Privacy-preserving mobile roaming authentication with security proof in global mobility networks

Xie, Qi; Hong, Dongzhao; Bao, Mengjie; Dong, Na; Wong, Duncan S.

Published in:
International Journal of Distributed Sensor Networks

Published: 01/01/2014

Document Version:
Final Published version, also known as Publisher's PDF, Publisher's Final version or Version of Record

Published version (DOI):
10.1155/2014/325734

Publication details:
Xie, Q., Hong, D., Bao, M., Dong, N., & Wong, D. S. (2014). Privacy-preserving mobile roaming authentication with security proof in global mobility networks. *International Journal of Distributed Sensor Networks*, *2014*, Article 325734. https://doi.org/10.1155/2014/325734

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 325734, 7 pages
http://dx.doi.org/10.1155/2014/325734

Research Article

Privacy-Preserving Mobile Roaming Authentication with Security Proof in Global Mobility Networks

Qi Xie,[1] Dongzhao Hong,[1] Mengjie Bao,[1] Na Dong,[1] and Duncan S. Wong[2]

[1] *Hangzhou Key Laboratory of Cryptography and Network Security, Hangzhou Normal University, Hangzhou 311121, China*
[2] *Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong, China*

Correspondence should be addressed to Qi Xie; qixie68@126.com

Received 11 February 2014; Revised 9 May 2014; Accepted 16 May 2014; Published 25 May 2014

Academic Editor: Jianliang Xu

Mobile roaming authentication scheme achieves the mutual authentication and session key establishment between the mobile user and the foreign agent. In 2013, Xie et al. pointed out that Chen et al.'s scheme is vulnerable to offline password attack, and does not achieve fair session key generation, user untraceability, user friendliness, and perfect forward secrecy, and then they proposed an improved scheme. In this paper, we propose an improvement of Xie et al.'s scheme, since the foreign agent may confuse the mobile users when multiple mobile users simultaneously access the foreign agent in Xie et al.'s scheme. Further, we prove the formal security of the proposed scheme, and present the performance comparison between our scheme and some related schemes. The proposed scheme is more efficient and secure than other related schemes and is suitable for using in the global mobility network.

1. Introduction

With the rapid development of mobile technology such as 3G and 4G wireless networks, more and more mobile users can access services in global mobility networks. A typical mobile roaming authentication scheme includes three parties: a mobile user, a foreign agent, and a home agent; both the mobile user and the foreign agent should authenticate each other before establishing the session key. Privacy-preserving is usually referred to as user anonymity and user untraceability. It is important to protect the user's privacy, such as what the users did or where the users accessed, from the attacker even if he accesses to user's records. Strong anonymous mobile roaming authentication means that only the home agent can know the mobile user's identity, but adversary or foreign agent cannot. Since wireless network is more vulnerable to several attacks and mobile terminals' computational power is limited, therefore, how to design the secure and efficient authentication scheme for roaming service with strong anonymity in global mobility networks is brought into much attention.

In 2004, Zhu and Ma [1] proposed a first anonymous authentication scheme for wireless communications. Lee et al. [2] showed that their scheme is vulnerable to forgery attacks and does not provide perfect backward secrecy and mutual authentication and proposed an improved scheme. Later, Chang et al. [3], Wu et al. [4], and Xu et al. [5] pointed out that Lee et al.'s scheme cannot achieve privacy-preserving and proposed an improved scheme, respectively. However, Youn et al. [6] showed that Chang et al.'s improved scheme does not achieve user anonymity and provide secure key establishing service, and Mun et al. [7] showed that Wu et al.'s scheme does not achieve anonymity and perfect forward secrecy. In 2011, He et al. [8] proposed a two-factor user authentication scheme for wireless communications. But Li and Lee [9] demonstrated that He et al.'s scheme has several weaknesses such as lacks of user friendliness, user anonymity, and fairness of key agreement, and then they proposed an improvement of He et al.'s scheme. However, Hu et al. [10] showed that Li et al.'s improved scheme cannot resist the foreign agent's impersonation attacks and proposed an improved scheme. In 2011, Chen et al. [11] proposed

a lightweight anonymous user authentication for roaming in the global mobility network, but Xie et al. [12] showed that their scheme is vulnerable to offline password attack and does not achieve fair session key generation, user untraceability, user friendliness, and perfect forward secrecy; then they proposed an improved scheme to overcome the weaknesses of Chen et al.'s scheme. Very recently, Chen et al. [13] and Xie et al. [14] proposed some other anonymous authentication schemes for roaming service in global mobility networks.

