A Self-Encryption Mechanism for Authentication of Roaming and Teleconference Services

Kuo-Feng Hwang and Chin-Chen Chang, *Fellow, IEEE*

***Abstract*—In this paper, a simple authentication technique for use in the global mobility network (GLOMONET) is proposed. This technique is based on the concept of distributed security management, i.e., the original security manager administrates the original authentication key (long-term secret key) acquired when a user makes contract with his home network, while a temporary security manager is generated for a roaming user in the visited network that provides roaming services. 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. In the proposed authentication protocol for the regular communication phase, the procedures of the original security manager and the temporary security manager are the same except for introducing different parameters. Furthermore, the proposed technique not only reduces the number of transmissions during the authentication phase, but it also can decrease the complexity of mobile equipment. The idea behind the proposed technique is to introduce a simple mechanism which is called "self-encryption." In this paper, we also suggest that this mechanism can be easily adopted as the authentication function for the secure teleconference service.**

***Index Terms*—Authentication, global mobility network, roaming, secure teleconference, symmetric cryptosystem.**

I. Introducion

THE use of personal communication systems (PCS), e.g., cellular phones, has been growing rapidly around the world. The mobility network provides service for a user to communicate with other users by moving inside and around networks. In other words, the user has the capability of mobility. Here, "user" is a general term representing a human being, a terminal, a mobile equipment, and so on. There are many mobility networks that have been developed, e.g., GSM, USDC, and PDC [1]. In particular, the GSM system has been implemented in more than 70 countries around the world. Furthermore, Suzuki and Nakada [1] pointed out that there were many intelligent network based systems that had also been rapidly developing in order to provide more effective personal communication services, e.g., the universal personal telecommunication (UPT) and the future public land mobile telecommunication systems (FPLMTS). Suzuki and Nakada referred the mobility network that has the capability of global mobility as global mobility network (GLOMONET).

A. Roaming Service

In GLOMONET, the malicious intruder has a greater possibility of obtaining a valid user's personal assets. Therefore, security management among plural networks is important for providing global mobility service to a valid user. In 1997, Suzuki and Nakada [1] developed an authentication scheme for the roaming service used in GLOMONET. Roaming service provides for the global mobility of a valid user between the contracted network (home network) and the roamed network (visited network). There are many mechanisms [2] that can be applied here for authenticating the validity of a user such as one-way authentication using a password, synchronized data, or public-key cryptosystems [3]. Suzuki and Nakada used a challenge/response interactive authentication mechanism with a symmetric cryptosystem to construct their authentication protocol.

The visitor location register (VLR) network architecture has been adopted in existing digital cellular systems for the roaming environment. In the VLR system, the authentication data travels among the home network, the visited network, and the user's terminal. Once the roaming service is successfully set up, the authentication data travel only between the visited network and the user's mobile equipment. Suzuki and Nakada also adopted this concept in their scheme, however, in the GSM authentication technique [4], the user authentication key is concealed from the visited network by sending only several RAND (challenge)/SRES (response) pairs to the visited network. This scheme increases the number of network signals. Suzuki and Nakada [1] argued that it is beneficial when users do not move around the networks frequently. In addition, because the authentication key or data is generated in the home network and is used in the visited network without being modified, the security responsibility allocation between the visited network and the home network is unclear if there is an illegal event discovered in the visited network. To overcome the problems in the GSM authentication scheme, Suzuki and Nakada [1] proposed an authentication management architecture based on distributed security management and a concrete authentication technique. Unfortunately, Buttyan *et al.* [5] pointed out that there are several security weaknesses in Suzuki and Nakada's scheme. They further proposed a modified scheme to avoid these weaknesses.

Manuscript received January 31, 2002; revised August 26, 2002; accepted September 3, 2002. The editor coordinating the review of this paper and approving it for publication is W. W. Lu.

K.-F. Hwang is with the Department of Multimedia Design, National Taichung Institute of Technology, Taichung 404, Taiwan R.O.C. (e-mail: kfhwang@ieee.org).

C.-C. Chang is with the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 621, Taiwan R.O.C. (e-mail: ccc@cs.ccu.edu.tw).

Digital Object Identifier 10.1109/TWC.2003.809452

B. Secure Teleconference Service

In 1995, Hwang and Yang [3] proposed a new service for mobility networks, called secure teleconference service. This service enables two or more users to hold a secure teleconference in the mobility network. In this service, privacy and authentication are two basic requirements. The idea behind Hwang and Yang's scheme is to establish a common secret key for the valid conferee to hold a secure teleconference. In 1999, Hwang [6] further proposed a modified secure conference scheme that allowed the active participant to join or to exit an in-progress conference. Both user authentication and session key distribution are simultaneously included in Hwang's conference key distribution protocol. Hwang used a public-key cryptosystem to simplify the transmission between the conferee and the network center.

C. Goals and Organization

When the mobility network becomes more popular, more applications and services are provided such as wireless application protocol (WAP) related services [7], secure teleconference [3], location-aware applications [8]–[10], and so on. The more services that are provided, the more complex the mobile equipment required. Clearly, the more complex the mobile equipment, the more difficult it is to implement and, therefore, the cost will increase. Consequently, how to reduce the complexity of the mobile equipment without losing these services is another important issue in the GLOMONET.

In this paper, we propose a simple mechanism called "self-encryption" that is used for authentication in the roaming environment. In the proposed authentication protocol, not only can the number of transmissions be reduced, but also mobile equipment is easier to implement. Furthermore, we also adopt the "self-encryption" mechanism into Hwang's conference key distribution protocol in order to simplify the complexity of mobile equipment. At the same time, the transmission between the conferee and the network center remains simple.

