A self-encryption authentication protocol for teleconference services

Yixin Jiang and Chuang Lin

Department of Computer Science and Technology,
Tsinghua University,
Beijing, China
E-mail: yxjiang@csnet1.cs.tsinghua.edu.cn
E-mail: clin@csnet1.cs.tsinghua.edu.cn

Minghui Shi and Xuemin Sherman Shen*

Department of Electrical and Computer Engineering,
University of Waterloo,
Waterloo, Ontario, Canada
E-mail: mshi@bbcr.uwaterloo.ca
E-mail: xshen@bbcr.uwaterloo.ca
*Corresponding author

Abstract: A novel authentication protocol for teleconference service is proposed. The main features of the proposed protocol include identity anonymity, one-time Pseudonym Identity (PID) renewal and location intracability. Identity anonymity is achieved by concealing the real identity of a mobile conferee in a prearranged PID. One-time PID Renewal mechanism, in which the mobile conferee's PID is frequently updated communicating with the network centre, is introduced to offer location intracability. It is shown that the security has been significantly enhanced, while the computation complexity is similar to the existing ones appeared in the literature.

Keywords: authentication; teleconference services; protocol; anonymity.

Reference to this paper should be made as follows: Jiang, Y., Lin, C., Shi, M. and Shen, X.S. (2006) 'A self-encryption authentication protocol for teleconference services', *Int. J. Security and Networks*, Vol. 1, Nos. 3/4, pp.198–205.

Biographical notes: Yixin Jiang received his MS in Computer Science from Huazhong University of Science and Technology in 2002. He is currently pursing his PhD at the Department of Computer Science and Technology, Tsinghua University, Beijing, China. His current research interests include network security.

Chuang Lin is a Professor of Computer Science at the Tsinghua University, Beijing, China. He received his BS and PhD in Computer Science from Tsinghua University. Her current research focuses on performance evaluation, Petri nets, temporal logics and network security.

Minghui Shi received a BS in 1996 from Shanghai Jiao Tong University, China and an MS in 2002 from the University of Waterloo, Ontario, Canada, both in electrical engineering. He is currently working towards a PhD at the University of Waterloo. His current research interests include wireless LAN/cellular network integration and network security.

Xuemin Sherman Shen is a Professor of Electrical and Computer Engineering at the University of Waterloo, Ontario, Canada. He received his PhD in control from Rutgers University, USA. His research interests include wireless/internet interworking, radio resource and mobility management, voice over mobile IP, WLAN/WiMAX, WAP, UWB wireless communications, wireless ad hoc and sensor networks, wireless network security, stochastic process and optimal control and filtering.

1 Introduction

Mobile teleconference is a synchronous collaboration session, in which conferees at remote locations cooperate with an interactive procedure, for example, a board meeting, a task force or a scientific symposium through wireless communications. When a conference chair holds a mobile teleconference, all conferees are required to connect to a centre node, called a Network Center (NC), via wireless access network. The NC receives messages from conferees, processes them in an appropriate way and then sends the results to conferees.

Privacy is very important to mobile teleconference. A secure conference service protocol for digital mobile networks has proposed by Hwang and Yang (1995). The protocol can establish a session key for a valid user to hold a teleconference. A modified secure teleconference protocol, which allows an active participant to join or exit on-going conference, has been presented by Hwang (1999). Both user authentication and session key distribution are simultaneously included in the conference protocol. The session key distribution uses a public key cryptosystem to simplify the communication between conferees and NC. However, the conferee's mobile device is required to use two cryptosystems, which is not friendly to the low computation power requirement. A simplified mechanism, called self-encryption, was given by Hwang and Chang (2003), which not only decreases the computation complexity in Hwang (1999), but also retains simple communications for the secure teleconference service. The self-encryption mechanism uses the plaintext as a long-term secret key to encrypt the corresponding cipher-text. The long-term secret key $s_i = f(\mathrm{ID}_i)$ for its ith mobile user T_i is maintained by NC, where f is a secret one-way hash function and ID_i denotes the identity of the mobile user. The self-encryption mechanism operates as follows:

Step 1 A chairman T_1 initiates a conference and then:

1. chooses two random numbers r_{11} and r_{12}
2. uses the long-term secret key $s_1(= f(\mathrm{ID}_1))$ to encrypt $\{t_1 \| s_1 \| r_{11} \| r_{12} \| \mathrm{ID}_2 \| \ldots \| \mathrm{ID}_m\}$ and
3. sends message $\{\mathrm{ID}_1, E_{s_1}(t_1 \| s_1 \| r_{11} \| r_{12} \| \mathrm{ID}_2 \| \ldots \| \mathrm{ID}_m)\}$ to the trusted NC.

