Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2013, Article ID 302582, 12 pages
http://dx.doi.org/10.1155/2013/302582

Research Article

Secure and Efficient Anonymous Authentication Scheme in Global Mobility Networks

Jun-Sub Kim[1] and Jin Kwak[2]

[1] *ISAA Lab, Department of Information Security Engineering, Soonchunhyang University, Asan, Chungchungnam-do 336-745, Republic of Korea*
[2] *Department of Information Security Engineering, Soonchunhyang University, Asan, Chungchungnam-do 336-745, Republic of Korea*

Correspondence should be addressed to Jin Kwak; jkwak@sch.ac.kr

Received 28 August 2013; Accepted 16 September 2013

Academic Editor: Jongsung Kim

In 2012, Mun et al. pointed out that Wu et al.'s scheme failed to achieve user anonymity and perfect forward secrecy and disclosed the passwords of legitimate users. And they proposed a new enhancement for anonymous authentication scheme. However, their proposed scheme has vulnerabilities that are susceptible to replay attack and man-in-the-middle attack. It also incurs a high overhead in the database. In this paper, we examine the vulnerabilities in the existing schemes and the computational overhead incurred in the database. We then propose a secure and efficient anonymous authentication scheme for roaming service in global mobility network. Our proposed scheme is secure against various attacks, provides mutual authentication and session key establishment, and incurs less computational overhead in the database than Mun et al.'s scheme.

1. Introduction

Global mobility network (GLOMONET) provides global roaming services for mobile user between the home agent and the foreign agent. The GLOMONET must have a user authentication scheme in which the mobile user has secure access to the foreign agent. 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) 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 [1, 2].

Many user authentication schemes for use in GLOMONET have been proposed [1–18]. In 2004, Zhu and Ma [4] proposed a simple, efficient wireless authentication scheme that provides user anonymity for wireless environments. However, Lee et al. [5] subsequently pointed out that Zhu et al.'s scheme does not achieve mutual authentication and perfect backward secrecy, and therefore cannot protect against forgery attacks. They then proposed a slight modification of Zhu et al.'s scheme. Unfortunately, Wu et al. [6] demonstrated that Lee et al.'s proposed scheme still failed to provide anonymity and perfect backward secrecy. Consequently, they proposed an improvement to overcome the weakness identified in Lee et al.'s scheme. In 2009, Zeng et al. [7] showed that Wu et al.'s scheme also fails to provide anonymity. In 2012, Mun et al. [12] showed that Wu et al.'s scheme discloses the password of legitimate users and does not achieve perfect forward secrecy. They subsequently proposed a new enhancement for anonymous authentication to overcome these security weaknesses. However, their scheme is vulnerable to replay attack and man-in-the-middle attack, and incurs a high overhead in the database of the home agent.

Therefore, in this paper, we analyze the existing schemes [5, 6, 12] and show that it is vulnerable to security requirement. And we propose a secure and efficient anonymous authentication scheme that is resistant to replay attack and man-in-the-middle attack. Our proposed scheme also incurs less computational overhead in the database than Mun et al.'s scheme.

The remainder of this paper is organized as follows. In Section 2, we review the existing schemes, while in Section 3,

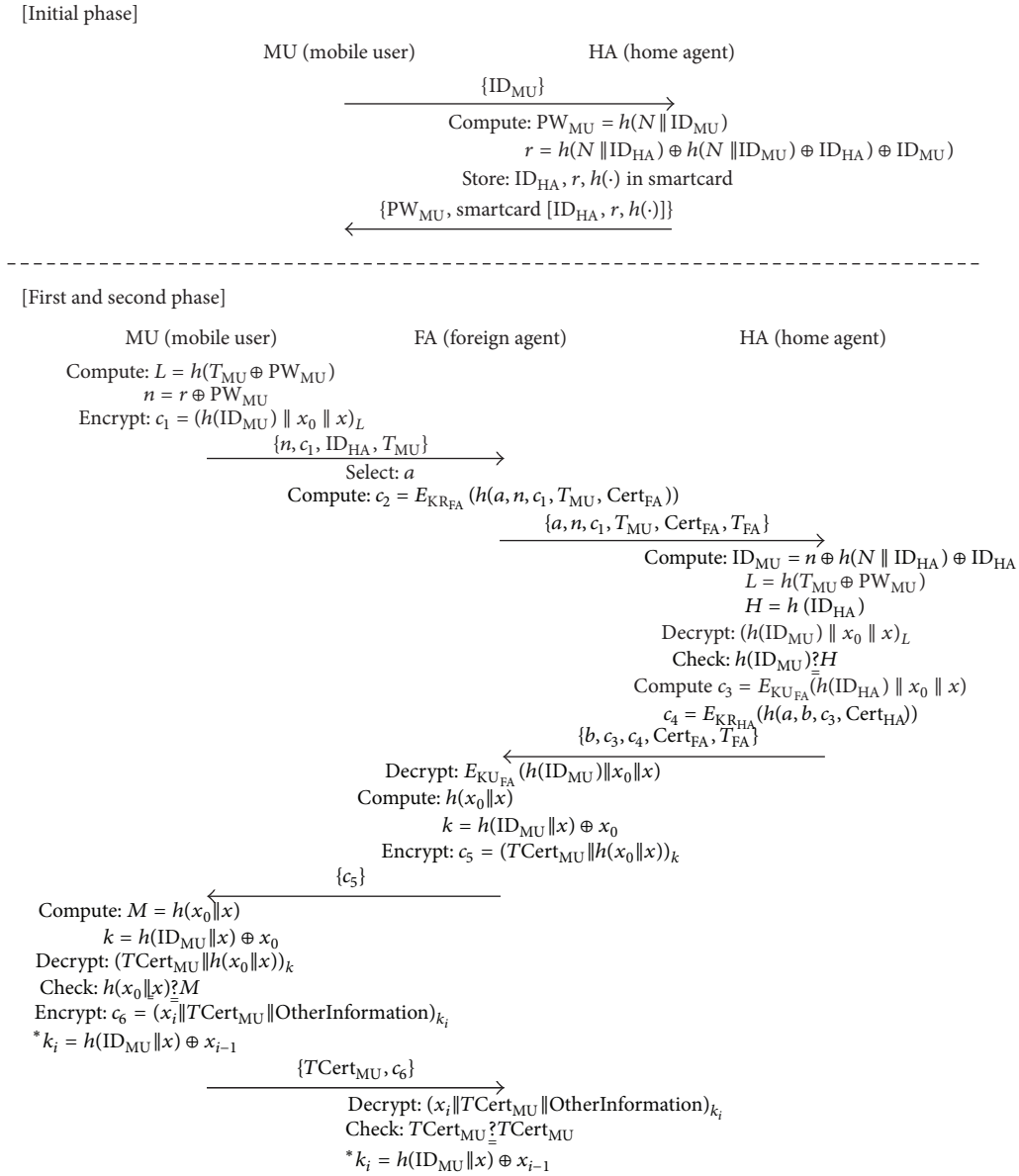

Figure 1: Procedure of Lee et al.'s scheme.

we investigate the security vulnerabilities mentioned above. In Section 4, we present our proposed secure and efficient anonymous authentication scheme. This scheme is analyzed and compared with other schemes in Section 5. Finally, Section 6 presents our conclusions.

2. Review of the Previous Schemes

In this section, we examine variety of authentication schemes with anonymity proposed by Lee et al. [5], Wu et al. [6], and Mun et al. [12].

2.1. Lee et al.'s Scheme. Figure 1 shows the procedure of Lee et al.'s scheme. Their scheme comprises three phases: an initial phase, a first phase, and a second phase.

2.1.1. Initial Phase. When a new mobile user MU wants to register with a home agent HA, he/she performs the following steps.

Step 1. Consider MU $\rightarrow$ HA : $\{ID_{MU}\}$.

MU sends his/her identifier ID_{MU} to HA for registration.

Step 2. HA computes $PW_{MU} = h(N \parallel ID_{MU})$ and $r = h(N \parallel ID_{HA}) \oplus h(N \parallel ID_{MU}) \oplus ID_{HA} \oplus ID_{MU}$, where N is a long random number kept by HA.

Step 3. Consider HA $\rightarrow$ MU : $\{PW_{MU}$, smart card $[ID_{HA}, r, h(\cdot)]\}$.

HA delivers PW_{MU} and a smart card containing $[ID_{HA}, r, h(\cdot)]$ to MU through a secure channel.

2.1.2. First Phase. In this phase, FA authenticates MU and issues a temporary certificate to MU, which will be used in the second phase when MU always communicates this FA within this area. MU performs the following steps.