The rest of this paper is organized as follows. Buttyan *et al.* authentication protocol and Hwang's conference key distribution protocol will be reviewed in Section II. In Section III, we propose an authentication technique which introduces the self-encryption mechanism for the roaming environment. In addition, the security analysis and the comparisons of the proposed scheme are described in this section. Section IV presents the idea that the self-encryption mechanism can be easily applied to the conference key distribution protocol. Finally, Section V states the conclusions of our work.

II. Previous Work

In this section, we will review two techniques that are related to authentication in the mobility network. In the first subsection, we review Buttyan *et al.* protocol for the roaming service. Then, Hwang's key distribution technique for the secure teleconference service will be introduced in the second section.

A. Buttyan et al. Protocol

In 2000, Buttyan *et al.* [5] pointed out that Suzuki and Nakada's [1] authentication protocol has some security weaknesses. The first weakness is the fact that an intruder has the capability to obtain the authentication key of a legal user. The second weakness enables an intruder to impersonate visited network V to cheat a legal user. Buttyan *et al.* also proposed a simplified protocol to prevent these weaknesses. In the modified authentication technique, Buttyan *et al.* assume that the home network H is trusted and, therefore, H can know the authentication key $K_{\rm auth}$. Fig. 1 shows the procedure of Buttyan *et al.* scheme which is used to authenticate the validity of a roaming user U_i, as well as to establish an authentication key $K_{\rm auth}$ for a valid user. We briefly describe the protocol as follows.

Let $K_{\rm uh}$ denote the long-term secret key belonging to a user U_i and its home network H, and $K_{\rm vh}$ denote the long-term secret key belonging to a visited network V and a user's home network H.

Step 1) U_i generates a random integer r_0 and sends it to V.
Step 2) V generates a random integer r_1 and sends it to H.
Step 3) H generates a random integer r_2 and sends $\{E_{K_{\rm vh}}(r_1), r_2\}$ to V.
Step 4) V computes $\hat{r_1} = D_{K_{\rm vh}}(E_{K_{\rm vh}}(r_1))$. If $\hat{r_1}$ equals r_1, then V sends $E_{K_{\rm vh}}(r_2, {\rm ID}_i, K_{\rm auth}, r_0)$ to H.
Step 5) If the decrypted r_2 is correct, then H computes $E_{K_{\rm uh}}(V, K_{\rm auth}, r_0)$ and sends it to V.
Step 6) V generates another random integer r_3, and then V sends r_3 to U_i, as well as passes $E_{K_{\rm uh}}(V, K_{\rm auth}, r_0)$ to U_i.
Step 7) U_i checks the correctness of the decrypted r_0 and obtains the authentication key $K_{\rm auth}$. If the decrypted r_0 is correct, then V sends $E_{K_{\rm auth}}(r_3)$ to V.
Step 8) V decrypts $E_{K_{\rm auth}}(r_3)$ and checks the correctness of r_3. If r_3 is correct, then V sends $E_{K_{\rm auth}}(E_{K_{\rm auth}}(r_3))$ to U_i.
Step 9) Finally, U_i checks weather or not the decrypted $E_{K_{\rm auth}}(E_{K_{\rm auth}}(r_3))$ is equal to $E_{K_{\rm auth}}(r_3)$. If so, the authentication protocol is completed.

Here, $E_{K_c}(X) = Y$ represents a symmetric cryptosystem with a secret key K_c to encrypt a plaintext X as a cipher-text Y, and $D_{K_c}(Y)$ denotes using the same symmetric cryptosystem used in the encryption with the secret key K_c to decrypt Y.

Obviously, Buttyan *et al.* authentication protocol requires two rounds of transmissions between U_i and V, as well as between V and H. In Section III, we propose a simpler protocol for the roaming service. In particular, the proposed protocol is not only usable in the roaming environment, but also workable in regular communication. In other words, only one mechanism is needed and, therefore, the complexity of mobile equipment can be simplified.

B. Hwang's Conference Key Distribution Protocol

In 1995, Hwang and Yang [3] proposed a new secure conference service for digital mobile networks. Their scheme establishes a common secret key for the valid conferee to hold a teleconference. In 1999, Hwang [6] further proposed a modified secure teleconference scheme, which allows the active participant to join or to exit an in-progress conference. In particular, both user authentication, as well as session key distribution are simultaneously included in Hwang's conference key distribu-