In this paper, we first propose a strong anonymous mobile roaming authentication scheme in the global mobility network, which is a modified version of [12], the preliminary version of our work. In [12], there is no formal model and no formal proof of the proposed scheme and no performance comparison between the proposed scheme and some related schemes. On the other hand, the scheme in [12] may be impractical; the reason is that the foreign agent does not confirm who is authenticated by the home agent; when multiple mobile users simultaneously access the foreign agent, the foreign agent may confuse the mobile users. Moreover, an adversary can know the MU's temporary certificate generated by FA if the adversary can know the session key; thus, the mobile user's information may be divulged. After that, we prove the formal security of the proposed scheme. Finally, we present the performance comparison between our scheme and some related schemes.

The rest of this paper is organized as follows. Section 2 introduces the security model. The proposed scheme and security proof are given in Sections 3 and 4, respectively. After that, we present the performance comparison between the related schemes and ours in Section 5. Finally, we conclude the paper in Section 6.

2. Security Model

In this section, we recall the security model based on [15, 16].

2.1. Participants. In an authenticated key exchange (AKE) protocol, there are three different participants: a mobile user MU, home agent HA, and foreign agent FA; each of them may have certain number I of instances and may execute in the protocol at the same time. Each MU has a low-entropy password PW_{MU} chosen from a small dictionary D, and HA and FA hold some high-entropy private keys, respectively. When MU registers to HA, HA will compute and store $\{TK_{MU}, h(\cdot), ID_{MU}\}$ to a smart card, which combined with PW_{MU}, MU's identity ID_{MU}, HA's identity ID_{HA}, and hash function $h(\cdot)$, and issue the smart card to MU. The instance I of MU (resp., FA and HA) is denoted by MU^i (resp., FA^j and HA^k); pid_U^i is the partner identifier for an instance i.

2.2. Queries. The adversary's capabilities are captured by the following oracle queries.

$Execute(MU^i, FA^j, HA^k)$. The passive attack is captured by this oracle query. The adversary can get access to the honest execution process of the protocol between the instances.

$Send(I, m)$. This query models an active attack; the adversary sends a message to instance I and gets the response message from instance I according to the protocol. A query $Send(MU^i, start)$ initializes the key agreement algorithm.

$Reveal(I)$. This query allows the adversary to get some information about the session key of instance I.

$Corrupt(I, a)$. The corruption capability of the adversary is modeled by this query. The adversary can obtain the secret value of MU and messages stored in the smart card.

(a) If $a = 1$, it outputs the MU's password PW_{MU}.

(b) If $a = 2$, it outputs messages stored in the smart card.

$Test(I)$. This oracle query is used to define semantic security of the session key of instance I. If session key is not defined or the instance is not fresh, then the invalid symbol $\perp$ is returned. Otherwise, one flips a coin b, if $b = 1$, and one returns the session key for instance I; otherwise, a random key with the same length is returned.

2.3. Freshness. The freshness of a session key is that the adversary does not trivially know the key. We say an instance I is fresh if (1) instance I has accepted; (2) no $Reveal(U^i)$ and no $Reveal(\text{pid}_U^i)$ are queried by the adversary; (3) less than 2 $Corrupt(U, a)$ are queried by the adversary.

2.4. Semantic Security. Finally, the adversary outputs a bit b'. Let $Succ$ be the event that the adversary A wins the game if $b' = b$. The AKE advantage of the adversary is defined as

$$Adv_{PA,D}(A) = 2\Pr[Succ] - 1. \quad (1)$$

3. The Proposed Scheme

In this section, we demonstrate a practical scheme which is a modified version of our preliminary scheme in [12]. Some notations which will be used in this paper are defined as follows:

E: an elliptic curve defined over a finite field with large order n,

G: a generator on E with large order n,

$h()$: a one-way hash function,

$E_k[]/D_k[]$: the symmetric encryption/decryption functions with key k,

T_x: a time stamp generated by an entity x,

N: a secret value of HA,

SK_{FH}: a long-term common secretkey shared between FA and HA,

$x_0 \in Z_q^*$, $y_0 \in Z_q^*$: random numbers chosen by MU and FA, respectively,

$S_{HA} = x_{HA}$, $P_{HA} = x_{HA}G$: HA's secret key and public key.