Here, ID_i $(i = 1, 2, \ldots, m)$ represents the conferees' identity, t_1 denotes the timestamp, and s_1 is generated by NC, such as $s_i = f(\mathrm{ID}_i)$, where f is a secret one-way function held by NC.

Step 2 On receiving message from T_1, NC decrypts the encrypted data by using the long-term secret key s_1, and then verifies whether s_1 is equal to $f(\mathrm{ID}_1)$ and the timestamp t_1 is within some reasonable range compared with its current time. If both are true, NC calls other mobile conferees $\mathrm{ID}_i (i = 2, 3, \ldots, m)$.

Step 3 Every participant T_i, for $i = 2, 3, \ldots, m$, does the same as chairman T_1 does, that is:

1. chooses two random numbers r_{i1} and r_{i2}
2. uses the long-term secret key $s_i(= f(\mathrm{ID}_i))$ to encrypt $(t_i \| s_i \| r_{i1} \| r_{i2})$ and
3. sends the message $\{\mathrm{ID}_i, E_{s_i}(t_i \| s_i \| r_{i1} \| r_{i2})\}$ to NC.

Step 4 When receiving the message from T_i, NC decrypts the encrypted data, then verifies the authenticity of s_i and the timestamp t_i. If both are true, NC selects two non-zero random numbers K_c and r_0 and calculates PI and PA by

$$\mathrm{PI} = K_c + \mathrm{lcm}(r_0, r_1, \ldots, r_m) \tag{1}$$

$$\mathrm{PA} = E_{K_c}(\mathrm{ID}_{\mathrm{NC}}) \tag{2}$$

where K_c denotes the session key of the conference and $\mathrm{lcm}\,(r_0, r_1, \ldots, r_m)$ denotes the least common multiple function. Finally, NC broadcasts tuple (Q, y, R, PA) to $T_i (i = 2, 3, \ldots, m)$. Here, Q, y and R are computed by $PI = Q2^y + R$.

Step 5 Each participant T_i obtains conference key K_C as

$$K_C = (Q2^y + R)\mathrm{mod}(r_i) \tag{3}$$

where the session key r_i is computed as $r_i = r_{i1} + r_{i2}$. They verify the validity of K_c by checking whether PA is equal to $E_{K_C}(\mathrm{ID}_{\mathrm{NC}})$.

Note that the self-encryption mechanism provides an implicit authentication (Steps 2 and 4). Once receiving message from T_i, NC decrypts the encrypted data by using the long-term secret key s_i. If the decrypted secret key s_i is equal to $f(\mathrm{ID}_i)$, the identity of conferee T_i is true.

However, the self-encryption mechanism cannot provide identity anonymity, and an intruder can easily obtain ID_i by intercepting the messages. If the secret one-way function f is spied, the intruder could compute all the long-term shared keys s_i and the cryptographic system would be promised. The disclosure of a user's identity will allow unauthorised entities to track his moving history and current location, which entails the violation of his privacy. Hence, the identity anonymity is one of the important factors that should be considered in mobile teleconference. On the other hand, the mechanism of issuing the session key to a new participant during a conference may cause that a participant who leaves right after the new participant joining the conference is still able to eavesdrop the conversation even when the session key is refreshed (Ng, 2001).

In this paper, we propose a simple authentication protocol with anonymity property for mobile teleconference services based on the *Secret Splitting* principle (Schneier, 1996). *Secret splitting* is a type of information-hidden technique, in which a message is divided into several components. The original message can be reconstructed if and only if the number of components gathered is equal or greater than the preset threshold. In the proposed protocol, the real identity of a mobile conferee is decomposed into a Pseudonym Identity (PID) used for transmission and a random number N, which is known by NC only, so that an intruder is unable to reconstruct the real identity from PID without the knowledge of N. In addition, to prevent the mobility of a particular mobile conferee from being traced, the PID is renewed frequently using proposed One-time PID Renewal mechanism. The conversation privacy is also guaranteed when participants join or leave the on-going teleconference meeting by properly renewing and re-distributing the conference session key.

The rest of this paper is organised as follows. In Section 2, the authentication protocol with anonymity for teleconference services is proposed. In Sections 3 and 4, the security and the performance analysis are presented, respectively, followed by the conclusion in Section 5.

2 The proposed authentication protocol with anonymity property

The proposed authentication protocol uses a simple secret splitting mechanism to provide the identity anonymity and prevent unauthorised entities from tracing a particular mobile user's roaming history and his current location. The security strength does not reply on the secrecy of the one-way function, so public one-way hash functions are used in the proposed protocol.

