Mutually Identity Authentications in GSM-based Anonymous Communications

Shiuh-Jeng Wang[1,*], Yuh-Ren Tsai[2], Lei-Sheng Chou[3], and I-Shan Lin[4]

[1,4] Department of Information Management,
Central Police University
Taoyuan 333, Taiwan

[2,3] Institute of Communications Engineering
National Tsing Hua University
Hsinchu 300, Taiwan

sjwang@mail.cpu.edu.tw

Received 29 March 2007; Revised 22 April 2007 ; Accepted 24 May 2007

Abstract. The Global System for Mobile Communication (GSM) is widely regarded as the most convenient digital mobile communications system. However, there are many problems relating to data confidentiality, user privacy, and computational load. This paper provides solutions to these problems without changing the architecture of the GSM. Our secure level is analyzed by a formal method of the BAN-logic regulations. Besides, our scheme provides an anonymous channel for user location privacy.

Keywords: Authentication, Wireless security, Mobile communications, GSM

1 Introduction

Today the Global System for Mobile Communications (GSM) [2] is the most popular standard for mobile phones in the world. The GSM system has undergone some very important changes. First, all the transmission signals are digital. Second, The GSM protects the transmitting messages by encryption. Third, the GSM system authenticates the subscriber, thereby ensuring that only legal subscribers can log into the network.

Today's GSM is the second generation mobile communications system [3], [4]. The main difference with the first generation, AMPS (Advanced Mobile Phone System), is that GMS transmits digitalized messages, while the AMPS is an analog system like the general telephone. The AMPS transmits via air-waves, so if anyone had the same equipment and frequency, they could intercept the signal and eavesdrop, even send a fake message to others or embezzle subscribers' accounts. The AMPS sends and receives messages by analog signal and plaintext, so crooks can easily get the contents of the communication without being detected [5], [6], [7].

In [8], the author proposed an anonymous channel on the GSM system based on a public key system [9], [10]. In it he utilizes a ticket issuing phase and ticket utilization phase to achieve an anonymous channel. In the ticket issuing phase, the author uses an asymmetric encryption/decryption systems and timestamps [11], [12] to protect against replay attack. By using an asymmetric key system the security level is raised, but it will also quickly deplete the available energy in mobile stations which is supplied by batteries. In addition, the author used timestamps T and Texpire to define ticket valid time intervals, which depends on time synchronization between network ends and mobile ends.

Modifying data, abusing the service and stealing information from a subscriber's account are the most serious problems that may happen in electronic communication. Consequently, security is very important to Mobile Communications. The GSM system has it own secret code and system of authentication to encrypt the messages, and only those who have been authenticated can decrypt and get the message. The GSM addresses several points of security, and they are as follows.

[*] Correspondence author

1. It protects networks from being used by unauthenticated subscribers.
2. It protects the subscribers' private information.
3. Base stations provide authentication if a mobile station has qualifications to log into the network.
4. The information has confidentiality during transmitting.
5. The confidential location of a mobile station is considered.

This paper presents a method to improve the GSM authentication in networks to make the system work efficiently. Our security is based on a symmetric key [13] and the *A3*, *A5* and *A8* algorithm in the original GSM architecture. We propose four important items to improve the original authentication protocols. First, the new architecture will be unable to reveal a subscriber's International Mobile Subscriber Identity (IMSI for short) and it protects the IMSI from being eavesdropped upon through the air medium. This new architecture is called anonymous communication [14], [15]. Let's assume that an intruder does not know the real location of the subscriber, and impersonates a legal subscriber to access the network by obtaining the IMSI, meaning the confidential location of the mobile station and the subscriber. Although our proposed method increases the message size which sent to the Visitor Location Register (VLR for short) from the MS, it increases the security level of the system, too. The second item is that we break the concept of inter-domain and intra-domain [16], [17]. The third item is that we can save overhead space on the VLR in this paper [18]. The last item is the most important one. We can provide mutual authentication between the MS and the VLR and protect the legal subscribers from the deceptions by the VLR/BS (Base Station).

The main purpose of the research in mutual authentications [19] and anonymous communications in the GSM system is to solve the subscriber's problem of unwillingly leaking his/her identity in a wireless environment and providing the MS authentication to the VLR and the Home Location Register (HLR for short) in the network. Some papers use a public key system to provide anonymity. Using a public key in wireless communication will increase the computational time and causes high battery power consumption in a mobile device. It has been proposed to access an anonymous channel by purchasing a ticket. This poses a large problem with time synchronization in the mobile network. If the mobile and the network time are not synchronized, then the ticket expires and results in the mobile subscriber failing to register. Another problem is that extending the valid date of the ticket can solve the time mismatch, but that may give intruders enough time to use a valid ticket to impersonate the ticket owner.

In the current GSM system, the MS sends the IMSI using plaintext to the VLR by radio channel when the MS first registers. This makes it easy for the subscriber's identity to be eavesdropped upon by some intruders via radio access methods. For example, the VLRs of region *A* can directly access the information from the HLR of region *B* when it is different from region *A*.

The rest of the paper is organized as follows. Sec. 2 describes the original GSM architecture and the related research. In Sec. 3, we propose an efficient authentication protocol for the GSM system. Sec. 4 analyzes the security of the proposed protocol. Finally, we draw our conclusions in Sec. 5.

2 Preliminaries

2.1 The GSM architecture

2.1.1 Original GSM authentication

In consideration of the background understanding to get more familiar with our scheme, the procedure of GSM authentication is reviewed as follows and the architecture is then shown in Fig. 1.

Step 1: When the mobile phone is turned on for the first time or turned on after being turned off for 48 hours, the MS will send the *IMSI* to the VLR as identification or send the *TMSI* (Temporal Mobile Subscriber Identity) to be saved in the mobile phone.

Step 2: When the VLR gets the *IMSI* from the MS, it will forward this message to the upper HLR to produce the authentication vector. If it gets the *TMSI*, the VLR will find out the corresponding *IMSI*, and then send it to the correct HLR.