Step 1. Consider MU $\rightarrow$ FA : $\{n, c_1, \mathrm{ID}_{\mathrm{HA}}, T_{\mathrm{MU}}\}$.

MU computes $n = r \oplus h(N \parallel \mathrm{ID}_{\mathrm{MU}})$ and temporary key $L = h(T_{\mathrm{MU}} \oplus \mathrm{PW}_{\mathrm{MU}})$, and encrypts $c_1 = (h(\mathrm{ID}_{\mathrm{MU}}) \parallel \|x_0\|x)_L$ using symmetric key L, where x_0 and x are secret random numbers. And, MU sends n, c_1, $\mathrm{ID}_{\mathrm{HA}}$, and T_{MU} to FA.

Step 2. Consider FA $\rightarrow$ HA : $\{a, n, c_1, T_{\mathrm{MU}}, c_2, \mathrm{Cert}_{\mathrm{FA}}, T_{\mathrm{FA}}\}$.

If timestamp is valid, FA generates a secret random number a and computes signature $c_2 = E_{\mathrm{KR}_{\mathrm{FA}}}(h(a, n, c_1, T_{\mathrm{MU}}, \mathrm{Cert}_{\mathrm{FA}}))$ using private key $\mathrm{KR}_{\mathrm{FA}}$. And, FA sends a, n, c_1, T_{MU}, c_2, $\mathrm{Cert}_{\mathrm{FA}}$, and T_{FA} to HA.

Step 3. Consider HA $\rightarrow$ FA : $\{b, c_3, c_4, \mathrm{Cert}_{\mathrm{HA}}, T_{\mathrm{HA}}\}$.

If certificate and timestamp are valid, HA computes $L = h(T_{\mathrm{MU}} \oplus \mathrm{PW}_{\mathrm{MU}})$ and $H = h(\mathrm{ID}_{\mathrm{HA}})$, and decrypts $(h(\mathrm{ID}_{\mathrm{MU}})\|x_0\|x)_L$ using symmetric key L. If $h(\mathrm{ID}_{\mathrm{HA}})$ is identical to H, HA authenticates MU. And, HA encrypts $c_3 = E_{\mathrm{KU}_{\mathrm{FA}}}(h(\mathrm{ID}_{\mathrm{MU}})\|x_0\|x)$ using public key $\mathrm{KU}_{\mathrm{FA}}$ and computes signature $c_4 = E_{\mathrm{KR}_{\mathrm{HA}}}(h(a, b, c_3, \mathrm{Cert}_{\mathrm{HA}}))$ using private key $\mathrm{KR}_{\mathrm{HA}}$. HA then sends b, c_3, c_4, $\mathrm{Cert}_{\mathrm{HA}}$, and T_{HA} to FA.

Step 4. Consider FA $\rightarrow$ MU : $\{c_5\}$.

If certificate and timestamp are valid, FA issues the temporary certificate $T\mathrm{Cert}_{\mathrm{MU}}$ and decrypts $E_{\mathrm{KU}_{\mathrm{FA}}}(h(\mathrm{ID}_{\mathrm{MU}})\|x_0\|x)$ using private key $\mathrm{KR}_{\mathrm{FA}}$. And, FA computes $h(x_0 \parallel x)$ and session key $k = h(\mathrm{ID}_{\mathrm{MU}} \parallel x) \oplus x_0$ and encrypts $c_5 = (T\mathrm{Cert}_{\mathrm{MU}} \parallel h(x_0 \parallel x))_k$ using symmetric key k. FA then sends c_5 to MU.

Step 5. MU computes $M = h(x_0 \parallel x)$ and session key $k = h(\mathrm{ID}_{\mathrm{MU}} \parallel x) \oplus x_0$ and decrypts $(T\mathrm{Cert}_{\mathrm{MU}} \parallel h(x_0 \parallel x))_k$ using symmetric key k. If is identical to M, MU authenticates FA.

2.1.3. Second Phase. In this phase, MU visits FA at ith session when he/she is always within this FA. MU performs the following steps.

Step 1. Consider MU $\rightarrow$ FA : $\{T\mathrm{Cert}_{\mathrm{MU}}, c_6\}$.

MU encrypts $c_6 = (x_i\|T\mathrm{Cert}_{\mathrm{MU}}\|\mathrm{OtherInfomation})_{k_i}$ using symmetric key k_i, where $k_i = h(\mathrm{ID}_{\mathrm{MU}} \parallel x) \oplus x_{i-1}$, for $i = 1, 2, \ldots, n$. And, MU sends $T\mathrm{Cert}_{\mathrm{MU}}$ and c_6 to FA.

Step 2. If $T\mathrm{Cert}_{\mathrm{MU}}$ is valid, FA decrypts $(x_i\|T\mathrm{Cert}_{\mathrm{MU}}\|\mathrm{OtherInfomation})_{k_i}$ using symmetric key k_i. If received $T\mathrm{Cert}_{\mathrm{MU}}$ if identical to obtained $T\mathrm{Cert}_{\mathrm{MU}}$, FA authenticates MU.

2.2. Wu et al.'s Scheme. Figure 2 shows the first and second phase of Wu et al.'s scheme. Their scheme comprises three phases: an initial phase, a first phase, and a second phase. The initial phase is the same as the initial phase of Lee et al.'s scheme.

2.2.1. First Phase. In this phase, FA authenticates MU and issues a temporary certificate to MU, which will be used in the second phase when MU always communicates this FA within this area. MU performs the following steps.

Step 1. Consider MU $\rightarrow$ FA : $\{n, c_1, \mathrm{ID}_{\mathrm{HA}}, T_{\mathrm{MU}}\}$.

MU computes $n = r \oplus h(N \parallel \mathrm{ID}_{\mathrm{MU}})$ and temporary key $L = h(T_{\mathrm{MU}} \oplus \mathrm{PW}_{\mathrm{MU}})$, and encrypts $c_1 = (h(\mathrm{ID}_{\mathrm{MU}}) \parallel \|x_0\|x)_L$ using symmetric key L, where x_0 and x are secret random numbers. And, MU sends n, c_1, $\mathrm{ID}_{\mathrm{HA}}$, and T_{MU} to FA.

Step 2. Consider FA $\rightarrow$ HA : $\{a, n, c_1, T_{\mathrm{MU}}, c_2, \mathrm{Cert}_{\mathrm{FA}}, T_{\mathrm{FA}}\}$.

If timestamp is valid, FA generates a secret random number a and computes signature $c_2 = E_{\mathrm{KR}_{\mathrm{FA}}}(h(a, n, c_1, T_{\mathrm{MU}}, \mathrm{Cert}_{\mathrm{FA}}))$ using private key $\mathrm{KR}_{\mathrm{FA}}$. And, FA sends a, n, c_1, T_{MU}, c_2, $\mathrm{Cert}_{\mathrm{FA}}$, and T_{FA} to HA.

Step 3. Consider HA $\rightarrow$ FA : $\{b, c_3, c_4, \mathrm{Cert}_{\mathrm{HA}}, T_{\mathrm{HA}}\}$.

If certificate and timestamp are valid, HA computes $L = h(T_{\mathrm{MU}} \oplus \mathrm{PW}_{\mathrm{MU}})$ and $H = h(\mathrm{ID}_{\mathrm{HA}})$, and decrypts $(h(\mathrm{ID}_{\mathrm{MU}})\|x_0\|x)_L$ using symmetric key L. If $h(\mathrm{ID}_{\mathrm{HA}})$ is identical to H, HA authenticates MU. And, HA encrypts $c_3 = E_{\mathrm{KU}_{\mathrm{FA}}}(h(h(N \parallel \mathrm{ID}_{\mathrm{MU}}))\|x_0\|x)$ using public key $\mathrm{KU}_{\mathrm{FA}}$ and computes signature $c_4 = E_{\mathrm{KR}_{\mathrm{HA}}}(h(a, b, c_3, \mathrm{Cert}_{\mathrm{HA}}))$ using private key $\mathrm{KR}_{\mathrm{HA}}$. HA then sends b, c_3, c_4, $\mathrm{Cert}_{\mathrm{HA}}$, and T_{HA} to FA.

Step 4. Consider FA $\rightarrow$ MU : $\{c_5\}$.

If certificate and timestamp are valid, FA issues the temporary certificate $T\mathrm{Cert}_{\mathrm{MU}}$ and decrypts $E_{\mathrm{KU}_{\mathrm{FA}}}(h(h(N \parallel \mathrm{ID}_{\mathrm{MU}}))\|x_0\|x)$ using private key $\mathrm{KR}_{\mathrm{FA}}$. And, FA computes $h(x_0 \parallel x)$ and session key $k = h(h(h(N \parallel \mathrm{ID}_{\mathrm{MU}}))\|x\|x_0)$ and encrypts $c_5 = (T\mathrm{Cert}_{\mathrm{MU}} \parallel h(x_0 \parallel x))_k$ using symmetric key k. FA then sends c_5 to MU.

