Enhanced Mutual Authentication Scheme for the Virtual Home Environment in 3G Mobile Network*

Hung-Min Sun(孫宏民), Cheng-Ta Yang(楊政達) , Bing-Cheng Chen(陳炳彰) , Her-Tyan Yeh(葉禾田)

National Tsing-Hua University

E-mail: hmsun@cs.nthu.edu.tw

†Department of Computer Science and Information Engineering
National Cheng Kung University

‡Department of Information Communication
Southern Taiwan University of Technology

Abstract

A Virtual Home Environment is a technique for the context-dependent provision of telecommunication-related services to nomadic users. Recently, two three party mutual authentication schemes for the VHE are proposed by Jeong, Lee and Lee. Their first scheme is the password based mutual authentication protocol; each network must maintain the password tables of other network. Their second scheme is the mutual authentication protocol with key exchange and challenge handshake authentication protocol (CHAP). In this paper, we propose a simple protocol that it is mutual authentication in VHE.

Keywords : mutual authentication, VHE, password

1 Introduction

With the growing of communication market, the advance of wireless communication and computer technologies, the mobile communication provides more convenient, portable, versatile and close to the people. The telecommunication industry is now planning for the evolution towards third generation mobile systems such as the Universal Mobile Telecommunication System (UMTS).

*This research was supported by the Communications Software Technology project of Institute for Information Industry and sponsored by MOEA ,R.O.C.

In 3GPP[1] (Third-Generation Partnership Project), the VHE (Virtual Home Environment) [2][3][4] is defined as a concept for personal service environment portability across network boundaries and between terminals. The concept of the VHE is such that users are consistently presented with the same personalized features wherever they may roam. The VHE enables a visited network to obtain information about the user's service provider during the registration procedure and other information such as the user's personalized service profile and the identification of service capabilities needed for the execution of service provider specific services. In other word, the VHE offers global roaming and personal service environment portability; user's profiles and service adaptation are transported from home network to visited network to provide services at the visited network. Therefore, a mutual authentication protocol is necessary among mobile station (MS), visited network (VN) and home network (HN) to keep the information is confident and secure.

Most of the literatures on 3-party authentication and key distribution protocols have focused on the environment that two users establish a session key through an authentication server[7]. Recently, The three party environment that one is an application server who provides service to the user; the other is a user who requests the service from the application server; and a server certifies the validity of entity and helps the user and application server to generate the session key. Such an environment is suitable for many applications[6], eg. virtual home environment in 3G.

Recently, two three party mutual authentication schemes for the VHE are proposed by Jeong, Lee and Lee[5]. Their first scheme is the password based mutual authentication protocol; each network has to maintain the password tables of other network. Their second scheme is the mutual authentication protocol with key exchange and challenge handshake authentication protocol (CHAP). It is too complexity. We would propose a new three party mutual authentication scheme in the virtual home environment.

The rest of this paper is organized as follows. Section 2 reviews Jeong et al.'s 3 party mutual authentication schemes. We proposed and analyzed a simpler protocol and compared it with the related works in section 3. Finally, we had a conclusion in section 4.

2 Review Jeong et al.'s Three Party mutual authentication schemes

In this section, we would review the Jeong et al.'s three party mutual authentication schemes in the virtual home environment briefly and point out some problems.

2.1 Jeong et al.'s first scheme

Jeong et al.'s first scheme is the password based mutual authentication protocol. All networks must maintain other networks' password table. MS and HN have established the shared secret key ($K_{MS/HN}$) already. We describe the protocol step by step as follows:

1. MS encrypts MS's identification (MS_ID), VN's identification (VN_ID) and nonce ($n1$) using shared secret key $K_{MS/HN}$ to $\{MS\_ID, VN\_ID, n1\}_{K_{MS/HN}}$, and sends $\{MS\_ID, VN\_ID, n1\}_{K_{MS/HN}}$, MS's temporary ID ($MS\_TID$) and HN's alias ($HN\_AID$) to VN.

2. VN encrypts $\{MS\_ID, VN\_ID, n1\}_{K_{MS/HN}}$, VN_ID, MS_ID, VN's password (VN_Pass) and nonce ($n2$) using HN's public key K_{HN+} and sends to HN.

3. HN decrypts and checks the VN's password to authenticate VN; and HN identifies MS by shared secret key ($K_{MS/HN}$).
   After HN authenticating VN and MS, HN encrypts HN's identification (HN_ID), HN's password (HN_Pass) and nonce ($n3$) using VN's public key K_{VN+} and sends to VN.
   HN encrypts MS's password (MS_Pass) and nonce ($n4$) using shared secret key $K_{MS/HN}$ to $\{MS\_Pass, n4\}_{K_{MS/HN}}$, and encrypt VN_ID, MS_ID and nonce ($n4$) using shared secret key $K_{MS/HN}$ to $\{VN\_ID, MS\_ID, n4\}_{K_{MS/HN}}$. Finally, HN encrypts MS_ID, $\{MS\_Pass, n4\}_{K_{MS/HN}}$, nonce ($n5$) and $\{VN\_ID, MS\_ID, n4\}_{K_{MS/HN}}$ with VN's public key K_{VN+} and sends to VN.