Step 3: After the HLR receives the *IMSI*, it will find out all of the data corresponding to the *IMSI*, like K_i. Next the HLR generates a set of $\{(RAND_l, SERS, K_c)| l=1,2,...,5\}$, i.e. 5 triples are generated, and then sends the 5 triples to the VLR, where $RAND_l$ is the random number (there are 5 distinct *RANDs*) and $SERS=A3(RAND_l, K_i)$ and $K_c = A8(RAND_l, K_i)$.

Step 4/Step 5: After the VLR receives 5 triplets, it will pick a triplet to authenticate the subscriber. At first, the VLR sends a *RAND* to the subscriber, and the subscriber receives it. The subscriber withdraws K_i and calculates *SRES* (Signature Response) and K_c with the *A3* and *A8* algorithms and sends the *SRES* to the VLR for comparison. If the result is the same, the VLR will take the K_c as the session key to encrypt the *TMSI* to the subscriber. As soon as the subscriber receives the *TMSI*, it means that the authentication is successful and that the network ends can communicate with the subscriber. Otherwise, the VLR will suspend the procedure.

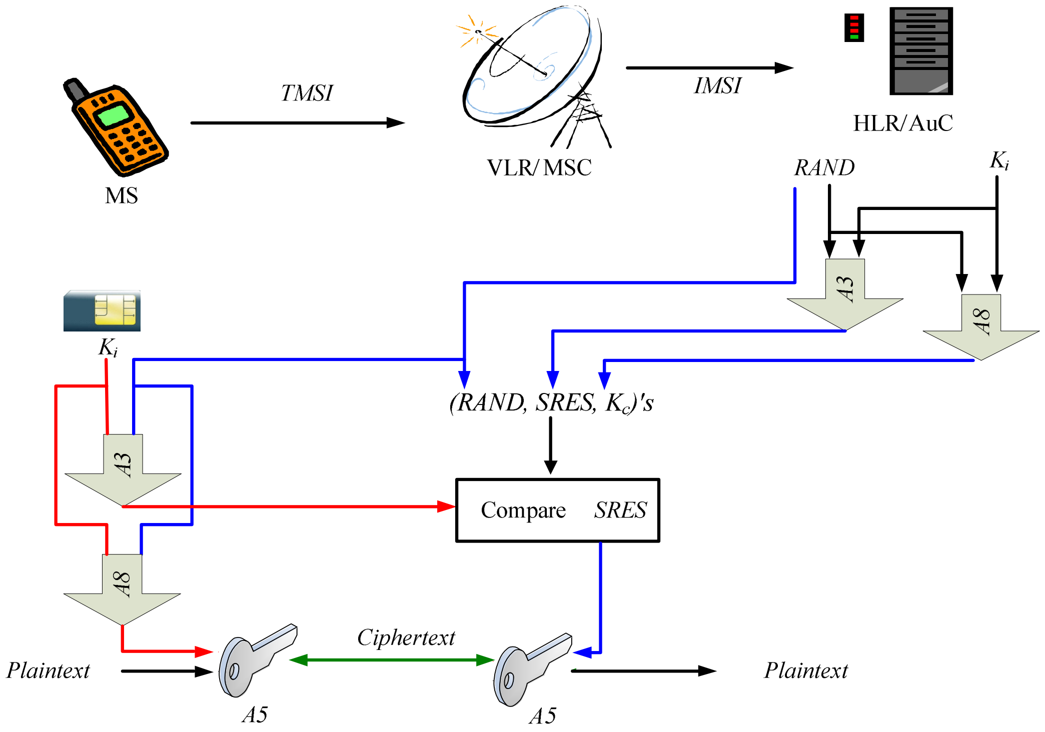

Fig. 1. The original GSM authentication protocol

2.1.2 Drawbacks of the GSM Security

There are crucial security flaws in the original GSM [17]:

1. When the mobile phone is turned on for the first time or turned on after having been turned off for 48 hours the subscriber will explore the IMSI in the wireless environment and it allows unscrupulous subscribers to eavesdrop IMSI via the radio route.
2. The procedure is only mentioned in Sec. 2.1 because the GSM system wants to authenticate the subscribers who want to access the network. This also makes it easy for unscrupulous subscribers to pretend to be the legal system without authentication.
3. In the information part, there are no procedures and mechanisms in the GSM to ensure the integrity of the information or to verify that the information is not modified.
4. An A5 algorithm is a lower security level, and the length of Kc is 64 bits. This will create a security problem which the length of Kc if it is not long enough.
5. The VLR needs to store 5 sets of triplets for each subscriber in its location, and cause a problem of space overhead.
6. Subscribers might use all of the 5 sets of triplets in the VLR if they communicate many times. So the VLR has to request new 5 sets of triplets from the HLR, and this may cause a system overload.

2.2 The Lee-Hwang-Yang Authentication Protocols for Mobile Communications

In [19], [20], the authors wanted to reduce the amount of information and decreased the stored sensitive information of the MS in the database of the VLR for the GSM. One of our concerns in the GSM authentication protocol is the fact that the traffic depends on internet security that is transferred by the VLR and the HLR. Therefore, the author proposes a method to increase security and solve some problem in existing system. The improved method is described in Fig. 2.

During the authentication process, the MS requests authentication, the HLR sends a provisional K_i (PK_i for short) and the *RAND* instead of sending a set of triplets *(RAND, SRES,* K_c*)* to the VLR. The PK_i is generated by the *RAND* and a PK_i as input with *A3* algorithm. When the VLR receives a message from the HLR, it decrypts the message with the associated secret key and then gets the *RAND* and PK_i. At that moment, the VLR generates another random number $RAND_1$ and computes the $SRES_1$, using the *A5* algorithm, using the $RAND_1$ and PK_i. It is finished by the VLR, and the VLR sends two random number *RAND* and $RAND_1$ to the MS in plaintext form to verify the identity of the MS. $RAND_1$ is generated by the VLR for the first call set-up of the MS. As the MS gets the message from the VLR, the MS computes two values, one is the provisional key PK_i, the other one is $SRES_1$ which is generated, with an A8 algorithm, by PK_i and $RAND_1$ as input. The MS signs the resulting $SRES_1$ and sends it back to the VLR to check if the VLR is able to certify the subscriber as a legal one. The authentication is then shown in Fig. 2 below.