MU	FA	HA
$X = x_0 G$		
$SID_{MU} = TK_{MU} \oplus h(ID_{MU} \oplus PW_{MU})$ $\xrightarrow{m_1=\{ID_{HA}, T_{MU}, E_1, X\}}$		
$DH_{MH} = x_0 P_{HA} = x_0 x_{HA} G$,		
$E_1 = E_{h(DH_{MH})}[SID_{MU} \parallel ID_{MU} \parallel T_{MU}]$		
	$Y = y_0 G$	
	$V = h(SK_{FH} \parallel m_1 \parallel ID_{FA} \parallel T_{FA} \parallel ID_{HA} \parallel Y)$ $\xrightarrow{m_2=\{m_1, ID_{FA}, T_{FA}, V, Y\}}$	
		Check T_{FA}, V
		$DH_{MH} = x_{HA} X = x_0 x_{HA} G$
		$\xleftarrow{m_3=\{T_{HA}, X, E_2\}}$ $D_{h(DH_{MH})}[E_1]$
		$D_N[SID_{MU}]$
		$ID_{MU}? = ID_{MU}$
		E_2
	$D_{SK_{FH}}(E_2)$	
	$\xleftarrow{m_4=\{E_3, Y, X\}}$ $T'_{HA}? = T_{HA}, X'? = X$	
	$sk = y_0 X = x_0 y_0 G$	
	E_3	
$sk = x_0 Y = x_0 y_0 G$		
$D_{sk}[E_3]$		
$h((SID_{MU} \parallel DH_{MH} \parallel T_{MU} \parallel Y))'? = h((SID_{MU} \parallel DH_{MH} \parallel T_{MU} \parallel Y))$		
The session key: $SK = h(sk \parallel X \parallel Y)$		

Algorithm 1: The proposed scheme: login and authentication phase.

3.1. Registration. When a mobile user MU wants to join the HA, he needs to perform the following steps.

Step 1. The mobile user MU freely chooses his identity ID_{MU} and password PW_{MU}. Then MU submits ID_{MU} to HA over a secure channel.

Step 2. Upon receiving the message from MU, the HA computes $SID_{MU} = E_N[(ID_{MU} \parallel ID_{HA})]$, stores $\{SID_{MU}, h(\cdot)\}$ into the smart card, and then returns it to the MU.

Step 3. The MU computes

$$TK_{MU} = SID_{MU} \oplus h(ID_{MU} \oplus PW_{MU}), \tag{2}$$

stores ID_{MU} into the smart card, and replaces SID_{MU} with TK_{MU}. Finally, the smart card contains $\{TK_{MU}, h(\cdot), ID_{MU}\}$.

The login and authentication phase of the proposed scheme is shown in Algorithm 1.

3.2. Login. When MU roams into the foreign network, he inserts his smart card into a device and inputs his password PW_{MU}. Then the smart card performs the following steps.

Step 1. It chooses a random number x_0 and computes $X = x_0 G$,

$$\begin{aligned} SID_{MU} &= TK_{MU} \oplus h(ID_{MU} \oplus PW_{MU}) \\ &= E_N[(ID_{MU} \parallel ID_{HA})], \\ DH_{MH} &= x_0 P_{HA} = x_0 x_{HA} G, \\ E_1 &= E_{h(DH_{MH})}[SID_{MU} \parallel ID_{MU} \parallel T_{MU}], \end{aligned} \tag{3}$$

where T_{MU} is current timestamp.

Step 2. It sends the login request $m_1 = \{ID_{HA}, T_{MU}, E_1, X\}$ to the foreign agent FA.

3.3. Authentication

Step 1. The FA checks the validity of the timestamp T_{MU} by checking $T'_{MU} - T_{MU} < \Delta t$, where T'_{MU} is the current time and Δt is a valid time interval. If it is valid, the FA chooses a random number y_0 and computes $Y = y_0 G$ and

$$V = h(SK_{FH} \parallel m_1 \parallel ID_{FA} \parallel T_{FA} \parallel ID_{HA} \parallel Y), \tag{4}$$

where a long-term common secret key SK_{FH} is shared between HA and FA, and T_{FA} is current timestamp. FA sends $m_2 = \{m_1, ID_{FA}, T_{FA}, V, Y\}$ to the HA.