Step 5. MU computes $M = h(x_0 \parallel x)$ and session key $k = h(h(h(N \parallel \mathrm{ID}_{\mathrm{MU}}))\|x\|x_0)$ and decrypts $(T\mathrm{Cert}_{\mathrm{MU}} \parallel h(x_0 \parallel x))_k$ using symmetric key k. If $h(x_0 \parallel x)$ is identical to M, MU authenticates FA.

2.2.2. Second Phase. In this phase, MU visits FA at ith session when he/she is always within this FA. MU performs the following steps.

Step 1. Consider MU $\rightarrow$ FA : $\{T\mathrm{Cert}_{\mathrm{MU}}, c_6\}$.

MU encrypts $c_6 = (x_i\|T\mathrm{Cert}_{\mathrm{MU}}\|\mathrm{OtherInfomation})_{k_i}$ using symmetric key k_i, where $k_i = h(h(h(N \parallel \mathrm{ID}_{\mathrm{MU}}))\|x\|x_{i-1})$, for $i = 1, 2, \ldots, n$. And, MU sends $T\mathrm{Cert}_{\mathrm{MU}}$ and c_6 to FA.

Step 2. If c_6 is valid, FA decrypts $(x_i\|T\mathrm{Cert}_{\mathrm{MU}}\|\mathrm{OtherInfomation})_{k_i}$ using symmetric key k_i. If received $T\mathrm{Cert}_{\mathrm{MU}}$ if identical to obtained $T\mathrm{Cert}_{\mathrm{MU}}$, FA authenticates MU.

2.3. Mun et al.'s Scheme. Their scheme comprises three phases: a registration phase, an authentication phase, and an update phase.

2.3.1. First Phase. Figure 3 shows the procedure of the first phase. When a new MU, wants to register with HA, he/she performs the following steps.

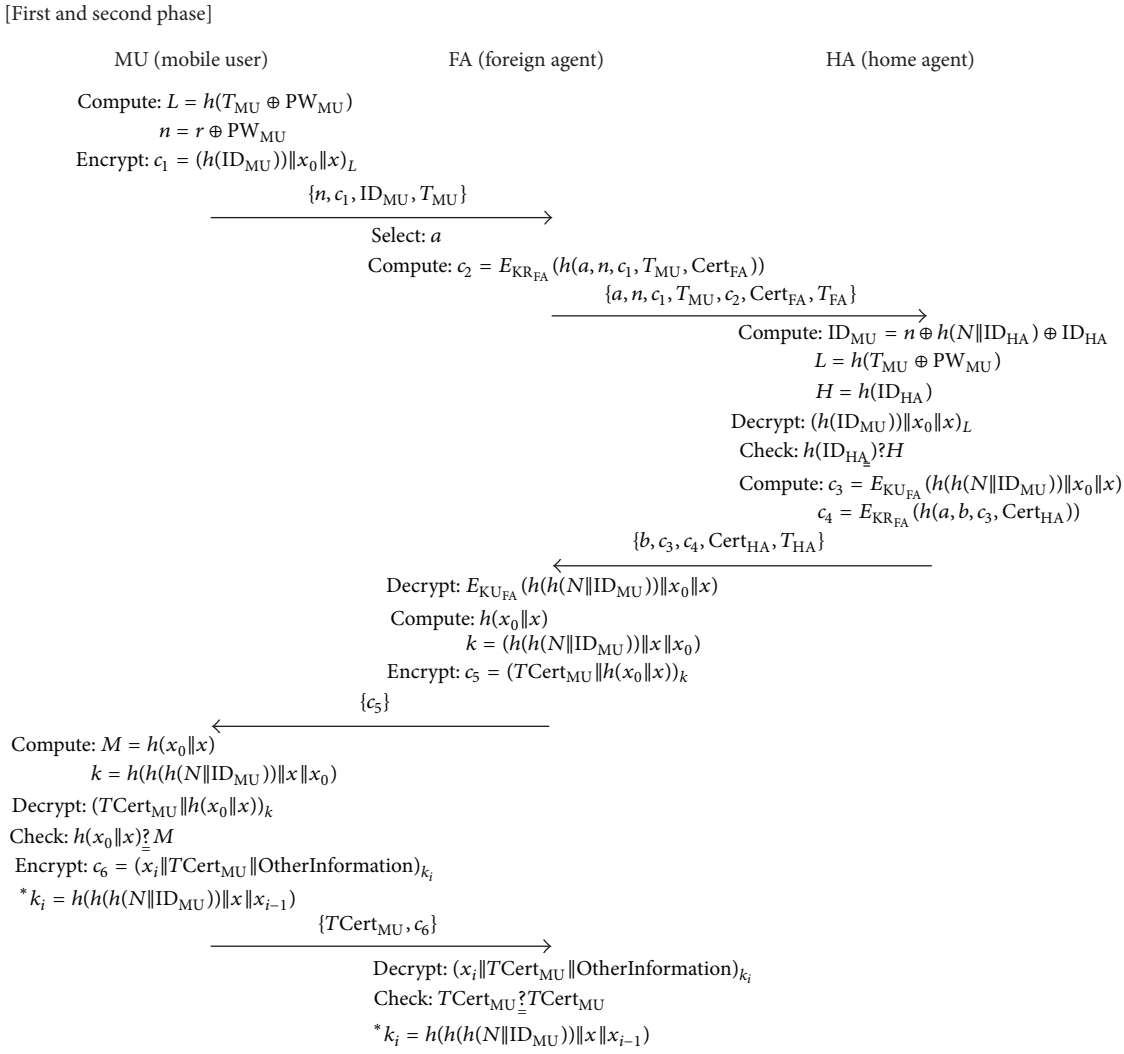

Figure 2: First and second phase of Wu et al.'s scheme.

Step 1. Consider MU $\rightarrow$ HA : $\{ID_{MU}, N_{MU}\}$.

MU sends his/her identifier ID_{MU} and nonce N_{MU} to HA for registration.

Step 2. HA generates nonce N_{HA} and computes $PW_{MU} = h(N_{MU} \parallel N_{HA})$ and $r_{MU} = h(ID_{MU} \parallel PW_{MU}) \oplus ID_{HA}$.

Step 3. Consider HA $\rightarrow$ MU : $\{r_{MU}, ID_{HA}, N_{HA}, PW_{MU}, h(\cdot)\}$.

HA sends r_{MU}, ID_{HA}, N_{HA}, PW_{MU}, and $h(\cdot)$ to MU through a secure channel.

2.3.2. Second Phase. Figure 4 shows the procedure of the second phase. In this phase, for mutual authentication between MU and HA and between MU and a foreign agent FA, the following steps are performed.

Step 1. Consider MU $\rightarrow$ FA : $\{ID_{HA}, N_{HA}, r_{MU}\}$.

MU accesses the new FA and sends ID_{HA}, N_{HA}, and r_{MU} to it.

Step 2. Consider FA $\rightarrow$ HA : $\{ID_{FA}, N_{FA}, r_{MU}\}$.

FA stores the message received from MU for further communication and generates nonce N_{FA}. FA then sends ID_{FA}, N_{FA}, and r_{MU} to HA.

Step 3. Consider HA $\rightarrow$ FA : $\{S_{HA}, P_{HA}\}$.

HA computes $r'_{MU} = h(ID_{MU} \parallel PW_{MU}) \oplus ID_{HA}$ and checks whether r'_{MU} is identical to the received r_{MU}. If they are identical, HA authenticates MU. Next, HA computes $P_{HA} = h(PW_{MU} \parallel N_{FA})$ and $S_{HA} = h(ID_{FA} \parallel N_{FA}) \oplus r_{MU} \oplus P_{HA}$, and sends the computed S_{HA} and P_{HA} to FA.

Step 4. Consider FA $\rightarrow$ MU : $\{S_{FA}, aP, P_{FA}\}$.

FA computes $S'_{HA} = h(ID_{FA} \parallel N_{FA}) \oplus r_{MU} \oplus P_{HA}$ and checks whether S'_{HA} is identical to the received S_{HA}. FA then computes $S_{FA} = h(S_{HA}\|N_{FA}\|N_{HA})$, selects a random number a, and then computes aP on E using the elliptic curve Diffie-Hellman (ECDH) protocol. Next, FA sends S_{FA}, aP, and $P_{FA} = (S_{HA}\|ID_{FA}\|N_{FA})$ to MU.