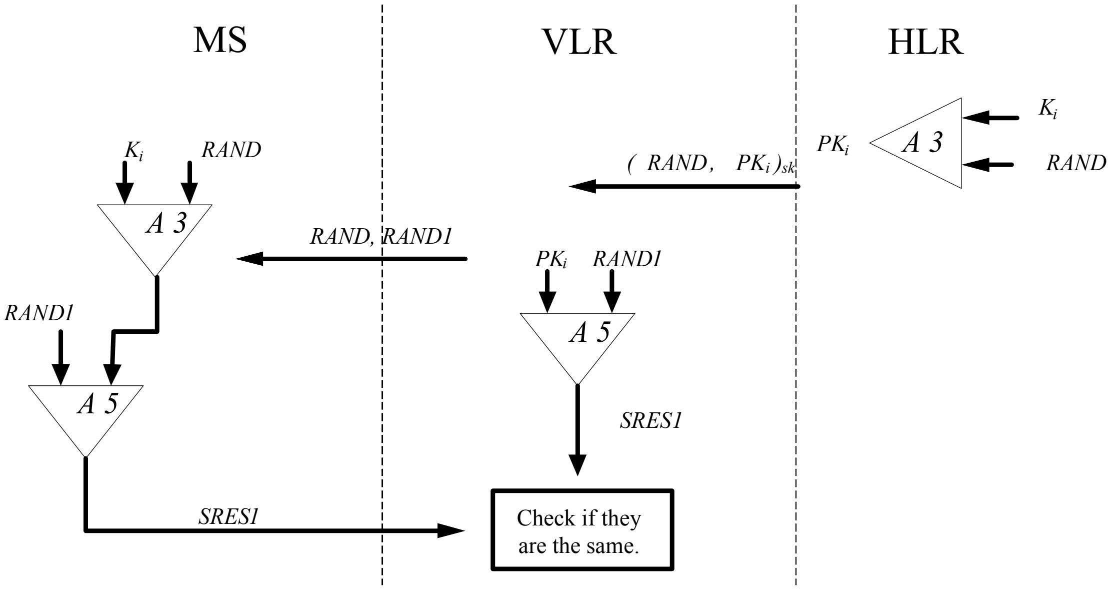

Fig. 2. Authentication of MS in Lee-Hwang-Yang's scheme

2.3 Peinado Authentication Protocol for the GSM

In [8], Peinado proposed an authentication and anonymous channel in the GSM. The main objective of the new protocol is to permit the legal subscribers anonymous access to the network resources, preventing illegal subscribers from accessing the system and to use the private key and public key for some unspecified asymmetric cryptosystem. The protocol has two phases: the ticket issuing phase and the ticket utilization phase. A detailed description is given below.

2.3.1 Ticket Issuing Phase

In this phase, the MS must prepay a ticket from the HLR. Therefore, the MS can use this ticket to authenticate the HLR. After the ticket generation, the HLR can authenticate the MS. The stated protocol is given as follows, and is shown in Fig. 3.

Step 1. $MS \rightarrow VLR:\ N_1, HD, \{ID_i,\ T,\ T_{\exp ire},\ Cert_i\}_{e_h}$,

where N_1 is a random number, T and T_{expire} are the timestamps, and $Cert_i = A3(K_i,(ID_i,T,T_{expire}))$ is the authentication certification. In this step, the MS sends request authentication information to the HLR which is passed on by the VLR. The MS encrypts the authentication data using the HLR's public key e_h.

Step 2. $VLR \rightarrow HLR:\ N_1, \{ID_i, T, T_{\exp ire}, Cert_i\}_{e_h}$.

The VLR forwards the message to the HLR and checks if the N_1 is repeating or not.

Step 3. $HLR \rightarrow VLR:\ N_1, Auth\_VLR_h, T, IK_i, T_{\exp ire}$,

where $(Auth\_VLR_h, IK_i, T_{\exp ire})$ is the ticket generated by HLR, and *Auth_VLR$_h$=A3(K$_i$,T), IK$_i$ =A3(K$_i$,T$_{expire}$)*. It is very important that the message be transmitted by a secure channel.

Step 4. $VLR \rightarrow MS:\ N_1, Auth\_VLR_h, T, T_{\text{expire}}$.

In this step, the VLR broadcasts the messages to every subscriber that only has the correct K_i and can confirm the messages.

Step 5. The MS checks the N_1 and the ticket validity by *Auth_VLR$_h$=A3(K$_i$,T)* and *IK$_i$ =A3(K$_i$,T$_{expire}$)* upon *A3* algorithm.