Step 2. The HA checks the validity of the timestamp T_{FA}. If it is valid, the HA computes

$$V' = h\left(SK_{FH} \parallel m_1 \parallel ID_{FA} \parallel T_{FA} \parallel ID_{HA} \parallel Y\right) \quad (5)$$

and compares it with the received V. If it does not match, the HA terminates this connection. Otherwise, it goes to the next step since only FA knows the SK_{FH} and only FA can generate the valid V.

Step 3. The HA computes $DH_{MH} = x_{HA}X = x_0x_{HA}G$, computes $D_{h(DH_{MH})}[E_1]$ to obtain $\{SID_{MU}, ID_{MU}, T_{MU}\}$, and computes $D_N[SID_{MU}]$ to get $\{ID_{MU}, ID_{HA}\}$. In order to verify if MU is a legal user or not, HA compares ID_{MU} with the decrypted ID_{MU}. If they are equal, HA believes that MU is a legal user. Otherwise, MU is illegal. Then HA computes

$$E_2 = E_{SK_{FH}}\left[h\left(SID_{MU} \parallel DH_{MH} \parallel T_{MU} \parallel Y\right) \parallel T_{HA} \parallel X\right] \quad (6)$$

and submits the message $m_3 = \{T_{HA}, X, E_2\}$ to the FA.

Step 4. The FA checks the validity of the timestamp T_{HA}. If it is valid, the FA decrypts $D_{SK_{FH}}(E_2)$ to get $\{h(SID_{MU} \parallel DH_{MH} \parallel T_{MU} \parallel Y), T'_{HA}, X'\}$. Then, the FA verifies HA by comparing the decrypted timestamp T'_{HA} and X' to the received T_{HA} and X. If so, FA can confirm that MU has been authenticated by HA, and FA computes

$$sk = y_0X = x_0y_0G,$$

$$SK = h\left(sk \parallel X \parallel Y\right), \quad (7)$$

$$E_3 = E_{sk}\left[h\left(SID_{MU} \parallel DH_{MH} \parallel T_{MU} \parallel Y\right) \parallel X\right].$$

Then the FA submits the message $m_4 = \{E_3, Y, X\}$ to MU.

Step 5. On receiving the message m_4 from the FA, the MU computes $sk = x_0Y = x_0y_0G$ and $D_{sk}[E_3]$ to get $\{(h(SID_{MU} \parallel DH_{MH} \parallel T_{MU} \parallel Y))', X\}$. Then, the MU computes $h(SID_{MU} \parallel DH_{MH} \parallel T_{MU} \parallel Y)$ and checks if it is equal to $(h(SID_{MU} \parallel DH_{MH} \parallel T_{MU} \parallel Y))'$. If they are equal, then MU believes that both himself and FA are authenticated by HA and computes the session key $SK = h(sk \parallel X \parallel Y)$, which is shared with FA.

3.4. Password Change. When mobile user MU wants to change his password, he first passes through the authentication process with the HA and FA and then inputs his new password $PW_{MU}{}^{\text{new}}$; the smart card computes

$$TK_{MU}{}^{\text{new}} = TK_{MU} \oplus h\left(ID_{MU} \oplus PW_{MU}\right) \oplus h\left(ID_{MU} \oplus PW_{MU}{}^{\text{new}}\right) \quad (8)$$

and replaces TK_{MU} with $TK_{MU}{}^{\text{new}}$.

4. Security Analysis

Theorem 1. *Let G and D be an elliptic curve group and a uniformly distributed password dictionary, respectively. Let P be our scheme, and let A be an adversary. Then, one has*

$$\begin{aligned} &Adv_{P,D}(A) \\ &\le \frac{2q_{send}}{|D|} + 2Adv_G^{ECDLP}\left(t + \left(q_{send} + q_{exe} + 1\right) \cdot \tau_G\right) \\ &\quad + \frac{2q_{send}}{p} + \frac{2q_e^2 + q_h^2 + \left(q_{send} + q_{exe}\right)^2}{p}, \end{aligned} \quad (9)$$

where q_{send}, q_{exe}, q_h, $|D|$, q_e, and τ_G denote the number of Send-queries, the number of Execute-queries, the number of Hash-queries, the size of D, the number of encryption/decryption queries, and the time of scale multiplication in G, respectively.