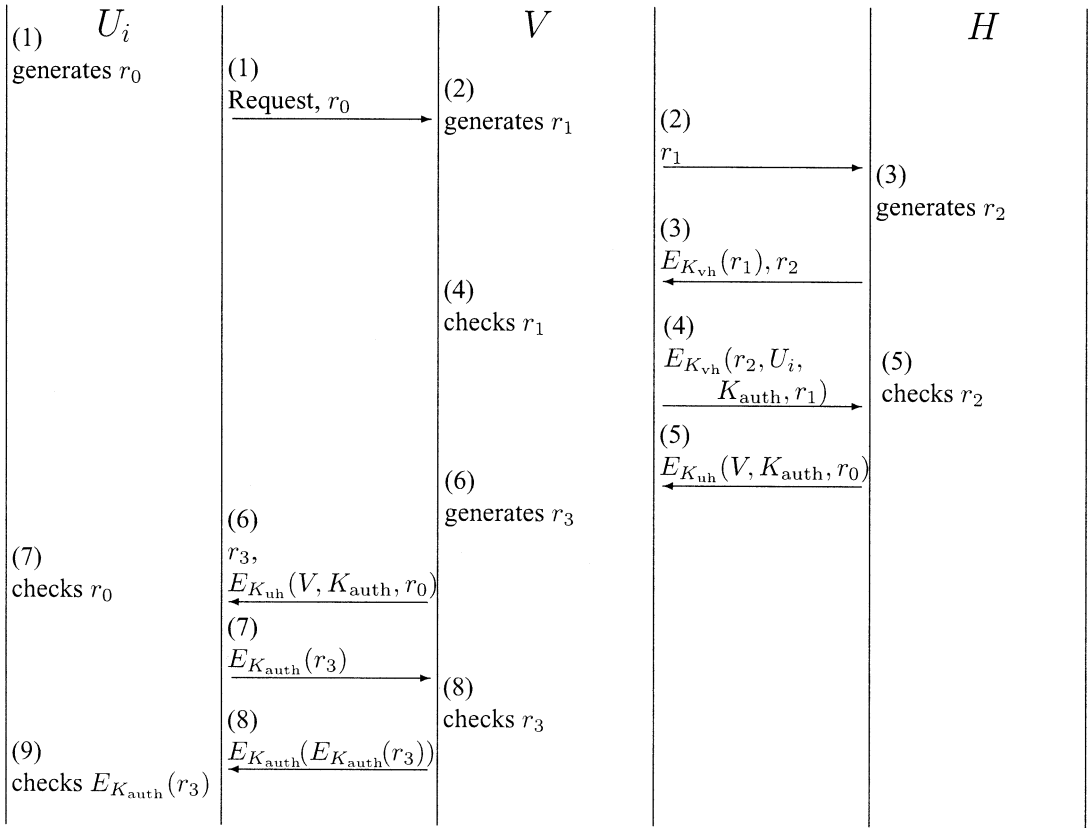

Fig. 1. Buttyan *et al.* authentication protocol.

tion protocol. Next, we review Hwang's scheme in the following (refer to Fig. 2).

Step 1) The initial conference participant, say T_1, selects two random numbers r_{11} and r_{12}. Note that for an authorized participant T_i, the session key-decryption key r_i is formed by $r_{i1} + r_{i2}$.

Step 2) U_1 sends $(t_1||s_1||r_{11}||r_{12}||\mathrm{ID}_i$, for $i = 1, 2, \ldots, m)^e \bmod n$ to the trusted network center (NC). Here, t_1 denotes the current date and time (timestamp), s_1 denotes T_1's authentication key which is generated by NC, such as $s_i = f(\mathrm{ID}_i)$, where f is a secret one-way function held by NC. Moreover, NCs public key is denoted as e, and ID_i, $i = 1, 2, \ldots, m$, represents the identity of users who are invited to join the conference.

Step 3) NC decrypts the encrypted data using its private key d, and then verifies whether s_1 is equal to $f(\mathrm{ID}_1)$ and the validity of t_1. Then, NC calls the other mobile terminals' ID_i's, $i = 2, 3, \ldots, m$.

Step 4) Each participant T_i, for $i = 2, \ldots, m$, selects two random numbers r_{i1} and r_{i2}. Afterward, the session key-decryption key r_i is obtained by $r_{i1} + r_{i2}$.

Step 5) T_i sends $(t_i||s_i||r_{i1}||r_{i2}||\mathrm{ID}_i)^e \bmod n$ to NC, for $i = 2, 3, \ldots, m$.

Step 6) NC decrypts the encrypted data and then verifies whether s_i is equal to $f(\mathrm{ID}_i)$ and the validity of timestamp t_i.

Step 7) NC selects two nonzero random numbers K_c and r_0. Here, K_c denotes the session key of the secret conference. Next, NC calculates $PI = K_c + lcm(r_0, r_1, \ldots, r_m)$ and $PA = E_{K_c}(\mathrm{ID_{NC}})$. Here, $lcm()$ denotes the least common multiple function.

Step 8) NC broadcasts Q, y, R, and PA to T_i, $i = 1, 2, \ldots, m$. Here, Q, y, and R are computed by the equation $PI = Q \cdot 2^y + R$.

Step 9) Each participant T_i obtains $K_c = (Q \cdot 2^y + R) \bmod r_i$, and then verifies the validity of K_c by checking whether PA is equal to $E_{K_c}(\mathrm{ID_{NC}})$.

When a participant wants to exit an in-progress teleconference, NC has to change the session key K_c and recompute PI. All of the participants do not need to alter their session key-decryption key r_i. We review the dynamic participation mechanism as follows.

Case 1) When a participant T_{m+1} wants to join an in-progress teleconference, the procedures are the same as Steps 4–9 for T_{m+1} to obtain K_c. But NC only sends Q, y, R to T_{m+1}, where $PI = K_c + r_{m+1} = Q \cdot 2^y + R$.

Case 2) When a participant T_j wants to exit a teleconference, the procedures are described as follows.

Step 1) NC selects a new session key K'_C, and then NC computes $PI' = K'_c + lcm(r'_i i = 0, 1, \cdots, i \neq j, \cdots, m)$, where $r'_i = r_i + t'$ and t' denotes the current date and time. Afterwards, NC broadcasts (t', Q', y', R'),