4. VN receives the ciphers and decrypts them. VN checks the HN's password to authenticate HN. At this time, VN and HN achieve to mutual authentication. And then, VH keeps $\{MS\_Pass, n4\}_{K_{MS/HN}}$ to authenticate MS later. Finally, VH conveys $\{VN\_ID, MS\_ID, n4\}_{K_{MS/HN}}$ to MS.

5. MS decrypts $\{VN\_ID, MS\_ID, n4\}_{K_{MS/HN}}$ to authenticate VN and obtain $n4$, and computes $\{MS\_Pass, n4\}_{K_{MS/HN}}$ to send to VN.

6. VN receives $\{MS\_Pass, n4\}_{K_{MS/HN}}$ and compares it with stored $\{MS\_Pass, n4\}_{K_{MS/HN}}$ at step 4 to authenticate MS.

In above protocol, HN/VN and MS/VN are mutual authentication. Obviously, VN and HN must keep the password tables each other that is superfluous. Without password table, VN and HN is still mutual authentication using PKI. Furthermore, after mutual authentication MS and VN have not shared secret informations.

2.2 Jeong et al.'s second scheme

Jeong et al.'s second scheme with key exchange and CHAP. We review as follows:

1. MS encrypts MS's identification (MS_ID), VN's identification (VN_ID) and nonce ($n1$) using shared secret key $K_{MS/HN}$ to $\{MS\_ID, VN\_ID, n1\}_{K_{MS/HN}}$, and sends $\{MS\_ID, VN\_ID, n1\}_{K_{MS/HN}}$, MS's temporary ID ($MS\_TID$) and HN's alias ($HN\_AID$) to VN.

2. VN encrypts $\{MS\_ID, VN\_ID, n1\}_{K_{MS/HN}}$, VN_ID, MS_ID, nonce ($n2$) and sequential integer value ($Count1$) using HN's public key K_{HN+} and sends to HN.

3. HN identifies MS by shared secret key ($K_{MS/HN}$). HN selects a random number X_{HN} and calculates $pubValue_{HN}$ with the random number. Then HN encrypts $pubValue_{HN}$, VN_ID and nonce ($n3$) using VN's public key K_{VN+} and sends to VN.

4. VN selects a random number X_{VN} and calculates $pubValue_{VN}$ with the random number. Then VN encrypts $pubValue_{VN}$, HN_ID and nonce ($n4$) using HN's public key K_{HN+} and sends to HN.
   VN and HN can obtain their shared secret key by computing

$$\begin{aligned} K_{VN/HN} &= (pubValue_{VN})^{X_{HN}} \bmod q \\ &= (pubValue_{HN})^{X_{VN}} \bmod q, \end{aligned}$$

   it is similar to Diffie-Hellmam key exchange. A more detailed discussion is given in [5].

5. HN selects a random challenger ($Rand1$) and encrypts $Rand1$ and nonce ($n3$) using shared secret key ($K_{VN/HN}$), then sends to VN.

6. After decrypting the ciphertext successfully, VN obtains $Rand1$, then encrypts it and sequential integer value ($Count2$) using shared secret key ($K_{VN/HN}$) and sends to HN.

7. HN and VN are mutual authentication. HN selects a random challenger ($Rand2$) and generates a shared secret key ($K_{MS/VN}$) between MS and VN, then encrypts MS_ID, $Rand2$, $K_{MS/VN}$ and nonce (n4) using shared secret key $K_{MS/HN}$ to $\{MS\_ID, Rand2, K_{MS/VN}, n4\}_{K_{MS/HN}}$. Finally, HN encrypts $\{MS\_ID$, $Rand2$, $K_{MS/VN}$, $n4\}_{K_{MS/HN}}$, VN_ID, $K_{MS/VN}$, $Rand2$, and nonce ($n5$) with $K_{VN/HN}$ and sends to VN.

8. VN decrypts and transports $\{MS\_ID, Rand2, K_{MS/VN}, n4\}_{K_{MS/HN}}$ to MS. MS and VN execute CHAP with the $Rand2$ for mutual authentication between MS and VN.

Clearly, this protocol is too complex to efficient. Later, we would propose a simpler protocol

3 The Proposed protocol

A Virtual Home Environment (VHE) is a means for the context-dependent provision of telecommunication-related services to nomadic users. In this paper, we proposed a simpler protocol about mutual authentication among MS, VN and HN. In the protocol, we assume that the mobile station M must register the validity of user to the home network H. The shared secret key K_{MH} between M and H is already established.