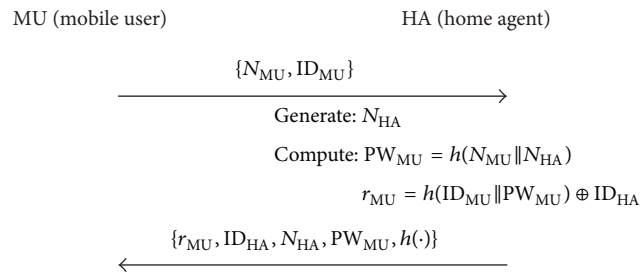

Figure 3: First phase of Mun et al.'s scheme.

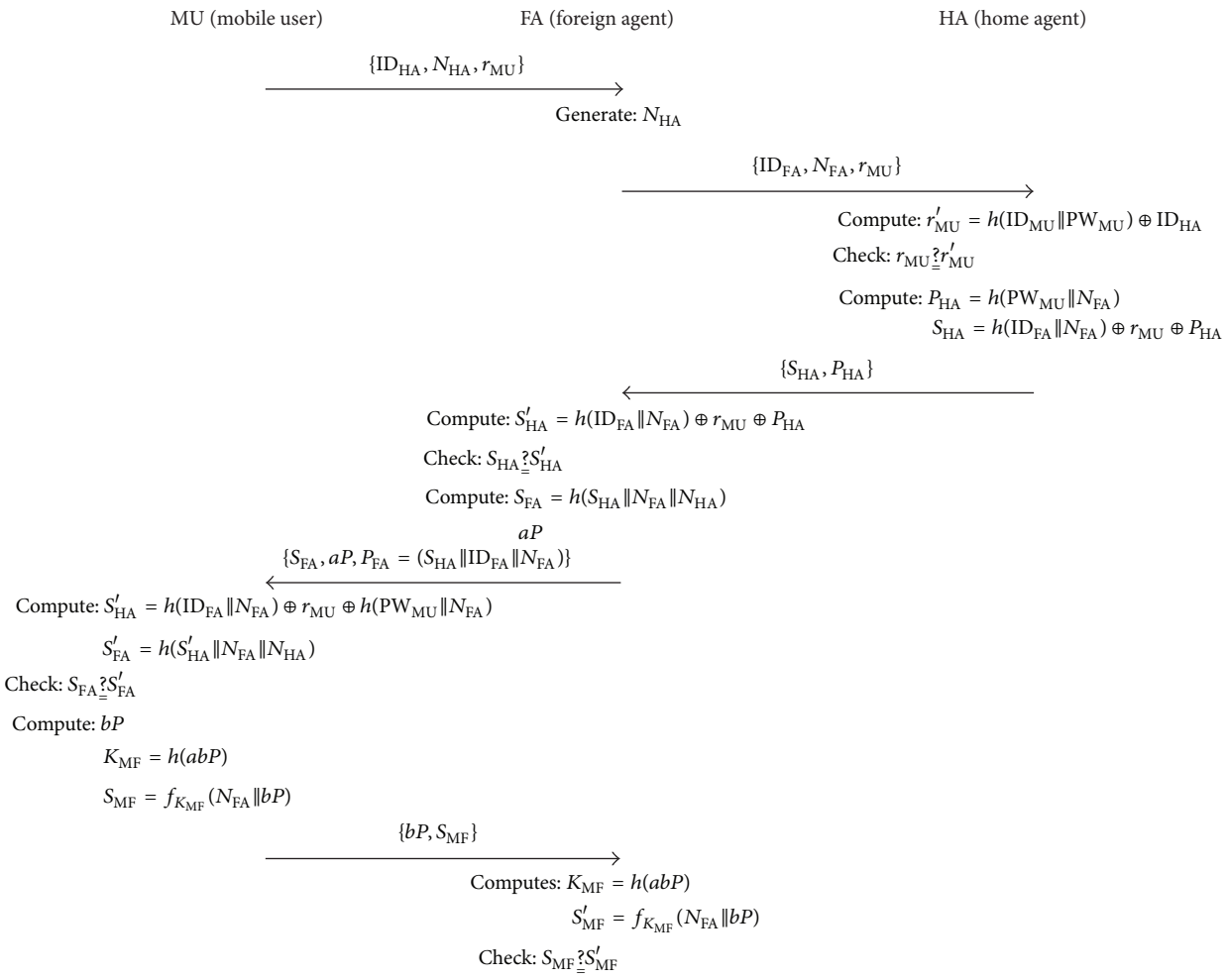

Figure 4: Second phase of Mun et al.'s scheme.

Step 5. Consider MU $\rightarrow$ FA : $\{bP, S_{MF}\}$.

MU computes $S'_{HA} = h(ID_{FA} \| N_{FA}) \oplus r_{MU} \oplus h(PW_{MU} \| N_{FA})$ and $S'_{FA} = h(S'_{HA} \| N_{FA} \| N_{HA})$, and checks whether S'_{FA} is identical to the received S_{FA}. If they are identical, MU authenticates HA and FA. After checking S_{FA}, MU selects a random number b and computes bP, a session key $K_{MF} = h(abP)$ using the received aP and the computed bP, and $S_{MF} = f_{K_{MF}}(N_{FA} \| bP)$. Next, MU sends the computed bP and S_{MF} to FA.

Step 6. FA computes $K_{MF} = h(abP)$ using private and public values, and $S'_{MF} = f_{K_{MF}}(N_{FA} \| bP)$. FA then checks whether S'_{MF} is identical to the received S_{MF}. If they are identical, FA authenticates MU.

2.3.3. Third Phase. The procedure followed in the third phase is depicted in Figure 5. The steps are as follows.

Step 1. Consider MU $\rightarrow$ FA : $\{b_i P\}$.

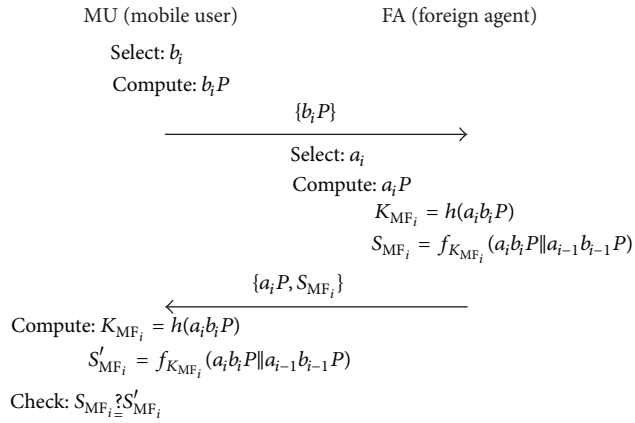

Figure 5: Third phase of Mun et al.'s scheme.

MU selects a new random number b_i and computes b_iP ($i = 1, 2, \ldots, n$). MU then sends b_i and b_iP to FA.

Step 2. Consider FA $\rightarrow$ MU : $\{a_iP, S_{MF_i}\}$.

FA selects a new random number a_i and computes a_iP ($i = 1, 2, \ldots, n$). It then computes a new session key $K_{MF_i} = h(a_ib_iP)$ and $S_{MF_i} = f_{K_{MF_i}}(a_ib_iP \parallel a_{i-1}b_{i-1}P)$. Next, it sends a_iP and S_{MF_i} to MU.

Step 3. MU computes a session key $K_{MF_i} = h(a_ib_iP)$, using the received a_iP, the computed b_iP, and $S'_{MF_i} = f_{K_{MF_i}}(a_ib_iP \parallel a_{i-1}b_{i-1}P)$. MU then checks whether S'_{MF_i} is identical to the received S_{MF_i}. If they are identical, MU and FA use the new session key K_{MF_i}.

3. Vulnerabilities in the Previous Schemes

3.1. Vulnerability of Lee et al.'s and Wu et al.'s Scheme. Lee et al.'s and Wu et al.'s scheme are almost the same. Therefore, their schemes are also the same vulnerabilities. Their scheme is vulnerable replay attack, is disclosed password, and cannot achieve anonymity and perfect forward secrecy.

3.1.1. Anonymity. An adversary A can eavesdrop on and record the message $\{n, c_1, \mathrm{ID_{HA}}, T_{MU}\}$ transmitted from MU to FA, and can obtain MU's $\mathrm{ID_{MU}}$ as follows.

Step 1. A register as legitimate user to HA and obtain own PW_A and r. And, A compute $h(N \parallel \mathrm{ID_{HA}})$ using PW_A, r, $\mathrm{ID_{HA}}$, and ID_A.

