Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks

Yixin Jiang, Chuang Lin, *Senior Member, IEEE,*
Xuemin (Sherman) Shen, *Senior Member, IEEE,* and Minghui Shi

***Abstract*— Two novel mutual authentication and key exchange protocols with anonymity are proposed for different roaming scenarios in the global mobility network. The new features in the proposed protocols include identity anonymity and one-time session key renewal. Identity anonymity protects mobile users privacy in the roaming network environment. One-time session key progression frequently renews the session key for mobile users and reduces the risk of using a compromised session key to communicate with visited networks. It has demonstrated that the computation complexity of the proposed protocols is similar to the existing ones, while the security has been significantly improved.**

***Index Terms*— Authentication, key exchange, roaming service, anonymity, secret-splitting, self-certified.**

I. Introduction

GLOBAL mobility network (GLOMONET) [1], such as GSM and CDMA networks etc., offers effective global roaming service for a legitimate user between the home network and the visited network. However, it also increases the possibility of illegal access from malicious intruders. Fig. 1 shows a general architecture of GLOMONET. The home network has a network prefix matching that of the mobile station's home address. The visited foreign network (*V*) and the home network have a roaming agreement and share a secret key. When a mobile station (*M*) roams to *V*, it performs authentication and updates its registration information with its home agent (*H*) in the home network, either directly or indirectly. A session key is setup to encrypt further communications in the session between the parties if the authentication is successful. In order to provide wireless access and especially roaming service in foreign network, strong authentication measures are required for all involved parties: the mobile device, the visited foreign network and its home network, to prevent privacy compromise and service abuse, etc. Several authentication protocols for global roaming service have been developed for the GLOMONET [2]. A challenge/response interactive authentication mechanism with a symmetric cryptosystem to construct their authentication protocol is introduced in [1]. However, there are several potential attacks to the protocol [3]. A legitimate, but malicious user may be able to obtain the authentication key K_{auth}. The intruder then can impersonate the roaming user or the visited network. The protocol may allow the intruder to feed the roaming user with a compromised and old authentication key, and thus to masquerade as the visited network. The home network may obtain the authentication key K_{auth}, which was originally designed to be kept confidential between the roaming user and the visited network only. In [4], a simpler and more efficient protocol based on self-encryption for roaming services is proposed. The home network H maintains a long-term secret key $K_{MH} = f(ID_M)$ for its user by using a secret one-way hash function f, where ID_M denotes the identity of the mobile device (or the user). However, since the protocol cannot provide identity anonymity, an intruder can obtain ID_M by intercepting the exchanged messages. If the function f is spied (which is not quite difficult by reverse-engineering on the mobile device), the intruder may compute K_{MH} of all mobile devices in such cryptosystem and the advantage of self-encryption would be counteracted. The disclosure of a user identity may also allow unauthorized entities to track his moving history and current location. Any illegal access to information related to the users location without his attention can be a serious violation of his privacy. The identity anonymity is an important property for roaming services.

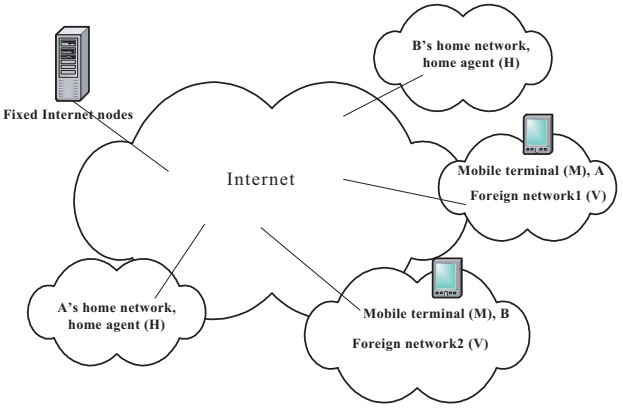


Fig. 1. A General Mobile Network

Manuscript received February 3, 2005; revised May 17, 2005; accepted September 3, 2005. The associate editor coordinating the review of this paper and approving it for publication was Y.-B. Lin. This relative work has been supported in part by the National Natural Science Foundation of China under contracts No.60573144, 60218003, 60429202, and 90412012; the Projects of Development Plan of the State High Technology Research under contract No. 2003CB314804, and Intel IXA University Research Plan; and a Postgraduate Scholarship and a Strategic Project Grant from Natural Science and Engineering Research Council of Canada (NSERC).

Y. Jiang and C. Lin are with Department of Computer Science and Technology Tsinghua University Beijing, China 100084. (e-mail: {yxjiang, clin}@csnet1.cs.tsinghua.edu.cn).

X. Shen and M. Shi are with Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1. (e-mail: {xshen, mshi}@bbcr.uwaterloo.ca).

Digital Object Identifier 10.1109/TWC.2006.05063.

On the other hand, a secure protocol design for roaming services requires: 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 freshness of the 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 mobile user's location information during the communication so that it is requisite to provide the identity anonymity mechanism [5]. Since the protocols are implemented on the mobile devices in wireless environment, there are other two factors to be considered: 1) 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 [6], [7], [8]; 2) 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.

In this paper, aiming at providing the identity anonymity and simplifying the existing authentication protocols for secure roaming service in GLOMONET environment, we propose two sets of mutual authentication and key exchange protocols with anonymity property for roaming service, by using use the secret-splitting principle and self-certified scheme [9], [10], [11], known as a public key authentication cryptosystem, respectively. The two protocols can be deployed depending on whether the home network and the mobile user share a fixed long-term secret key. The mutual authentication with anonymity property prevents the disclosure of mobile users real identities and protects their privacy in the roaming network environment. The proposed authentication protocols use the temporary identity (*TID*) for a mobile user instead of his real one. *TID* is prearranged and distributed by the home network H in advance or temporarily generated by encrypting the real identity [12], [13], [14], [15], [16]. The key exchange renews a mobile users session key for each session, and therefore, reduces the risk of using a compromised session key to communicate with visited networks. The proposed protocols can improve security features significantly, while requiring similar computation power as the existing protocols.

