A New Anonymous Channel Protocol in Wireless Communications*

Min-Shiang Hwang[†] Cheng-Chi Lee[‡] Ji-Zhe Lee[§]

Department of Management Information System[†]
National Chung Hsing University,
250 Kuo Kuang Road,
402 Taichung, Taiwan, R.O.C.
Email:mshwang@nchu.edu.tw

Department of Computer and Information Science[‡]
National Chiao-Tung University
1001 Ta Hsueh Road,
Hsinchu, Taiwan, R.O.C.

Department of Information Management[§]
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.

August 15, 2003

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC91-2213-E-324-003.

[†]Responsible for correspondence: Prof. Min-Shiang Hwang.

A New Anonymous Channel Protocol in Wireless Communications

Abstract

In this paper, the authors shall propose a new anonymous channel protocol for wireless communications. Compared with Juang et al's protocol and Jan et al's protocol, our protocol is more efficient. In addition, our protocol saves the trouble of employing public key cryptography in the anonymous channel ticket authentication phase just as Jan et al's protocol.

Keywords: Anonymous channel, authentication, security, wireless communications.

1 Introduction

Wireless mobile communication is gaining popularity in recent years. People can roam freely and use the mobile service almost everywhere. Thanks to the wireless telecommunication infrastructure, we can enjoy mobile services through portable devices such as cellular phones, PDA, laptops, etc. Mobile service systems are oftentimes called Personal Communication Systems (PC-S's). These modern digital cellular systems include AMPS, GSM [4, 5], IS-54 (TDMA), and IS-95 (CDMA) for voice communication as well as CDPD [3] and GPRS [6] for other forms of data communication.

Current protocols for location management are based on a two-level data hierarchy such that the two types of databases, the home location register (HLR) and the visitor location register (VLR), are involved in tracking an MS. Under such a design the radio scope from the HLR to its MS is called the home network, while the visit network is just the opposite. To integrate all those above, all the protocols we mention in this paper are under the mobile communication system architecture of a GSM-style system.

Through a valid authentication protocol, mobile users can obtain services from wireless communication networks. Much research has been invested in the privacy and authentication of wireless communications [1, 2, 7, 8, 9, 10, 11, 12, 13, 14]. In 1999, Juang et al. proposed an anonymous channel protocol where the mobile station could request services privately under the visit network [11]. This is the so-called unlinkability. However, in their scheme, the visit network alone cannot verify the requester; it requires the assistance of the home network. So, the mobile station must ask the home network to certify the identity and sign an anonymous channel ticket blindly. Then the mobile station and the visit network can authenticate each other via the signed blind ticket.

However, Jan et al. pointed out that Juang et al.'s protocol is traceable and inefficient [10]. According to Jan et al.'s attack, the location anonymity (unlinkability) requirement can be broken because the blind ticket is used time after time and then the anonymous PA (Pseudo Account) is also used time and again. So, the home network gets to know the PA roaming path [10]. Besides, Jan et al. also claimed that their protocol is more efficient than Juang et al.'s protocol in the anonymous channel ticket authentication phase. They could reduce the communication cost by $2m$ each time in the authentication phase, where m is anonymous message's bits [10].

Observing Jan et al.'s protocol, we find that the efficiency of their protocol shows only in the ticket authentication phase. The contribution of Jan et al.'s protocol is reducing the cost in the ticket authentication phase, which is a high frequency phase. However, the need for the data renewal is also large when the ticket is replaced, and furthermore there is no real pattern to this ticket indicating whether time or deadline is used. As a result the computation cost is still more than that of Juang et al.'s protocol in the ticket-issuing phase. In this article, we shall propose a new protocol which is better than Jan et al.'s protocol. Our protocol is more efficient than Juang et al's protocol and the Jan et al.'s protocol.

The rest of this paper is organized as follows. First, our new protocol will be illustrated in Section 2. Then, in Section 3, we shall analyze the security and show the features of our protocol; besides we shall also compare our protocol with the other two protocols. Finally the conclusion will be in the fourth section.

2 The Proposed Protocol

There are two phases, *Anonymous Channel Ticket Issuing Phase* and *Anonymous Channel Ticket Authentication Phase*, in our proposed protocol for wireless communications. The main task of the first phase is that the mobile station (MS) must require the anonymous channel ticket from the home location register (HLR) through the visitor location register (VLR). After receiving the ticket, the MS can use mobile services, such as mobile calls, provided by the VLR. If the MS continues using mobile services from the VLR, it must enter the second phase of our protocol. The second phase is mainly about checking the validity of the anonymous channel ticket. We will describe the details of our protocol in the following subsections. Before the description of our protocol starts, we first show some system symbols in the following table.

