A SELF-CERTIFIED MECHANISM FOR MUTUAL AUTHENTICATION AND KEY EXCHANGE IN ROAMING SERVICES

RENYI XIAO

National Nature Science Foundation of China
xiaory@mail.nsfc.gov.cn

Abstract: In this paper, a novel mutual authentication and key exchange protocol based on self-certified mechanism is proposed for roaming services in the global mobility network (GLOMONET). The main new features of the proposed protocol include identity anonymity, one-time session key renewal, and distributed security management scheme. Identity anonymity protects location privacy of mobile users in the roaming network environment. One-time session key renewal protocol frequently updates the session key for mobile users and hence reduces the risk of using a compromised session key to communicate with visited networks. The distributed security management scheme provides an efficient management mechanism: the original security manager in home network is responsible for providing local services for his mobile user whilst a temporary security manager dynamically generated for a roaming user in the visited network is in charge of providing roaming services. After certification, the temporary security manager will take the place of the original security manager when the roaming user stays in the service area of the visited network. The results of performance analysis show that the computation complexity of our protocol is not high and does satisfy the computation capacity requirement for mobile device while these new security features have been significantly enhanced.

Keywords—Authentication, key exchange, roaming service, anonymity, self-certified.

1. INTRODUCTION

Global mobility network (GLOMONET) [1], such as GSM and CDMA etc., increases the possibility of illegal access from a malicious intruder while offering more effective global roaming service for a legitimate user between the home network and the visited network. Several authentication protocols for global roaming service have been developed in the GLOMONET [1-5]. Suzuki et al developed an authentication protocol for roaming service [1]. They introduced a challenge/response interactive authentication mechanism with a symmetric cryptosystem to construct their authentication protocol. Buttyan et al pointed out that there are several drawbacks feasible for attacking Suzuki et al authentication protocol, and further proposed a modified protocol to eliminate these drawbacks and made it resistant against the presented attacks [3]. Subsequently, Hwang et al [4] introduced a new mechanism, self-encryption, to simplify Buttyan et al protocol. In this protocol, the number of message transmissions is reduced to only five. Hence, the mechanism is easier to be implemented in the mobile equipment.

Unfortunately, there is short of identity anonymity in Hwang et al scheme. Hence the security of the long-term shared key K_{MH} between the mobile user and his home network would be compromised, since the shared key K_{MH} is calculated as $K_{MH} = f(ID_M)$, where ID_M is the identity of mobile user M and f is assumed to be a secret one-way function. This limitation may permit some attacks once the user identity ID_M is illegal obtained by intercepting the exchanged message, and then the advantage of self-encryption mechanism is counteracted. Moreover, the disclosure of a user identity will allow unauthorized entities to track his moving history and current location. Any illegal access to information related to the user location without his notice can be a serious violation of his privacy, whereas assuring the identity anonymity of a mobile user can effectively prevent unintended parties from associating him with the sessions in which he participates. Hence, the identity anonymity is one of the important properties that should be considered for roaming services.

The basic solution for providing anonymity in authentication protocols is to use the temporary identity (TID) for a mobile user instead of his real one [5-9]. The TID is prearranged and distributed by the home network in advance. A mobile user stores TID in which his real identity is hidden and only known to his home network and himself. The other solution is to generate TID by encrypting the real identity with the shared key or the public key of his home network which has already given to him.

A. Security Requirements for Roaming Service

Generally, a secure protocol design for roaming services requires, as pointed out in [10], (1) Prevention of fraud by ensuring that the mobile user and network entity are authentic, that is, there are a mutual authentication mechanism between a network entity and a mobile user; (2) Assuring mutual agreement and the freshness of session key; (3) Prevention of replaying attack, so that intruders are not able to obtain sensitive data by relaying a previously intercepted message; (4) Privacy of information about mobile user's locations during the communication so that it is requisite to provide the identity anonymity mechanism.

Additionally, since the protocols are implemented on the mobile device used in wireless environment, there are other two factors to be considered. Firstly, the low computational power of mobile devices should be a concern, which means a security protocol requiring heavy computation on the mobile is not feasible [11-13]. Secondly, since the bandwidth is lower and the channel error is higher in wireless networks than that in wired networks, the security protocols should be designed to minimize the message size and the number of message exchanges.