Step 2. A eavesdrops on and records messages $\{n, c_1, \mathrm{ID_{HA}}, T_{MU}\}$ transmitted from FA to MU.

Step 3. A compute $\mathrm{ID_{MU}}$ using n, $h(N \parallel \mathrm{ID_{HA}})$, and $\mathrm{ID_{HA}}$.

Therefore, Lee et al.'s and Wu et al.'s scheme cannot achieve anonymity [7].

3.1.2. Replay Attack. Legitimate FA_i can record the message $\{n, c_1, \mathrm{ID_{HA}}, T_{MU}\}$ transmitted from MU, and can then impersonate MU by using the recorded message $\{n, c_1, \mathrm{ID_{HA}}, T_{MU}\}$ to another FA_j as follows.

Step 1. FA_i accesses another FA_j and sends recorded message $\{n, c_1, \mathrm{ID_{HA}}, T_{MU}\}$ to this FA_j. FA_i can replay this message within the lifetime of T_{MU}. After receiving this message, FA_j sends the message $\{a, n, c_1, T_{MU}, c_2, \mathrm{Cert_{FA}}, T_{FA}\}$ to HA.

Step 2. HA compute $h(\mathrm{ID_{MU}})$ and checks whether the computed $h(\mathrm{ID_{MU}})$ is identical to the received $h(\mathrm{ID_{MU}})$. If they are identical, HA authenticate FA_i, then sends the message $\{b, c_3, c_4, \mathrm{Cert_{HA}}, T_{HA}\}$ to FA_j.

Step 3. FA_j computes session key k and sends the message $\{c_5\}$ to FA_i. FA_i computes the session key k between FA_i and MU, which is the same as the session key between FA_i and FA_j. And, FA_i decrypts c_5 and authenticates FA_j.

Therefore, Lee et al.'s and Wu et al.'s scheme is vulnerable to replay attack [11].

3.1.3. Disclosure Password. If an adversary A can steel MU's smart card, A can obtain MU's password $\mathrm{PW_{MU}}$ as follows.

Step 1. A can record the message $\{n, c_1, \mathrm{ID_{HA}}, T_{MU}\}$ transmitted from MU to FA. And, as described in Section 3.1.1, A can obtain the message $\{h(N \parallel \mathrm{ID_{HA}}), \mathrm{ID_{HA}}, \mathrm{ID_{MU}}\}$.

Step 2. A stole MU's smart card, inserts MU' smart card into the device, and enters the fake password $\mathrm{PW}^* = 0$. The smart card computes $n^* = r \oplus \mathrm{PW}^* = h(N \parallel \mathrm{ID_{HA}}) \oplus h(N \parallel \mathrm{ID_{MU}}) \oplus \mathrm{ID_{HA}} \oplus \mathrm{ID_{MU}}$ and A obtains n^* by eavesdropping.

Step 3. A computes $\mathrm{PW_{MU}}$ using n^*, $h(N \parallel \mathrm{ID_{HA}})$, $\mathrm{ID_{HA}}$, and $\mathrm{ID_{MU}}$.

Therefore, Lee et al.'s and Wu et al.'s scheme are disclosed password [11].

3.1.4. Perfect Forward Secrecy. Assume that an adversary A obtain MU's password $\mathrm{PW_{MU}}$. Failing to provide perfect forward secrecy is as follows.

Step 1. A computes L using T_{MU} and $\mathrm{PW_{MU}}$ and decrypts $(h(\mathrm{ID_{MU}}) \| x_0 \| x)_L$ using L. Thus, A obtains x_0, x, and $h(\mathrm{ID_{MU}})$.

Step 2. A computes session key k_1 using x_0, x, and $\mathrm{PW}_{\mathrm{MU}}$ and decrypts $(x_1 \| T\mathrm{Cert}_{\mathrm{MU}} \| \mathrm{OtherInformation})_{k_1}$ using k_1. Thus, A obtains x_1.

Step 3. A computes session key k_2 using x_1, x, and $\mathrm{PW}_{\mathrm{MU}}$.

Therefore, Lee et al.'s and Wu et al.'s scheme cannot achieve perfect forward secrecy [11].

3.2. Vulnerability of Mun et al.'s Scheme. Mun et al. claimed that their scheme can thwart a variety of known attacks. Unfortunately, we found that their scheme is vulnerable to replay attack and man-in-the-middle attack. In addition, their scheme incurs a high overhead in the database of the home agent.

3.2.1. Replay Attack. In Mun et al.'s scheme, an adversary A can eavesdrop on and record the message $\{\mathrm{ID}_{\mathrm{HA}}, N_{\mathrm{HA}}, r_{\mathrm{MU}}\}$ transmitted from MU to FA; and can then impersonate MU by using the recorded message $\{\mathrm{ID}_{\mathrm{HA}}, N_{\mathrm{HA}}, r_{\mathrm{MU}}\}$ as follows.

Step 1. A accesses a new FA and sends the recorded message $\{\mathrm{ID}_{\mathrm{HA}}, N_{\mathrm{HA}}, r_{\mathrm{MU}}\}$ to this FA. After receiving this message, the FA sends the message $\{\mathrm{ID}_{\mathrm{FA}}, N_{\mathrm{FA}}, r_{\mathrm{MU}}\}$ to HA.

Step 2. HA computes r'_{MU} and checks whether r'_{MU} is identical to the received r_{MU}. If they are identical, HA authenticates A, then computes P_{HA} and S_{HA}, and sends the message $\{S_{\mathrm{HA}}, P_{\mathrm{HA}}\}$ to FA. On receiving this message, FA computes S'_{HA} and checks whether S'_{HA} is identical to the received S_{HA}. Next, FA sends the message $\{S_{\mathrm{FA}}, aP, P_{\mathrm{FA}}\}$ to A.

Step 3. A computes S'_{FA} and checks whether S'_{FA} is identical to the received S_{FA}. If they are identical, A authenticates HA and FA, then computes bP and S_{MF}, and sends the message $\{bP, S_{\mathrm{MF}}\}$ to FA. On receiving this message, FA computes S'_{MF} and checks whether S'_{MF} is identical to the received S_{MF}. If they are identical, FA authenticates A.

Therefore, Mun et al.'s scheme is vulnerable to replay attack [18].

3.2.2. Man-in-the-Middle Attack. In Mun et al.'s scheme, an adversary A can eavesdrop on messages transmitted between FA and MU. Consequently, A can also successfully mount a man-in-the-middle attack as follows.

Step 1. A blocks and copies the message $\{S_{\mathrm{FA}}, aP, P_{\mathrm{FA}}\}$ transmitted from FA to MU. It then selects a new random number a', computes $a'P$, replaces message $\{S_{\mathrm{FA}}, aP, P_{\mathrm{FA}}\}$ with $\{S_{\mathrm{FA}}, a'P, P_{\mathrm{FA}}\}$, and sends this to MU.

Step 2. MU computes S'_{HA} and S'_{FA}, and checks whether S'_{FA} is identical to the received S_{FA}. After checking S_{FA}, MU selects a random number b and computes bP, a session key $K_{\mathrm{MF}} = h(a'bP)$ using the received $a'P$, the computed bP, and $S_{\mathrm{MF}} = f_{K_{\mathrm{MF}}}(N_{\mathrm{FA}} \parallel bP)$. Next, MU sends the message $\{bP, S_{\mathrm{MF}}\}$ to FA.

Step 3. A blocks and copies the message $\{bP, S_{MF}\}$ transmitted from MU to FA. It then selects a new random number b' and computes $b'P$, a session key $K_{\mathrm{MF}} = h(ab'P)$ using the copied aP and the computed $b'P$, and $S'_{\mathrm{MF}} = f_{K_{\mathrm{MF}}}(N_{\mathrm{FA}} \parallel b'P)$. Next, A replaces message $\{bP, S_{\mathrm{MF}}\}$ with $\{b'P, S'_{\mathrm{MF}}\}$ and sends this to FA.

Table 1: Notation used in our proposed scheme.

Notation	Description
MU	Mobile User
FA	Foreign Agent
HA	Home Agent
ID_X	Identity of an entity X
PW	Password of mobile user
N_X	Random nonce for current session of an entity X
N'_X	Random nonce for next session of an entity X
x	Master secret key of home agent
y	Secret number of each mobile user generated by home agent
$h(\cdot)$	A one-way hash function
$\oplus$	Exclusive OR operation
$\|\|$	Concatenation operation
E_K/D_K	Encryption/Decryption function of symmetric key cryptosystem using key K
f_K	MAC generation function by using the key K
K_{XY}	Session key between entity X and Y
$A \rightarrow B : X$	X is transmitted from A to B

Step 4. FA computes $K_{\mathrm{MF}} = h(ab'P)$ using private and public values and $S''_{\mathrm{MF}} = f_{K_{\mathrm{MF}}}(N_{\mathrm{FA}} \parallel b'P)$. It then checks whether S''_{MF} is identical to the value received for S'_{MF}. If they are identical, FA authenticates MU. However, the session key between FA and MU is different.