2.1 Anonymous Channel Ticket Issuing Phase

In our new protocol, three entities are involved, which are the MS, VLR, and the HLR. The steps of this phase are as follows. The statement $A \Rightarrow B : \{messages\}$ means that the left-hand side entity sends messages to the right-hand side entity.

1. MS $\Rightarrow$ VLR: $\{HD, TN_h, T, (ID_i, T)_{K_{h,i}}\}$

   MS sends VLR the messages HD, the token TN_h issued by HLR, the

Table 1: System symbols of the proposed scheme

Symbol	Meaning
δ	the signed ticket information by HLR
VT	the valid time of the anonymous channel ticket
$Tkt(m)$	the anonymous channel ticket to be used m times
$K_{h,v}$	the shared key between HLR and VLR
$K_{h,i}$	the shared key between HLR and MS (ID_i)
TN_h	the authentication token which HLR issues to MS
HD	the identity of HLR
VD	the identity of VLR
p_h	the public key of HLR
s_h	the secret key of HLR
$\{m\}_{p_h}$	to encrypt the message m by public key cryptosystem using public key p_h
$(m)_k$	to encrypt the message m by secure cryptosystem using symmetric key k

time stamp T, and (ID_i, T), which is encrypted by the shared key $K_{h,i}$.

2. VLR $\Rightarrow$ HLR: $\{VD, TN_h, T, (ID_i, T)_{K_{h,i}}\}$

   VLR passes the received message to HLR, and she/he replaces the HD with the VD. HLR receives the message from VLR and then verifies the identity of MS. HLR finds the shared key of this MS by searching TN_h, and HLR takes this key to decrypt $(ID_i, T)_{K_{h,i}}$. Therefore, HLR can check the identity of the MS, and then HLR calculates the anonymous channel ticket $\delta = \{(ID_i, T)_{K_{h,i}} || VT\}_{s_h}$ and $Tkt(m) = (\delta, m)_{K_{h,v}}$, where $||$ stands for concatenation.

3. HLR $\Rightarrow$ VLR: $\{TN_h, (\delta, n)_{K_{h,v}}, (TN'_h, Tkt(m), m, n)_{K_{h,i}}\}$

   HLR encrypts δ and the seed n by using the key $K_{h,v}$. Then, HLR encrypts the new token $TN'_h, Tkt(m)$, m, and n by using the key $K_{h,i}$. Next, HLR transmits them to VLR. VLR can decrypt the value $(\delta, n)_{K_{h,v}}$ by using the key $K_{h,v}$ and record these parameters δ and n.

4. VLR $\Rightarrow$ MS: $\{TN_h, r, (TN'_h, Tkt(m), m, n)_{K_{h,i}}\}$

Upon receiving the messages from HLR, VLR generates a random value r and passes the messages $\{TN_h, r, (TN'_h, Tkt(m), m, n)_{K_{h,i}}\}$ to MS. VLR records r and the token TN_h of MS.

This phase is mainly that HLR verifies MS's identity and produces the anonymous channel ticket to MS. VLR also receives the proof values from HLR and uses them to negotiate with MS in the ticket authentication phase.

2.2 Anonymous Channel Ticket Authentication Phase

In this phase, MS encrypts the anonymous channel ticket by using the session key computed by r and n. He/She sends the encrypted ticket to VLR. Next, VLR can decrypt and verify the validity of the ticket. After that, MS can use the anonymous service through the authentication of VLR.

1. MS $\Rightarrow$ VLR: $\{TN_h, (Tkt(m))_{f(r\oplus n)}\}$

   MS sends the token TN_h and the anonymous channel ticket $Tkt(m)$ encrypted by the session key $f(r \oplus n)$ to VLR, where $f(\cdot)$ is one-way hash function. Based on the token TN_h, VLR can find the recorded information (r, n, δ) of this MS. VLR can compute the session key $f(r\oplus n)$ and decrypt the anonymous channel ticket $Tkt(m)$. And then VLR can verify the validity of the anonymous channel ticket. Next VLR derives the using time m from $Tkt(m) = \{\delta, m\}_{K_{h,v}}$ and computes the next ticket $Tkt(m-1) = \{\delta, (m-1)\}_{K_{h,v}}$.