B. Major Contributions and Organization

In this paper, aiming at enhancing the security of the existing authentication protocol for roaming service in GLOMONET environment, we propose a set of mutual authentication and key exchange protocols for roaming service. Our protocol is based on self-certified scheme [15-17], known as a public key authentication cryptosystem. In this protocol, the home network is not required to setup a long-term secret key with his mobile users in advance.

Moreover, we propose three new mechanisms for roaming service, which are identity anonymity, one-time session key renewal mechanism, and distributed security management scheme, respectively. The *identity anonymity* property prevents the disclosure of mobile users' real identities and protects their privacy in the roaming network environment. The *one-time session key renewal mechanism* can assure the mutual authentication and the freshness of session key. It provides a way for a mobile user to update his session key with visited network frequently, and therefore, reduces the risk of using a compromised session key to communicate with visited networks. In *distributed security management scheme*, the original security manager in home network is responsible for providing local services for his mobile user, while a temporary security manager is in charge of providing roaming services, which is temporarily generated for a roaming user in the visited network. After certification, the temporary security manager will take the place of the original security manager when the roaming user stays in the service area of the visited network.

Although we increase such security features, the computation requirement for our protocol is not high. Moreover, in our scheme, the number of exchanged messages is decreased to only four in Phase I and two in Phase II.

The rest of this paper is organized as follows. In section II, the basic self-certified scheme is reviewed. In section III, based on self-certified scheme and Diffe-Hellman mechanism, a new authentication and key exchange protocol for roaming service is proposed. In section V, security analysis is also discussed. In Section VI, the performance comparisons between previous roaming protocols and our proposed protocol are investigated. Finally, Section VI concludes our related work.

2. BASIC SELF-CERTIFIED SCHEME

The Self-Certified scheme [15-17] combines the advantages of certificated-based and identity-based public key cryptosystems [18-19], and it also can provide a mechanism for authenticating a user's public key. In this scheme (contrary to identity-based schemes), each user chooses his secret key and computes his public key. Then, instead of signing the pair of public key and identity string (contrary to certificate-based schemes), the authority create a certificate from that pair in such a way that it can not be computed without the knowledge of some trapdoor, known only to the authority.

For simplicity, we only describe a simple self-certified scheme. In the setup phase, the TTP chooses a modulus $n = p \cdot q$, as the product of two random safe primes p and q (i.e., such that $p-1 = 2p'$, and $q-1 = 2q'$, where p' and q' are also primes), generates a base element $g \neq 1$ of order $r = p' {\cdot} q'$ (i.e., such that $g \neq 1 \bmod (n)$), and picks a large integer u<r. Let $t \in Z_u^*$ be an element of Z_u^* of order u. A one-way function f will output positive integers less than p' and q'. The TTP makes g, u, f and n public and keeps r secret. Then p and q are discarded.

Next, any user U_i can register with TTP by performing the following steps.

Step 1) User U_i chooses a random x {2, 3, .., u-1} as his secret key, computes $y = g^x (\bmod n)$ as his public key and sends y to the TTP.

Step 2) The TTP prepares a string associated I_i with the personal information (Name, Address, etc.) of U_i and computes $w_i = y_i^{f(I_i)^{-1}}$ mod (n) as a witness for user U_i and sends message $\{I_i, w_i\}$ to U_i.

Step 3) User U_i verifies I_i and witness w_i by checking whether the equation $y_i = w_i^{I_i} (\bmod n)$ holds.

Regarding to the security strength of self-certified scheme, Saeednia [13] claimed that forging a valid witness w_i for user U_i is equivalent to break an instance of RSA cryptosystem.

Suppose that user U_i and U_j intend to exchange a secret key to be used for secure communication. They can perform the following protocol, which is based on the well-known Diffie-Hellman key distribution system.

Step 1) User U_i sends $\{w_i \| I_i\}$ to U_j, where $w_i = y_i^{f(I_i)^{-1}} \bmod n$ is a witness for user U_i.

Step 2) User U_j sends $\{w_j \| I_j\}$ to U_i, where $w_i = y_i^{f(I_i)^{-1}} \bmod n$ is a witness for user U_j.

Step 3) User U_i can compute the secret key shared with U_j as $k = w_j^{f(I_i)\cdot x_i} \bmod(n)$.