Therefore, Mun et al.'s scheme is vulnerable to man-in-the-middle attack [18].

3.2.3. High Overhead. For authentication, MU sends message $\{\mathrm{ID}_{\mathrm{HA}}, N_{\mathrm{HA}}, r_{\mathrm{MU}}\}$ to FA. After receiving this message, FA sends message $\{\mathrm{ID}_{\mathrm{FA}}, N_{\mathrm{FA}}, r_{\mathrm{MU}}\}$ to HA. In order to authenticate MU, HA computes $r'_{\mathrm{MU}} = h(\mathrm{ID}_{\mathrm{MU}} \parallel \mathrm{PW}_{\mathrm{MU}}) \oplus \mathrm{ID}_{\mathrm{HA}}$. To compute r_{MU} for MU, HA must find $\mathrm{ID}_{\mathrm{MU}}$ and $\mathrm{PW}_{\mathrm{MU}}$ in its own database to compute the authentication message. However, HA incurs a high overhead because of the difficulty of finding $\mathrm{ID}_{\mathrm{MU}}$ and $\mathrm{PW}_{\mathrm{MU}}$ in the authentication message. In addition, HA incurs computational cost because of the one-way hash function and exclusive OR operation used to compute the authentication message. In other words, HA computes the authentication message using $\mathrm{ID}_{\mathrm{MU}}$ and $\mathrm{PW}_{\mathrm{MU}}$ in its own database, and incurs a high overhead because it has to compare it with the received authentication message.

4. Our Proposed Scheme

In this section, we propose a secure and efficient anonymous authentication scheme for roaming services in GLOMONETs. This scheme consists of three phases: a registration phase, an authentication and key establishment phase, and an update session key phase.

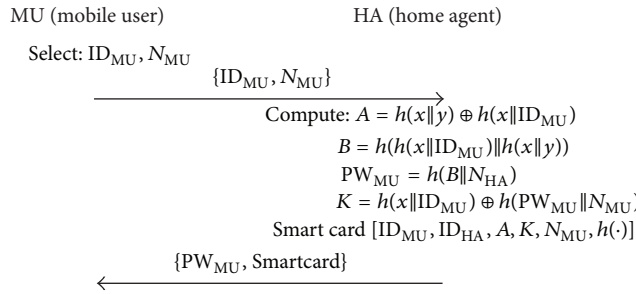

Figure 6: Registration phase of our proposed scheme.

4.1. Notation. Table 1 shows the notation used to describe our proposed scheme.

4.2. Registration Phase. Figure 6 illustrates the procedure of the registration phase. When a new MU wants to register with HA, he/she performs the following steps.

Step R1. Consider MU $\rightarrow$ HA : $\{ID_{MU}, N_{MU}\}$.

MU selects the identity ID_{MU} and a random nonce N_{MU}, and sends ID_{MU} and N_{MU} to HA for registration.

Step R2. Consider HA $\rightarrow$ MU : {Smart card $[ID_{MU}, ID_{HA}, K, N, h(x), h(\cdot)]$}.

After receiving the registration message from MU, HA selects a random nonce N_{HA} and computes the following:

$$\begin{aligned} A &= h(x \parallel y) \oplus h(x \parallel ID_{MU}), \\ B &= h(h(x \parallel ID_{MU}) \parallel h(x \parallel y)), \\ PW_{MU} &= h(B \parallel N_{HA}), \\ K &= h(x \parallel ID_{MU}) \oplus h(PW_{MU} \parallel N_{MU}). \end{aligned} \tag{1}$$

HA then issues a smart card containing $[ID_{MU}, ID_{HA}, A, K, N_{MU}, h(\cdot)]$ and delivers it to MU through a secure channel.

4.3. Authentication and Key Establishment Phase. The procedure followed in the authentication and key establishment phase is illustrated in Figure 7. In this phase, to attain mutual authentication between MU and HA, and between MU and FA, the following actions are performed.

Step A1. Consider MU $\rightarrow$ FA : $\{ID_{HA}, A, c_1, c_2, aP, N_{MU}\}$.

For authentication, MU selects a random nonce N'_{MU} and a random number a, and computes aP value on E using ECDH. MU then computes the following:

$$\begin{aligned} c_1 &= K \oplus h(PW_{MU} \parallel N'_{MU}), \\ c_2 &= h(aP \parallel h(PW_{MU} \parallel N'_{MU}) \parallel h(PW_{MU} \parallel N_{MU})). \end{aligned} \tag{2}$$

Next, MU sends ID_{HA}, A, c_1, c_2, aP, and N_{MU} to FA.

Step A2. Consider FA $\rightarrow$ HA : $\{ID_{FA}, A, c_1, c_2, aP, bP, N_{MU}\}$.

FA stores the ID_{HA} and aP received from MU for further communication, selects a random number b, and computes the bP value on E using ECDH. FA then sends ID_{FA}, A, c_1, c_2, aP, bP, and N'_{MU} to HA.

Step A3. Consider HA $\rightarrow$ FA : $\{ID_{HA}, ID_{FA}, c_3, aP, bP\}$.

On receiving the authentication message from FA, HA computes the following:

$$\begin{aligned} h(x \parallel ID_{MU}) &= A \oplus h(x \parallel y), \\ B' &= h(h(x \parallel ID_{MU}) \parallel h(x \parallel y)), \\ PW_{MU} &= h(B' \parallel N_{HA}), \\ K &= h(x \parallel ID_{MU}) \oplus h(PW_{MU} \parallel N_{MU}), \\ h(PW_{MU} \parallel N'_{MU}) &= c_1 \oplus K, \\ c'_2 &= h(aP \| h(PW_{MU} \parallel N'_{MU}) \| h(PW_{MU} \parallel N_{MU})). \end{aligned} \tag{3}$$

HA then checks whether c'_2 is identical to c_2. If they are identical, HA authenticates MU. HA then computes $c_3 = h(ID_{FA} \parallel aP \parallel bP \parallel K \parallel h(PW_{MU} \parallel N'_{MU}) \parallel h(PW_{MU} \parallel N_{MU}))$ and sends ID_{HA}, ID_{FA}, c_3, aP, and bP to FA.

Step A4. FA $\rightarrow$ MU : $\{ID_{HA}, ID_{FA}, c_3, aP, bP\}$.

FA checks ID_{HA}, ID_{FA}, and aP, and sends ID_{HA}, ID_{FA}, c_3, aP, and bP to MU.

Step A5. MU $\rightarrow$ FA : $\{S_{MF}\}$.

MU checks ID_{HA} and aP, and computes $c'_3 = h(ID_{FA} \parallel aP \parallel bP \parallel K \parallel h(PW_{MU} \parallel N'_{MU}) \parallel h(PW_{MU} \parallel N_{MU}))$. MU checks whether c'_3 is identical to c_3. If they are identical, MU authenticates HA and FA. MU then computes $K_{MF} = h(abP)$ using private and public keys and $S_{MF} = f_{K_{MF}}(ID_{FA} \| aP \| bP)$. Next, MU sends S_{MF} to FA.

Step A6. FA computes $K_{MF} = h(abP)$ using private and public keys and $S'_{MF} = f_{K_{MF}}(ID_{FA} \| aP \| bP)$. FA then checks whether S'_{MF} is identical to S_{MF}. If they are identical, FA authenticates MU. Otherwise, the procedure is terminated.

4.4. Update Session Key Phase. The update session key phase is the same as the third phase of Mun et al.'s scheme, as shown in Figure 5.