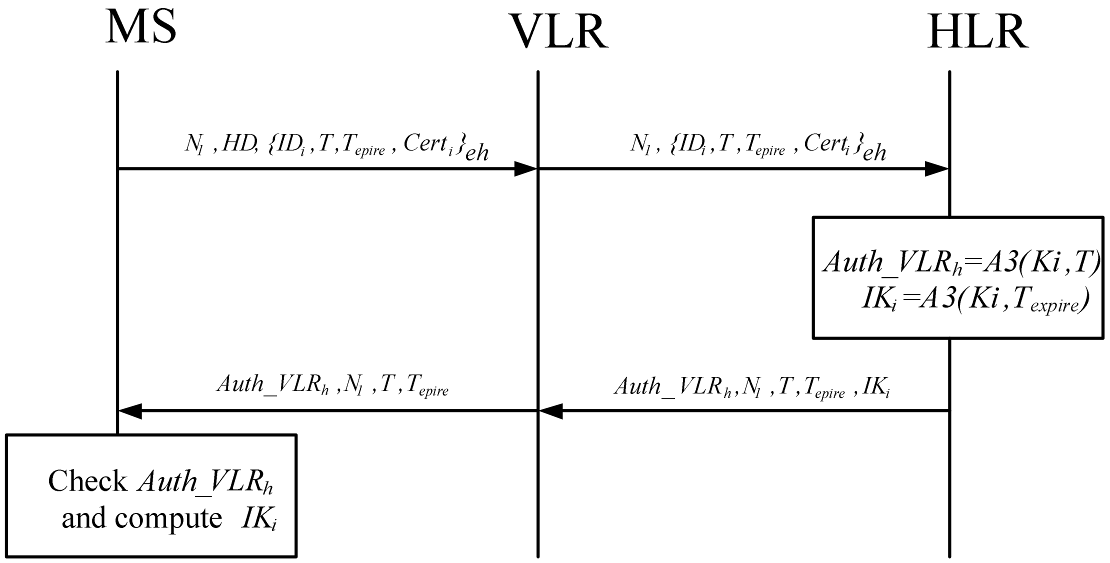
MS
VLR
HLR
N_1 ,HD, {ID_i ,T,T_{epire} , $Cert_i$}$_{eh}$
N_1 , {ID_i ,T,T_{epire} ,$Cert_i$}$_{eh}$
$Auth\_VLR_h$=A3(Ki,T)
IK_i=A3(Ki,T_{expire})
$Auth\_VLR_h$,N_1 ,T,T_{epire}
$Auth\_VLR_h$,N_1 ,T,T_{epire} ,IK_i
Check $Auth\_VLR_h$
and compute IK_i

Fig. 3. Ticket issuing phase

2.3.2 The Ticket Utilization Phase

When a mobile finishes the ticket issuing phase, it gets a valid ticket which is generated by the HLR, it then proceed to access an anonymous channel. The method is briefly outlined below, and shown in Fig. 4.

Step 1. $MS \rightarrow VLR:\ Auth\_VLR_h, T_{\exp ire}, A$, where *A=A5(IK$_i$,RAND$_m$)*, *RAND$_m$* is a random number chosen by the MS.

Step 2. $VLR \rightarrow MS:\ RAND_i, RAND_m$. After VLR receiving a request from the MS, the VLR decrypts A to get a *RAND$_m$* and selects the *IK$_i$* corresponding to the pair of *(Auth_VLR$_h$, T$_{expire}$)*. Then, the VLR computes *SRES=A5(TK$_i$,RAND$_i$)* and sends *RAND$_i$* to the MS.

Step 3. $MS \rightarrow VLR$: $SRES_m$. The MS computes $SRES_m$ by IK_i and $RAND_i$ and then sends $SRES_m$ to the VLR.

Step 4. The VLR checks the correctness of $SRES_m$. In this method, the HLR does not participate in the authentication phase. The communication session key K_c is generated by $A8(IK_i, RAND_i)$ and shared with MS and the VLR.

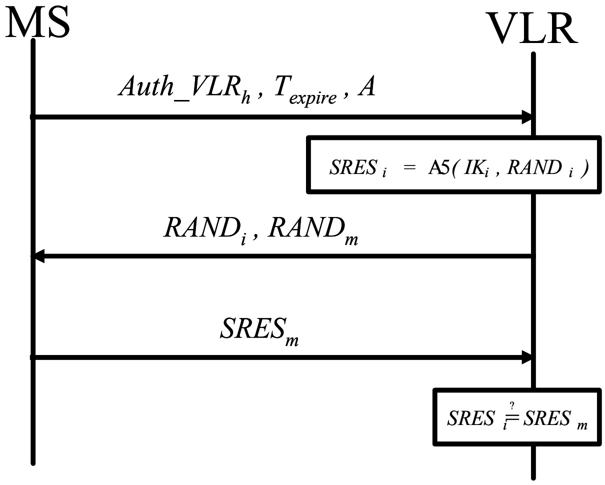
MS
VLR
$Auth\_VLR_h$, T_{expire}, A
$SRES_i = A5(IK_i, RAND_i)$
$RAND_i$, $RAND_m$
$SRES_m$
$SRES_i \overset{?}{=} SRES_m$

Fig. 4. Ticket authentication phase

3 Our Scheme

3.1 Notations

First of all, we will interpret some parameters and functions before discussing the main proposition.

1. $V=\{VLR_1, VLR_2, \cdots, VLR_i, \cdots\}$: A set V containing all of the VLRs in the wireless systems.
   $H=\{HLR_a, HLR_b, \cdots, HLR_j, \cdots\}$: A set H containing all of the HLRs in the wireless systems.
2. f: A function to generate a necessary key used in our protocol.
3. K_j: A master key of the HLR_j, where $HLR_j \in H$.
4. K_c: A session key which is used in each communication.
5. $h(\bullet)$: A one-way hash function.
6. K_{ms}=A8(N_{ms}, K_i): A subscriber's secret key. It is devoted to encrypt nonce.
7. TK_i =A8(N_{ms}, K_i): A key which is kept by both the MS and HLR.
8. K_c =h($RAND$, TK_i): A session key which is computed by the $RAND$ and the TK_i.
9. $SRES$=A3(N_{ms}, K_i): A response which is calculated from MS.

3.2 The Environment Setting

The effects are as follows. In the beginning, the HLR will save a random number R in the subscriber's SIM card as well as in the database. The existence of R is just like a secret key. It is as important as K_i for supporting the anonymity of the subscribers, and the subscriber pre-stores the identity of the HLR in the mobile device. While completing the initial authentication phase, the HLR will produce a new R' to replace the old R inside the mobile station. Therefore, MS will update the new pseudonym $h(IMSI||R')$ which pre-store inside the subscriber device.

This scheme does not divide the subscriber's area into inter-domains and intra-domains. The definition of inter-domain is the subscriber roams in the certain area of VLR, which was not subscriber registered at first. For example, if there is a subscriber who used the mobile phone to register abroad had already registered in Taiwan, the HLR would be different between the overseas one and the local one, and is referred to as inter-domain. Intra-domain means that the HLR must be the original one when a subscriber sends an application of request. For example, if a subscriber has registered in Taiwan and then s/he asks for the other permissions in the other areas of Taiwan. That is what we refer to as intra-domain.