Step 4) User U_j can compute the secret key shared with U_i as $k = w_i^{f(I_j)\cdot x_j} \bmod(n)$.

Note that there are two weaknesses in the basic self-certified key exchange scheme. One is that the secret session key exchanged in this protocol is invariant. The other is that the witness w_i computed by TTP is not self-certified, even though forging a valid witness is equivalent to breaking an instance of the RSA cryptosystem. This defect makes that it is possible for a cheating user to have a chance to get a forged self-certified witness.

3. PROPOSED PROTOCOL FOR ROAMING SERVICES: BASED ON SELF-CERTIFIED SCHEME

Our proposed protocol is based on the above Self-Certified scheme. It includes two phases: (1) Mutual authentication protocol (Phase I); (2) Session key renewal protocol (Phase II). In phase I, the visited network *V* authenticates a roaming user *M* through his home network *H*. The key idea is to regard home network *H* as a temporary TTP for roaming services. When user *M* roams into a visited network *V*, both of them will initialize a registration procedure with *H*, where *V* acts as an access agent for *M*. If *M* and *V* successfully register with *H*, they will obtain a witness from *H* respectively and further the trust relations between *M* and *V* are established. Afterwards, *M* can directly establish or negotiate the session key with *V* without accessing his home network to authenticate the identity of the visited network *V*.

In phase II, the user *M* can establish or renew a session key with *V*. Then, *M* can directly visit *V* and *V* can provide responding services for *M*. Here we also introduce a novel mechanism called “one-time session key renewal” to assure the mutual authentication and the freshness of session key.

a. Phase I: Mutual Authentication Protocol (MAP)

The aim of MAP protocol is to provide a mechanism for user *M* and *V* to authenticate mutually and then establish a trusted relation between them.

Our MAKEP protocol for roaming services is described in Fig. 2. Compared with the previous roaming protocols, we mainly introduce a new feature, *identity anonymity*, which can efficiently prevent unauthorized entities from tracing the mobile user’s roaming history and his current location. Our solution for identity anonymity is to replace the real identity ID_M of a mobile user *M* with his temporary identity TID_M.

Suppose $y_M = g^{r_M} (\bmod n)$ and $y_V = g^{r_V} (\bmod n)$, where random r_M and r_V are generated by user *M* and *V* respectively. Let I_M and I_V be two strings associated with the personal information (Name, Address, etc.) of user *M* and *V* respectively. In addition, let w_M and w_V be the witness of user *M* and *V*, which are issued and calculated by *H* as follows:

$$w_M = ((y_M \oplus I_M)^{f(I_M)^{-1}}) \bmod(n) \qquad (1)$$

$$w_V = ((y_V \oplus I_V)^{f(I_V)^{-1}}) \bmod(n) \qquad (2)$$

In the following, we describe the proposed MAP protocol according to the order of message exchange and also discuss the security goals which can be achieved during the execution of each protocol message.

Message 1. *M*→*V*: y_M, ID_H, TID_M

Message 2.

V→*H*: $y_M, y_V, E_{K_{VH}}(y_V \,||\, ID_V \,||\, TID_M \,||\, T_V)$

Message 3.

V←*H*: $E_{K_{VH}}(w_V \,||\, I_V), E_{K_{MH}}(w_M \,||\, I_M \,||\, ID_V)$

Message 4. *M*←*V*: $E_{K_{MH}}(w_M \,||\, I_M \,||\, ID_V)$

Fig. 1. Proposed Mutual Authentication Protocol for Roaming Services

As shown in Fig. 1, the shared key K_{MH} are computed as $K_{MH} = (PK_H)^{r_M}$, where the random r_M is generated by *M* and the public key $PK_H = g^{SK_H}$ of *H* is already delivered to user *M* through a secure channel in advance. And the real identity ID_M of user *M* is hidden in the temporary identity TID_M, which is computed as

$$TID_M = E_{K_{MH}}(g^{r_M} \oplus ID_M) \tag{3}$$

Then, we describe our proposed protocol in detail according to the message exchange order as follows.