The rest of this paper is organized as follows. Two new authentication and key exchange protocols with anonymity for secure roaming service are proposed in Sections 2 and 4, each of which is followed by the security analysis in Section 3 and 5, respectively. The performance comparisons between the protocol in [4] and the proposed two protocols are presented in Section 6, and conclusion is given in Section 7.

II. Protocol I Based on Secret-splitting Principle

Secret splitting [17] is a type of information-hidden technique that divides a message into pieces. Each piece by itself has no meaning, but when these pieces are put together, the original message can be restored. Using the *secret splitting* principle, we propose a simple authentication and key exchange protocol with anonymity property for roaming services. The protocol includes two phases. In phase I, the visited network *V* authenticates a roaming user *M* through his home network *H*. After a successful validation, an authentication key is established between *M* and *V*. In the subsequent communication sessions, *V* can directly authenticate *M* by using the authentication key rather than doing it again through *H*. In phase II, a novel mechanism called "one-time session key Renewal" is introduced to assure the mutual authentication and freshness of the session key. User *M* establishes or renews a session key with *V*, and *M* can get the service from *V* directly.

A. Phase I: Mutual Authentication Protocol (MAP)

Firstly, we introduce the concept of pseudonym identity PID_M for user *M*. Let *H* generate a secret m-bits random number N_M for each user and records the mapping relation of *i*th user's PID_i and N_i ($PID_i \leftrightarrow N_i$). To prevent the exclusive search attack, m should be sufficiently large, e.g. 256 bits. When a user *M* registers with his home network *H*, he submits his identity ID_M to *H*. Then, *H* computes PID_M for user *M* as:

$$PID_M = h(N_M \parallel ID_H) \oplus ID_M \oplus ID_H, \qquad (1)$$

where $\oplus$ denotes bitwise XOR operation and h is a public strong one-way hash function. (1) is constructed so that both *M* and *H*'s identity information is associated to PID_M. Subsequently, *H* delivers PID_M to *M* through a secure channel, such as issuing a smart card for user *M*. By this secret-splitting mechanism, we can conceal the real identity ID_M in PID_M and provide identity anonymity for *M* without increasing the computation complexity.

Message 1. $M \rightarrow V: ID_H, PID_M, E_{K_{MH}}(r_M \| K_{MH})$

Message 2. $V \rightarrow H: PID_M, E_{K_{VH}}(r_V \| t_V \| E_{K_{MH}}(r_M \| K_{MH}))$

Message 3. $V \leftarrow H: E_{K_{VH}}(r_V \| r_M \| h(ID_M)), E_{K_{MH}}(r_M \| r_V \| ID_V)$

Message 4. $M \leftarrow V: E_{K_{MH}}(r_M \| r_V \| ID_V)$

Message 5. $M \rightarrow V: E_{K_{auth}}(K_{auth})$

Fig. 2. Authentication Protocol I for Roaming Services

The goal of MAP is to provide a mutual authentication mechanism for users *M* and *V*. Our proposed protocol for the roaming services (Phase I) is described as in Fig. 2. Two new features are introduced. A simple secret splitting mechanism is utilized to provide the identity anonymity, which prevents that unauthorized entities from tracing the mobile users roaming history and his current location. The generation mechanism of authentication key K_{auth} is also improved such that:

$$K_{auth} = r_M \oplus r_V, \qquad (2)$$

where r_M and r_V are sufficiently large random number generated by *M* and *V*, respectively. K_{auth} is computed with the random numbers chosen by both parties, while K_{auth} in [4] was only determined by *V*, i.e. $K_{auth} = r_V$. The modified mechanism makes the protocol fairer and more secure without increasing the computation complexity since the XOR is a very simple operation.

In the following, we describe the proposed MAP protocol according to the order of message exchange and discuss the

security goals that can be achieved during the execution of each protocol message.

1) When a mobile user *M* enters a new visited network *V*, he initiates a registration authentication process with *V* in order to identify himself to be a legal subscriber of his home network *H*. *M* generates a secret random number r_M, computes the long-term secret key $K_{MH} = f(ID_M)$, where f is a public one way function, and sends $E_{K_{MH}}(r_M \parallel K_{MH})$, PID_M, and ID_H to the visited network *V*, respectively.
2) On receiving message 1 from *M*, *V* forwards PID_M and sends $E_{K_{MH}}(r_V \parallel t_V \parallel E_{K_{MH}}(r_M \parallel K_{MH}))$ to *H* for identity authentication, where K_{VH} is the shared secret key between *V* and *H*, r_V is a secret random number generated by *V*, and t_V is a time stamp.
3) After receiving the message from *V*, *H* first decrypts $E_{K_{MH}}(r_V \parallel t_V \parallel E_{K_{MH}}(r_M \parallel K_{MH}))$ by using K_{VH}. Then *H* determines whether the time stamp is within some allowable range compared with its current time. If t_V is not within the range, *H* terminates the execution. Otherwise, *H* gets *M*'s real identity by computing:
$$ID_M = PID_M \oplus h(N_M \parallel ID_H) \oplus ID_H \quad (3)$$
Afterwards, *H* calculates the long-term key K_{MH} by $K_{MH} = f(ID_M)$ and uses it to decrypt $E_{K_{MH}}(r_M \parallel K_{MH})$. If the decrypted secret key, K_{MH}, is equal to $f(ID_M)$, the authenticity of user *M* is authenticated. It also provides the implicit identity authentication of *V*. Subsequently, *H* sends $E_{K_{VH}}(r_V \parallel r_M \parallel h(ID_M)$ and $E_{K_{MH}}(r_M \parallel r_V \parallel ID_V)$ to *V*.
4) Messages 4 and 5 show the process of the mutual authentication and key negotiation between *M* and *V*. On receiving the message from *H*, *V* first decrypts $E_{K_{VH}}(r_V \parallel r_M \parallel h(ID_M))$. If the decrypted r_V in $E_{K_{VH}}(r_V \parallel r_M \parallel h(ID_M))$ is the same as its original r_V, then *V* believes that *M* is an authorized user. Subsequently, *V* does the following: 1) Saving the value $h(ID_M)$ for identifying the identity of user *M* in Phase II; 2) Setting $K_{auth} = r_M \oplus r_V$ as the authentication key K_{auth}; 3) Forwarding message $E_{K_{MH}}(r_M \parallel r_V \parallel ID_V)$ to *M*.
5) *M* decrypts $E_{K_{MH}}(r_M \parallel r_V \parallel ID_V)$ using K_{MH}. If the decrypted r_M^* is equal to its original value r_M, then *M* can compute the authentication key as $K_{auth} = r_M \oplus r_V$. Afterwards, *M* sends to *V* to verify the key K_{auth}.
6) If $E^{-1}_{K_{auth}}(E_{K_{auth}}(K_{auth})) = K_{auth}$, *V* records the authentication key K_{auth} for user *M*. *V* has finished the authentication process with *M* and established an authentication key K_{auth}.