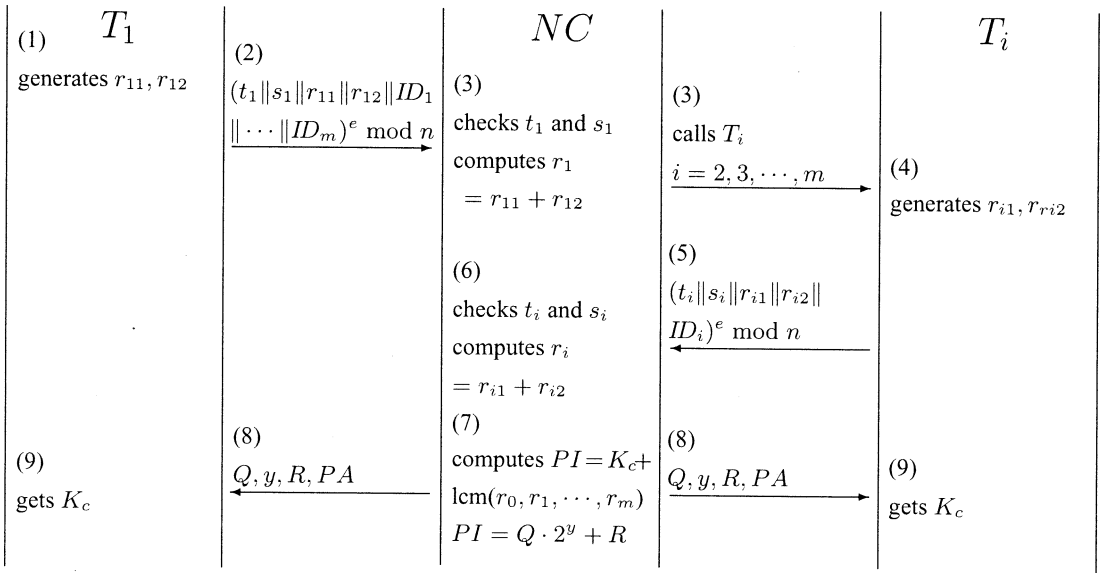

Fig. 2. Hwang's conference key distribution protocol.

where Q', y', and R' are obtained by $PI' = Q' \cdot 2^{y'} + R'$.

Step 2) The participant T_i, $i \neq j$, can obtain the new session key by $K_c' = Q' \cdot 2^{y'} + R' (\text{mod } r_i + t')$.

In 2001, Ng [11] pointed out that there is a weakness in Hwang's conference key distribution protocol in the above mentioned Case 1. Ng also suggested that NC must recompute $PI = K_c + r_{m+1} \cdot k$ rather than $PI = K_c + r_{m+1}$ for T_{m+1} in order to protect r_{m+1} from an eavesdropping attack. Here, k represents a random number.

Hwang's conference key distribution protocol uses a public key cryptosystem to simplify the communication between T_i and NC. Hwang has analyzed that the computation complexity of his method is acceptable even though there are exponential computations. However, two cryptosystems are needed in the mobile equipment. In Section IV, we will propose a symmetric cryptosystem based protocol, which not only simplifies the complexity of mobile equipment, but also retains simple communication for the secure teleconference service.

III. Proposed Protocol for Roaming Service

In Buttyan *et al.* protocol, two rounds of transmissions are needed between the user and the visited network, as well as between the visited network and the home network. Here, we propose a simpler protocol in order to reduce the number of transmission rounds. In particular, the proposed protocol is not only usable in the roaming environment, but also workable in regular communication. In other words, only one mechanism is needed and, therefore, the complexity of mobile equipment can be simplified. The idea behind the proposed scheme is quite simple. The plaintext involves a secret key, which is used to encrypt the corresponding ciphertext. This mechanism is called "self-encryption." We use this simple mechanism to accomplish our goal of simplifying the authentication protocol. At the end of this section, we will analyze the security of the proposed scheme and compare it to Buttyan's method.

A. Proposed Authentication Protocol

In the roaming environment, the visited network authenticates a roaming user through the user's home network. After certification, an authentication key is established between the roaming user and the visited network. In later communication, the visited network directly authenticates the user using the authentication key rather than authenticating it through the user's home network. In the proposed protocol, the home network maintains a long-term secret key for his client using a secret one-way function $f()$, such as $K_{\text{uh}} = f(U_i)$, where U_i denotes the user's identity. Besides, without loss of generality, K_{vh} denotes the long-term secret key belonging to the visited network and the home network. Note that K_{vh} is acquired when the visited network makes contract with the home network. We describe the proposed authentication protocol for the roaming service as follows (refer to Fig. 3).

Step 1) First, the roaming user U_i generates a random number r_0, and then sends his request with $E_{K_{\text{uh}}}(K_{\text{uh}} \| r_0)$ to the visited network V. Here, " $\|$ " denotes the concatenation, and it further implies that if the correct key K_{uh} is used to decrypt $E_{K_{\text{uh}}}(K_{\text{uh}} \| r_0)$, both the correct K_{uh} and r_0 will be obtained simultaneously, and vice versa.

Step 2) After V receives the request, he discovers that because U_i's home network is H rather than his own network, V has to obtain a certification from H to authenticate the validity of U_i. Subsequently, V sends $E_{K_{\text{vh}}}(U_I \| r_1 \| t)$ and passes $E_{K_{\text{uh}}}(K_{\text{uh}} \| r_0)$ to H for authentication, where r_1 is a random number chosen by V and t is the current date and time.

Step 3) H decrypts $E_{K_{\text{vh}}}(U_i \| r_1 \| t)$ using K_{vh}. If the timestamp t is reasonable, then H calculates U_i's long-term secret key K_{uh} by $K_{\text{uh}} = f(U_i)$. Afterwards, H uses K_{uh} to decrypt $E_{K_{\text{uh}}}(K_{\text{uh}} \| r_0)$. If the decrypted secret key, say K_{uh}, and $f(U_i)$ are the same, then the validity of U_i is certified; and furthermore, it implies that the validity of V is