Step 1) The mobile user *M* does the following: (1) Generates a random $r_M \in Z_u^* \setminus \{1\}$ and computes $y_M = g^{r_M}$; (2) Computes the shared key K_{MH} by $K_{MH} = (PK_H)^{r_M}$ and use it to compute $TID_M = E_{K_{MH}}(g^{r_M} \oplus ID_M)$; (3) Sends ID_M, y_M and TID_M to *V*.

Step 2) The visited network *V* chooses a random $r_V \in Z_u^* \setminus \{1\}$,computes $y_V = g^{r_V}$, and sends message $\{y_M, y_V, E_{K_{VH}}(y_V \,||\, ID_V \,||\, TID_M \,||\, T_V)\}$ to *H*.

Step 3) *H* first decrypts $E_{K_{VH}}(y_V \,||\, ID_V \,||\, TID_M \,||\, t_V)$ by using shared key K_{VH}. If the timestamp t_V is reasonable and the decrypted value y_V^* is equal to clear-text y_V, *H* computes the shared key K_{MH} by $K_{MH} = (g^{r_M})^{SK_H}$ and then decrypts $TID_M = E_{K_{MH}}(g^{r_M} \oplus ID_M)$ with K_{MH}. Then he can get the real identity of user *M* by computing the following formula:

$$ID_M = D_{K_{MH}}(E_{K_{MH}}(g^{r_M} \oplus ID_M)) \oplus g^{r_M} \tag{4}$$

Afterwards, *H* can verify the authenticity of ID_M. If it is legal, *H* does the following: (1) Preparing two strings I_M and I_V associated with the personal information (Name, Address, etc.) of user *M* and *V*, respectively; (2) Computing the witness w_M and w_V for *M* and *V* according to Eq.(1) and (2)). Then, *H* sends $E_{K_{VH}}(w_V \,||\, I_V)$ and $E_{K_{MH}}(w_M \,||\, I_M \,||\, ID_V)$ to *V*.

Step 4) *V* decrypts $E_{K_{VH}}(w_V \,||\, I_V)$ and verifies witness w_V and I_V by checking whether the following equation holds.

$$y_V = ((w_V)^{f(I_V)} \bmod(n) \oplus I_V) \tag{5}$$

If true, then *V* successfully registers with *H* and he believes that *M* is an authorized user. Subsequently, *V* forwards $E_{K_{MH}}(w_M \,||\, I_M \,||\, ID_V)$ to *M*.

Step 5) Similarly, *M* decrypts $E_{K_{MH}}(w_M \,||\, I_M \,||\, ID_V)$ and verifies I_M and witness w_M by checking

$$y_M = ((w_M)^{f(I_M)} \bmod(n) \oplus I_M) \tag{6}$$

If true, *M* successfully registers with *H* and he believes that the trust relations between *M* and *V* are also established with the help of home network *H*.

In the above steps, we illustrate the proposed authentication protocol for roaming services. In addition, we also consider the authentication protocol when user *M* is located in his home network. The corresponding authentication protocol for local services is shown in Fig. 2.

Message 1. *M*→*H*: y_M, ID_H, TID_M

Message 2. *M*←*H*: $E_{K_{MH}}(w_M \,||\, I_M \,||\, ID_H)$

Fig. 2. Proposed Mutual Authentication Protocol for Local Services

Note that the difference between Fig. 1 and Fig. 2 is that the authentication protocol for local services ignores the original Message 2 and 3 in Fig. 1.

Additionally, compared with the Fig. 1 and Fig. 2, it can be seen that the mechanism in the mobile equipment for local service is the same as that for roaming services except for the introduction of different parameters according to the specific environment. Hence, we preserve the consistency of protocol architecture and then decrease the complexity of protocol implementation. In other words, the complexity of the mobile equipment can be further simplified.

b. Phase II: One-time Session Key Renewal Protocol (SKRP)

The main functions in phase II are to establish or renew a session key between user *M* and *V*. Compared with the previous roaming protocols, in this phase, we introduce a novel mechanism called "One-time session key renewal". This new feature allows mobile user *M* to establish or renew his session key frequently and reduces the risk that he uses a compromised session key to communicate with *V*.

The secret session key exchanged in basic self-certified key exchange scheme is invariant. Here, we propose a time-variant session key renewal scheme by utilizing a modified self-certified scheme and Diffie-Hellman mechanism.

Suppose that a mobile user *M* is required to renew his session key K_{MV} with *V* for the i^{th} time, he could obtain the new session after he exchanges the two messages in Fig. 3 with *V*.