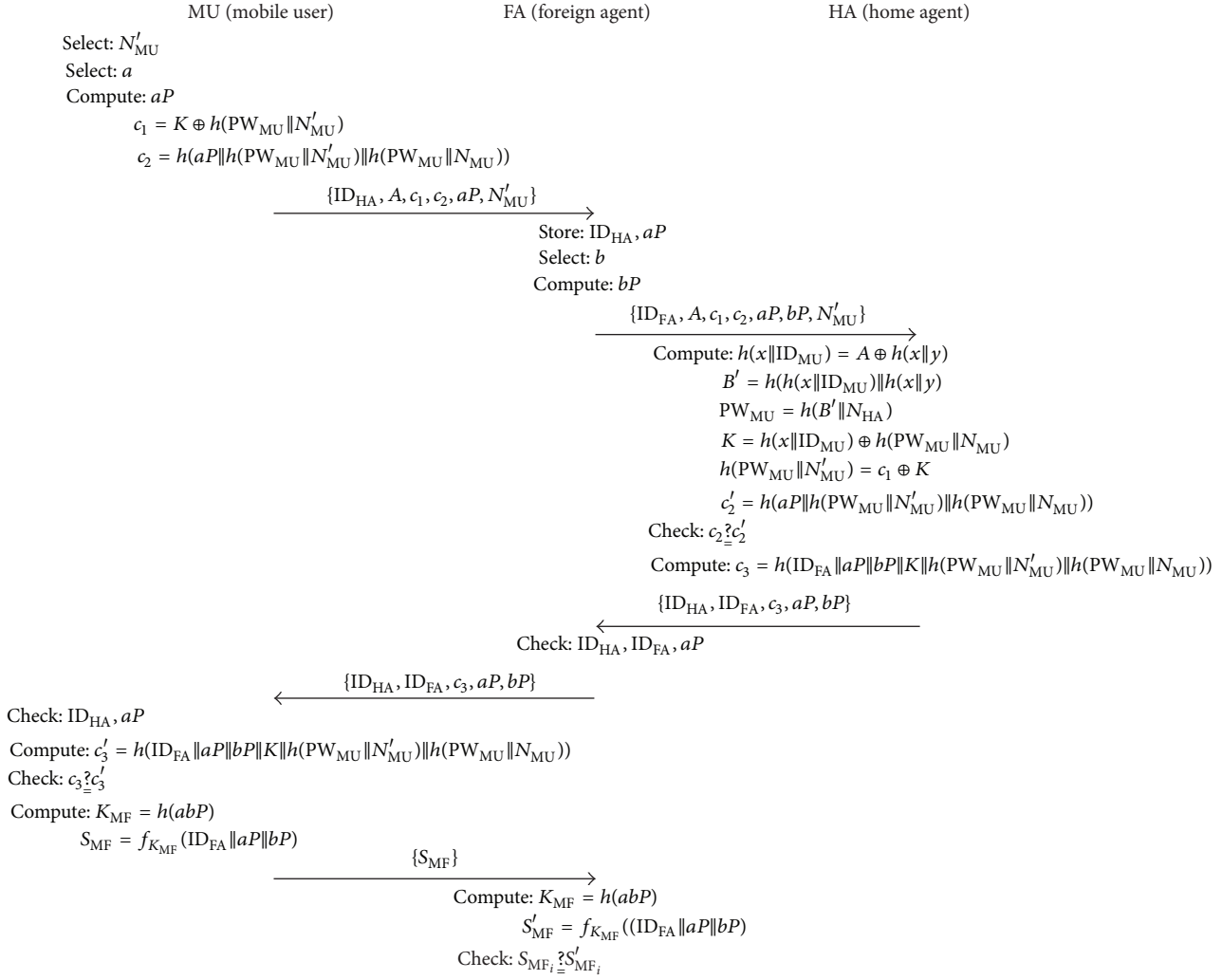

Figure 7: Authentication and key establishment phase of our proposed scheme.

Table 2: Security analysis of the compared schemes.

Scheme	Proposed scheme	Zhu and Ma [4]	Lee et al. [5]	Wu et al. [6]	Mun et al. [12]
Anonymity	Yes	No	No	No	Yes
Perfect forward secrecy	Yes	No	No	No	Yes
Mutual authentication (MU-HA)	Yes	No	No	No	Yes
Mutual authentication (MU-FA)	Yes	No	Yes	Yes	Yes
Replay attack	Yes	Yes	No	No	No
Impersonation attack	Yes	Yes	Yes	Yes	Yes
Disclosure of password	Yes	Yes	No	No	Yes
Man-in-the-middle attack (MU-HA)	Yes	No	No	No	Yes
Man-in-the-middle attack (MU-FA)	Yes	No	Yes	Yes	No

5. Analyses

5.1. Security Analysis. Table 2 compares the security of existing schemes with that of our proposed scheme. Our scheme has the following security properties.

Anonymity. Assume that an adversary A intercepts the message $\{c_1, c_2, c_3, A\}$ over a public network. An adversary cannot derive the identifier ID_{MU} of the mobile user from c_1, c_2, c_3, and A. This is because an adversary does not know x, y, and PW_{MU}.

Perfect Forward Secrecy. The authentication and key establishment and update session key phases of our scheme use ECDH to provide perfect forward secrecy. To establish a session key, MU and FA use different a_iP and b_iP for each session, and

Table 3: Performance analysis of the compared schemes.

Scheme	Proposed scheme	Zhu and Ma [4]	Lee et al. [5]	Wu et al. [6]	Wu et al. [6]
Registration					
MU	—	—	—	—	—
HA	$5T(\mathrm{h}) + 2T(\oplus)$	$2T(\mathrm{h}) + 3T(\oplus)$	$2T(\mathrm{h}) + 3T(\oplus)$	$2T(\mathrm{h}) + 3T(\oplus)$	$2T(\mathrm{h}) + 1T(\oplus)$
Authentication and key establishment					
MU	$4T(\mathrm{h}) + 1T(\oplus) +$ 1 Asym	$2T(\mathrm{h}) + 3T(\oplus) +$ 2 Sym	$4T(\mathrm{h}) + 3T(\oplus) +$ 2 Sym	$3T(\mathrm{h}) + 1T(\oplus) +$ 1 Sym	$5T(\mathrm{h}) + 2T(\oplus) +$ 1 Asym
FA	$1T(\mathrm{h}) + 1$ Asym	$2T(\mathrm{h}) + 1T(\oplus) +$ 1 Sym + 2 Asym	$4T(\mathrm{h}) + 1T(\oplus) +$ 2 Sym + 2 Asym	$5T(\mathrm{h}) + 3$ Asym	$4T(\mathrm{h}) + 2T(\oplus) +$ 1 Asym
HA	$6T(\mathrm{h}) + 3T(\oplus)$	$3T(\mathrm{h}) + 1$ Sym + 3 Asym	$3T(\mathrm{h}) + 1$ Sym + 2 Asym	$2T(\mathrm{h}) + 2$ Sym	$3T(\mathrm{h}) + 3T(\oplus)$
Total	$16T(\mathrm{h}) + 6T(\oplus) +$ 2 Asym	$9T(\mathrm{h}) + 7T(\oplus) +$ 3 Sym + 5 Asym	$13T(\mathrm{h}) + 7T(\oplus) +$ 5 Sym + 4 Asym	$12T(\mathrm{h}) + 4T(\oplus) +$ 3 Sym + 3 Asym	$14T(\mathrm{h}) + 8T(\oplus) +$ 2 Asym

$T(\mathrm{h})$: number of hash operation, $T(\oplus)$: number of XOR operation, Sym: number of symmetric key operation, Asym: number of asymmetric key operation.

thus they are not related to previous values $a_{i-1}P$ and $b_{i-1}P$. Thus, if the previous session key $K_{\mathrm{MF}_{i-1}} = h(a_{i-1}b_{i-1}P)$, is disclosed, an adversary A cannot guess $K_{\mathrm{MF}_i} = h(a_ib_iP)$. In other words, guessing K_{MF_i} is a computationally difficult problem.

Mutual Authentication. HA can authenticate MU by checking c_2 in Step A3 of the authentication and key establishment phase, and MU can authenticate HA and FA by checking c_3 in Step A5 of the authentication and key establishment phase. And, FA can authenticate MU by checking S_{MF} in Step A6 of the authentication and key establishment phase.

Impersonation Attack. An adversary A cannot compute the authentication message $\{\mathrm{ID}_{\mathrm{HA}}, A, c_1, c_2, aP, N'_{\mathrm{MU}}\}$ because he/she cannot know $\mathrm{ID}_{\mathrm{MU}}$, x, y, $\mathrm{PW}_{\mathrm{MU}}$, and N_{HA}. Even if A is a legitimate user of HA, he/she cannot compute the authentication message $\{\mathrm{ID}_{\mathrm{HA}}, A, c_1, c_2, aP, N'_{\mathrm{MU}}\}$.

Disclosure of Password. We assume that an adversary A eavesdrops on MU's authentication message $\{\mathrm{ID}_{\mathrm{HA}}, A, c_1, c_2, aP, N'_{\mathrm{MU}}\}$ in the authentication and key establishment phase. However, A cannot know MU's $\mathrm{PW}_{\mathrm{MU}}$ from the authentication message $\{\mathrm{ID}_{\mathrm{HA}}, A, c_1, c_2, aP, N'_{\mathrm{MU}}\}$ by the nature of a one-way hash function.