We still retain the self-encryption mechanism in the proposed scheme, that is, the NC also maintains a long-term secret key $s_i = f(\mathrm{ID}_i)$ for his conferee T_i by using a one-way function *f*. By extracting the real identity ID_i of user T_i from PID_i, we can further compute the shared key s_i, which is used to encrypt the exchanged messages. However, we provide identity anonymity mechanism by using a Pseudonym Identity PID_i for a mobile user T_i instead of his real identity ID_i. The Pseudonym Identity PID_i is prearranged and distributed by NC in advance. And the mobile user T_i stores PID_i, which is only known to NC and himself.

2.1 Mutual Authentication Protocol (MAP)

When a user T_i registers with NC, he submits his identity ID_i to NC, whose identity is $\mathrm{ID}_{\mathrm{NC}}$. NC generates an *m*-bits random number N_i and keeps it secret. In order to prevent the exclusive search attack, *m* should be sufficiently large, for example, 128 bits or longer. NC computes a Pseudonym Identity PID_i for T_i as:

$$\mathrm{PID}_i = h(N_i \,\|\, \mathrm{ID}_{\mathrm{NC}}) \oplus \mathrm{ID}_i \oplus \mathrm{ID}_{\mathrm{NC}} \tag{4}$$

where '⊕' denotes bitwise XOR operation and *h* is a public strong one-way hash function. Then, NC delivers PID_i to T_i through a secure channel and NC records the mapping relation of PID_i and $N_i(\mathrm{PID}_i \leftrightarrow N_i)$ in distributed database servers. By this secret-splitting mechanism, we can conceal the real identity ID_i in PID_i and provide identity anonymity for T_i while keeping the algorithm simple.

In the following, we describe the proposed authentication 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 (see Figure 1).

Step 1 The conference chairman T_1:

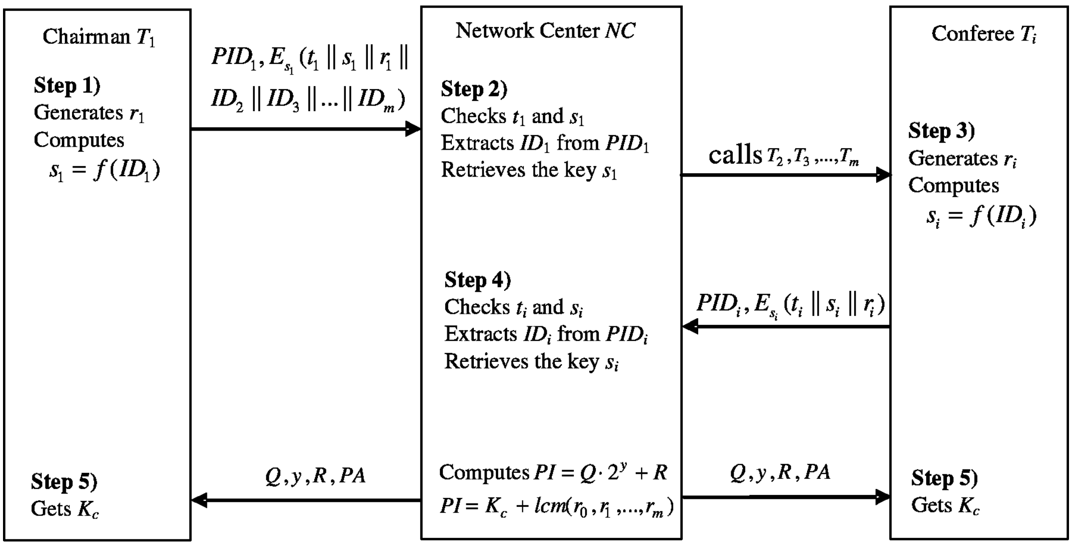
1. chooses a random number r_1
2. computes the long-term key s_1 by $s_1 = f(\mathrm{ID}_1)$
3. uses key s_1 to encrypt $(t_1 \| s_1 \| r_1 \| \mathrm{ID}_2 | \ldots \| \mathrm{ID}_m)$ and
4. sends message $\{\mathrm{PID}_1, E_{s_1}(t_1 \| s_1 \| r_1 \| \mathrm{ID}_2 \| \ldots \| \mathrm{ID}_m)\}$ to NC. Here, $\mathrm{PID}_i (i = 1,2,\ldots,m)$ represents the PID of T_i.

Step 2 On receiving the message from T_1, NC retrieves the corresponding N_1 of mobile conferee T_1 by searching the $\mathrm{PID}_i \leftrightarrow N_i$ mapping table. NC derives the real identity of mobile conferee T_1 by computing

$$\mathrm{ID}_1 = \mathrm{PID}_1 \oplus h\left(N_1 \,\|\, \mathrm{ID}_{\mathrm{NC}}\right) \oplus \mathrm{ID}_{\mathrm{NC}} \tag{5}$$

Hence, NC can retrieve corresponding shared key s_1 and decrypt $E_{s_1}(t_1 \| s_1 \| r_1 \| \mathrm{ID}_2 \| \ldots \| \mathrm{ID}_m)$. Then, NC verifies the authenticity of the secret key s_1 and the timestamp t_1. If both are true, NC calls the other mobile user $ID_i (i = 2,3,\ldots,m)$. Note that all of the shared keys $s_i (i = 1,2,\ldots,m)$ are precomputed by NC.