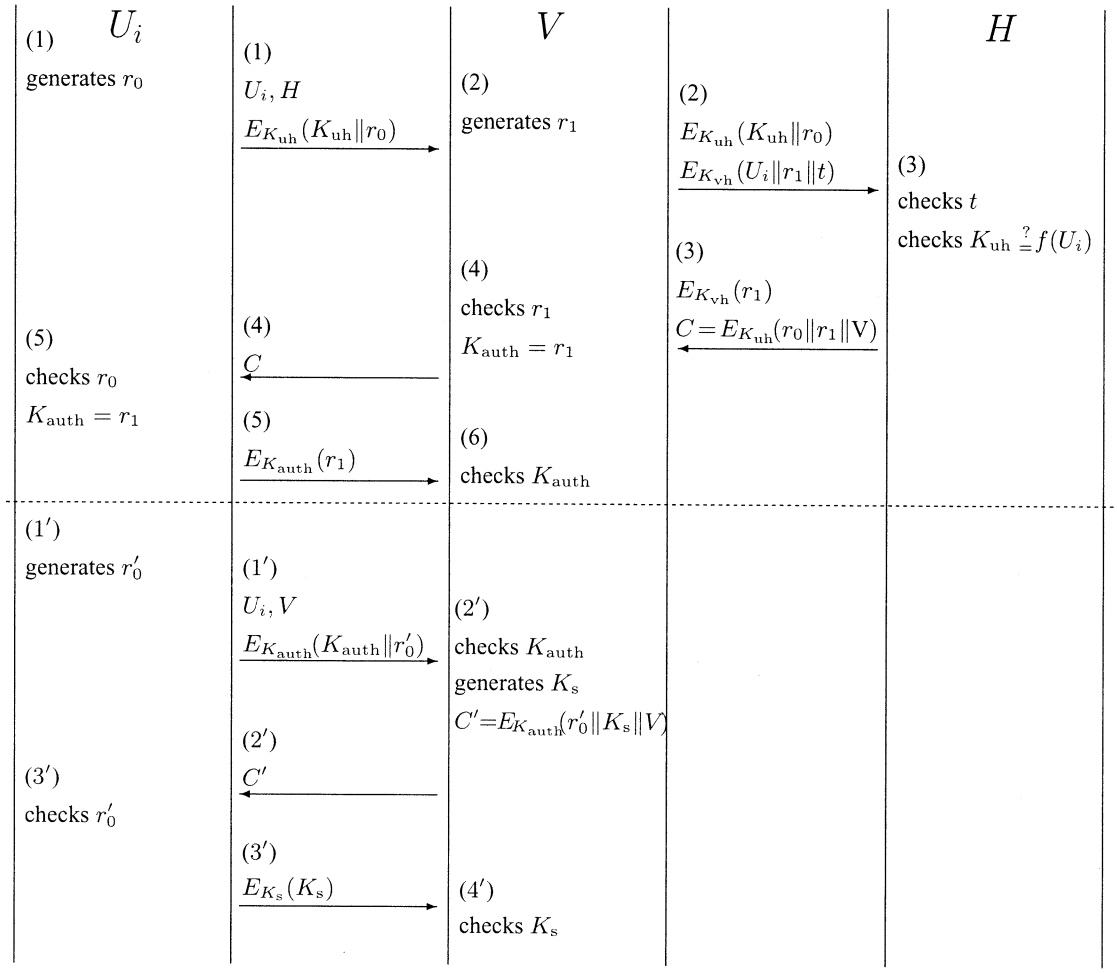

Fig. 3. Proposed authentication protocol for roaming service.

verified too. Subsequently, H sends $E_{K_{\rm vh}}(r_1)$ and $C = E_{K_{\rm uh}}(r_0\|r_1\|V)$ to V.

Step 4) If $D_{K_{\rm vh}}(E_{K_{\rm vh}}(r_1))$ equals r_1, then V believes that U_i is an authorized user. Otherwise, V rejects U_i's request. Subsequently, V sets r_1 as the authentication key $K_{\rm auth}$ and passes C to U_i.

Step 5) Upon U_i's receipt of C, U_i decrypts it using $K_{\rm uh}$. If the decrypted random number, say $\hat{r_0'}$, is the same as the original generated one, U_i certainly obtains the correct authentication key $K_{\rm auth} = r_1$. Afterwards, U_i sends $E_{K_{\rm auth}}(r_1)$ to V to confirm that U_i has received $K_{\rm auth}$.

Step 6) If the decrypted $E_{K_{\rm auth}}(r_1)$ equals $K_{\rm auth}$, then V records the authentication key $K_{\rm auth}$ for U_i.

The upper portion of Fig. 3 illustrates the proposed authentication protocol for the roaming environment while the lower portion of Fig. 3 demonstrates the establishment of the session key for regular communication. Note that if U_i stays in the service area of his home network H, the session key establishment protocol for regular communication is the same as the above mentioned one. That is H instead of V in the lower potion of Fig. 3 and the authentication key will be $K_{\rm uh}$ rather than $K_{\rm auth}$. Consequently, the mechanism in the mobile equipment for regular communication is the same as that for the roaming service except for the introduction of the different parameters according to the specific environment. In other words, the complexity of the mobile equipment can be progressively simplified. In particular, the proposed protocol has reduced the number of transmission rounds between the members which meets our expectations.

Next, we analyze the security of the proposed protocol, and then, the comparisons between Buttyan's scheme and ours are described at the end of this section.

B. Security Analysis

The user's long-term secret key $K_{\rm uh}$ is used for authentication to his home network. We assume that $K_{\rm uh}$ has been kept secretly meaning that an intruder cannot obtain $K_{\rm uh}$. Moreover, the long-term secret key $K_{\rm vh}$ held by the visited network and the home network also cannot be obtained by an intruder. We also assume that the pseudo-random number generator, which is used to generate a random number is secure. According to the above assumptions, we analyze the security of the following two aspects of the proposed scheme against replaying attacks and impersonating attacks. The first attack involves the case in which if an intruder illegally becomes a legitimate user while the second one involves an intruder impersonating V or H.

