A Wireless-based Authentication and Anonymous Channels for GSM System

Ren-Junn Hwang[1], Jing-Feng Li[2], and Yu-Kai Hsiao[3]

Department of Computer Science and Information Engineering, Tamkang University
Tamshui 251, Taiwan, ROC

[1]junhwang@ms35.hinet.net, [2]ljf0030@ms11.hinet.net, [3]shiau.kae@msa.hinet.net

Received 1 May 2006; Revised 16 June 2006 ; Accepted 22 June 2006

Abstract. For mobile roaming environment, the mobile uses visiting network's services, the mobile station and the visiting network must authenticate each other. We propose a new authentication and anonymous channels protocol for roaming mobile communication. Our scheme can securely apply to GSM and CDPD wireless communication system, it's not only supporting the mobile anonymity but also resolving the charging problem. The mobile station only takes one modular multiplication and one modular addition computation time when it roams in the visiting network.

Keywords：Authentication, Anonymous Channel, GSM

1 Introduction

Wireless communication systems such as GSM [6] and CDPD [8] systems have become more and more popular. Wireless communication system contains: the mobile station (*MS*) , base stations (*BSs*) and mobile network switching centers(*MSCs*). *MS* links to *BS* and use the mobile network resource. *MSC* authenticates any calling linked to *BS* from *MS*. When a user wants to use his mobile station by network's service or network's resource, the network domain must authenticate its identity. In general, a user registers at network domain named home network. Home network issues SIM card to user, which contains the authentication information of user. We say that *MS* roams in a network domain, if it does not register in this network domain. We also called this network domain as visiting network. There is a serious problem, how the visiting network authenticates the roaming *MS*. We need an authentication and anonymous channels service scheme such that the visiting network can verify the mobile user is legal but need not know his identity in home network. The roaming mobile station anonymity and security are very important. It is needed for authentication and anonymous channels service [2,3] using in confidentiality of identity and the privacy of the legal user. We also should consider that the ability of computation of mobile station is weak in comparison with personal computer or notebook.

In typical identification systems such as secret-key base identification, public-key base identification [4] and ID base identification [15] systems are lack of supporting authentication and anonymous channels service for roaming mobile stations. For authentication and anonymous channels service, Lin and Jan had proposed some solutions [9,10], but they only consider identity authentication and identity anonymous. In this paper, we propose a scheme that provides the authentication and anonymous channel service, and it also satisfies the following properties: (a) The visiting network can verify that *MS* is legal but the visiting network can't trace any information about t *MS*'s real identification. (b) *MS* can't repudiate using visiting network's service. (c) the visiting network can charge for service. (d) The proposed scheme can suit mobile with little computation for roaming.

Section 2 describes the proposed scheme. We discuss the properties of anonymity, security, non-repudiation and the charging-problem in Section 3. In section 4, we make the comparison with other similar schemes. Finally, we make conclusions in Section 5.

2 The authentication and anonymous channels scheme

The proposed scheme contains two phases: ticket-granting phase and ticket authentication phase. In the ticket-granting phase, the *MS* gets a ticket from home network. By using this ticket, the *MS* roams in the visiting network authorized. The *MS* should perform this phase to get this ticket during awaiting-time before it roams through visiting network. When the *MS* roams in the visiting network, it should provide the ticket to the visiting network. The visiting network verifies the *MS* through the ticket authentication phase. To introduce our scheme clearly, we define some symbols and make some assumptions as follow:

(a) There is a public key cryptographic scheme: RSA [14].

(b) There are symmetric cryptographic scheme [16] and one-way hash function [11,13]

(c) *MS* denotes a mobile station, *VN* denotes the visiting network for *MS*, *H* denotes home network for *MS* and $MS \rightarrow H : m$ denotes that *MS* sends a message *m* to *H*.

(d) *H* has a public key e_h and O_h and the corresponding secret key p_h and q_h based on RSA [14] considerations, where $O_h = p_h * q_h$.

(e) $\{m\}_{e_h}$ denotes the message: *m* is encrypted by RSA cryptographic scheme using RSA public key e_h and O_h

(f) $(m)_r$ denotes the message: *m* is encrypted by symmetric cryptographic scheme using secret key *r*.

(g) Let *P* be a large strong prime number and *Q* be a prime factor of $(P–1)$. *g* is a generator of order Q in Z_p^*. *H* has a secret key *x* and public key y_h , where $y_h = g^x \, mod \, p$.

(h) Every mobile station has a unique identification *ID* registered in the home network, and the information $(ID, Cert(ID), O_h , P, Q)$ stored in SIM card, where $Cert(ID) = h(ID \oplus x \oplus p_h)$ is a certificate for *MS*'s *ID* issued by the home network.