Message 1. *M*→*V*: w_M, I_M, g^{t_M}

Message 2. *M*←*V*: w_V, I_V, g^{t_V}

Fig. 3. Proposed Session Key Renewal Protocol

In Fig. 3, random $t_M, t_V \in Z_u^*$ denotes two different elements of Z_u^* of order *u*. And the session key K_{MV} can be calculated respectively by user *M* and *V* as follows.

For mobile user *M*, the session key can be computed as

$$y_V = (w_V^{f(I_V)} \bmod(n)) \oplus I_V \tag{7}$$

$$K_M = y_V^{t_M} \cdot (g^{t_V})^{r_M} = g^{r_V t_M + r_M t_V} \bmod(n) \tag{8}$$

$$K_{MV} = h(K_M) \tag{9}$$

For *V*, the session key is acquired similarly as follows:

$$y_M = (w_M^{f(I_M)} \bmod(n)) \oplus I_M \tag{10}$$

$$K_V = y_M^{t_V} \cdot (g^{t_M})^{r_V} = g^{r_V t_M + r_M t_V} \bmod(n) \tag{11}$$

$$K_{MV} = h(K_V) \tag{12}$$

Evidently, the session key calculated by *M* and *V* respectively is equal because of the following equation:

$$K_{MV} = h(K_M) = h(g^{r_V t_M + r_M t_V} \bmod(n)) = h(K_V) \tag{13}$$

where *h* is a collision-resistant hash function. Key confirmation is done implicitly during the session. Moreover, this protocol can yield a different key for each session renewal.

The security of the key exchange is especially enhanced by using this approach, since every session key is used for only once. Moreover, compared with the previous protocols, the number of message exchanges is decreased to only two, while the one-time session key renewal mechanism is preserved.

Next, we shall analyze the security of this protocol. The performance analysis will be described in the later section.

4. SECURITY ANALYSIS FOR PROPOSED PROTOCOL

The security requirements for mobile communication have been introduced in Section 1. In this section we analyze the security of our proposed protocol to see whether these requirements have been satisfied.

a. Identity Anonymity and Untraceability Analysis

As shown in Fig. 1, the real identity ID_M of mobile user *M* is replaced with his temporary identity TID_M, which is computed as $TID_M = E_{K_{MH}}(g^{r_M} \oplus ID_M)$, where $K_{MH} = (PK_H)^{r_M}$. Since only home network H knows his own secret key SK_H, nobody except H can calculate the shared key K_{MH} as $K_{MH} = (g^{r_M})^{SK_H}$. Hence, only H can decrypt the temporal identity TID_M with key K_{MH} and obtain the real identity ID_M by computing:

$$ID_M = D_{K_{MH}}(TID_M) = D_{K_{MH}}(E_{K_{MH}}(g^{r_M} \oplus ID_M)) \oplus g^{r_M}$$

Since an illegal tracker cannot obtain the shared key K_{MH}, it is impossible for him to extract the real identity ID_M from TID_M and then trace the location of a mobile target user.

The identity untraceability is assured by two measures: (1) When user M roams in different visited networks, TID_M is different in each session due to the different random r_M; (2) The shared key $K_{MH} = (PK_H)^{r_M}$ is *one-time-use* so that there is no direct relationship between these shared keys. The change of random r_M guarantees the freshness of TID_M and the shared key in different roaming domains.

b. Prevention of Fraud

Firstly, our MAP scheme can efficiently prevent an intruder from impersonating attacks, since our scheme provides secure mutual authentication mechanisms between mobile user M and V, M and H, or V and H. Consider the following impersonation attack scenarios in MAP Protocol (See Fig. 1).

Case 1) An intruder has no way to impersonate H to cheat V, since he does not possess the long-term secret key K_{VH}. Hence it is impossible for an intruder to generate the responding confirmation $E_{K_{VH}}(w_V \| I_V \| g^{r_M})$ to V.

Case 2) V has no way to impersonate H to cheat user M. Since the shared key K_{MH} is unknown to V, and V cannot generate $E_{K_{MH}}(w_M \| I_M \| ID_V \| g^{r_M} \| g^{r_V})$ where w_M contains y_M generated by user M.