Replaying Attacks: An intruder plans to impersonate a legal user and to obtain the authentication key by replaying the user's

transmitting contents in the roaming environment. That is, the intruder intercepts the transmitted messages between a legal user U_i and his visited network V. Afterwards, the intruder replays U_i's request, as well as $E_{K_{\rm uh}}(K_{\rm uh}||r_0)$ to V (Step 1) to steal an authentication key. Note that the authentication key has been randomly changed from r_1 to $\tilde{r_1}$. Although he can successfully obtain $\tilde{C}$ from V (Step 4), which contains the authentication key $\tilde{r_1}$, he still cannot get the authentication key because he does not possess $K_{\rm uh}$ to decrypt $\tilde{C}$. Of course, he does not have the capability to confirm V by sending $E_{K_{\rm auth}}(\tilde{r_1})$ and, therefore, V will drop his request. Notice that even if the intruder is a legitimate user, he still cannot perpetrate the above mentioned attack because he does not possess the other legitimate user's long-term secret key. From the above analysis, one sees that the proposed protocol is secure against replaying attacks.

Impersonating Attacks: An intruder can impersonate the visited network V to the roaming user U_i, which results in U_i being cheated. Although this attack seems to be impossible, Buttyan *et al.* [5] argued that it can be achieved using a device called "IMSI catchers." In the following, we show that our scheme has the capability to resist this attack. The intruder first intercepts the messages from Steps 2 and 3 to obtain $E_{K_{\rm vh}}(U_i||r_1||t)$ and $C = E_{K_{\rm uh}}(r_0||r_1||V)$. Afterwards, he cuts off the communication between V and H, as well as between V and U_i. When he receives the request, as well as $E_{K_{\rm uh}}(K_{\rm uh}||r_0')$ from U_i, the intruder replays C to U_i to cheat him. However, the random number r_0' is different from that within C and, therefore, U_i will discover this fault and drop his request. The other way to cheat U_i is when the intruder passes $E_{K_{\rm uh}}(K_{\rm uh}||r_0')$ and $E_{K_{\rm vh}}(U_i||r_1||t)$ to H to obtain $\hat{C}$ which will contain the correct r_0'. However, H will discover that the timestamp t is out of the expected legal time interval and, therefore, his request will be dropped. Regarding the problem of synchronizing clocks in computer communications, the solution can be found in [12] an d[13].

There is a possible method that enables a legitimate user to impersonate the visited network, i.e., a legitimate user uses his long-term secret key $K_{\rm uh}$ to pretend to be a valid visited network. However, the home network can easily discover that $K_{\rm uh}$ does not belong to a valid visited network because only his client's long-term secret key is maintained by a secret one-way function. Consequently, the home network will reject the authentication service requested by a client. In other words, a legitimate user cannot successfully impersonate a visited network in the proposed protocol.

An intruder has no way to impersonate H in the proposed protocol, because he does not possess the long-term secret key $K_{\rm vh}$ and, therefore, he cannot generate the confirmation $E_{K_{\rm vh}}(r_1)$ to V (Step 3). Also, we will prove that V also has no way to impersonate H to cheat U_i. Since V does not possess the long-term secret key $K_{\rm uh}$, he cannot generate the correct C which contains the random number r_0 chosen by U_i. Thus, V also cannot impersonate H in the proposed protocol, even though V impersonating H is an unreasonable attack.

C. Comparisons

The comparisons between our proposed protocol and Buttyan *et al.* protocol are listed in Table I. The first item in the comparison is the number of the transmissions. This represents how many times messages must be transmitted between U_i and V, as well as between V and H in order to authenticate the validity of U_i and to establish an authentication key for U_i if he has been certified. Our method requires three transmissions between U_i and V, and only requires two transmissions between V and H. Obviously, these numbers are less than that of Buttyan *et al.* method. Consequently, our method can reduce the requirement of the channel capacities in the roaming environment.

TABLE I
COMPARISONS BETWEEN BUTTYAN *et al.* PROTOCOL AND OURS

Item		Buttyan et al.'s	Ours
Transmission	$U_i \leftrightarrow V$	4 (two rounds)	3
	$V \leftrightarrow H$	4 (two rounds)	2
Encryption	U_i	1 (Step 7)	2 (Steps 1,5)
	V	3 (Steps 4,6,8)	1 (Step 2)
	H	2 (Steps 3,5)	2 (Step 3)
Decryption	U_i	2 (Steps 7,9)	1 (Step 5)
	V	2 (Steps 4,8)	2 (Steps 4,6)
	H	1 (Step 5)	2 (Step 3)
Used variables		5 $(r_0, r_1, r_2, r_3, K_{\rm auth})$	3 (r_0, r_1, t)

Next, the numbers from the encryption process and the decryption process are also compared in Table I. We would like to focus on the required encryption and decryption processes for U_i because in general, mobile equipment provides low computation capability. For a mobile user U_i, two encryption processes and one decryption process are needed in the proposed protocol while one encryption process and two decryption processes are needed in Buttyan *et al.* protocol. If the encrypting performance and the decrypting performance of a cryptosystem are equivalent, e.g., DES, then there is no difference between Buttyan *et al.* method and ours regarding this point. However, if we introduce the Rijndael cryptosystem [14] for encrypting messages, our protocol will be beneficial because the encrypting performance of Rijndael is better than that of decryption. Daemen and Rijmen indicated that the decrypting performance of Rijndael is approximately 30% slower than its encrypting performance. Most importantly, Rijndael has been selected to be the advanced encryption standard (AES) by the National Institute of Standards and Technology (NIST) since 2001. Consequently, Rijndael will become a popular symmetric cryptosystem in the future.

Finally, the number of variables used in the proposed protocol is less than that of Buttyan *et al.* protocol. Therefore, our method is easier than Byttuan's method to implement. This is another advantage of the proposed authentication protocol.