Message 1. $M \rightarrow H: ID_H, PID_M, E_{K_{MH}}(r_M \| K_{MH})$

Message 2. $M \leftarrow H: E_{K_{MH}}(r_M \| r_H \| ID_H)$

Message 3. $M \rightarrow H: E_{K_{auth}}(K_{auth})$

Fig. 3. Authentication Protocol I for Local Services

As a special case, consider the authentication protocol when user *M* is located in his home network. The corresponding authentication protocol for local services is shown in Fig. 3. Note that the difference between Fig. 2 and Fig. 3 is that the authentication protocol for local services ignores the original Messages 2 and 3 in Fig. 2.

In the protocol, the self-encryption property of the protocol in [4] is maintained, that is, the home network also maintains a long-term secret key K_{auth} for its user *M* by using a one-way function. By extracting the real identity ID_M of user *M* from PID_M, the shared key K_{MH} can be generated, which is used to encrypt the corresponding text.

B. Phase II: One-time session key Renewal Protocol (SKRP)

The goal of SKRP protocol is to establish or renew a session key between *M* and *V*. In this phase, a novel mechanism called "One-time session key renewal" is introduced, which allows mobile user *M* to renew his session key frequently and reduces the risk that he uses a compromised session key to communicate with *V*.

Message 1. $M \rightarrow V: ID_V, PID_{M,i}, E_{K_{i-1}}(r_{M,i} \| K_{i-1})$

Message 2. $M \leftarrow V: E_{K_{i-1}}(r_{M,i} \| r_{V,i} \| ID_H)$

Message 3. $M \rightarrow V: E_{K_i}(K_i)$

Fig. 4. One-time Session Key Renewal Protocol I

Suppose that *M* need to renew his session key K_{i-1} with *V* for the *i*th time, he can obtain the new session K_i according to the steps shown in Fig. 4. The new session key K_i is calculated as
$$K_i = r_{M,i} \oplus r_{V,i}, \ i = 1, 2, 3, ..., n, \quad (4)$$
and K_0 is set as the authentication key K_{auth} (Phase I), that is, $K_0 = K_{auth}$. The pseudonym identity $PID_{M,i}$ for M is computed as
$$PID_{M,i} = h(ID_M) \oplus r_{M,i}. \quad (5)$$
Clearly, $PID_{M,i}$ will vary in each session key negotiation because of $r_{M,i}$.

As shown in Fig. 4, on receiving the message 1 from *M*, *V* can obtain the original $r_{M,i}$ as
$$\begin{aligned} r_{M,i} &= PID_{M,i} \oplus h(ID_M) \\ &= (h(ID_M) \oplus r_{M,i}) \oplus h(ID_M). \end{aligned} \quad (6)$$
Then, *V* uses the previous session key K_{i-1} to decrypt $E_{K_{i-1}}(r_{M,i} \parallel K_{i-1})$ and checks whether $r_{M,i}$ and K_{i-1} in $E_{K_{i-1}}(r_{M,i} \parallel K_{i-1})$ are the same as that in (6) and the previous key K_{i-1} kept by *V*, respectively. If it is not, *V* terminates the execution. Otherwise, $PID_{M,i}$ of *M* is authenticated. Subsequently, *V* does the following: 1) Generating a random number $r_{V,i}$; 2) Setting as the next session key $K_i = r_{M,i} \oplus r_{V,i}$ and keeping it secretly; 3) Sending $E_{K_{i-1}}(r_{M,i} \parallel r_{V,i} \parallel ID_V)$ to *M*.

Since $r_{M,i}$ and $r_{V,i}$ are generated by *M* and *V*, respectively, $K_i = r_{M,i} \oplus r_{V,i}$ plays a role of one-time key when *M* accesses *V*. We call this new mechanism "One-time session key renewal".

In addition, comparing with Fig. 2, 3 and 4, it can be seen that the mechanism in the mobile device for session key renewal is the same as that for roaming services except the introduction of different parameters according to the specific environment. Hence, though there are redundant fields in SKRP protocol (e.g., ID_V in Message 1, we preserve the consistency of protocol architecture and decrease the complexity of implementation. In other words, the complexity of the mobile device can be further simplified.

III. Security Analysis for Protocol I

In this section, we analyze the security of the proposed protocol I to verify whether the security requirements introduced in Section I have been satisfied.

A. Identity Anonymity and Intractability Analysis

Our scheme provides identity anonymity in all procedures by replacing the real identity with a pseudonym identity.