The main idea of this proposition states that the GSM system must have the Key Distribution Center (KDC for short). The function of the KDC puts the secret keys K_{v_h}'s, in all VLR HLRs. All the VLRs must keep all the secret keys of the HLR secret, but the HLR does not store any secret key. The HLR can compute the secret key K_{v_h} that only has the VLR's identity and master key. The ratio of HLR over VLR in the general wireless systems is approximately 20 to 1. This is the reason that more overhead can be saved in the HLR.

Fig. 5 shows the three areas which are controlled by HLR_a, HLR_b and HLR_c, where VLR_1 and VLR_2 are covered in the service area of HLR_b, VLR_6 and VLR_7 are in HLR_a, and VLR_3 VLR_4 and VLR_5 are all in HLR_c. VLR_1 stores K_{v1_ha}, K_{v1_hb} and K_{v1_hc} corresponding to HLR_a, HLR_b and HLR_c respectively. Other VLRs are similar to this. HLR_a only has a master key K_a in its database and keeps it secret. HLR_a can compute a secret key, $K_{vi\_ha}=f(VLR_1.ID, K_a)$, where $VLR_1.ID$ is the identity of VLR_1 and K_a is the mater key in HLR_a.

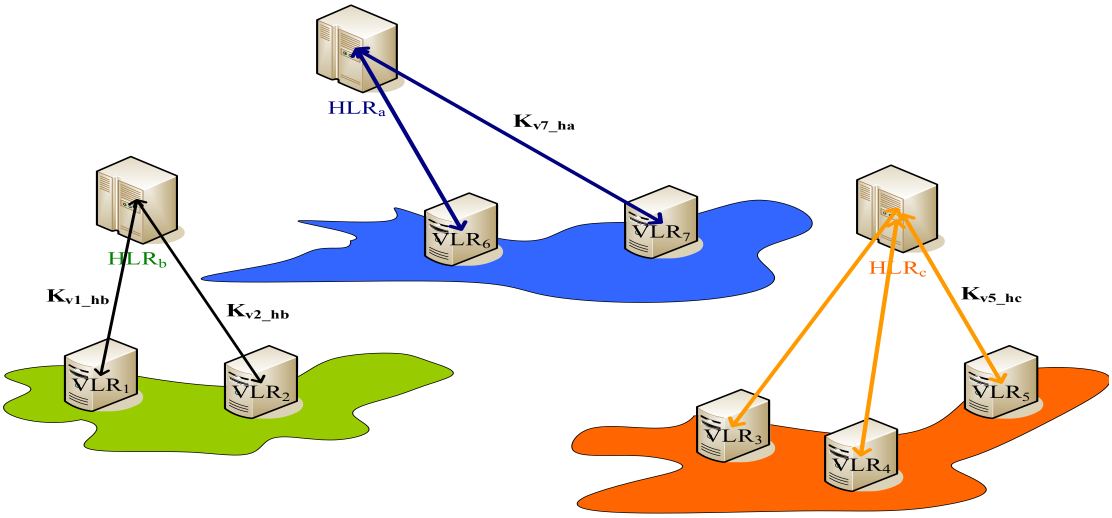

Fig. 5. Topology for the improved GSM

3.3 Enhancement Authentication Protocol for the GSM System

3.3.1 The Initial Authentication Phase

At first, the MS generates nonce N_{ms} and calculates $h(N_{ms})$ and $h(IMSI||R))$, where R is pre-stored in the SIM card. Then the messages of $h(N_{ms})||\{N_{ms}\}_{Kms}$, $h(IMSI||R)$, and HLR_r.ID are sent to the local VLR. The identity of the HLR is considered in the set of messages, since we want to ensure that the message set is sent to the correct HLR. The functionality of $h(IMSI||R)$ is to provide anonymity. The entire procedure is shown in Fig. 6.