Figure 1 The proposed scheme with anonymity property for secure teleconference



Step 3 *The participant Ti, for i = 2, 3, …, m, does the same as chairman T1 in Step 1. Conferee Ti:*

1 chooses a random r_i

2 computes the long-term secret key s_i as $s_i = f(\mathrm{ID}_i)$

3 uses secret key s_i to encrypt $\{t_i \| s_i \| r_i\}$ and

4 sends the message $\{\mathrm{PID}_i, E_{s_i}(t_i \| s_i \| r_i)\}$ to NC.

Step 4 On receiving the message from T_i, NC retrieves the corresponding N_i of T_i by searching the $\mathrm{PID}_i \leftrightarrow N_i$ mapping table. NC extracts the identity ID_i of T_i by

$$\mathrm{ID}_i = \mathrm{PID}_i \oplus h\left(N_i \| \mathrm{ID}_{\mathrm{NC}}\right) \oplus \mathrm{ID}_{\mathrm{NC}} \tag{6}$$

Then, NC can retrieve corresponding shared key s_i and further decrypt $E_{s_i}(t_i \| s_i \| r_i)$.

Next, NC checks the authenticity of secret key s_i and timestamp t_i. If it is true, NC selects two non-zero random numbers K_c and r_0, and further calculates PI and PA by

$$\mathrm{PI} = K_c + \mathrm{lcm}\left(r_0, r_1, \ldots, r_m\right) \tag{7}$$

$$\mathrm{PA} = E_{K_C}\left(\mathrm{ID}_{\mathrm{NC}}\right) \tag{8}$$

where K_c is the session key and $\mathrm{lcm}\,(r_0, r_1, \ldots, r_m)$ denotes the least common multiple function. Finally, NC broadcasts tuple (Q, y, R, PA) to all $T_i (i = 2, 3, \ldots, m)$, where Q, y and R are computed by $\mathrm{PI} = Q2^y + R$ for saving transmission bandwidth.

Step 5 Each participant T_i obtains

$$K_C = (Q2^y + R) \bmod (r_i) \tag{9}$$

Then T_i verifies the validity of K_c by checking whether PA is equal to $E_{K_C}(\mathrm{ID}_{\mathrm{NC}})$.

2.2 Dynamic participant mechanism

To assure the freshness of session key K_c, when a participant wants to exit an in-process teleconference, NC must change the session key K_c and re-compute PI.

Member join: when a participant T_{m+1} joins a conference that is already in-process, the procedures of obtaining K_c for T_{m+1} are the same as in steps 3–5 except that NC sends Q, y and R to conferee T_{m+1}, where $\mathrm{PI} = K_c + r_{m+1} s_{m+1} = Q2^y + R.$

Member quit: when a participant T_j leaves a conference that is already in-process, the renewing procedures for session key K_c are described as follows.

Step 1 NC selects a new session key $K_C^{'}$ and further calculates PI′ and PA′ as follows

$$\mathrm{PA}' = E_{K_C'}\left(\mathrm{ID}_{\mathrm{NC}}\right) \tag{10}$$

$$\mathrm{PI}' = K_C' + \mathrm{lcm}\left(r_0', r_1', \ldots, r_{j-1}', r_{j+1}', \ldots, r_m'\right) \tag{11}$$

where $r_i' = r_i + t'$ and t′ denotes the current time. Then NC broadcasts four-tuple (t', Q', y', R') to T_i, where parameters Q', y', R' and PI′ satisfy the equation $\mathrm{PI}' = Q'2^{y'} + R'$.

Step 2 The remaining conferee $T_i (i \neq j)$ obtains the new session key by $K_C' = (Q'2^{y'} + R') \bmod (r_i + t')$ and verifies the authenticity of session key K_C' by checking whether PA′ is equal to $E_{K_C^{'}}\left(\mathrm{ID}_{\mathrm{NC}}\right)$

2.3 Pseudonym Identity Renewal Protocol

Though in previous MAP scheme we provide an identity anonymity mechanism by using a Pseudonym Identity PID_i for a mobile conferee T_i instead of his real identity ID_i, there are still some security issues to be consider. For example, even when the mobile conferee T_i never reveals his identity ID_i to parties other than NC, he does reveal his long-term Pseudonym Identity PID_i during mutual authentication in MAP. Therefore, illegal parties can still track a conferee's location by his long-term PID_i, although they have no way to extract the real identity ID_i.