IV. SELF-ENCRYPTION MECHANISM USED IN SECURE TELECONFERENCE

A. The Modified Protocol

In Section II-B, we have reviewed Hwang's conference key distribution scheme [6]. We know that Hwang's scheme not only allows the active participant to join or to exit an in-progress conference, but it also simultaneously includes both user authentication, as well as session key distribution. In this section, we propose a modified scheme which only alters the user authentication mechanism in Hwang's protocol. Since Hwang uses a public-key cryptosystem in his authentication mechanism, two cryptosystems are needed in mobile equipment. Note

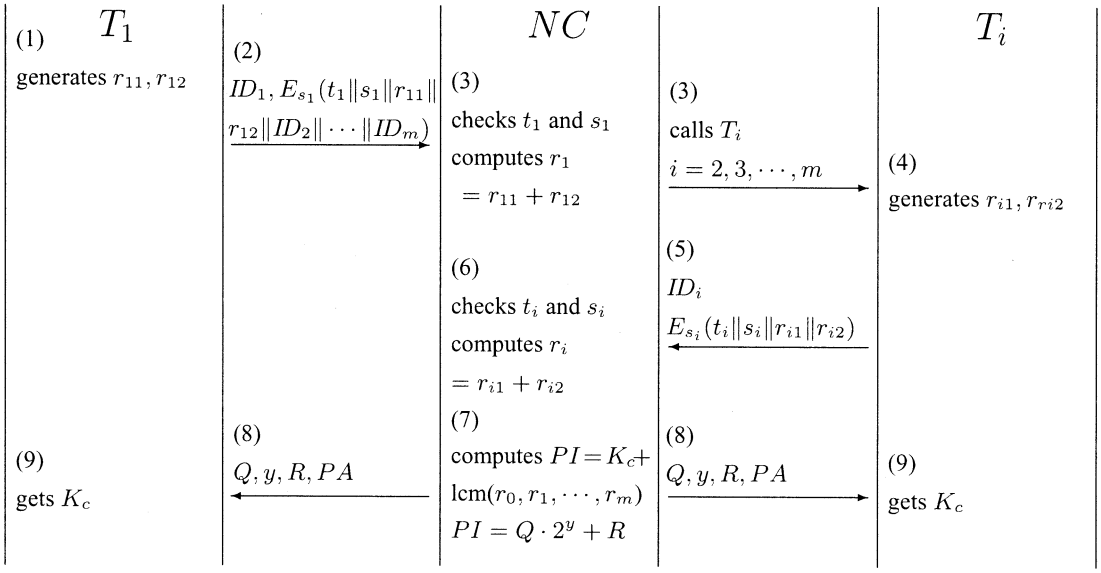

Fig. 4. Proposed authentication protocol for secure teleconference.

that the symmetric cryptosystem is used to protect the conversation content. In this work, our main goal is to simplify the complexity of mobile equipment as much as possible. Therefore, we modify Hwang's key distribution protocol in order to adopt only symmetric cryptosystems, and hence, the complexity of mobile equipment can be reduced.

Fig. 4 illustrates the modified key distribution protocol. In the following, we only describe the alterations in the modified protocol. The encrypting algorithm used in Steps 2 and 5 has been altered from a public-key cryptosystem to a symmetric cryptosystem. The mechanism "self-encryption" also has been adopted here to accomplish the authentication work.

For the network center NC, a few processes must be altered according to the above mentioned modifications. In Steps 3 and 6, NC has to find the corresponding secret $s_i = f(\mathrm{ID}_i)$ in order to decrypt the ciphertext sent by the user T_i. After the ciphertext has been decrypted using s_i, NC checks whether or not the decrypted secret key, say $\hat{s}_i$, is equal to s_i. If it is, then the validity of T_i is certified. Except for all of the previously mentioned modifications, the other processes remain unchanged in the modified key distribution protocol.

B. Security Analysis and Discussions

In this section, we will analyze the security of the modified key distribution protocol, as well as discuss its performance.

Hwang [6] pointed out that there are five security objectives for the secure conference service. We list these objectives as follows:

1) allowance for any active participant to join or to exit a conference;
2) prevention of fraud;
3) prevention of replaying attack;
4) privacy of conversation content;
5) privacy of participant's location information.

Since only the authentication mechanism has been altered in the modified key distribution protocol, the first objective remains. The second objective is achieved by verifying the correctness of the participant's identity ID_i and its secret key s_i. A timestamp has been used here to resist the replaying attack. Thus, the modified protocol remains the third objective. Certainly, once the conference key has been successfully established, i.e., only the valid participants hold the correct conference key, the conversation content of the conference will be protected by a cryptosystem. The modified protocol also achieves the fourth objective, because the key distribution mechanism remains unchanged.

Finally, the last objective ensures that the information about participants' locations cannot be intercepted. In other words, any participant's identity ID_i cannot be obtained by an intruder during the teleconference. Hwang's scheme uses a public-key cryptosystem to prevent the participant's identity from being revealed. Nevertheless, the modified protocol removes the public-key cryptosystem in order to simplify the complexity of mobile equipment. Therefore, the participant's identity ID_i has to be revealed to the network center in order to obtain the corresponding secret key s_i. In other words, the information about participants' locations will be intercepted by an intruder. However, location-aware applications for the mobile user have been proven to have significant relevance for future telecommunication [8]–[10]. That is to say, location-aware services and applications will become more popular in the future. Therefore, the importance of protecting the information about participants' locations is decreasing. Although the modified key distribution protocol may disclose information about the participant's location, it is still practical thanks to the location-aware service that has been increasingly used.