1) In MAP, the real identity ID_M of M is replaced with his pseudonym identity PID_M, which is computed as $PID_M = h(N_M \parallel ID_H) \oplus ID_M \oplus ID_H$. Since only home network *H* knows the secret , nobody except *H* can obtain the real identity ID_M from PID_M by $ID_M = PID_M \oplus h(N_M \parallel ID_H) \oplus ID_H$. Therefore, a tracker cannot obtain the secret $h(N_M \parallel ID_H) \oplus ID_H$, and it is impossible for him to extract the real identity ID_M from the transmitted messages and then trace the location of a mobile target user. Since each mobile user *j*'s PID_j is computed using unique N_j, the legitimate mobile user *j* cannot compute another mobile user k's ID_k by intercepting PID_k and impersonate user k.
2) In SKRP, the identity anonymity is guaranteed by the similar mechanism. In other words, *M* substitutes his real identity ID_M with the pseudonym identity $PID_{M,i}$, where $PID_{M,i}$ is computed as $PID_{M,i} = h(ID_M) \oplus r_{M,i}$.

The identity intractability is assured by two measures: 1) When *M* roams in a visited network, the pseudonym identity $PID_{M,i} = h(ID_M) \oplus r_{M,i}$ will vary in each session key renewal because of the variance of $r_{M,i}$; 2) Once *M* roams into a different visited network, the pseudonym identity $PID'_{M,i}$ also varies due to $r'_{M,i}$, which guarantees the freshness of the pseudonym identity $PID'_{M,i}$ in different roaming domains.

Finally, we analyze the *cooperation* attacks in identity anonymity. Assume that there are separate domains between visited networks. When a user enters a new visited network, he will send a new different pseudonym identity $PID_{M,i}$ to the new visited network. Moreover, the session key K_i changes with the variation of $r_{M,i}$ and $r_{V,i}$. So even though there is a cooperation between visited networks, a new visited network still cannot recognize the users real identity.

B. Prevention of Fraud

To prevent fraud, the mobile user, the visited network, and home network should authenticate each other, which requires that our scheme provide mutual authentication mechanism between any two of them. The proposed MAP protocol can efficiently prevent impersonation attacks from an intruder by considering the following scenarios:

1) An intruder cannot 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 valid response $E_{K_{VH}}(r_V \parallel r_M \parallel h(ID_M))$ to *V*.
2) *V* cannot impersonate *H* to cheat *M*. Since the shared key K_{MH} is unknown to *V*, and *V* cannot send user *M* the valid response $E_{K_{MH}}(r_M \parallel r_V \parallel ID_V)$ which is generated by *H*.
3) An intruder cannot impersonate *M* either since he cannot know the real identity of *M*. If the intruder uses a phony identity ID'_M, the corresponding spurious pseudonym identity PID'_M can be identified by home network, because H cannot obtain the ID'_M by computing

$$ID'_M = PID'_M \oplus h(N'_M \parallel ID_H) \oplus ID_H$$

Given that the real identity is kept anonymity in our scheme, only the user himself and his home network *H* can know his real identity.

Similarly, in SKRP Protocol, the identities of *M* and *V* are also compulsorily authenticated with each other. We consider the following impersonation attack scenarios in SKPP protocol.

1) An intruder cannot impersonate *V* to cheat *M*, since he does not possess the previous session key K_{i-1}. Hence it is impossible for an intruder to send the authentic message $E_{K_{i-1}}(r_{M,i} \parallel K_{i-1})$ to *M*.
2) An intruder cannot impersonate *M* to cheat *V*. Since the previous shared session key $K_{i-1} = r_{M,i-1} \oplus r_{V,i-1}$ is unknown to anyone except only *M* and *V*, the intruder cannot send the authentic message $PID_{M,i}, E_{K_{i-1}}(r_{M,i} \parallel K_{i-1})$to *V*, where $PID_{M,i} = h(ID_M) \oplus r_{M,i}$. Actually, $PID_{M,i}$ also provides an implicit signature $r_{M,i}$ for with the shared key K_{i-1}. Moreover, *M* is required to send back the message $E_{K_i}(K_i)$ to *V* for mutual implicit key authentication.

Therefore, due to the mandatory mutual authentication between *M* and *V*, our SKRP protocol is efficiently refrained from fraudulent attacks.

C. Mutual Agreement and the Freshness of Session Key

Consider the mutual key exchange mechanism in MAP protocol. According to (2), $K_{auth} = r_M \oplus r_V$. It can be shown that the authentication key K_{auth} is determined by two random numbers r_M and r_V, which are chosen by *M* and *V*, respectively.

Similarly, in SKRP, it can be seen that the session key K_i can be also obtained from the mutual agreement mechanism, since the key K_i is derived as $K_i = r_{M,i} \oplus r_{V,i}$, $(i = 1, 2, ..., n)$, where the two random numbers $r_{M,i}$ and $r_{V,i}$ are respectively determined by *M* and *V* independently (4).

In addition, in our scheme the freshness of session key is guaranteed by executing SKRP protocol. The exchanged Messages 1 and 2 in SKRP protocol provide two fresh random numbers $r_{M,i}$ and $r_{V,i}$, respectively. Due to $K_i = r_{M,i} \oplus r_{V,i}$, the freshness of $r_{M,i}$ and $r_{V,i}$ guarantees the freshness of the session key K_i in each session key renewal (Fig. 2).

D. Prevention of Replaying Attack

A replaying attack is a method that an intruder stores "stale" intercepted messages and retransmits them at a later time. In order to illegally obtain an authentication key, an intruder will attempt to impersonate a legal user by replaying the users exchanged messages. He intercepts the Message 1 (step 1) sent by *M* and then replays Message 1 $\{ID_H, PID_M, E_{K_{MH}}(r_I \parallel K_{IH})\}$ to *V*, where $E_{K_{MH}}(r_M \parallel K_{MH})$ has changed to $E_{K_{MH}}(r_I \parallel K_{IH})$. However, the intruder cannot get the correct message 3 from *H*, because the relationship between PID_M and $E_{K_{MH}}(r_M \parallel K_{MH})$ in the original message 1 is self-encryption and can authenticate each other (step 3). According to above analysis, our proposed protocol is able to resist such replaying attacks.