2. VLR $\Rightarrow$ MS: $\{TN_h, (Tkt(m-1))_{f((r-1)\oplus n)}\}$

   VLR encrypts the next anonymous channel ticket $Tkt(m-1)$ by using the next session key $f((r-1) \oplus n)$, and VLR sends it to MS. After receiving the message from VLR, MS decrypt the next ticket by using the session key $f((r-1) \oplus n)$. Once the ticket of the using time m is exhausted, MS would request the new anonymous ticket from HLR. In our protocol, we assume that the random value r is bigger than the ticket of the using time m. Therefore, the session key sequences are sufficient. According to the decreasing of the random value r, we can obtain the $(r+1)$ sequences of session keys:

$$\begin{cases} f(r \oplus n) \\ f((r-1) \oplus n) \\ f((r-2) \oplus n) \\ \vdots \\ f(n) \end{cases}$$

This phase is mainly that MS takes the ticket to demand the anonymous channel service from VLR. VLR will deduct the using times from the ticket until the number of times is empty. In such situation, MS shall refresh the ticket by inquiring HLR.

3 Analysis and Comparison

In the first subsection below we will evaluate our protocol in terms of its security and features. Then, in the second subsection, we shall compare the performance of our protocol with those of two other protocols: Juang et al.'s protocol and Jan et al.'s protocol. The comparison will have two parts: the communication cost part and the computation cost part. The communication cost part is mainly to compare the traffic transmission time of the three protocols, and the computation cost part is to compare the total computation time of the three protocols in each phase.

3.1 Security and Feature Analysis

Our protocol can satisfy all the security demands in Jan et al.'s protocol does. Our analysis is as follows.

1. The MS can get the correct anonymous channel ticket from the home network: The ticket is encrypted by the key $K_{h,i}$ shared between MS and HLR, so the VLR or the others cannot derive the ticket. Only the

MS who has the valid secret shared key can decrypt the message and obtain the ticket.

2. The visit network can authenticate the MS and support the anonymous channel service: Based on the anonymous channel ticket and the seed n, VLR can authenticate the MS. Then the MS can send messages to the VLR privately because the message is encrypted by the sequences of session keys under the visit network.

3. The proposed protocol can support the anonymous channel service and the nameless location service: In our protocol, there is no identity information of the MS revealed. Therefore, the unlinkability requirement is achieved in our protocol.

4. There are sequences of session keys between the MS and the visit network: According to the seed n and the random value r, the MS and the VLR can communicate with each other privately by using the un-fixed session key.

5. Real ticket patterns of our anonymous channel ticket: In our protocol, our anonymous channel ticket issued by the HLR exists the real ticket patterns in the actual application. The patterns are like the using time m of the ticket, the expiring period, and the using site.

In the above-mentioned analysis, we mainly focus on the anonymity feature. Because of this feature is the chief point in the anonymous channel protocol including the unlinkability. Then we also think about the other security methods such as symmetric cryptography and using the un-fixed session keys. Last, our ticket form is also satisfying the real ticket patterns.

3.2 Cost Comparisons

In this subsection, we shall compare our protocol with the other two protocols as to the communication cost and the computation cost. First, the communication cost comparison is in Table 2. Since the communication cost is the same in the anonymous channel ticket-issuing phase, we focus only on the anonymous channel ticket authentication phase. The symbol c stands for the count of the transmission time.

Table 2: Comparisons with the communication cost in the ticket authentication phase

Protocols	Communication costs
Juang et al.'s Protocol [11]	$5c$
Jan et al.'s protocol [10]	$3c$
Our protocol	$2c$

In Table 2, the communication costs of Juang et al.'s and Jan et al.'s protocols are separately $5c$ and $3c$. The illustration is depicted in the Ref. [10]. However, the cost of our protocol is just $2c$ because we reduce one step in the ticket authentication phase. In Jan et al.'s protocol [10], they consume three steps on ticket authentication. But our protocol has only two steps to obtain the same effect. We see that Juang et al.'s protocol takes the more communication cost in the ticket authentication phase because their protocol needs the help of HLR in this phase. Without the requirement of the support of HLR, the communication cost of Jan et al.'s protocol is lower. As for our protocol, we take one transmission less than Jan et al's protocol. Therefore, we have the lowest communication cost. Next, we shall show the comparison of computation cost in Tables 3 and 4, the two of which are for the ticket issuing phase and the ticket authentication phase, respectively. The notations used in the tables are defined as follows:

- T_h: the time for computing a hash function.
- T_{inv}: the time for finding the inverse.
- T_{mul}: the time for modular multiplication.
- T_{exp}: the time for modular exponentiation.
- T_{pub}: the time for enciphering/deciphering with an asymmetric cryptosystem.
- T_{sym}: the time for enciphering/deciphering with a symmetric cryptosystem.
- T_{add}: the time for modular addition.