In this section, we have shown that the self-encryption mechanism can be easily adopted for the secure conference service. As we expected, since only one cryptosystem is needed for mobile equipment, its complexity can be reduced.

V. Conclusion

In this paper, a simple authentication technique for use in the GLOMONET has been proposed. This technique introduces a

quite simple mechanism called "self-encryption" to simplify the authentication protocol. The comparisons show that not only the proposed protocol is simpler than Buttyan *et al.* protocol, but it is also easier to implement. In the proposed authentication protocol, the temporary security manager in the visited network performs the same work that the original security manager in the home network does for regular communication. In other words, we simplified the authentication protocol both for the roaming service and the regular communication. Thus, the complexity of mobile equipment can be decreased. Furthermore, the proposed technique reduces the number of transmissions during the authentication phase and, therefore, the requirement of the channel capacities has been reduced. On the other hand, we also have proven that the self-encryption mechanism can be successfully adopted to another application in the mobility network, the secure teleconference service, to act as the authentication function. Thanks to the self-encryption mechanism, only one cryptosystem is needed in the modified conference key distribution protocol and, therefore, the complexity of mobile equipment can also be reduced. In summary, we have achieved the main goal of this work, the fact that a more complex mobile equipment is unnecessary in order to provide both the roaming service and the secure teleconference service. In addition, we believe that the self-encryption mechanism can find a wide application more than roaming and teleconference services.

REFERENCES

[1] S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," *IEEE J. Select. Areas Commun.*, vol. 15, pp. 1608–1617, Oct. 1997.

[2] "Interface Recommendations for Intelligent Network CS-2,", ITU-T Draft Recommendation Q.ASEC, Jan. 1997.

[3] M. S. Hwang and W. P. Yang, "Conference key distribution protocols for digital mobile communication systems," *IEEE J. Select. Areas Commun.*, vol. 13, pp. 416–420, Feb. 1995.

[4] D. Brown, "Techniques for privacy and authentication personal communication systems," *IEEE Pers. Commun.*, pp. 6–10, Aug. 1995.

[5] L. Buttyan, C. Gbaguidi, S. Staamann, and U. Wilhelm, "Extensions to an authentication technique proposed for the global mobility network," *IEEE Trans. Commun.*, vol. 48, pp. 373–376, Mar. 2000.

[6] M. S. Hwang, "Dynamic participation in a secure conference scheme for mobile communications," *IEEE Trans. Veh. Technol.*, vol. 48, pp. 1469–1474, Sept. 1999.

[7] Wireless Application Protocol [Online]. Available: http://www.wapforum.org

[8] S. Basagni, I. Chlamtac, and V. R. Syrotiuk, "Location aware one-to-many communication in mobil multi-hop wireless networks," in *Proc. IEEE Int. Conf. Vehicular Technology*, Tokyo, Japan, 2000, pp. 288–292.

[9] H. Maass, "Location-aware mobile applications based on directory services," *Mobile Networks and Appl.*, vol. 3, pp. 157–173, Aug. 1998.

[10] T. Pfeifer and R. Popescu-Zeletin, "A modular location-aware service and application platform," in *Proc. IEEE Int. Symp. Computers and Communications*, Sharm El Sheikh, Egypt, 1999, pp. 137–148.

[11] S. L. Ng, "Comments on dynamic participation in a secure conference scheme for mobile communications," *IEEE Trans. Veh. Technol.*, vol. 50, pp. 334–335, Jan. 2001.

[12] D. L. Mills, "Precision synchronization of computer network clocks," *ACM Comput. Commun. Rev.*, vol. 24, pp. 28–43, 1994.

[13] ——, "Adaptive hybrid clock discipline algorithm for the network time protocol," *IEEE/ACM Trans. Networking*, vol. 6, pp. 505–514, 1998.

[14] J. Daemen and V. Rijmen. *Rijndael Block Cipher* [Online]. Available: www.esat.kuleuven.ac.be/~rijmen/rijndael/

Kuo-Feng Hwang was born in Changhua, Taiwan, R.O.C., on October 11, 1970. He received the B.S. degree in construction engineering from National Lien-Ho College of Technology and Commerce, Taiwan, R.O.C., in 1991, the M.S. degree in information management from Chaoyang University of Technology, Taichung, Taiwan, R.O.C., in 1999, and the Ph.D. degree in computer engineering and information science from National Chung Cheng University, Chiayi, Taiwan, R.O.C., in 2002. He also studied information management at Chaoyang University, Taiwan, R.O.C., from 1996 to 1997.

From July 1993 to September 1994, he was the Associate Manager at the Spiringfront Computer Company, Ltd., Taipei, Taiwan, R.O.C. From October 1994 to June 1995, he was a Structural Engineer at the Paoshan Construction Company, Ltd., Taichung, Taiwan, R.O.C. He also was a Structural Engineer at the Cahsin Corporation, Taichung, Taiwan, R.O.C., from 1995 to 1996. Since August 2002, he has worked as an Assistant Professor in the Department of Multimedia Design, National Taichung Institute of Technology, Taichung, Taiwan, R.O.C. His research interests include cryptography, image processing, and wireless communications.

Chin-Chen Chang (M'88–S'92–F'99) was born in Taichung, Taiwan, R.O.C., on November 12, 1954. He received the B.S. degree in applied mathematics, the M.S. degree in computer and decision sciences from National Tsing Hua University, Hsinchu, Taiwan, R.O.C., in 1977 and 1979, respectively, and the Ph.D.degree in computer engineering from National Chiao Tung University, Hsinchu, Taiwan, R.O.C., in 1982.

From 1983 to 1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan, R.O.C. Since August 1989, he has worked as a Professor in the Institute of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan, R.O.C. His research interests include computer cryptography, data engineering, and image compression.

Dr. Chang is a Member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China.