(i) Home and visiting-network also have the opposite party's public key.

2.1 The ticket-granting phase

If the *MS* wants to roam through visiting network, it must apply a ticket from its home network during awaiting-time and stored it in SIM card form. This ticket has a valid period is up to home network. The *MS* uses this ticket to roam in visiting network. The ticket-granting phase is introduced in the following. We also show this phase briefly in Fig. 1.

Firstly, *H* selects $k \in Z^*_Q$ to compute $K = g^k \, mod \, p$, and sends *K* to *MS*. Secondly, *MS* select $a \in Z^*_Q$ to compute $A = g^a \, mod \, p$ and session key $r = K^a \, mod \, p$. *MS* encrypts *A*, *ID*, *Cert*(*ID*) by symmetric cryptographic scheme [16] with secret key *r* and encrypts *A*, $(A, ID, Cert(ID))_r$ by RSA scheme [14] using *H*'s public key e_h and O_h. *MS* sends encrypted message$\{A ,(A ,ID , Cert(ID))_r\}_{e_h}$ to *H*. Thirdly, *H* decrypts message: $\{A ,(A ,ID ,Cert(ID))_r\}_{e_h}$ by his secret keys and generates secret key $r = A^k \, mod \, p$. *H* decrypts $(A, ID, Cert(ID))_r$ with r, and verifies the mobile station's identification and the correctness of *A* and *r.* *H* computes $s = un\_code + k + x*t \, mod \, (p-1)$, where $un\_code \in Z^*_Q$ is unique, *t* is a valid period for ticket. *H* also computes $R = g^{un\_code + k} \, mod \, p$, where $R \neq y^{-t} \, mod \, p$, *R* must be unique, *H* also generates $Cert(R) = [h(R,t,y_h)]^{1/2} \, mod \, (p_h * q_h)$ [1,12]. *H* encrypts $(s, t, h(s), Cert(R), R)$ by symmetric cryptographic scheme with *r* and sends it to *MS,* where *h*(*s*) *is a hash value of s*. Finally, The ticket for the *MS* is (*s*, *t*, *h*(*s*), *Cert*(*R*), *R*). *MS* decrypts the message $(s ,t, h(s), Cert(R), R)_r$ to get the ticket *s*. *MS* verify correctness of *s*, *t* and *R* by *h*(*s*) and $h(R, t, y_h) \equiv Cert(R)^2 \, (mod \, O_h)$.

Step 1 : $H \rightarrow MS : K$

Step 2 : $MS \rightarrow H : \{A, (A, ID, Cert(ID))_r\}_{e_h}$

Step 3 : $H \rightarrow MS : (s , t, h(s), Cert(R) , R)_r$

Fig. 1. The ticket-granting phase

2.2 The ticket authentication phase

The visiting network authenticates the *MS* by the ticket authentication phase. To protect the privacy of the user, the visiting network verify the user is a legal user of one cooperation network domain, but the visiting network can not get any information about the user including its identity. Although the visiting network doesn't know any information of *MS*, it can charge the service from the home network of *MS*. We introduce the process in the following. We also show this phase briefly in Fig. 2.

At first, the visiting network sends random number *N* and time stamp $T_{challenge}$ to the *MS*. Secondly, the *MS* selects $b \in Z^*_Q$ to compute *NEW-ID* and *w* as $w = s + b * T_{challenge} * R \ mod\ (p\text{-}1)$ and $NEW\text{-}ID = (B \,||\, R \,||\, t \,||\, Cert(R) \,||\, N)$, where $B = g^b \ mod\ p$. *MS* sends *w*, *New-ID*, *R* and its home-ID to the visiting network. Thirdly, the visiting network verifies the mobile station by checking the equations $g^w \equiv R * y_h^t * B^{T_{challenge} * R} \ (mod\ p)$ and $h(R, t, y_h) \equiv Cert(R)^2 \ (mod\ O_h)$ are hold or not. There is a unique number *R* in the *Ms*'s ticket, equations are hold, the visiting network will make contact with home network to confirm *R*. The *R* is unique, so the visiting network can charge the service based on *R*. The visiting network confirm *R* is valid by sending *R*, a random number N_l and visiting network's name to home network. Fourthly, the home network verifies *R* is valid and record, that the mobile station is roaming in visiting network. It sends a confirmation message $h(Cert(R)||N_l)$ to the visiting network.

Step 1 : $VN \rightarrow MS : N, T_{challenge}$

Step 2 : $MS \rightarrow VN : NEW\text{-}ID, w, Home\text{-}ID$

Step 3 : $VN \rightarrow H : \{N_l, R, Visit\text{-}ID\}_{e_h}$

Step 4 : $H \rightarrow VN : h(\ Cert(R) \,||\, N_l)$

Fig. 2. The ticket authentication phase

3 Discussions

In this section we will discuss some important properties of the proposed scheme. Subsection 3.1 shows its anonymity. Subsection 3.2 discusses its security. The Non-repudiation and the charging-problem are discussed in Subsection 3.3. Finally, we make the comparisons with the other schemes in Section 4.