Case 3) An intruder also has no way to impersonate M since he cannot know the real identity of user M. If the intruder uses a phony identity $ID_M^{'}$, the corresponding spurious temporal identity $PID_M^{'}$ can be identified by home network, since H can obtain the $ID_M^{'}$ by computing $ID_M^{'} = D_{K_{MV}^{'}}(TID_M^{'}) = D_{K_{MV}^{'}}(E_{K_{MV}^{'}}(g^{r_M} \oplus ID_M^{'})) \oplus g^{r_M}$ and then H can detect the spurious identity $ID_M^{'}$. Moreover, the real identity is kept anonymity in our scheme. Hence nobody except the user himself and his home network H can know his real identity.

Similarly, we can also consider the impersonation attack scenarios in SKRP Protocol (Fig. 3) as follows.

Case 1) An adversary has no way to impersonate M to cheat V. Since it is impossible for an adversary to obtain the secret r_M unless he can resolve the problem of computing discrete logarithm modulo a large composite. Hence, the adversary can not pretend to act as user M to share or obtain the same session key K_{MV} with the visited network V, even though any adversary can easily compute an authenticated pair (w_M, I_M) for user M satisfying the following equation

$$y_M = g^{r_M} = (w_M^{f(I_M)} \oplus I_M)\,\mathrm{mod}(n)$$

Case 2) Owing to the same mechanism, an adversary also has no way to impersonate V to cheat mobile user M.

Compared with the basic self-certified scheme, we only replace the witness $w_M = ((y_M \oplus I_M)^{f(I_M)^{-1}})\,\mathrm{mod}(n)$ with the original $w_M = y_M^{f(I_M)^{-1}}\,\mathrm{mod}(n)$. Our improvement provides a self-certified mechanism to prevent a cheating user from having a chance to get forged self-certified witness, while it only requires one more XOR operation than the original step.

c. Mutual Agreement and the Freshness of Session Key

In our scheme, the mutual key agreement mechanism is evident. Consider such mechanism in SKRP protocol. The new session key K_{MV} is obtained with the mutual agreement mechanism. The reason is that according to Eq. (13) we can derive key K_{MV} as follows.

$$K_{MV} = h(g^{r_V t_M + r_M t_V} \bmod(n))$$

where the two random numbers t_M and t_V are respectively determined by *M* and *V* independently. In addition, the two numbers, t_M and t_V , are also randomly selected by *M* and *V*, respectively.

Finally, the freshness of session key is evidently assured, since the exchanged Message 1 and 2 in SKRP protocol safeguard the freshness of the two numbers t_M and t_V , which are randomly selected by *M* and *V*, respectively (See Fig. 3).

d. Prevention of Replaying Attack

Finally, we analyze the *relaying attacks* in session key renewal protocol (Fig. 3). Consider the case that an adversary pretends to act as *M* and tries to exchange a secret key with *V* such that *V* intends to share the secret key with *M*. The adversary can randomly choose an integer $\alpha \in Z_u^*$; then he sets $r_M^* = \alpha \cdot f(I_M)$ as a fake secret key for *M* and replace *M*'s original public key y_M with $y_M^* = g^{r_M^*} \bmod(n)$. However, the adversary cannot compute a valid witness w_M^* for *M*, because the original witness $w_M = ((y_M \oplus I_M)^{f(I_M)^{-1}}) \bmod(n)$ for user *M* is self-certified. Therefore although the adversary can intercept the message $\{w_M, I_M, g^{t_M}\}$, he still cannot forge the correct message $\{w_M^*, I_M, g^{t_M}\}$ which satisfies the following relation: $w_M^* = ((y_M^* \oplus I_M)^{f(I_M)^{-1}}) \bmod(n)$, unless he can compute discrete logarithm modulo a large composite. So it can be seen that the proposed protocol is able to resist such replaying attacks, i.e., the adversary and *V* cannot obtain the same secret key. Similarly, an adversary that impersonates *V* also cannot obtain the same secret key with mobile user *M*.

5. Performance Analysis

The performance comparisons between our protocol and previous protocols are shown in Table I and II, in which the Phase I and Phase II of these three schemes are described respectively. We mainly compare the number of hash operation, symmetric encryption/decryption, and exponential operation in different protocols. Moreover, the number of transmissions (message exchanges) is also compared. Since ASPeCT [5] protocol can not provide session key renewal mechanism, we only compare the performance between Hwang et al protocol and our scheme in Table II.