The goal of Pseudonym Identity Renewal Protocol (PIRP) protocol is to renew a new PID for a mobile conferee. We introduce a new mechanism called 'One-time Pseudonym Identity Renewal'. This new feature allows mobile conferee to renew his PID frequently and reduces the risk that he uses a compromised PID to communicate with NC.

Suppose that a mobile conferee T_i is required to renew his Pseudonym Identity $\mathrm{PID}_{i,j-1}$ with NC for the *j*th time, he can obtain the new $\mathrm{PID}_{i,j}$ according to the steps shown in Figure 2.

Figure 2 The pseudonym identity renewal protocol

Msg 1: $T_i \rightarrow \mathrm{NC}: \mathrm{PID}_{i,j-1}, E_{K_C}(t_i \| \mathrm{ID}_i \| \mathrm{PID}_{i,j-1} \| r_{i,j})$

Msg 2: $T_i \leftarrow \mathrm{NC}: E_{K_C}(t_i \| \mathrm{PID}_{i,j-1} \| r_{i,j} \| r_{\mathrm{NC},j})$

Msg 3: $T_i \rightarrow \mathrm{NC}: E_{K_C}(\mathrm{PID}_{i,j})$.

As shown in Figure 2, the new Pseudonym Identity $\mathrm{PID}_{i,j}$ is calculated as follows.

$$\mathrm{PID}_{i,j} = \mathrm{PID}_{i,j-1} \oplus r_{i,j} \oplus r_{\mathrm{NC},j}, \quad j = 1, 2, \ldots, n \tag{12}$$

Evidently, it will vary in each pseudonym identity renewal because of the two random number $r_{i,j}$ and $r_{\mathrm{NC},j}$. Note that $\mathrm{PID}_{i,0}$ of mobile conferee T_i is set as the original Pseudonym Identity PID_i in MAP phase, that is, $\mathrm{PID}_{i,0} = \mathrm{PID}_i$.

In the following, we describe this sub-protocol according to the order of message exchanges in Figure 2.

Step 1 The conferee T_i does the following:

1 choose a new random number $r_{i,j}$

2. use the conferee key K_c generated in previous MAP protocol to encrypt text $\{t_i \| \mathrm{ID}_i \| \mathrm{PID}_{i,j-1} \| r_{i,j}\}$ and
3. send the message $\{\mathrm{PID}_{i,j-1}, E_{K_C}(t_i \| \mathrm{ID}_i \| \mathrm{PID}_{i,j-1} \| r_{i,j})\}$ to NC.

Step 2 On receiving the message 1 from T_i, NC uses the conference session key K_c to decrypt the message $E_{K_C}(t_i \| \mathrm{ID}_i \| \mathrm{PID}_{i,j-1} \| r_{i,j})$ and checks whether $\mathrm{PID}_{i,j-1}$ in $E_{K_C}(t_i \| \mathrm{ID}_i \| \mathrm{PID}_{i,j-1} \| r_{i,j})$ is the same as the $\mathrm{PID}_{i,j-1}$ reserved by NC in previous renewal session. If it is false, NC terminates the execution. Otherwise, the Pseudonym Identity $\mathrm{PID}_{i,j-1}$ of mobile conferee T_i is authenticated. Subsequently, NC does the following:

1. generate a random $r_{\mathrm{NC},j}$
2. set $\mathrm{PID}_{i,j} = \mathrm{PID}_{i,j-1} \oplus r_{i,j} \oplus r_{\mathrm{NC},j}$ as the new Pseudonym Identity and keeping it secretly and
3. send message $E_{K_C}(t_i \| \mathrm{PID}_{i,j-1} \| r_{i,j} \| r_{\mathrm{NC},j})$ back to conferee T_i.

Step 3 Conferee T_i decrypts $E_{K_C}(t_i \| \mathrm{PID}_{i,j-1} \| r_{i,j} \| r_{\mathrm{NC},j})$ with conference key K_c. If the decrypted random $\mathrm{r}_{i,j}$ in $E_{K_C}(t_i \| \mathrm{PID}_{i,j-1} \| r_{i,j} \| r_{\mathrm{NC},j})$ is equal to its original random $\mathrm{r}_{i,j}$, then T_i can compute the new Pseudonym Identity $\mathrm{PID}_{i,j}$ as $\mathrm{PID}_{i,j} = \mathrm{PID}_{i,j-1} \oplus r_{i,j} \oplus r_{\mathrm{NC},j}$. Then, conferee T_i sends $E_{K_C}(\mathrm{PID}_{i,j})$ to NC to verify the new $\mathrm{PID}_{i,j}$.

Step 4 If $D_{K_C}(E_{K_C}(\mathrm{PID}_{i,j})) = \mathrm{PID}_{i,j}$, then NC records the new $\mathrm{PID}_{i,j}$ for mobile conferee T_i. So far, NC has finished the authentication process with T_i and obtained a new $\mathrm{PID}_{i,j}$ for T_i.