IV. Protocol II Based on Self-certified Scheme

The proposed protocol II is based on the Self-certified scheme [9], [10], [11]. In the protocol, home network *H* is considered as a temporary Trusted Third Party (TTP) for roaming services. When user *M* visits the visited network *V*, both of them initialize a registration procedure with *H* (*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 the trust relations between *M* and *V* can be established. *M* can then directly negotiate the session key with *V* without accessing his home network.

A. Self-Certified Scheme

The self-certified scheme combines the advantages of certificated-based and identity-based public key cryptosystems [18], [19], and it can also provide a mechanism for authenticating a user's public key. In this scheme (contrary to identity-based schemes), each user (mobile device) 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 creates a certificate from that pair in such a way that it cannot be computed without the knowledge of some trapdoor, known only to the authority, which is *H*, in this case.

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 ($p - 1 = 2p'$, and $q - 1 = 2q'$, where p' and q' are also primes), generates a base element $g \neq 1$ of order $r = p' \cdot q'$ ($g \neq 1 \bmod(n)$), and picks a large integer $u < r$. Let $t \in Z_u^*$ be an element Z_u^* of 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. p and q are discarded.

Any user U_i then can register with TTP by performing the following steps.

1) User U_i chooses a random number $x_i \in \{2, 3, ..., u - 1\}$ as his secret key, computes $y_i = g^{x_i} \bmod(n)$ as his public key and sends y to the TTP.
2) The TTP prepares a string I_i associated with the personal information (Name, Address, etc.) of U_i and computes $w_i = y_i^{f(I_i)^{-1}}$ as a witness for user U_i and sends message $\{I_i, w_i\}$ to U_i.
3) User U_i verifies I_i and witness w_i by checking whether the equation $y_i = w_i^{f(I_i)} \bmod(n)$ holds.

Regarding to the security strength of self-certified scheme, it is shown in [8] that forging a valid witness w_i for user U_i is equivalent to break an instance of RSA cryptosystem.

Based on the self-certified scheme, we propose the Protocol II for secure roaming services. Similar to Protocol I, it composes of two phases: 1) the mutual authentication protocol (Phase I); 2) Session key renewal protocol (Phase II).

B. Phase I: Mutual Authentication Protocol (Registration)

Suppose $y_M = g^{r_M} \bmod(n)$ and $y_V = g^{r_V} \bmod(n)$, where 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 *M* and *V*, respectively. In addition, letw_M and w_V be the witness of *M* and *V*, which are issued and calculated by *H* as follows:

$$w_M = ((y_M \oplus I_M)^{f(I_M)^{-1}}) \bmod(n) \tag{7}$$

$$w_V = ((y_V \oplus I_V)^{f(I_V)^{-1}}) \bmod(n) \tag{8}$$

Then the new authentication protocol for roaming services can be described in Fig. 5. The shared key K_{MH} is computed as $K_{MH} = (PK_H)^{r_M}$, where 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. The real identity ID_M of user *M* is hidden in the temporary identity TID_M, which is computed as $TID_M = E_{K_{MH}}(g^{r_M} \oplus ID_M)$.

Message 1. $M \rightarrow V: y_M, ID_H, TID_M$

Message 2. $V \rightarrow H: y_M, y_V, E_{K_{VH}}(y_V \| ID_V \| TID_M \| T_V)$

Message 3. $V \leftarrow H: E_{K_{VH}}(w_V \| I_V), E_{K_{MH}}(w_M \| I_M \| ID_V)$

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

Fig. 5. Authentication Protocol II for Roaming Services

We explain our proposed protocol II in detail according to the order of message exchanges as follows.

1) *M* generates a random number $r_M \in Z_u^* \backslash \{1\}$, computes $y_M = g^{r_M}$ and $K_{MH} = (PK_H)^{r_M}$. *M* then computes $TID_M = E_{K_{MH}}(y_M \oplus ID_M)$, and sends ID_M and y_M to *V*.
2) *V* chooses a random number $r_V \in Z_u^* \backslash \{1\}$ to compute $y_V = g^{r_V}$, and sends $\{y_M, y_V, E_{K_{VH}}(y_V \parallel ID_V \parallel TID_V \parallel T_V)\}$ to *H*.
3) *H* decrypts $E_{K_{VH}}(y_V \parallel ID_V \parallel TID_V \parallel T_V)$ by using shared key K_{VH}. If the time stamp T_V is within a reasonable threshold 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 *H* can get the real identity of *M* by computing

$$ID_M = E_{K_{MH}}^{-1}(E_{K_{MH}}(g^{r_M} \oplus ID_M)) \oplus g^{r_M}. \tag{9}$$

If it is legal, *H* does the following: 1) Prepare two strings I_M and I_V associated with the personal information (Name, Address, etc.) of *M* and *V*, respectively;

2) Compute the witness w_M and w_V for *M* and *V* according to (7) and (8). 3) H sends $E_{K_{VH}}(w_V \parallel I_V)$ and $E_{K_{MH}}(w_M \parallel I_M \parallel ID_V)$ to *V*.

4) *V* decrypts $E_{K_{VH}}(w_V \parallel I_V)$ and verifies witness and by checking whether (10) holds.

$$y_V = ((w_v)^{f(I_V)} \bmod(n)) \oplus I_V. \tag{10}$$

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

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

$$y_M = ((w_M)^{f(I_M)} \bmod(n)) \oplus I_M. \tag{11}$$

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

In addition, when *M* is located in his home network, the authentication protocol can be described in Fig. 6.