Replay Attacks. MU uses a random nonce N_{MU} and checks c_2 to resist replay attacks in each authentication session. If an adversary A is replaying the previous authentication message, but he/she cannot authenticate from HA because c_2 fail to check.

Man-in-the-Middle Attacks. Man-in-the-middle attacks are thwarted because of the authentication between MU and HA. Similarly, man-in-the-middle attacks can be thwarted by the establishment of a session key between MU and FA.

5.2. Performance Analysis. Table 3 compares the performance of existing schemes with that of our proposed scheme. Our scheme incurs less communication cost than conventional schemes [4–6]. Although our scheme incurs a little more communication cost than Mun et al.'s scheme, it incurs less computational overhead in the database than Mun et al.'s scheme [12].

No Need for Time Synchronization. Conventional schemes use timestamps to resist replay attacks. Thus, time synchronization takes place when each entity is located in a different time zone. However, our scheme does not use timestamps, so there is no need to synchronize time between different entities.

Use of ECDH. Conventional schemes use certificates. However, mobile devices have power limitations; low-level computation based on certificates incurs a significant overhead. Our scheme uses ECDH instead of a public key cryptosystem with certificates in order to reduce the communication overhead. ECDH provides the same security properties and uses fewer resources than a public key cryptosystem with certificates. The performance advantage of ECDH is improved further as security needs increase.

Overhead Analysis. Our proposed authentication scheme can be compared with Mun et al.'s scheme in terms of the database overhead incurred by HA as the number of devices increase. In order to compare the overhead, the following terms are defined: the number of devices is d ($d = 1, 10, 20, \ldots, 100$), the identifier stored in the database of the home agent is i, the computational cost for a one-way hash function and exclusive OR operation is c (it is assumed that the computational cost for a one-way hash function and exclusive OR operation is 2, thus, $c = 2$), and, finally, the overhead in the database of the home agent is O. Thus, the overhead can be expressed as $O = d \times i \times c$, that is, $O = 10 \times 10 \times 2 = 200$. Mun et al.'s scheme must obtain identifier and password information from its own database in order to compute the authentication message. However, their scheme compares the authentication message to compute the identifier and password of all the mobile users stored in its own database because of the difficulty of finding identifier and password information in the authentication message. For example, in Mun et al.'s scheme, if the number of devices to be authenticated by HA is 30, the number

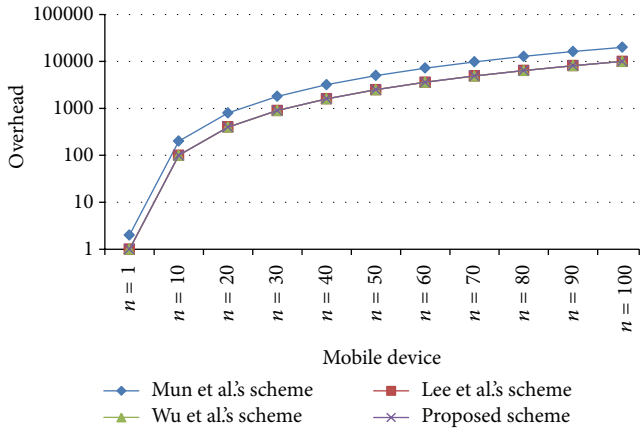

FIGURE 8: Analysis of overhead incurred versus number of devices.

of identifiers stored in the database of the home agent is also 30, the computational cost for a one-way hash function and exclusive OR operation is 2 (according to Mun et al.'s scheme, $c = 2$ because of the computational cost incurred); therefore, the overhead incurred in the database of HA is $O = 30 \times 30 \times 2 = 1800$. Our proposed scheme can compute the authentication message in its own database because the identifier information can be found in the authentication message. For example, in our proposed scheme, if the number of devices to be authenticated by the home agent is 30, the number of identifiers stored in the database of the home agent is also 30, the computational cost for a one-way hash function and exclusive OR operation is 1 (our proposed scheme does not incur computational cost; thus, $c = 1$), and thus, the overhead incurred in the database of HA is $O = 30 \times 30 \times 1 = 900$. Just like our proposed scheme, Lee et al.'s and Wu et al.'s scheme are the same overhead analysis. Compared to the existing scheme, our proposed scheme incurs less computational overhead in the database (Figure 8).

6. Conclusion

In this paper, we examined the previous schemes and security vulnerabilities of the previous schemes. Lee et al.'s and Wu et al.'s scheme was vulnerable to replay attack, cannot achieved perfect forward secrecy, cannot provided anonymity. And Mun et al.'s scheme was vulnerable to replay attack and man-in-the-middle attack, and incurred a high overhead in the database. Therefore, we proposed a secure and efficient anonymous authentication scheme for roaming service in GLOMONET. Our scheme was developed using ECDH instead of the authentication mechanism used by Mun et al.'s scheme. Consequently, unlike Mun et al.'s scheme, our scheme achieves anonymity, provides perfect forward secrecy and mutual authentication, and is resistant to replay attack and man-in-the-middle attack. And our scheme incurs less overhead in the database than Mun et al.'s scheme does. In addition, our scheme does not use timestamps, and as a result, it does not need to synchronize time between different entities.

Acknowledgments

This research was funded by the MSIP (Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013. This work was supported by the Soonchunhyang University Research Fund. The authors declare that there is no conflict of interests regarding the publication of this article.

References

[1] S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," *IEEE Journal on Selected Areas in Communications*, vol. 15, no. 8, pp. 1608–1617, 1997.

[2] D. He and S. Chan, "A secure and lightweight user authentication scheme with anonymity for the global mobility network," in *Proceedings of the 13th International Conference on Network-Based Information Systems (NBiS '10)*, pp. 305–312, Takayama, Japan, September 2010.

[3] L. Buttyán, C. Gbaguidi, and S. Staamann, "Extensions to an authentication technique proposed for the global mobility network," *IEEE Transactions on Communications*, vol. 48, no. 3, pp. 373–376, 2000.

[4] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 231–235, 2004.

[5] C. Lee, M. Hwang, and I. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1687, 2006.

[6] C. Wu, W. Lee, and W. Tsaur, "A secure authentication scheme with anonymity for wireless communications," *IEEE Communications Letters*, vol. 12, no. 10, pp. 722–723, 2008.

[7] P. Zeng, Z. Cao, K. R. Choo, and S. Wang, "On the anonymity of some authentication schemes for wireless communications," *IEEE Communications Letters*, vol. 13, no. 3, pp. 170–171, 2009.

[8] J. Lee, J. H. Chang, and D. H. Lee, "Security flaw of authentication scheme with anonymity for wireless communications," *IEEE Communications Letters*, vol. 13, no. 5, pp. 292–293, 2009.

[9] C. Chang, C. Lee, and Y. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks," *Computer Communications*, vol. 32, no. 4, pp. 611–618, 2009.

[10] T. Youn, Y. Park, and J. Lim, "Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks," *IEEE Communications Letters*, vol. 13, no. 7, pp. 471–473, 2009.

[11] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," *Computer Communications*, vol. 34, no. 3, pp. 367–374, 2011.

[12] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks," *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 214–222, 2012.

[13] Q. Pu, "An enhanced authentication scheme with anonymity for roaming service in global mobility networks," in *Proceedings of the 2nd International Conference on MultiMedia and Information Technology (MMIT '10)*, pp. 219–222, Kaifeng, China, April 2010.

[14] T. Zhou and J. Xu, "Provable secure authentication protocol with anonymity for roaming service in global mobility networks," *Computer Networks*, vol. 55, no. 1, pp. 205–213, 2011.

[15] T. Lee and T. Hwang, "Provably secure and efficient authentication techniques for the global mobility network," *Journal of Systems and Software*, vol. 84, no. 10, pp. 1717–1725, 2011.

[16] C. C. Lee, Y. M. Lai, and C. T. Li, "An improved secure dynamic ID based remote user authentication scheme for multiserver environment," *International Journal of Security and Its Applications*, vol. 6, pp. 203–210, 2012.

[17] Y. An and Y. Joo, "Security analysis and improvements of a password-based mutual authentication scheme with session key agreement," *International Journal of Security and Its Applications*, vol. 7, pp. 85–94, 2013.

[18] J. S. Kim and J. Kwak, "Improved secure anonymous authentication scheme for roaming service in global mobility networks," *International Journal of Security and Its Applications*, vol. 6, pp. 45–54, 2012.