Proof. We define a sequence of experiments starting at the real attack experiment Exp_0 and ending up the experiment Exp_5. Let $Succ_i$ be the event that the adversary guesses the bit b correctly involved in the $Test$-query in the experiment Exp_i, where $i = 0, 1, \ldots, 5$. Let Δ_i be the distance between Exp_i and Exp_{i+1}. Then, we have

$$\begin{aligned} &Adv_{P,D}(A) \\ &= 2\Pr\left[Succ_0\right] - 1 \\ &\le 2\Pr\left[Succ_1\right] + 2\left(\Pr\left[Succ_0\right] - \Pr\left[Succ_1\right]\right) - 1 \\ &\le 2\Pr\left[Succ_2\right] + 2\left(\Pr\left[Succ_1\right] - \Pr\left[Succ_2\right]\right) \\ &\quad + 2\left(\Pr\left[Succ_0\right] - \Pr\left[Succ_1\right]\right) - 1 \\ &\vdots \\ &\le 2\Pr\left[Succ_n\right] + 2\sum_{i=0}^{n-1}\Delta_i - 1. \end{aligned} \quad (10)$$

Experiment Exp_0. In the random oracle model, this experiment is the real attack. By definition, we have

$$Adv_{P,D}(A) = 2\Pr\left[Succ_0\right] - 1. \quad (11)$$

Experiment Exp_1. In this experiment, we simulate hash oracles and the encryption/decryption oracles (see Algorithm 2). *Execution*, *Reveal*, *Send*, *Corrupt*, and *Test* oracles are also simulated (see Algorithms 3 and 4). We can see that Exp_0 and Exp_1 are indistinguishable unless the permutation property of E or D does not hold; we have

$$\Delta_0 = \Pr\left[Succ_0\right] - \Pr\left[Succ_1\right] \le \frac{q_e^2}{2p}. \quad (12)$$

Experiment Exp_2. In this experiment, we simulate all oracles as in the experiment Exp_1 except that we cancel all executions in which some collisions occur in the transcript

(i) On a hash query $h(m)$, for which there exists a record (m, r) appears in Λ_h, return r.
Otherwise, choose an element $r \in Z_p^*$, add the record (m, r) to the list Λ_h and return r.
(ii) On a query $E(M)$, for which there exists a record $(M, *, *, C)$ appears in Λ_E, return C.
Otherwise, choose an element C, add the record $(M, \perp, E, C)$ to the list Λ_E and return C.
(iii) On a query $D(C)$, for which there exists a record $(M, *, *, C)$ appears in Λ_E, return M.
Otherwise, choose an element M, add the record $(M, \perp, D, C)$ to the list Λ_E and return M.

Algorithm 2: Simulation of random oracle h, encryption oracle E, and decryption oracle D.

(i) On a query $Send\left(MU^i, start\right)$, assuming MU^i is in the correct state, we proposed as login algorithm. Then the query is answered with $\{ID_{HA}, T_{MU}, E_1, X\}$.

(ii) On a query $Send\left(FA^i\left(ID_{HA}, T_{MU}, E_1, X\right)\right)$, assuming FA^i is in the correct state, we proposed as login algorithm and authentication Step 1 algorithm. Finally, the query is answered with $\{ID_{HA}, T_{MU}, E_1, X, Y, ID_{FA}, T_{FA}, V\}$.

(iii) On a query $Send\left(HA^i\left(ID_{HA}, T_{MU}, E_1, X, ID_{FA}, T_{FA}, V, Y\right)\right)$, assuming HA^i is in the correct state, we proposed as authentication Step 2 and Step 3 algorithm. At last, the query is answered with $\{T_{HA}, X, E_2\}$.

(iv) On a query $Send\left(FA^i\left(T_{HA}, X, E_2\right)\right)$, assuming FA^i is in the correct state, we proposed as authentication Step 4 algorithm. The query is answered with $\{E_3, Y, X\}$.

Algorithm 3: Simulation of *Send*-query.

(i) On a query $Reveal(MU^i/FA^i)$, we proposed as follows:
If the instance MU^i has accepted, the query is answered with the session key.