According to Table I and II, it can be generally conclude that though the identity anonymity capability, session key renewal mechanism, and distributed security management scheme are introduced into our schemes for roaming service, the complexity of our protocols is still less than or equal to Hwang et al protocol and the computation requirement for mobile device is quite low.

TABLE I

PERFORMANCE COMPARISONS (PHASE I)

Comparison Item		Hwang et al	ASPeCT [5]	Proposed Protocol
Exponential operation	*M*	N/A	2	1+2 Pre.
Hash Operation	*M*	1 (step 1)	1	1 (step 1)
Symmetric Encryption	*M*	2 (step 1, 5)	2	1 (step 1)
Symmetric Decryption	*M*	1 (step 5)	N/A	1 (step 5)
Transmissions	*M* ↔ *V*	3	3	2
Anonymity		No	No	Yes
Session Key Renew		Yes	No	Yes

TABLE II

PERFORMANCE COMPARISONS (PHASE II)

Comparison Item		Hwang et al protocol	Our Proposed Protocol
Exponential operation	*M*	N/A	1+2Pre
Symmetric Encryption	*M*	1	N/A

Symmetric Decryption	M	1	N/A
Transmissions	$M \leftrightarrow V$	3	2
Identity Anonymity		N/A	Yes

Note: *M*: Mobile; *V*: Visited Network

Pre: Pre-computation exponentiation operation

Compared with other two schemes, the proposed protocol reduces the number of symmetric encryption/decryption operations as well as requires the exponentiation operations. Though the exponentiation is a relatively time-consuming operation, some exponentiation operation can be pre-computed, e.g., g^{r_M} , g^{t_M} , g^{r_V} and g^{t_V} . Hence, as a result of these improvements, the real exponentiation computation load is not remarkable. The scheme also provides: (1) Identity anonymity; (2) The mutual authentication between the two entities without pre-setup shared secret key; (3) The session keys are independently generated for each session; (4) Distributed security management scheme. All the features are especially favorable and safer in the roaming environment. Moreover, the increase of computation load resulting from the identity anonymity and one-time session key renewal provide the enhanced securities that are not considered in other schemes.

Note that the exponentiation operations required for *M* is in Eq.(6) (Phase I) and Eq.(8) (Phase II), respectively. If we only consider the exponentiation operations except those pre-computed exponentiation operations, the average computation complexity is $\frac{3}{2}\cdot\left\lfloor \log(\frac{n}{2}) \right\rfloor \cdot M(n)$ where $M(n)$ denote the computation complexities of modular modulo *n*. In fact, according to the binary algorithm for fast exponentiation [20], computing g^x will take $2\cdot\lfloor \log x \rfloor$ multipliers in worst case and $\frac{3}{2}\cdot\lfloor \log x \rfloor$ on the average. So the complexity of computing Eq.(6) and Eq.(8) all can be approximately regarded as $\frac{3}{2}\cdot\left\lfloor \log(\frac{n}{2}) \right\rfloor$ on the average. In Eq.(10), the exponentiation operation for $y_V^{t_M} \bmod(n)$ can be pre-computed while $(g^{t_V})^{r_M} \bmod(n)$ cannot be computed in advance since the random t_V is only determined by *V* and variable in every session key renewal phase.

6. CONCLUSION

In this paper, based on self-certified scheme, we propose a new mutual authentication and key exchange protocol for roaming service in GLOMONET. Our proposed protocol is suitable to for distributed security management in global communication, since the temporary security manager in the visited network performs the same work that the original security manager in the home network does for subsequently regular communication.

Moreover, with the goal of enhancing the security and further simplifying previous protocols for roaming service, we introduce two new mechanisms in our protocols: identity anonymity and one-time session key renewal mechanism. For anonymity, we generate the temporary identity by encrypting the real identity with the shared key. For one-time session key renewal, we update the session key by utilizing a modified self-certified scheme based on the Diffie-Hellman system. This proposed protocol can be deployed in such environment that the mobile user is not required to setup a long-term secret key with his the home network in advance.