Message 1. $M \rightarrow H: y_M, ID_H, TID_M$

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

Fig. 6. Mutual Authentication Protocol II for Local Services

C. Phase II: Session Key Renewal Protocol

In phase II, we also use one-time session key renewal mechanism. Being different from previous protocols, the mechanism for this protocol renews the session key by utilizing a modified self-certified scheme and Diffie-Hellman mechanism (Fig. 7).

Message 1. $M \rightarrow V: w_M, I_M, g^{t_M}$

Message 2. $M \leftarrow V: w_V, I_V, g^{t_V}$

Fig. 7. Session Key Renewal Protocol II

In Fig. 7, $t_M, t_V \in Z_u^*$ denotes two different elements of Z_u^* of order u. And the session key K_{MV} can be calculated respectively by users *M* and *V* as follows.

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

$$y_V = ((w_v)^{f(I_V)} \bmod(n)) \oplus I_V, \tag{12}$$

$$K_M = y_V^{t_M} \cdot (g^{t_V})^{r_M} = g^{r_V t_M + r_M t_V} \bmod(n), \tag{13}$$

$$K_{MV} = h(K_M). \tag{14}$$

For *V*, the session key can be computed similarly as follows:

$$y_M = ((w_M)^{f(I_M)} \bmod(n)) \oplus I_M, \tag{15}$$

$$K_V = y_M^{t_V} \cdot (g^{t_M})^{r_V} = g^{r_V t_M + r_M t_V} \bmod(n), \tag{16}$$

$$K_{MV} = h(K_V). \tag{17}$$

Clearly, the session key calculated by *M* and *V*, respectively, is equal since

$$K_{MV} = h(K_M) = h(g^{r_V t_M + r_M t_V} \bmod(n)) = h(K_V), \tag{18}$$

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 greatly improved by this approach, since each session key is renewed for each session. Moreover, compared with our Protocol I, the number of message exchanges is reduced to two, while the one-time session key renewal mechanism is preserved.

V. Security Analysis for Proposed Protocol II

Similar to the analysis in Section III, we analyze the security of protocol II to verify the security requirements.

A. Identity Anonymity and Intractability Analysis

As shown in Fig. 5, the real identity ID_M of *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 its 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

$$\begin{aligned} ID_M &= E_{K_{MH}}^{-1}(TID_M) \\ &= E_{K_{MH}}^{-1}(E_{K_{MH}}(g^{r_M} \oplus ID_M)) \oplus g^{r_M}. \end{aligned} \tag{19}$$

Since an illegal tracker cannot obtain the shared key K_{MH}, he cannot extract the real identity ID_M from TID_M and trace the location of a targeted mobile user.

The identity intractability is assured by two measures: 1) When user *M* roams in different visited networks, TID_M is different in each session because of different 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 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 the scheme provides secure mutual authentication mechanisms between mobile users *M* and *V*, *M* and *H*, or *V* and *H*. Consider the following impersonation attack scenarios in MAP scheme (Fig. 5):

1) An intruder cannot impersonate *H* to cheat *V*, since he does not possess the long-term secret key K_{VH}. Hence an intruder cannot to generate the responding confirmation $E_{K_{VH}}(w_V \parallel I_V \parallel g^{r_M})$ to *V*.
2) *V* cannot impersonate *H* to cheat user *M*. Since the shared key K_{MH} is unknown to *V*, and *V* cannot generate $E_{K_{MH}}(w_M \parallel I_M \parallel ID_V \parallel g^{r_M} \parallel g^{r_V})$ where w_M contains y_M generated by *M*.
3) An intruder also cannot impersonate *M* since he cannot know the real identity and/or the password 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 $ID_M^{'}$ by computing $ID_M' = E_{K'_{MH}}^{-1}(TID_M') = E_{K'_{MH}}^{-1}(E_{K'_{MH}}(g^{r_M} \oplus ID_M')) \oplus g^{r_M}$, 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* know his real identity. If the real identity is shared by other application, the authenticity is further protected by the password of user *M*.

Similarly, we also consider the impersonation attack scenarios in SKRP Phase (Fig. 7) as follows.

1) An adversary is not able 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 equation $y_M = g^{r_M} = (w_M^{f(I_M)} \oplus I_M) \mathrm{mod}(n)$.
2) Similarly, an adversary also cannot impersonate *V* to cheat *M*.

Comparing with the basic self-certified scheme, we use $w_M = ((y_M \oplus I_M)^{f(I_M)^{-1}}) \mathrm{mod}(n)$ as the witness in stead of the original $w_M = y_M^{f(I_M)^{-1}} \mathrm{mod}(n)$. The improvement is to prevent a cheating user from having a chance to get forged self-certified witness, by requiring only one more XOR operation.

C. Mutual Agreement and the Freshness of Session Key

Consider the mutual key exchange mechanism in SKRP protocol. The new session key is obtained with the mutual agreement mechanism since according to (18) we can derive key K_{MV} as follows

$$K_{MV} = h(g^{r_V t_M + r_M t_V} \mathrm{mod}(n)), \tag{20}$$

where the two random numbers r_M and r_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.

The freshness of session key is evidently assured, since the exchanged Messages 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.

D. Prevention of Replay Attack

Finally, we analyze the *replay attack* in session key renewal protocol (Fig. 7). 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 $y_M^* = g^{r_M^*} \mathrm{mod}(n)$. However, the adversary cannot compute a valid witness w_M^* for *M*, because the original witness $w_M = ((y_M \oplus I_M)^{f(I_M)^{-1}}) \mathrm{mod}(n)$ 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: $w_M^* = ((y_M^* \oplus I_M)^{f(I_M)^{-1}}) \mathrm{mod}(n)$, unless he can compute discrete logarithm modulo a large composite. So the proposed protocol is able to resist such replay attack, i.e., the adversary and *V* cannot obtain the same secret key. Similarly, an adversary that impersonates *V* cannot obtain the same secret key with *M* either.