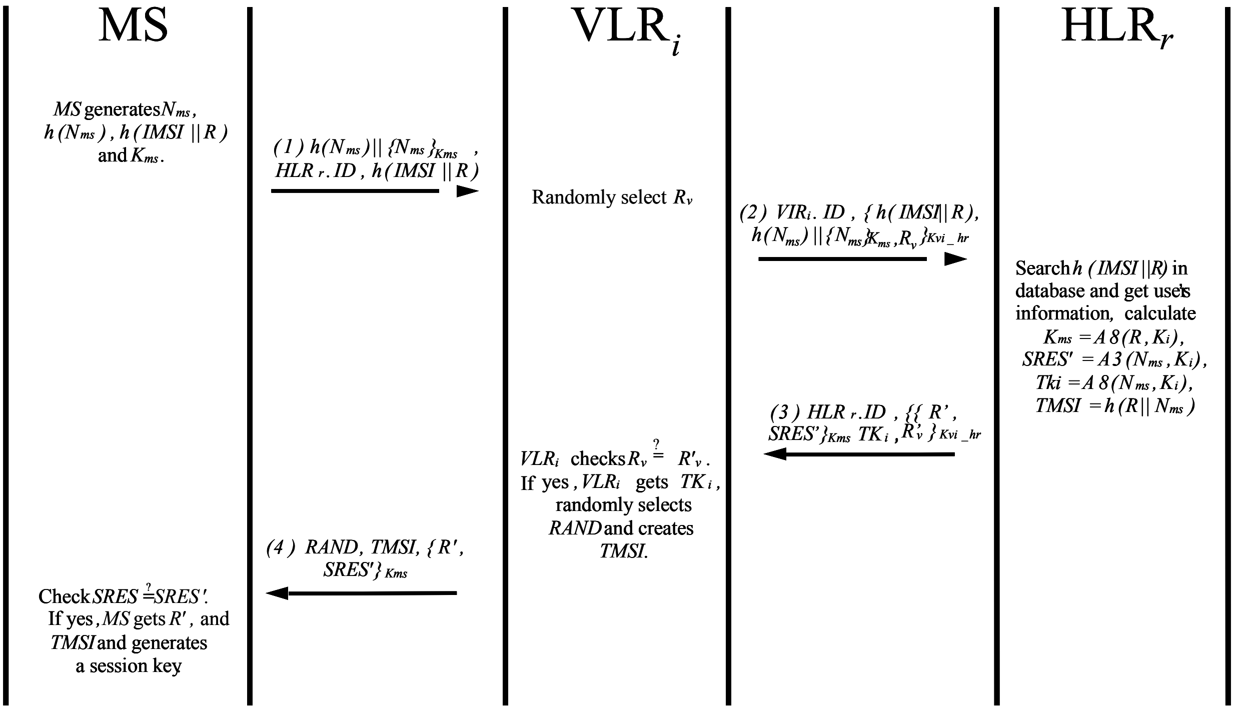
MS
VLR$_i$
HLR$_r$
MS generates N_{ms}, $h(N_{ms})$, $h(IMSI \| R)$ and K_{ms}.
(1) $h(N_{ms}) \| \{N_{ms}\}_{K_{ms}}$, $HLR_r.ID$, $h(IMSI \| R)$
Randomly select R_v
(2) $VlR_i.ID$, $\{h(IMSI \| R), h(N_{ms}) \| \{N_{ms}\}_{K_{ms}}, R_v\}_{Kvi\_hr}$
Search $h(IMSI \| R)$ in database and get user's information, calculate $K_{ms} = A8(R, K_i)$, $SRES' = A3(N_{ms}, K_i)$, $Tki = A8(N_{ms}, K_i)$, $TMSI = h(R \| N_{ms})$
(3) $HLR_r.ID$, $\{\{R', SRES'\}_{Kms}\ TK_i, R'_v\}_{Kvi\_hr}$
VLR_i checks $R_v \overset{?}{=} R'_v$. If yes, VLR_i gets TK_i, randomly selects $RAND$ and creates $TMSI$.
(4) $RAND$, $TMSI$, $\{R', SRES'\}_{Kms}$
Check $SRES \overset{?}{=} SRES'$. If yes, MS gets R', and $TMSI$ and generates a session key

Fig. 6. The initial authentication phase

3.3.2 The Subsequence Authentication Phase

After the initial authentication phase has been completed, the user can be permitted to talk to the VLR_i through the TMSI. At the beginning, the MS sends the TMSI and the N_a to the local VLR. The VLR then obtains all the information from the TMSI and generates RAND for the MS. The user calculates $N_c = (N_a \oplus RAND)$ after receiving RAND and generates session key K_c via N_c and TK_i. The MS encrypts the $RAND+1$ with K_c and forwards it to the VLR. The VLR decrypts the message by K_c. If the random number is the same as the past one, the authentication will fail. Otherwise, the VLR believes the MS is the legal user. See Fig. 7 for the message transmissions in this phase.

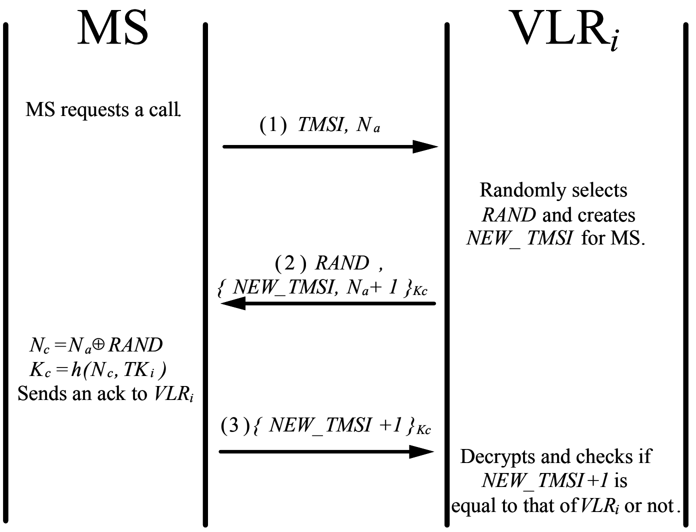
MS
VLR$_i$
MS requests a call.
(1) $TMSI$, N_a
Randomly selects $RAND$ and creates NEW_TMSI for MS.
(2) $RAND$, $\{NEW\_TMSI, N_a+1\}_{Kc}$
$N_c = N_a \oplus RAND$
$K_c = h(N_c, TK_i)$
Sends an ack to VLR_i
(3) $\{NEW\_TMSI + 1\}_{Kc}$
Decrypts and checks if NEW_TMSI+1 is equal to that of VLR_i or not.

Fig. 7. The subsequence authentication phase

4 Discussions

4.1 Security Analysis

4.1.1 Analysis of the Proposed Protocol with BAN-logic

The BAN-logic [1] is utilized as the basis to analyze our protocols. The BAN-logic is devoted to offer a more formal proof with a high-level security. We would translate our proposed protocols to an idealized form and give some reasonable assumptions before analyzing the protocols. The BAN-logic adopted in our scheme is given in 5 steps shown as follows before its analysis [1].

1. Address the initial security assumptions in the statements of BAN-logic.
2. Idealize the protocol in the statements of the formal logic.
3. Use the productions and rules of the logic to reduce the unnecessary predicates in the original protocol and deduce the efficient predicates.
4. Illustrate the statements that have proved by this process.
5. Check the analysis to reach the security level.