Table 1: Notations

ID_X	Identification of X
TID_X	Temporary ID of X
AID_X	Alias of X
K_{XY}	Secret key shared between X and Y
K_X	Public key of X
T_X	Timestamp generated by X
n_1, n_2	Random numbers
$X \rightarrow Y : M$	X sends a message M to Y
$[info]_K$	Symmetric encryption of "$info$" with shared secret key K
$\{info\}_K$	Asymmetric encryption of "$info$" with the public key K

3.1 Description of Notations

The notations in Table 1 are used throughout this paper.

3.2 The proposed mutual authentication protocol

We show our protocol in Figure 1 and the detailed steps are described as follows:

1. M $\longrightarrow$ V : $[ID_M, ID_V, n_1, T_M]_{K_{MH}}, TID_M, AID_H, T_M$
   The mobile station M chooses a random number n_1, and sends $[ID_M, ID_V, n_1, T_M]_{K_{MH}}$, TID_M, AID_H to the visited network V.

2. V $\longrightarrow$ H : $\{[ID_M, ID_V, n_1, T_M]_{K_{MH}}, ID_M, ID_V, T_V, T_M, n_2\}_{K_H}$
   After receiving the messages from mobile station, V checks if the timestamp T_M is within some allowable range compared with its current time first. If the decision is correct, the visited network V chooses a random number n_2, and encrypts $[ID_M$,

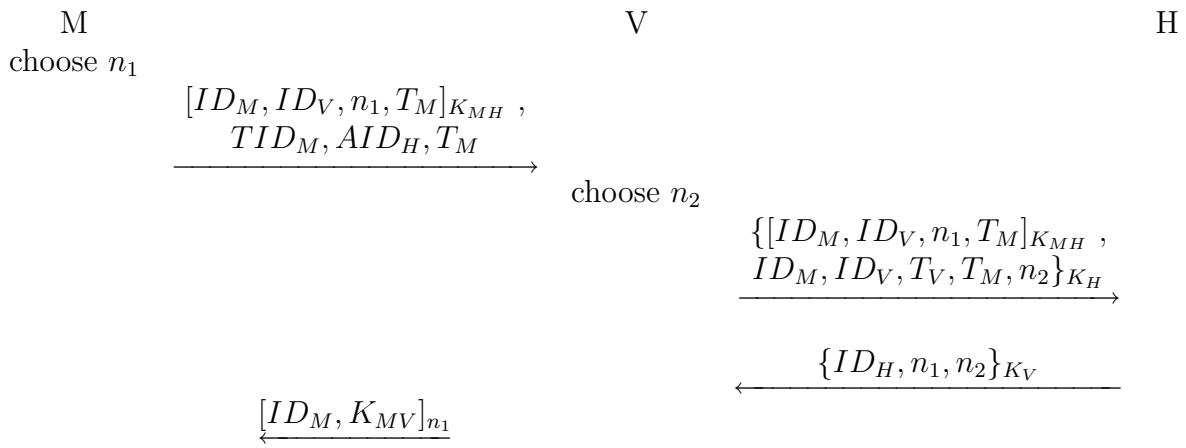

Figure 1: The proposed mutual authentication protocol

ID_V, n_1, $T_M]_{K_{MH}}$, ID_M, ID_V, T_V, T_M, n_2 with the M's home network H's public key K_H. And then, V sends $\{[ID_M, ID_V, n_1, T_M]_{K_{MH}}, ID_M, ID_V, T_V, T_M, n_2\}_{K_H}$ to H for authentication.

3. H $\longrightarrow$ V : $\{ID_H, n_1, n_2\}_{K_V}$
   H decrypts $\{[ID_M, ID_V, n_1, T_M]_{K_{MH}}, ID_M, ID_V, T_V, n_2\}_{K_H}$ using private key. If T_V is within reasonable range. H decrypts $[ID_M, ID_V, n_1, T_M]_{K_{MH}}$ using shared secret key K_{MH}. If ID_M, ID_V are correct and T_M is reasonable, H can authenticate M; and furthermore, it implies that H authenticates V. Afterward, H encrypts ID_H, n_1, n_2 using V's public key K_V,and sends it to V.

4. V $\longrightarrow$ M : $[ID_M, K_{MV}]_{n_1}$
   V decrypts $\{ID_H, n_1, n_2\}_{K_V}$ using private key. If n_2 is correct, then V accepts that M is authenticated by H. And then, V determines a shared secret key K_{MV} between M and V and encrypts ID_M, K_{MV} using n_1. V sends $[ID_M, K_{MV}]_{n_1}$ to M.