TABLE I
PERFORMANCE COMPARISONS (PHASE I)

Performance Metrics		Protocol in [4]	Protocol I	Protocol II
Exponential operation	***M***	**N/A**	**N/A**	**1+2 Pre.**
	V	N/A	N/A	1+1 Pre.
	H	N/A	N/A	3
Hash operation	***M***	**1 (step 1)**	**N/A**	**1 (step 1)**
	V	N/A	N/A	N/A
	H	1 (step 3)	1 (step 3)	1 (step 3)
Symmetric encryption	***M***	**2 (step 1, 5)**	**2 (step 1, 5)**	**1 (step 1)**
	V	1 (step 2)	1 (step 2)	1 (step 2)
	H	2 (step 3)	2 (step 5)	2 (step 5)
Symmetric decryption	***M***	**1 (step 5)**	**1 (step 5)**	**1 (step 5)**
	V	2 (step 4, 6)	2 (step 4, 6)	1 (step 4)
	H	2 (step 3)	2 (step 3)	1 (step 3)
Transmissions	***M*↔*V***	**3**	**3**	**2**
	V↔*H*	2	2	2
Anonymity		N/A	Yes	Yes

TABLE II
PERFORMANCE COMPARISONS (PHASE II)

Performance Metrics		Protocol in [4]	Protocol I	Protocol II
Exponential operation	***M***	**N/A**	**N/A**	**1+2 Pre.**
	V	N/A	N/A	1+1 Pre.
Symmetric encryption	***M***	**1**	**1**	**N/A**
	V	1	1	N/A
Symmetric decryption	***M***	**1**	**1**	**N/A**
	V	1	1	N/A
Transmissions	***M*↔*V***	**3**	**3**	**2**
Anonymity		N/A	Yes	Yes

Note:
M: Mobile; V: Visited Network; H: Home Network
Pre: Pre-computed exponentiation operation

VI. PERFORMANCE ANALYSIS

The performance comparisons, specifically the number of hash operation, symmetric encryption/decryption, exponential operation, and the number of message exchanges, between the proposed two protocols and the protocol in [4] are given in Table I and Table II. Note that the rows in bold font show the comparisons related to mobile user *M*. It can be generally concluded that though the identity anonymity mechanism is introduced into our protocols for roaming service, the complexity of the proposed protocols is equivalent to or less than the protocol in [4] and the computation requirement for mobile device is quite low.

The proposed protocol II increases the exponentiation operations, however it reduces the number of symmetric encryption/decryption 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}. As a result of these improvements, the real exponentiation computation load is not remarkable. The protocol also provides: 1) identity anonymity; 2) the mutual authentication between the

two entities without pre-setup shared secret key; 3) the session keys renewal for each session. All the features are especially favorable and safer in the roaming environment. Moreover, the reasonable increase of computational load resulting from the identity anonymity and one-time session key renewal provide the improved security strength that are not considered in [4].

Note that the exponential operations required for *M* are in (11) (Phase I) and (13) (Phase II), respectively. If we only consider the exponential operations except those pre-computed exponential operations, the average computation complexity is $\frac{3}{2}\left\lfloor \log \frac{n}{2} \right\rfloor \cdot M(n)$, where $M(n)$ denotes the computation complexities of modular modulo n. In fact, according to the binary algorithm for fast exponentiation [20], computing g^x will take $2\lfloor \log x \rfloor$ multipliers in the worst case and $\frac{3}{2}\lfloor \log x \rfloor$ on the average. So the complexity of computing (11) and (13) can be approximately considered as $\frac{3}{2}\left\lfloor \log \frac{n}{2} \right\rfloor$ on the average. In (13), the exponential operation for $y_V^{t_M}$ can be pre-computed while $(g^{t_V})^{r_M} \bmod (n)$ cannot be computed in advance since the random variable t_V is only determined by *V* and varies in every session key renewal phase.

VII. Conclusion

Two novel mutual authentication and key exchange protocols with identity anonymity and one-way session key progression have been proposed for GLOMONET. The protocols are suitable for distributed security management, since the temporary security manager in the visited network performs the same as that of the original security manager in the home network for subsequent communication. For each protocol, the identity anonymity has been achieved by hiding the real user identity in prearranged PIDs based on the secret-splitting principle or by encrypting the real identity with the shared key, respectively. The proposed protocols can protect a mobile users privacy in the roaming network environment by hiding the real identity and reduces the risk that a mobile user uses a compromised session key to communicate with visited networks by refreshing the session key frequently. The two protocols can be applied depending on the availability of the long-term shared secret key shared by the home network and its mobile users. The performance comparisons have shown that significant security improvement can be achieved while the complexity of our protocols is similar to [4].

Acknowledgment

The authors would like to thank the anonymous reviews for their valuable comments and suggestions.

References

[1] S. Suzukiz and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," *IEEE J. Sel. Areas in Commun.*, vol. 15, no. 8, pp. 1606-1617, Oct. 1997.

[2] Z.-J. Tzeng and W.-G. Tzeng, "Authentication of mobile users in third generation mobile system," *Wireless Personal Commun.*, vol. 16, no. 1, pp. 35-50, Jan. 2001.

[3] L. Buttyan, C. Gbaguidi, and et al., "Extensions to an authentication technique proposed for the global mobility network," *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 373-376, Mar. 2000.

[4] K.-F. Hwang and C.-C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," *IEEE Trans. Wireless Commun.*, vol. 2, no.2 pp. 400-407, Mar. 2003.

[5] S. Patel, "Weakness of north American wireless authentication protocol," *IEEE Pers. Commun.*, vol. 4, no. 3, pp. 40-44, June 1997.