3.1 Anonymity

In the ticket-granting phase, the mobile station encrypts the message: $\{A\ ,(A\ ,ID\ ,Cert(ID))_r\}$ by home network's public key. The ticket authentication phase does not use any information about the mobile station's real identification. In the proposed scheme, the information of the mobile station only shows in Step 2 of the ticket-granting phase. However, the mobile station encrypts this message with the home network's public key as $\{A\ ,(A\ ,ID\ ,Cert(ID))_r\}_{e_h}$. By the property of public key cryptosystem, nobody except the home network can get the mobile station's information from this message in the proposed scheme. The visiting network only makes sure that the mobile station is a authorized user, but it can't get any identification information about the roaming mobile station. The proposed scheme provides the anonymity.

3.2 Security Considerations

In the ticket-granting phase, the security focuses on data authentication, data privacy and data integrity. *MS*'s SIM card records *ID* and *Cert*(*ID*). In Step 2, home receives $\{A, (A, ID, Cert\ (ID))_r\}_{e_h}$ from *MS*. Home network verifies *MS*'s identity by $Cert\ (ID) = h(ID \oplus x \oplus p_h)$. In Step 3 of the ticket-granting phase, the message $(s, t, h(s), Cert(R), R)_r$ is encrypted by session key *r*. Only home network can decrypt $\{A, (A, ID, Cert\ (ID))_r\}_{e_h}$ to get *A* and use it go generate *r*. *MS* authenticates that $(s, t, h(s), Cert(R), R)_r$ is sent by real home network. The data authentication is made. The session key r between *MS* and home network is generated based on Diffie-Hellman key exchange [4], it is secure.

In Step 3 of the ticket-granting phase, the home network sends $(s, t, h(s), Cert(R), R)_r$ to *MS*, *MS* can verify *s* and *t* by $h(s)$ and $h(R, t, y_h) \equiv Cert(R)^2$ $(mod\ O_h)$ respectively. The integrity of *s* and *R* are made.

In the ticket authentication phase, the security focuses on the attacker can't forge valid *R* and the ticket valid in the period *t*. If anyone wants to forge R, he also should compute $Cert(R) = [h(R,t,y_h)]^{1/2}\ mod\ (p_h * q_h)$, it must factor O_h to get p_h and q_h [12]. It is hard if p_h and q_h are large primes. Our scheme can prevent replay attack by the third party. By the equation $g^w \equiv R * y_h{}^t * B^{T\,challenge\,*\,R}$ $(mod\ \ p)$, where $w = s + b * T_{challenge} * R\ \ mod\ \ (p\text{-}1)$, we know that if the mobile station or the third party wants to forge *s*, a valid period *t* or *w* such that making the equation $g^w \equiv R * y_h{}^t * B^{T\,challenge\,*\,R}$ $(mod\ \ p)$ is hold, it has to solve the discrete logarithm problem.

3.3 Non-repudiation and the charging-problem Issues

The proposed scheme provides anonymous authentication scheme. The visiting network can't know the information of the roaming mobile station, but it can charge the services for mobile station. In the proposed scheme, the home network generates a unique value *R* and its certification for the mobile station. The special value R satisfies the equation $R = g^{un\_code+R}$ $(mod\ p)$. The certification $Cert(R) = [h(R,t,y_h)]^{1/2}\ \ mod\ \ (p_h * q_h)$. Nobody except the home network can generate *R* and *cert*(*R*). The visiting network can charge the service from the home network based on the roaming mobile station's *R*, although he does not know the real identity of the roaming mobile station. The mobile station also can not repudiate the charge based on *R*. Clearly, the visiting network can charge the service of the roaming mobile station and the mobile can not repudiate it.

4 Comparisons

The computation ability of the mobile station is weak. We should reduce the computation load of the mobile station. This section we discuss the computation load of the proposed scheme. We also make some comparisons with other methods in Table 1. To show the computation load clearly, we use the following symbols to express the computation load.

T_h : the time for executing one-way hash function.
T_{exp} : the time for executing modular exponentiation.
T_{pub} : the time for executing public key cryptographic scheme.
T_{mul} : the time for executing modular multiplication.
T_{square} : the time for executing modular square.
$T_{square\ root}$: the time for executing modular square root.
T_{add} : the time for executing modular addition.
$T_{symmetric}$: the time for executing symmetric cryptographic scheme.