(ii) On a query $Execute\left(MU^i, FA^j, HA^k\right)$, we proposed as follows:
$\{ID_{HA}, T_{MU}, E_1, X\} \leftarrow Send\left(MU^i, Start\right)$
$\{ID_{HA}, T_{MU}, E_1, X, ID_{FA}, T_{FA}, V, Y\}$
$\leftarrow Send\left(FA^i\left(ID_{HA}, T_{MU}, E_1, X\right)\right)$
$\{T_{HA}, X, E_2\}$
$\leftarrow Send\left(HA^i\left(ID_{HA}, T_{MU}, E_1, X, ID_{FA}, T_{FA}, V, Y\right)\right)$
$\{E_3, Y, X\} \leftarrow Send\left(FA^i\left(T_{HA}, X, E_2\right)\right)$
The query is answered with the transcript
$\{ID_{HA}, T_{MU}, E_1, X\}$, $\{ID_{HA}, T_{MU}, E_1, X, ID_{FA}, T_{FA}, V, Y\}$,
$\{T_{HA}, X, E_2\}$, $\{E_3, Y, X\}$.

(iii) On a query $Test(MU^i/FA^i)$, we proposed as follows:
Get the session key SK from the $Reveal(MU^i/FA^i)$ and flip a coin b, if $b = 1$, we return the session key, otherwise we return a random value with the same length.

Algorithm 4: Simulation of *Execute*-, *Reveal*-, and *Test*-query.

$\{m_1, m_2, m_3, m_4\}$ in the output of the hash queries. According to the birthday paradox, we have

$$\Delta_1 \leq \frac{q_h^2 + q_e^2 + \left(q_{send} + q_{exe}\right)^2}{2p}. \tag{13}$$

Experiment Exp_3. In this experiment, we cancel the executions wherein the adversary may be lucky in guessing the authentication values E_1, V, E_2, and E_3. Since experiments Exp_3 and Exp_2 are indistinguishable unless home agent/foreign agent (or the mobile user) rejects a correct authentication value, we could get $\Delta_2 = q_{send}/p$.

Experiment Exp_4. In this experiment, we use random value ($A = aG$, $B = bG$, $Z = abG$) instead of ($X = x_0G$, $Y = y_0G$, $sk = x_0y_0G$) to compute SK so that SK is independent of X and Y. The experiments Exp_4 and Exp_3 are indistinguishable

unless the event $AskH_4$ occurs, where $AskH_4$ denotes the event that the adversary uses (A, B) to compute SK. Therefore, we could get that $\Delta_3 \leq \Pr[AskH_4]$, $\Pr[Succ_4] = 1/2$.

Experiment Exp_5. In this experiment, we introduce a random self-reducibility of the ECDL problem into the executions, given one ECDLP instance (x_0G, y_0G). The event that the adversary uses the (A, B) to compute the session key is denoted by k_4; we may have $\Pr[AskH_4] = \Pr[AskH_5]$ and $Z = ECDLP(aG, bG)$.

If the $Corrupt(U, 2)$ query has been made, it shows that the password-corrupt query $Corrupt(U, 1)$ has not been made. Then, in every transcript, the adversary only tests one password. Therefore, we can conclude that

$$\Pr\left[AskH_5\right] \leq \frac{q_{send}}{|D|} + Adv_G^{ECDLP}\left(t + \left(q_{send} + q_{exe} + 1\right) \cdot \tau_G\right). \quad (14)$$

Therefore, Theorem 1 is concluded. □

5. Performance Comparison

Since Chen et al.'s [11] scheme is more efficient than other schemes without perfect forward secrecy, to the best of our knowledge, only Mun et al. [7], Li and Lee [9], Hu et al. [10], Xie et al. [12], Chen et al. [13], and Xie et al. [14] schemes can provide perfect forward secrecy. Therefore, we will present performance comparison between our scheme and these related schemes. Table 1 is performance comparison of login and key agreement phase, as we know that login and key agreement is the main body of an authentication scheme, and registration phase only performs one time before authentication.

Let T_e, T_h, T_s, and T_m be the time for performing a modular exponentiation, a one-way hash function, a symmetric encryption/decryption, and a scalar multiplication on elliptic curve, which need 0.522 seconds, 0.0005 seconds, 0.0087 seconds, and 0.063075 seconds [17–19], respectively. We ignore modular addition, exclusive OR operation, and string concatenation operation which are negligible compared to others.