Since the two random $r_{i,j}$ and $r_{\mathrm{NC},j}$ are generated by mobile conferee T_i and NC, respectively, $\mathrm{PID}_{i,j} = \mathrm{PID}_{i,j-1} \oplus r_{i,j} \oplus r_{\mathrm{NC},j}$ plays a role of one-time PID when T_i access NC. We call this new mechanism as 'One-time Pseudonym Identity Renewal'.

Next, we shall analyse the security of this protocol. The performance comparison between our protocol and the one in Hwang and Chang (2003) scheme will be described in the later section.

3 Security analysis

Generally, there are five basic security requirements for secure teleconference services (Hwang, 1999):

1. Privacy of participant's location information during the communication so that it is requisite to provide the identity anonymity and intracability mechanism.
2. Prevention of replay attacking, so that intruders are not able to obtain sensitive data by relaying a previously intercepted message.
3. Privacy of conference conversation content.
4. Prevention of fraud by ensuring that mobile conferees and NC are authentic, that is, there is a mutual authentication mechanism between NC and a mobile conferee.
5. Secure dynamic participation, so that any active participant can join or leave a teleconference while assuring the freshness of conference session key.

Next we analyse the security of our proposed protocol to see whether these security requirements have been satisfied.

3.1 Identity anonymity and intracability analysis

The security requirement for concealing participants' location information is achieved by introducing a simple identity anonymity mechanism. This feature makes an intruder unable to trace a particular mobile user's location by intercepting the conversation. Our scheme provides identity anonymity in all procedures by replacing conferees' real identity with a PID.

Case 1 In MAP phase, the real identity ID_i of T_i is replaced with $\mathrm{PID}_i (= h(N_i \| \mathrm{ID}_{\mathrm{NC}}) \oplus \mathrm{ID}_i \oplus \mathrm{ID}_{\mathrm{NC}})$. Since only NC knows the secret number N_i and $h(N_i \| \mathrm{ID}_{\mathrm{NC}})$, nobody except NC can obtain real ID_i from PID_i by computing $\mathrm{ID}_i = \mathrm{PID}_i \oplus h(N_i \| \mathrm{ID}_{\mathrm{NC}}) \oplus \mathrm{ID}_{\mathrm{NC}}$ and it is impossible for a tracker to extract the real identity ID_i from the transmitted messages and then trace the location of a mobile targeted user. Since each conferee's PID_i is computed using unique N_i, the legitimate conferee T_i cannot compute another conferee T_k's ID_k by intercepting PID_k and impersonate T_k.

Case 2 In PIRP phase, the identity anonymity is guaranteed by the similar mechanism. That is, the conferee T_i substitutes the Pseudonym Identity $\mathrm{PID}_{i,j}$ with his real identity ID_i, where the Pseudonym Identity $\mathrm{PID}_{i,j}$ is computed as $\mathrm{PID}_{i,j} = \mathrm{PID}_{i,j-1} \oplus r_{i,j} \oplus r_{\mathrm{NC},j}$.

The identity intracability is also assured. When a conferee T_i participates a teleconference, his Pseudonym Identity $\mathrm{PID}_{i,j} = \mathrm{PID}_{i,j-1} \oplus r_{i,j} \oplus r_{\mathrm{NC},j}$ will be renewed frequently because of the variance of random number $r_{i,j}$ and $r_{\mathrm{NC},j}$. The dynamics of random $r_{i,j}$ and $r_{\mathrm{NC},j}$ guarantees the freshness of the Pseudonym Identity $\mathrm{PID}_{i,j}$ in different session phases.

Although location-awareness services and applications will become more popular in the future; the importance of protecting information about participants' locations would not be decreasing, accordingly, especially considering such confidential applications in military environment. It seems that the identity anonymity may contradict with the location-awareness services and applications. Actually, by introducing some other mechanisms, such as the key escrow or recovery scheme (Abe and Kanda, 2002; Gonzáles Nieto et al., 2002), we can still provide the location-awareness services as well as safeguard the privacy of a participant's location information with the aid of identity anonymity mechanism.

3.2 *Prevention of relaying attacking*

A replaying attack is a method that an intruder stores 'stale' intercepted messages and retransmits them at a later time. An efficient measure against a replaying attack is to introduce timestamp t and lifetime L into the transmitted messages and set an expected legal time interval Δt for transmission delay.

All transmitted messages in each step of our scheme contain timestamps. According to the timestamp t and Δt, the receiver can efficiently verify the validity of these messages by checking if $t - t_i < \Delta t$ is true, where t_j is the timestamp of a message while t is current time when it is received. If this inequality holds, the message is valid. Otherwise, NC regards this message as a replaying message. By this mechanism, a replaying attack can be avoided.