Table 3: Comparisons with the computation cost in the ticket issuing phase

Protocols	Computation costs
Juang et al.'s Protocol [11]	$1T_{pub} + 2T_{sym} + 2T_{exp} + 1T_{inv} + 1T_h + 2T_{mul}$
Jan et al.'s protocol [10]	$1T_{pub} + 3T_{sym} + 6T_{exp} + 2T_h + 5T_{mul} + 2T_{add}$
Our protocol	$1T_{pub} + 4T_{sym}$

In Table 3, we survey the computation costs of Juang et al.'s protocol first [11]. In their ticket issuing phase, we can find these equations: $\Psi = \beta^{e_h}(Tkt) \bmod n_h$, $Cert_i = (T_1, \gamma)_{f(Key_i)}$, and $\{ID_i, \Psi, Cert_i, T_1\}_{e_r}$. The computation costs of these equations are $T_{pub} + T_{sym} + 2T_{exp} + T_h + T_{mul}$ and owing to HLR sends VLR $(\Gamma, N_2)_{K_{vh}}$, therefore, the cost is one T_{sym} in addition. MS receives the blind ticket Γ and check it by $\beta^{-1}\Gamma \bmod n_h$, the costs are thus $T_{inv} + T_{mul}$. Due to above-mentioned statements, we conclude the total computation costs of Juang et al.'s protocol are $T_{pub} + 2T_{sym} + 2T_{exp} + T_{inv} + T_h + 2T_{mul}$.

In Jan et al.'s protocol [10], the computation cost of $\{ID_i, A, B, T, T_{expire}, Cert_i\}_{e_h}$ is $T_{pub} + T_{sym}$. HLR sends VLR, $(d_M, T_{expire}, D_M)_{K_{h,v}}$ and $(C, T_{expire}, E_M)_{K_{h,i}}$, the cost is $T_{sym} + 3T_{exp} + T_h + 4T_{mul} + 2T_{add}$. Next, VLR makes $NEWID = f_2(d_M)$ and sends MS, $(C, T_{expire}, E_M)_{K_{h,i}}$, then MS receives the values from VLR and check them by $g^{E_M} = y_h^{A \cdot K_{h,i}} \cdot C^C \bmod P$. Therefore, the total computation costs are $T_{pub} + 3T_{sym} + 6T_{exp} + 2T_h + 5T_{mul} + 2T_{add}$.

As for the computation cost of our protocol, there are one T_{sym} in $(ID_i, T)_{K_{h,i}}$. Next, HLR computes $\delta = \{(ID_i, T)_{K_{h,i}} || VT\}_{s_h}$ and $Tkt(m) = (\delta, m)_{K_{h,v}}$ to VLR. The costs are $T_{pub} + T_{sym}$. Last, VLR receives $(\delta, n)_{K_{h,v}}$ and $(TN'_h, Tkt(m), m, n)_{K_{h,i}}$ from HLR. The costs are $2T_{sym}$. The total computation costs are thus $T_{pub} + 4T_{sym}$.

We can see the computation cost of Jan et al.'s protocol is still higher than that of Juang et al.'s protocol in the ticket issuing phase because Jan et al.'s protocol needs $6T_{exp}$ while Juang et al.'s protocol takes only $2T_{exp}$. Since T_{exp} is the longest of all the time units defined above, we come to the conclusion that Jan et al.'s protocol consumes the most time in the ticket issuing phase. Our protocol in contrast, needs the shortest computation time.