According to real conditions, we consider 9 assumptions shown in Fig. 8 shown as follows.

$$\begin{array}{l}
a.\ MS\ believes\ MS \xleftrightarrow{Kms} HLR_r.\\
b.\ VLR_i\ believes\ VLR_i \xleftrightarrow{Kvi\_hr} HLR_r.\\
c.\ HLR_r\ believes\ MS \xleftrightarrow{Kms} HLR_r.\\
d.\ HLR_r\ believes\ VLR \xleftrightarrow{Kvi\_hr} HLR_r.\\
e.\ VLR_i\ believes\ (\ HLR_r\ controls\ MS \xleftrightarrow{K_c} VLR_i).\\
f.\ MS\ believes\ (\ HLR_r\ controls\ MS \xleftrightarrow{K_c} VLR_i).\\
g.\ MS\ believes\ fresh(N_{ms}).\\
h.\ VLR_i\ believes\ fresh(R_v).\\
i.\ VLR_i\ believes\ fresh(RAND).
\end{array}$$

Fig. 8. Assumptions with BAN-logic presented in our protocol

Following up the assumptions, the idealized forms are then translated and shown in Fig. 9 as follows.

$$\begin{array}{lll}
\text{step 1:} & MS \rightarrow VLR_i & :\ (N_{ms})_{Kms},\ <IMSI>_R\ .\\
\text{step 2:} & VLR_i \rightarrow HLR_r & :\ ((N_{ms})_{Kms},\ <IMSI>_R,\ R_v)_{Kvi\_hr}.\\
\text{step 3:} & HLR_r \rightarrow VLR_i & :\ ((R', SRES)_{Kms}, MS \xleftrightarrow{Kc} VLR_i,\ R_v+1)_{Kvi\_hr}.\\
\text{step 4:} & VLR_i \rightarrow MS & :\ RAND,\ (MS \xleftrightarrow{Kc} VLR_i,\ <N_{ms}>_{Ki})_{Kms}.\\
\text{step 5:} & MS \rightarrow VLR_i & :\ (RAND+1)_{Kc}.
\end{array}$$

Fig. 9. The ideal form

As the postulates defined in the BAN-logic analysis, a derivation can be deduced by the step 3 in Fig. 9 and assumption (*a*) upon the <u>*message-meaning rule*</u>:

$$\begin{gathered} VLR_i \textit{ believes } HLR_r \textit{ said} \\ (MS \xleftrightarrow{Kc} VLR_i, < N_{ms} >_{Ki})_{Kms}, MS \xleftrightarrow{Kc} VLR_i,\ R_v \end{gathered} \qquad (1)$$

Statement (1) can be then transformed to the following statement.

$$VLR_i \textit{ believes } HLR_r \textit{ said } MS \xleftrightarrow{Kc} VLR_i,\ R_v \qquad (2)$$

By the statement (2) and assumption *(h),* a new statement can be derived as follows upon the <u>*nonce-verification rule*</u>:

$$VLR_i \textit{ believes } HLR_r \textit{ believes } MS \xleftrightarrow{Kc} VLR_i \qquad (3)$$

By the statement (3), assumption (*e*), the next statement is obtained upon the <u>*jurisdiction rule*</u>:

$$VLR_i \textit{ believes } MS \xleftrightarrow{Kc} VLR_i \qquad (4)$$

According to the step 4 in Fig. 9, the form of

$$MS \text{ sees } RAND,\ \{MS \xleftrightarrow{Kc} VLR_i,\ < N_{ms} >_{K_i}\}_{K_{ms}}$$

is explained. By the explained form and the assumption (*a*), we can obtain the statement shown as follows upon the <u>*message-meaning rule*</u>:

$$\begin{gathered} MS \textit{ believes } HLR_r \textit{ said} \\ MS \xleftrightarrow{Kc} VLR_i,\ < N_{ms} >_{Ki} . \end{gathered} \qquad (5)$$

By the statement (5) and assumption (*g*), the following statement can be derived upon the <u>*nonce-verification rule*</u>:

$$MS \textit{ believes } HLR_r \textit{ believes } MS \xleftrightarrow{Kc} VLR_i \qquad (6)$$

By the statement (6) and assumption (*f*), we can then derive the statement shown as follows using the <u>*jurisdiction rule*</u>:

$$MS \textit{ believes } MS \xleftrightarrow{Kc} VLR_i \qquad (7)$$

Observe (4) and (7). It turns out that MS and *VLR_i* shares a session key with each other. In the following derivations, we further deduce a fact that the same session key is shared between MS and VLR_i. According to the step 5 in Fig. 9, the VLR_i receives message from the MS. It means that

$$VLR_i \textit{ sees } \{MS \xleftrightarrow{Kc} VLR_i, RAND\}_{K_c} \qquad (8)$$

By the statement (8) and the statement (4), a statement can be derived upon <u>*message-meaning rule*</u>:

$$\begin{gathered} VLR_i \textit{ believes } MS \textit{ said} \\ MS \xleftrightarrow{Kc} VLR_i, RAND+1. \end{gathered} \qquad (9)$$

By the statement (9) and the assumption (*i*)

$$VLR_i \ believes \ MS \ believes \ MS \xleftrightarrow{Kc} VLR_i \qquad \textbf{(10)}$$

Due to MS successfully obtains the message from the VLR_i, MS, therefore, believes that VLR_i holds the session key the same as that of oneself. In other words, the statement is derived as follows.

$$MS \ believes \ VLR_i \ believes \ MS \xleftrightarrow{Kc} VLR_i \qquad \textbf{(11)}$$

By the way, the session key is totally agreed in our authentication protocols using the BAN-logic derivations.

4.2 The Subscriber Identity Privacy

In our proposed protocol, the real identity of the MS is never transmitted over the whole network for authentication purposes. Therefore, the intruders can not get any information about the MS who he/she wants to impersonate or steal from the personal account. We use a pseudonym $h(IMSI||R)$ to represent a mobile user in the registration, someone who has the correct *R* and the personal secret key K_i can justify the MS that s/he is legitimate. Once the MS has been successfully authenticated, the HLR creates a new *R'* to replace the old *R* in the mobile user device for each registration. So the pseudonym will be changed by the new *R'*, and so it will protect someone that utilizes the former pseudonym to access the network.