The performance comparisons between our protocol with the previous roaming protocols show that though we increase such new security mechanisms, the complexity of our protocols is still no more than other protocols and the computation requirement for mobile device is not high. Especially, in our protocol we obtain two extra good properties by using the self-certified scheme: (1) Reducing the number of exchanged message, only four messages in Phase I and two messages in Phase II; (2) Assuring the one-time session key renewal mechanism. The key idea hidden in this protocol is that we regard home network as a temporary TTP for roaming services.

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, Issue:8, pp.1606-1617, 1997.

[2] Z.J.Tzeng, W.G.Tzeng. "Authentication of Mobile Users in Third Generation Mobile System." Wireless Personal Communication, Vol.16, No.2, pp.35-50, 2002.

[3] L.Buttyan, C.Gbaguidi, et al. "Extensions to an authentication technique proposed for the global mobility network." IEEE Transaction on Communication, Vol.48, Issue:3, pp.373-376, 2000.

[4] Kuo-Feng Hwang, Chin-Chen Chang. "A self-encryption mechanism for authentication of roaming and teleconference services." IEEE Trans. on Wireless Communications, Vol. 2, Issue:2, pp.400 – 407, 2003.

[5] G. Horn, B.Preneel. "Authentication and Payment in Future Mobile Systems." Proceedings of the 5th European Symposium on Research in Computer Security, LNCS, Vol.1485, pp.277-293, 1998.

[6] A. Mehrotra, L.S.Golding. Mobility and Security Management in the GSM System and Some Proposed Future Improvements. Proceedings of the IEEE, Vol.86, Issue:7, pp.1480 – 1497, 1998.

[7] Jianming Zhu, Jianfeng Ma. "A new authentication scheme with anonymity for wireless environments." IEEE Transactions on Consumer Electronics, Vol.50, Issue:1, pp.231-235, 2004.

[8] D.Samafat, R.Molva and N.Asokan. "Untraceability in Mobile Networks". Proc. of the First Annual International Conference on Mobile Computing and Networking, pp26-36, 1995.

[9] J.Go, M. Groschel, et al. "Wireless Authentication Protocol Preserving User Anonymity." SCIS 2001, Japan, 2001.

[10] S.Patel. "Weakness of North American wireless authentication protocol," IEEE Personal Communication, Vol.4, pp.40-44, 1997.

[11] D.S.Wong, A.H.Chan. "Mutual authentication and key exchange for low power wireless communications." Proceedings of IEEE Military Communications Conference, MILCOM 2001, Vol.1, pp.39-43, 2001.

[12] Kyungah Shim. "Cryptanalysis of mutual authentication and key exchange for low power wireless communications." IEEE Communications Letters, Vol.7, Issue:5, pp.248–250, 2003.

[13] Siaw-Lynn Ng, C.Mitchell. "Comments on mutual authentication and key exchange protocols for low power wireless communications." IEEE Communications Letters, Vol.8, Issue:4, pp.262 – 263, 2004.

[14] Bruce Schneier. "Applied Cryptography: Protocols, Algorithm, and Source Code C". John Wiely & Sons, Inc (Second Edition), pp.70-72, 1996.

[15] S. Saeednia. "Identity-based and Self-certified Key Exchange Protocols." Proc. of the Second Australian Conference on Information Security and Privacy, pp.303-313, 1997.

[16] S. Saeednia. "A Note on Girault's Self-certified Model." Information Processing Letters, Elsiver, Vol 86. Issue:6, pp.323-327, 2003.

[17] Tzong-Chen Wu, Yuh-Shihng Chang, Tzouh-Yi Lin. "Improvement of Saeedni's self-certified key exchange protocols." Electronics Letters, Vol.34, Issue:11, pp.1094 – 1095, 1998.

[18] S. Saeednia and R.Safavi-Naini. "A New Identity-based Key Exchange Protocol Minimizing computation and Communication." Proc. of Information Security Workshop (ISW'97), LNCS, Vol.1396, pp.328-334, 1998.

[19] M. Girault. "Self-Certified Public Keys." Advance in Cryptology – Eurocrypt'91, pp.491-497, 1991.

[20] R.L.Adelman and K.S.McCURLEY. "Open problem in number theoretic complexity." Proceedings of the 1994 Algorithmic Number Theory Symposium, Springer-verlag, pp291-322, 1994.