Table 4: Comparisons with the computation costs in the ticket authentication phase

Protocols	Computation costs
Juang et al.'s Protocol [11]	$1T_{pub} + 2T_{sym} + 1T_{exp} + 2T_h + 2T_{mul}$
Jan et al.'s protocol [10]	$3T_{exp} + 3T_h + 9T_{mul} + 3T_{add}$
Our protocol	$3T_{sym} + 2T_h$

In Table 4, we also view the computation costs of Juang et al.'s protocol first [11]. Because MS makes $\{K_{sh}, r_i\}_{e_r}$ to VLR, VLR pass it to HLR. Then HLR computes the session key K_i by $h(K_{sh} \cdot r_i)$ and sends VLR, $(K_i, r_i, PA, lifetime, N_4)_{K_{vh}}$. Next, VLR sends MS, $(I_i, r_i)_{K_i}$. Therefore, we can obtain the computation costs are $T_{pub} + 2T_{sym} + T_h$. Furthermore, HLR makes $K'_{sh} = (Tkt')^{d_h}$ and VLR produces $(K'_{sh})_{h(K_{sh})}$ both for ticket renewal. The costs are thus $T_{exp} + T_h + 2T_{mul}$. We can judge the total computation costs are $T_{pub} + 2T_{sym} + T_{exp} + 2T_h + 2T_{mul}$.

In Jan et al.'s protocol [10], the computation costs of $NEWID, J, L$ are $3T_{exp} + 3T_h + 9T_{mul} + 3T_{add}$. As regards our protocol, we has the computation costs $3T_{sym} + 2T_h$ for that MS sends VLR, $(Tkt(m))_{f(r\oplus n)}$, VLR computes $Tkt(m-1) = \{\delta, (m-1)\}_{K_{h,v}}$, and VLR transmits $(Tkt(m-1))_{f((r-1)\oplus n)}$ to MS.

The computation cost of Jan et al.'s protocol is lower than that of Juang et al.'s cost because the former protocol needs no assistance of HLR and no public key cryptosystem. Although we use the symmetric key encryption in our ticket authentication phase, our computation cost is still lower than that of Jan et al.'s scheme. We have the best efficiency because the time unit T_{sym} stands for a cost lower than T_{exp}. Altogether, our protocol is the most efficient of the three.

4 Conclusion

In this paper, we have proposed a new anonymous channel protocol for wireless communications. Compared with two well received protocols, our protocol is quite efficient. In addition, the session key between MS and VLR is variable in our anonymous channel ticket authentication phase.

Acknowledgements

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC91-2213-E-324-003.

References

[1] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks," *IEEE Personal Communications*, vol. 1, no. 1, pp. 24–31, 1994.

[2] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," *IEEE Journal on Selected Areas in Communications*, vol. 11, pp. 821–829, Aug. 1993.

[3] CDPD Forum. "Cellular digital packet data (CDPD) system specification,". Tech. Rep. Release 1.1, CDPD Forum, Jan. 1995.

[4] ETSI. "Recommendation GSM 02.09: Security related network functions,". tech. rep., European Telecommunications Standards Institute, ETSI, June 1993.

[5] ETSI. "Recommendation GSM 03.20: Security related network functions,". tech. rep., European Telecommunications Standards Institute, ETSI, June 1993.

[6] H. Granbohm and J. Wiklund, "GPRS - general packet radio service," *Ericsson Review*, vol. 76, no. 2, pp. 82–88, 1999.

[7] Min-Shiang Hwang and Chii-Hwa Lee, "Authenticated key-exchange in a mobile radio network," *European Transactions on Telecommunications*, vol. 8, no. 3, pp. 265–269, 1997.

[8] Min-Shiang Hwang and Chii-Hwa Lee, "Secure access schemes in mobile database systems," *European Transactions on Telecommunications*, vol. 12, no. 4, pp. 303–310, 2001.

[9] Min-Shiang Hwang and Wei-Pang Yang, "Conference key distribution protocols for digital mobile communication systems," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 2, pp. 416–420, 1995.

[10] Jinn Ke Jan and Whe Dar Lin, "An efficient anonymous channel protocol in wireless communications," *IEICE Transactions on Communication*, vol. E84-B, pp. 484–491, March 2001.

[11] W. S. Juang, C. L. Lei, and C. Y. Chang, "Anonymous channel and authentication in wireless communication," *Computer Communications*, vol. 22, pp. 1502–1511, 1999.

[12] Chii-Hwa Lee, Min-Shiang Hwang, and Wei-Pang Yang, "Enhanced privacy and authentication for the global system of mobile communications," *Wireless Networks*, vol. 5, pp. 231–243, July 1999.

[13] H. Lin and L. Harn, "Authentication protocols for personal communication system," *ACM SIGCOMM'95*, pp. 256–261, Aug. 1995.

[14] R. Molva, D. Samfat, and G. Tsudik, "Authentication of mobile users," *IEEE Network*, vol. 8, no. 2, pp. 26–34, 1994.