3.3 *Privacy of conferee conversation content*

Evidently, the privacy of conferee conversation content in our scheme is guaranteed. Once the valid participants hold the session key K_c, the conversation of the conference content will be encrypted by K_c.

Hence, any intruder cannot know the conversation content without knowing the session key K_c. To obtain conference session key K_c, an intruder must first obtain the private random r_i and then use it to calculate K_c, as in Equation (9).

However, in our scheme, the random $r_i (i = 1,2,\ldots,m)$ is only generated secretly by conferee T_i. Nobody except T_i himself and NC knows the random r_i. Therefore, even though all of the messages $\{\mathrm{PID}_1, E_{s_1}(t_1 \| s_1 \| r_1 \| \mathrm{ID}_2 \| \ldots \| \mathrm{ID}_m)\}$ and $\{Q, y, R, \mathrm{PA}\}$ in Figure 1 can be intercepted, the intruder cannot obtain $r_i (i = 1,2,\ldots,m)$ and furthermore compute conferee session key $K_C = (Q2^y + R)\mathrm{mod}(r_i)$, since it is important for him to get the secret key $s_i (s_i = f(\mathrm{ID}_i))$ unless he knows the real identity ID_i of the conferee T_i. Hence, the intruder is prohibited from stealing the session key K_c and eavesdropping any communication content.

3.4 *Prevention of fraud*

In order to prevent fraud, the NC and conferees should be authenticated with each other. This requires that our scheme provide mutual authentication mechanism between NC and each conferee.

Firstly, assume that we consider the following impersonation attack scenarios in MAP protocol. This security requirement can be achieved by verifying the correctness of the conferee's identity ID_i and his secret key s_i.

Case 1 An intruder has no way to impersonate NC to cheat conferee T_i. Since the shared key s_i is only known to conferee T_i and NC, and an intruder cannot send conferee T_i the valid response $\{Q, y, R, \mathrm{PA}\}$, which is generated by NC. Once each participant T_i receives the message $\{Q, y, R, \mathrm{PA}\}$ in Figure 1, he can compute $K_C = (Q2^y + R)\mathrm{mod}(r_i)$ and then verifies the validity of K_c by checking whether PA is equal to $E_{K_C}(\mathrm{ID}_{\mathrm{NC}})$.

Case 2 An intruder cannot impersonate T_i to cheat NC since he cannot know the real identity of T_i. If the intruder uses a phony identity $\mathrm{ID}_i^{'}$, the corresponding spurious $\mathrm{PID}_i^{'}$ can be identified by NC, since NC can obtain the $\mathrm{ID}_i^{'}$ by computing $\mathrm{ID}_i^{'} = \mathrm{PID}_i^{'} \oplus h(N_i \| \mathrm{ID}_{\mathrm{NC}}) \oplus \mathrm{ID}_{\mathrm{NC}}$. And then NC can detect the spurious $\mathrm{ID}_i^{'}$. Given that ID_i is kept secretly in our protocol, nobody except T_i himself and NC can know his real identity.

Therefore, our MAP protocol can efficiently prevent an intruder from impersonating attacks because of the mandatory mutual authentication mechanism between mobile conferee T_i and NC.

Similarly, in PIRP protocol, the identities of conferees T_i and NC are also compulsorily authenticated each other. Suppose that we consider the following impersonation attack scenarios in this protocol.

Case 1 An intruder has no way to impersonate NC to cheat conferee T_i, since he does not possess the previous Pseudonym Identity $\mathrm{PID}_{i,j-1}$. Hence it is impossible for an intruder to send the authentic message $\{\mathrm{PID}_{i,j-1}, E_{K_C}(t_i \| \mathrm{ID}_i \| \mathrm{PID}_{i,j-1} \| r_{i,j})\}$ to NC.

Case 2 An intruder also has no way to impersonate conferee $T_i (i = 1,2,\ldots,m)$ to cheat NC. Since the shared conference session key K_c is unknown to anyone only except conferee $T_i (i = 1,2,\ldots,m)$ and NC, the intruder impossibly sends the authentic message $E_{K_C}(t_i \| \mathrm{PID}_{i,j-1} \| r_{i,j} \| r_{\mathrm{NC},j})$ to conferee T_i. Moreover, M is required to send back the message $E_{K_C}(\mathrm{PID}_{i,j})$ to NC for mutual implicit key authentication.

3.5 *Dynamic participant mechanism*

Our proposed protocol meets the requirement of secure dynamic participation, since the key distribution mechanism in our scheme can update the session key K_c

when a member joins or leaves the in-process conference. As described in Section 2, NC can assure the freshness of conference session key K_c by changing the session key K_c, re-computing PI, and then re-distributing the requisite updating messages to corresponding conferees.