[6] D. S. Wong and A. H. Chan, "Mutual authentication and key exchange for low power wireless communications," in *Proc. IEEE Military Commun. Conf. 2001*, pp. 39-43.

[7] K. Shim, "Cryptanalysis of mutual authentication and key exchange for low power wireless communications," *IEEE Commun. Lett.*, vol. 7, no. 5, pp. 248-250, May 2003.

[8] S. L. Ng and C. Mitchell, "Comments on mutual authentication and key exchange protocols for low power wireless communications," *IEEE Commun. Lett.*, vol. 8, no. 4, pp. 262-263, Apr. 2004.

[9] S. Saeednia, "Identity-based and Self-certified Key Exchange Protocols," in *Proc. Second Australian Conf. on Info. Security and Privacy 1997*, pp. 303-313.

[10] S. Saeednia, "A note on Girault's self-certified model," *Info. Processing Letters, Elsiver*, vol. 86, no. 6, pp. 323-327, June 2003.

[11] T.-C. Wu, Y.-S. Chang, and T.-Y. Lin, "Improvement of Saeedni's self-certified key exchange protocols," *Electronics letters*, vol. 34, no. 1, pp. 1094-1095, May 1998.

[12] A. Mehrotra and L. S. Golding, "Mobility and security management in the GSM system and some proposed future improvements," *Proc. IEEE*, vol. 86, no. 7, pp. 1480-1497, July 1998.

[13] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Trans. Consum. Electron.*, vol. 50, no.1, pp. 231-235, Feb. 2004.

[14] D. Samafat, R. Molva, and N. Asokan, "Untraceability in mobile networks," in *Proc. First Annual International Conf. on Mobile Computing and Networking 1995*, pp. 26-36.

[15] J. Go, M. Groschel, and et al., "Wireless authentication protocol preserving user anonymity," SCIS 2001, Japan, 2001.

[16] H. Y. Lin and B. Preneel, "Authentication protocols for personal Communication systems," in *Proc. ACM SIGCOMM 1995*, pp. 256-261.

[17] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd edition, Wiley, 1996.

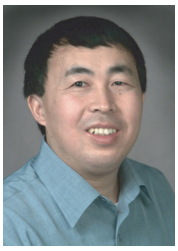
[18] S. Saeednia and R. Safavi-Naini, "A new identity-based key exchange protocol minimizing computation and Communication," in *Proc. Info. Security Workshop (ISW '97)*, *LNCS*, pp. 328-334.

[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," in *Proc. Algorithmic Number Theory Symposium 1994*, pp. 291-322.

Yixin Jiang is a Ph.D candidate of the Department of Computer Science and Technology, Tsinghua University, China. He received the M.E degree in Computer Science from Huazhong University of Science and Technology in 2002. In 2005, he was a Visiting Scholar with the Department of Computer Sciences, Hong Kong Baptist University. His current research interests include security and performance evaluation in wireless communication and mobile computing. He has published more than 20 papers in research journals and IEEE conference proceedings in these areas.

Chuang Lin (SM) is a professor and the head of the Department of Computer Science and Technology, Tsinghua University, Beijing, China. He received the Ph.D. degree in Computer Science from Tsinghua University in 1994. In 1985-1986, he was a Visiting Scholar with the Department of Computer Sciences, Purdue University. In 1989-1990, he was a Visiting Research Fellow with the Department of Management Sciences and Information Systems, University of Texas at Austin. In 1995-1996, he visited the Department of Computer Science, Hong Kong University of Science and Technology. His current research interests include computer networks, performance evaluation, network security, logic reasoning, and Petri net and its applications. He has published more than 200 papers in research journals and IEEE conference proceedings in these areas and has published three books. Professor Lin is an IEEE senior member and the Chinese Delegate in IFIP TC6. He serves as the General Chair, ACM SIGCOMM Asia workshop 2005; the Associate Editor, IEEE Transactions on Vehicular Technology; and the Area Editor, Journal of Parallel and Distributed Computing.



Xuemin (Sherman) Shen (SM) received the B.Sc. (1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. From September 1990 to September 1993, he was first with the Howard University, Washington D.C., and then the University of Alberta, Edmonton (Canada). Since October 1993, he has been with the Department of Electrical and Computer Engineering, University of Waterloo, Canada, where he is a Professor and the Associate Chair for Graduate Studies. Dr. Shen's research focuses on mobility and resource management in interconnected wireless/wireline networks, UWB wireless communications systems, wireless security, and ad hoc and sensor networks. He is a coauthor of two books, and has published more than 200 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen was the Technical Program Co-Chair for IEEE Globecom '03 Symposium on Next Generation Networks and Internet, ISPAN '04, IEEE Broadnet '05, QShine '05, and is the Special Track Chair of 2005 IFIP Networking Conference. He serves as the Associate Editor for IEEE Transactions on Wireless Communications; IEEE Transactions on Vehicular Technology; ACM/Wireless Networks; Computer Networks; Wireless Communications and Mobile Computing (Wiley); and International Journal of Computers and Applications. He also serves as Guest Editor for IEEE JSAC, IEEE Transactions Vehicular Technology, IEEE Wireless Communications, and IEEE Communications Magazine. Dr. Shen received the Premiers Research Excellence Award (PREA) from the Province of Ontario, Canada for demonstrated excellence of scientific and academic contributions in 2003, and the Distinguished Performance Award from the Faculty of Engineering, University of Waterloo, for outstanding contribution in teaching, scholarship and service in 2002. Dr. Shen is a registered Professional Engineer of Ontario, Canada.

Minghui Shi received a B.S. degree in 1996 from Shanghai Jiao Tong University, China, and an M.S. degree in 2002 from the University of Waterloo, Ontario, Canada, both in electrical engineering. He is currently working toward a Ph.D. degree at the University of Waterloo. His current research interests include wireless LAN/cellular network integration and network security.