According to Table 1, we can conclude that Chen et al.'s [11] and Mun et al.'s [7] schemes are more efficient than others since Chen et al.'s scheme is completely based on hash and symmetric encryption/decryption operations but does not provide perfect forward secrecy and Mun et al.'s scheme is vulnerable to several attacks such as impersonation attack, replay attack, man-in-the-middle attack, and verification table stolen attack. And our scheme only needs 0.44 seconds in login and key agreement which keeps low performance cost.

Table 1: Performance comparison.

	Performance cost	Estimated time (s)
Mun et al. [7]	$11T_h + 4T_m$	0.2578
Li and Lee [9]	$15T_e + 7T_h + 14T_s$	7.9553
Hu et al. [10]	$11T_m + 6T_h + 8T_s$	0.77
Chen et al. [11]	$6T_s + 16T_h$	0.0602
Xie et al. [12]	$6T_m + 9T_h + 7T_s$	0.44385
Chen et al. [13]	$6T_e + 11T_h + 4T_s$	3.1723
Xie et al. [14]	$8T_e + 8T_h + 9T_s$	4.2501
Our scheme	$6T_m + 7T_h + 7T_s$	0.44285

6. Conclusions

In this paper, we proposed a modified scheme of our preliminary work, which was presented in ISBAST 2013. Compared with the preliminary work, the modified scheme can eliminate the weaknesses of the previous version. Further, we proved the security of the modified scheme and showed that the proposed scheme is efficient according to the performance comparison between our scheme and some related schemes. Therefore, the proposed scheme is secure and efficient and is suitable for using in the global mobility network.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the Major State Basic Research Development (973) Program of China (no. 2013CB834205), the National Natural Science Foundation of China (no. 61070153), the Natural Science Foundation of Zhejiang Province (nos. LZ12F02005, LY12F02006), and a Grant from the RGC of the HKSAR, China (no. CityU 121512).

References

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

[2] C.-C. Lee, M.-S. Hwang, and I.-E. 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.

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

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

[5] J. Xu, W.-T. Zhu, and D.-G. Feng, "An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks," *Computer Communications*, vol. 34, no. 3, pp. 319–325, 2011.

[6] T.-Y. Youn, Y.-H. 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.

[7] 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.

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

[9] C.-T. Li and C.-C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications," *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 35–44, 2012.

[10] B. Hu, Q. Xie, M. J. Bao, and N. Dong, "Improvement of user authentication protocol with anonymity for wireless communications," *Kuwait Journal of Science & Engineering*, vol. 41, no. 1, pp. 155–169, 2014.

[11] C. Chen, D. He, S. Chan, J. Bu, Y. Gao, and R. Fan, "Lightweight and provably secure user authentication with anonymity for the global mobility network," *International Journal of Communication Systems*, vol. 24, no. 3, pp. 347–362, 2011.

[12] Q. Xie, M. J. Bao, N. Dong, B. Hu, and D.-S. Wong, "Secure mobile user authentication and key agreement protocol with privacy protection in global mobility networks," in *Proceedings of the International Symposium on Biometrics and Security Technologies (ISBAST '13)*, Chengdu, China, July 2013.

[13] Y.-C. Chen, S.-C. Chuang, L.-Y. Yeh, and J.-L. Huang, "A practical authentication protocol with anonymity for wireless access networks," *Wireless Communications and Mobile Computing*, vol. 11, no. 10, pp. 1366–1375, 2011.

[14] Q. Xie, B. Hu, X. Tan, M.-J. Bao, and X.-Y. Yu, "Robust anonymous two-factor authentication scheme for roaming service in global mobility network," *Wireless Personal Communications*, vol. 74, no. 2, pp. 601–614, 2014.

[15] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Advances in Cryptology—EUROCRYPT 2000*, vol. 1807 of *Lecture Notes in Computer Science*, pp. 139–155, Springer, Berlin, Germany, 2000.

[16] E. Bresson, O. Chevassut, and D. Pointcheval, "Security proofs for an efficient password-based key exchange," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03)*, pp. 241–250, New York, NY, USA, October 2003.

[17] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2803–2814, 2008.

[18] J.-S. Lee and C.-C. Chang, "Secure communications for cluster-based ad hoc networks using node identities," *Journal of Network and Computer Applications*, vol. 30, no. 4, pp. 1377–1396, 2007.

[19] W.-M. Li, Q.-Y. Wen, Q. Su, and Z.-P. Jin, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network," *Computer Communications*, vol. 35, no. 2, pp. 188–195, 2012.