4 Performance analysis

The portable devices usually have low power and computation capacity, so it is impractical to implement certain complex cryptography algorithms which require high computation complexity in portable devices. There are two performance factors to be considered in wireless environment. Firstly, the low computational power of mobile devices should be a concern, which means a security protocol requiring heavy computation on the mobile device is not feasible (Ng and Mitchell, 2004; Shim, 2003; Wong and Chan, 2001). 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 minimise the message size and the number of message exchanges.

The performance comparison between our protocol and the one in Hwang and Chang (2003) scheme is shown in Table 1. We mainly compare the number of hash operations, exponentiation operations, symmetric encryption/decryption operations and the number of transmissions (message exchanges) in the two protocols.

Table 1 Performance comparison

Comparison item		*Hwang and Chang protocol*	*Our protocol*
Exponential operation	T	1 (step 5)	1 (step 5)
	NC	1 (step 4)	1 (step 4)
Hash operation	T	N/A	1 (step 1)
	NC	N/A	N/A
Symmetric encryption	T	1 (step 1 or 5)	1 (steps 1 or 5)
	NC	N/A	N/A
Symmetric decryption	T	N/A	N/A
	NC	m (steps 2 and 5)	m (steps 2 and 5)
Transmission messages	T ↔ NC	2 + 3(m − 1)	2 + 3(m − 1)
Identity anonymity		N/A	Yes
Location intracability		N/A	Yes

Note that the rows in shadow show the differences between them. Though one Hash operation (computing the long-term shared secret key s_i) is added in our scheme, we obtain the following extra security features:

1. The identity anonymity and intracability mechanism are offered so that it is difficult for an intruder to trace the location of a target conferee.
2. The one-way hash function f can be public in our scheme.
3. The security when a participant joins an in-process teleconference is further strengthened.

5 Conclusion and future work

In this paper, we propose a novel authentication protocol with anonymity property for teleconference services to resolve the security issues in previous teleconference protocols. Two new mechanisms are introduced in our protocols: identity anonymity and one-time pseudonym identity renewal. For offering anonymity, we conceal the real identity of a mobile conferee in a prearranged PID by utilising the secret-splitting principle. In order to provide location intracability, one-time pseudonym identity renewal mechanism is introduced. We utilise iterative algorithm to update PID frequently and thus reduce the risk that a conferee uses a compromised PID to communicate with NC.

The performance comparisons show that though we achieve such new security features, the complexity of our protocols is similar to the one in the literature and the computation requirement for mobile device is quite low.

Acknowledgement

This relative work was supported in part by the NSFC of China under contracts No.90104002, 60273009, 60373013, 60372019 and 60218003; the Projects of Development Plan of the State High Technology Research under contract No. 2003CB314804 and Intel IXA University Research Plan.

References

Abe, M. and Kanda, M. (2002) 'A key escrow scheme with time-limited monitoring for one-way communication', *The Computer Journal*, Vol. 45, No. 6, pp.661–671.

Gonzáles Nieto, J.M., Viswanathan, K., Boyd, C., Clark, A. and Dawson, E. (2002) 'Key recovery for the commercial environment', *International Journal of Information Security*, Vol. 1, No. 3, pp.161–174.

Hwang, K.F. and Chang, C.C. (2003) 'A self-encryption mechanism for authentication of roaming and teleconference services', *IEEE Transactions on Wireless Communications*, Vol. 2, pp.400–407.

Hwang, M.S. (1999) 'Dynamic participation in a secure conference scheme for mobile communications', *IEEE Transactions on Vehicular Technology*, Vol. 48, pp.1469–1474.

Hwang, M.S. and Yang, W.P. (1995) 'Conference key distribution schemes for secure digital mobile communications', *IEEE Journal on Selected Areas in Communications*, Vol. 13, pp.416–420.

Ng, S.L. (2001) 'Comments on "Dynamic participation in a secure conference scheme for mobile communications"', *IEEE Transactions on Vehicular Technology*, Vol. 50, pp.334–335.

Ng, S.L. and Mitchell, C. (2004) 'Comments on mutual authentication and key exchange protocols for low power wireless communications', *IEEE Communications Letters*, Vol. 8, pp.262–263.

Schneier, B. (1996) *Applied Cryptography: Protocols, Algorithm, and Source Code C*, 2nd edition, John Wiely & Sons, Inc., pp.70–72.

Shim, K. (2003) 'Cryptanalysis of mutual authentication and key exchange for low power wireless communications', *IEEE Communications Letters*, Vol. 7, pp.248–250.

Wong, D.S. and Chan, A.H. (2001) 'Mutual authentication and key exchange for low power wireless communications', *Proceedings of IEEE Military Communications Conference, MILCOM 2001*, Vol. 1, pp.39–43.