Table 1. The comparison among Lin et al., Juang et al. and the proposed scheme

	Pre-share key between Home and *MS*	**Solving Charging-problem**	**The least computation cost**	**SIM card lost problem**	**Generate session key**
Our scheme	No	Yes	$T_{add} + T_{mul}$	No	No
Lin and Jan's scheme	Yes	No	$T_{add} + 2T_{mul}$	Yes	No
Juang et al. 's scheme	Yes	Yes	$T_{pub} + T_{mul} + T_{hash}$	No	Yes

In our scheme, the mobile station pre-computes all of parameters during awaiting-time in home network domain. In the ticket authentication phase, the mobile station only compute $w = s + b * T_{challenge} * R \bmod (p-1)$ online. The message, $s + b*R \bmod (p-1)$, of the ticket granting phase can be pre- compute in the ticket granting phase. The mobile side computation cost is $1T_{mul} + 1T_{add}$ in roaming visiting network domain. The total executing time in our scheme without pre-computing is $9T_{exp} + 4\ T_{symmetric} + 2\ T_{pub} + 2\ T_{square} + T_{square\ root} + 4\ T_{add} + 6\ T_{mul} + 6T_{hash}$. Lin and Jan [10] also proposed an authentication and anonymous scheme. The total executing time in their protocol without pre- computing is $10\ T_{exp} + 4\ T_{symmetric} + 2\ T_{pub} + 12\ T_{mul} + 4T_{add}$. Juang et al.'s [7] also proposed an authentication and anonymous scheme, too. Lin and Jan [10] showed that their methods is more efficient than Juag et al.'s method. Our proposed scheme is more efficient than Lin and Jan's. We make some other comparisons with their methods in Table 1. It is clearly that our method is more efficient than their methods. Our method is more practical.

5 Conclusions

This paper proposes a new authentication and anonymous channels protocol for roaming mobile communication. In our scheme, we employ pre-computing mode during awaiting-time to reduce computing load. We also consider the anonymity security, Non-repudiation and the charging-problem in our scheme. The mobile station only takes $1T_{mul} + 1T_{add}$ computation time in roaming mode. It is practicable to use our scheme in GSM-style system.

References

[1] M. J. Beller and Y. Yacobi, "Fully-fledged Two-way Public Key Authentication and Key Agreement for Low-cost Terminals", Electronics Letters, Vol. 29, No. 11, May 1993.

[2] D. Chaum, "The Dining Cryptographers Problem, Unconditional Sender and Recipient Intractability", J. Cryptology, Vol. 1, 1988, pp. 65-75.

[3] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, Vol. 24 No. 2, 1981, pp. 84-88.

[4] W.Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT-22, No. 6, Nov 1976, pp. 644-654.

[5] T. ElGamal, "A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithm", IEEE Trans. Inform, Theory, Vol. IT-31, No. 4, July 1985, pp. 468-472.

[6] ETSI, "GSM Recommendations", GSM Release 92, 01.02-12.21, February 1993.

[7] W. S. Juang, C.L. Lei, C.Y. Chang, "Anonymous Channel and Authentication in Wireless Communications", Computer communications, Vol. 22, 1999, pp. 1502-1511.

[8] P. J.B King, "Cellular Digital Packet Data System Specification", Release 1.1, CDPD Forum Inc., January 1995.

[9] Whe Dar Lin, Jinn-Ke Jan, "A Efficient Anonymous Channel Protocol In Wireless Communications", IEICE Trans., Communication, Vol. E84-B, No. 3, March 2001.

[10] Whe Dar Lin, Jinn-Ke Jan, "A Wireless Based Authentication and Anonymous Channels for Large Scale Area", in Proceedings of Sixth IEEE Symposium on Computers and Communications, 2001.

[11] NIST FIPS PUB 180, "Secure Hash Standard, National Institute of Standards and Technology", US Department of Commerce, Draft, 1993.

[12] M.O. Rabin,“Digitalized Signatures and Public Key Functions as Intractable as Factorization”, MIT Lab. Computer Science , TR 212, Jan 1979.

[13] R.L Rivest, “The MD5 Message-digest Algorithm”, RFC 1321, Internet Activities Board, Internet Privacy Task Force, 1992.

[14] R. Rivest, A. Shamir, L. Adleman, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems”, Communications of the ACM, Vol. 21, No. 2, Feb. 1978, pp. 120-126.

[15] A. Shamir,“Identity-based Cryptosystems and Signature Schemes”, Proc. Crypto 84, Santa Barbara, Springer-Verlag, LNCS 196, 1984, pp. 47-53.

[16] M. F. Smid, D. K. Branstd, “The Data Encryption Standard: Past and Future”, Proc. IEEE, Vol. 76, No.5, 1988, pp. 550-559.