fan, R. (2011). Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks. Wireless Personal Communications, 61(2), 465–476.
10. Das, A. (2013). A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications. Networking Science, 2(1–2), 12–17.
11. Yoon, E., Yoo, K., & Ha, K. (2011). A user friendly authentication scheme with anonymity for wireless communications. Computers & Electrical Engineering, 37(3), 356–364.
12. Ou, H., Hwang, M., & Jan, J. (2010). A cocktail protocol with the authentication and key agreement on the UMTS. Journal of Systems and Software, 83(2), 316–325.
13. Yang, G., Huang, Q., Wong, D., & Deng, X. (2010). Universal authentication protocols for anonymous wireless communications. IEEE Transactions on Wireless Communication, 9(1), 168–174.
14. Lee, C., Chen, C., Ou, H., & Chen, L. (2013). Extension of an efficient 3GPP authentication and key agreement protocol. Wireless Personal Communications, 68(3), 861–872.
15. Juang, W., Chen, S., & Liaw, H. (2008). Robust and efficient password-authenticated key agreement using smart cards. IEEE Transactions on Industrial Electronics, 55(6), 2551–2556.
16. Yang, G., Wong, D., & Deng, X. (2007). Anonymous and authenticated key exchange for roaming networks. IEEE Transactions on Wireless Communications, 6(9), 1035–1042.
17. Wen, F., Susilo, W., & Yang, G. (2013). A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. Wireless Personal Communications, 73(3), 993–1004.
18. He, D., Zhang, Y., & Chen, J. (2014). Cryptanalysis and improvement of an anonymous authentication protocol for wireless access networks. Wireless Personal Communications, 74(2), 229–243.
19. Kim, J., & Kwak, J. (2012). Improved secure anonymous authentication scheme for roaming service in global mobility networks. International Journal of Security and Its Applications, 6(3), 45–54.
20. Chang, C., Le, H., & Chang, C. (2013). Novel untraceable authenticated key agreement protocol suitable for mobile communication. Wireless Personal Communications, 71(1), 425–437.
21. Jiang, Q., Ma, J., Li, G., & Yang, L. (2013). An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. Wireless Personal Communications, 68(4), 1477–1491.
22. Xie, Q., Hu, B., Tan, X., Bao, M., & Yu, X. (2014). Robust anonymous two-factor authentication scheme for roaming service in global mobility network. Wireless Personal Communications, 74(2), 601–614.
23. Xu, J., & Zhu, W. T. (2013). A generic framework for anonymous authentication in mobile networks. Journal of Computer Science and Technology, 28(4), 732–742.
24. Kim, J. S., & Kwak, J. (2013). Secure and efficient anonymous authentication scheme in global mobility networks. Journal of Applied Mathematics, Volume 2013, Article ID 302582.
25. Hankerson, D., Menezes, A., & Vanstone, S. (2004). Guide to elliptic curve cryptography. New York: Springer.
26. Koblitz, N. (1987). Elliptic curve cryptosystem. Journal of Mathematics of Computation, 48(177), 203–209.
27. Miller, V. S. (1985). Use of elliptic curves in cryptography. Proceeding on Advances in Cryptology-CRYPTO’85 (pp. 417–426). New York: Springer.
28. Burrows, M., Abadi, M., & Needham, R. (1990). A logic of authentication. ACM Transaction on Computer System, 8(1), 18–36.
29. Zhao, D., Peng, H., Wang, C., & Yang, Y. (2012). A secret sharing scheme with a short share realizing the (t, n) threshold and the adversary structure. Computers & Mathematics with Applications, 64(4), 611–615.
30. Yoo, S., Lee, H., & Kim, J. (2013). A performance and usability aware secure two-factor user authentication scheme for wireless sensor networks. International Journal of Distributed Sensor Networks Volume 2013, Article ID 543950.

Dawei Zhao received the M.S. degree in applied mathematics from Civil Aviation University of China, Tianjin, China, in 2011. He is currently a Ph.D. student in Beijing University of Posts and Telecommunications, Beijing, China. His research interests include information security and network security, in particular, cryptographic protocols.

Haipeng Peng received the M.S. degree in system engineering from Shenyang University of Technology, Shenyang, China, in 2006, and the Ph.D. degree in signal and information processing from Beijing University of Posts and Telecommunications, Beijing, China, in 2010. He is currently an associate professor at the School of Computer Science and Technology, Beijing University of Posts and Telecommunications, China. His research interests include information security, network security, complex networks and control of dynamical systems. Dr. H. Peng is the coauthor of 50 scientific papers and over 10 Chinese patents.
Lixiang Li received the M.S. degree in circuit and system from Yanshan University, Qinhuangdao, China, in 2003, and the Ph.D. degree in signal and information processing from Beijing University of Posts and Telecommunications, Beijing, China, in 2006. She is currently a professor at the School of Computer Science and Technology, Beijing University of Posts and Telecommunications, China. Her research interests include swarm intelligence, information security and network security. Dr. L. Li is the co-author of 70 scientific papers and 10 Chinese patents.

Yixian Yang received the M.S. degree in applied mathematics in 1986 and the Ph.D. degree in electronics and communication systems in 1988 from Beijing University of Posts and Telecommunications, Beijing, China. He is the Managing Director of information security center, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include network security, information security and coding theory. Dr. Y. Yang is the co-author of 300 scientific articles and 50 patents.