5. M decrypts $[ID_M, K_{MV}]_{n_1}$ using n_1. If ID_M is correct, then M authenticates V and obtains a shared secret key K_{MV}.

Next, we would analyze the security of the proposed protocol, and compare with two Jeong et al.'s protocols.

3.3 Security Analysis

We assume the shared secret key K_{MH} between M and H has been kept secretly. Any intruder can not obtain the shared secret key.

3.3.1 Mutual authentication

In our protocol, H decrypts the ciphertext that is encrypted by V (step 2) and return correct n_2 (step 3), V authenticate H. V decrypts the ciphertext that is encrypted by H and obtains n_1, n_2 (step 3), H authenticate V and M. V and H are mutual authentication each other. Furthermore, H can decrypts the ciphertext that is encrypted by M using shared secret key, the validity of M is certified. Finally, M can authenticate V by encrypting a shared secret key K_{MV} using n_1 that is chosen by M. So we can assert that mutual authentication between V and H is completed.

3.3.2 Entity privacy

Traffic analysis consists of an attack whereby the communication channel is tapped and statistical information about the data traffic is accumulated. Our protocol just transmits the ciphertext, alias name and temporary name at air interface that defends the traffic analysis attack. That is, the entity privacy is promised.

Table 2: Comparisons of two Jeong et al.'s protocols and Ours

	Jeong et al.'s 1st	Jeong et al.'s 2nd	Ours
Password table	Yes	No	No
Exponent computing	No	Yes	No
The numbers of symmetric encryption/decryption	3/3	5/5	2/2
The numbers of asymmetric encryption/decryption	3/3	3/3	2/2

3.3.3 Replay attack

An intruder can replay an old message (step 1), V and H can check the timestamp whether it is within allowable range or not. Although an intruder can successfully get $[ID_M, K_{MV}]_{n_1}$ (step 4). Because he is unable to know the random numbers n_1 included in old message to decrypt this messages. Thus, our protocol is secure against the message replay attacks.

3.3.4 Impersonating attack

An intruder can impersonate the visited network V to the mobile station M. Because an intruder can not directly obtain random number n_1, that is kept for M or is passed from H. M can detect the fault and stop his request. This means that our protocol is secure against Impersonating attack.

3.4 Comparison

In this section, we compare our protocol with two Jeong et al.'s protocols, The comparisons are listed in Table 2. The first item in the comparison is password table. In Jeong et al.'s first protocol, all networks have to maintain other networks' password tables. The second item is exponent computing. In Jeong et al.'s second protocol, a key exchange protocol is executed and there are exponent computing among networks. Next, the numbers of symmetric encryption/decryption are compared in Table 2. In general, the mobile station provides low-power computation capability. The symmetric encryption/decryption technique is the better choice for the mobile station. Finally, the numbers of asymmetric encryption/decryption in these protocol. The asymmetric encryption/decryption need more computation power, it suit the network environment.

Clearly, there are not password tables and exponent computation in our protocol, there is one time symmetric encryption (step 1) and one time symmetric decryption (step 5) for mobile station. Our protocol is more efficient than Jeong et al.'s.

4 Conclusion

In this paper, we improve a simpler mutual authentication scheme in virtual home environment in 3G mobile network. One of the key features of VHE, is the adjustment that it provides to terminal capabilities and user preferences. In order to adapt personal service portability, subscribers confidence in security of VHE services is necessary. Our proposed protocol fits for the VHE in 3G and is easiler than Jeong et al.'s scheme to implement.

References

[1] http://www.3gpp.org, 3rd Generation Partnership Project (3GPP).

[2] T. SUGIYAMA, K. NAKADA, S. SUZUKI, "A Study of Virtual Home Environment (VHE) in IMT-2000–Requirements, Issues and Resolution for Realization of VHE", IEICE Trans. FUNDA., Vol.E86-D, No.11, pp.2479-2482, Jul. 1999.

[3] "Virtual Home Environment / Open Service Architecture", TS 23.127, 3GPP project.

[4] "The Virtual Home Environment", TS 22.121, 3GPP project.

[5] J. M. Jeong, G. Y. Lee, Y. Lee, "Three Party Mutual Authentication Schemes for the Virtual Home Environment in the Next Generation Mobile Network", IEICE Trans. INF. & SYST., Vol. E82-A No.7, pp.1269-1277, Nov. 2003.

[6] C. C. Lee, M. S. Hwang, W. P. Yang, "Extension of Authentication Protocol for GSM", IEE Proceedings – Communications, Vol. 150, No. 2, pp. 91-95, Apr. 2003.

[7] C. L. Lin, H. M. Sun, T. Hwang, "Three-Party Encrypted Key Exchange: Attacks and A Solution. ACM Operating System Reviews", 34(4), pp. 12-20, 2000.