4.3 The Mutual Authentication between the Network End and the Mobile Subscriber

In our proposed method, we first pre-store a new nonce *R* and keep it secret in the HLR and the MS. A nonce *R* can derive many kinds of parameter to be used in authentication procedures. The MS also generates a secret key K_{ms} that is equal to $A8(R, K_i)$ and is pre-stored in the HLR's database. So far, in the HLR's database for each user there are the $IMSI$, K_i, $h(IMSI||R)$, K_{ms}, and *R*. When the MS wants to make a registration, the MS generates the $\{h(N_{ms})||(N_{ms})\}_{Kms}$, the $h(IMSI||R)$ and transmits it to the home domain. The HLR receives the message and searches the real identity of the user. Finally, when the HLR obtains the true identity and K_{ms} of this user, it decrypts the $\{N_{ms}\}_{Kms}$ get the packed one N_{ms}'. At that moment, the HLR can check if the previous one $h(N_{ms})$ is equal to $h(N_{ms}')$, where N_{ms}' is just decrypted one. If it is equal, the HLR regards this MS as a legitimate one, produces a new nonce *R'* to replace *R* stored in MS and forwards $\{R',SRES'\}_{Kms}$ to the MS. The *SRES'* is generated from the $A3(K_i, N_{ms})$.

After the MS receives the message, it decrypts the message by K_{ms} to get the *SRES*" and *R"*. MS checks the *SRES*" which is obtained from the message, and the *SRES* which is generated by the MS itself, to determine if they are equal or not. After comparing, the MS can authenticate if the network end is legitimate. Through this method, MS and the network end can authenticate each other via *R*, and both are pre-stored in the user and the home domain. So, if the MS wants to make another registration, it has to derive some kind of parameter by using a new *R'* to pass authentication.

Each successful registration causes three situations. One is that the HLR generates a new *R'* to replace the old one, second, the pseudonym will be changed with *R'*, and third, the secret key of the MS will also be altered. The updating *R* can increase the degree of security of our proposed method and achieves mutual authentication between the network ends and the mobile users.

4.4 Comparisons

In this subsection we provide a comparison table, Table 1, including the protocols of Shieh et al. [16], Lee et al. [19] and Peinado [8], where the minimum number of messages for authentication, the number of rounds in subsequence phase, and the cryptographic technology are compared. Among these protocols, only the Peinado's protocol uses the public key system as a secure skill. Although, the public key can provide a more secure level, in his protocol it result in much energy consumption of the mobile device and having a long latency between the mobile and the VLR.

In the protocol of Shieh et al. [16], they defined the two environments, one is the intra-domain where the mobile moves within his service area, the other is the inter-domain where the mobile leaves his service area and moves to a visited area. So it has two different numbers in the chart. The extra three rounds are to communicate and exchange information of the mobile between the service area agent and the visited area agent. The other protocol, including ours does not have a definition like this. The numbers of sequence phase in this chart are all the same, because it only exchanges messages between the VLR and the MS. In terms of cryptographic technology, only Shieh et al. and Peinado used the timestamp property that might have perfect time synchronization and extend the valid period in the entire network.

Lee et al. [19] emphasized that not only did they provide confidentiality of the subscriber's data from the mobile stations to the mobile stations and from the mobile stations to the fixed stations, but they also reduced the storages of the subscriber's sensitive data in the database of the VLR. Consequently the original GSM architecture improved the authentication protocol between the mobile stations and the HLRs. Therefore the number of the message rounds in the inter domain and the intra domain are the same as in the original one.

Table 1. Comparisons of functionality and performance

	Our contributed scheme	Shieh et al. [16]	Lee et al. [19]	Peinado [8]
CT	Symmetric key, nonce	Symmetric key, nonce, timestamp	Symmetric key, nonce	Public key, nonce, timestamp
IP	5 (*5)	8 (*5)	5 (*5)	4 (*4)
SP	3	3	3	3
RSVD	Yes	No	Yes	Yes
MA	Yes	Yes	No	Yes
AP	Yes	No	No	Yes

CT: Cryptographic technology
IP: Number of the message rounds in initial phase (*inter domain/intra domain)
SP: Number of the message rounds in subsequence phase
RSVD: Reduction of the storage of VLR database
MA: Mutual authentication
AP: Anonymous property

5 Conclusions

This paper presented a method to improve the GSM authentication in the network to make the system work more efficiently. We proposed four important items to improve the original authentication protocol. In the new architecture, the subscriber's IMSI can not be revealed and it protects the IMSI from being eavesdropped upon through the air medium, when an intruder does not know the real location of the subscriber, and impersonates a legitimate subscriber to access the network by getting the IMSI. In other words, it is anonymous in the location of subscriber during the mobile call. Although our proposed method increases the message size which is send to the VLR by the MS, it does increase system security level. We also make a break with the concept of the inter-domain and the intra-domain, and decrease the complexity of the transmitting signal and the transmission latency. In addition, our proposed method saves more space overhead on the VLR. As a whole, the superior efforts achieved in this scheme are the mutual authentication provided between the entities of MS and VRL, and the intrusions to illegal VLR/BS efficiently deterred upon the discussions over the existing GSM authentication studies.

Acknowledgement

This work was supported in part by National Science Council, Taiwan, R.O.C., under contract number NSC-95-2221-E-015-003.

References

[1] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication," *ACM Trans. Computer Systems*, Vol. 1, pp. 18–36, 1990.

[2] ETSI, "Recommendation GSM 03.20: Security Related Network Functions," Tech. Rep., *European Telecommunications Standards Institute*, June 1993.

[3] B. Mallinder, "An Overview of the GSM System," *in Proc. of Third Nordic Seminar on digital band mobile radio comm.*, Copenhagen, Denmark, pp. 12-15, 1988.

[4] M. Rahnema, "Overview of the GSM System and Protocol Architecture," *IEEE Communications Magazine*, Vol. 31, pp. 92-100, 1993.

[5] A. Aziz and W. Diffie, "Privacy and Authentication for Wireless Local Area Networks," *IEEE, Personal Communications*, Vol. l, pp. 24-31, 1994.

[6] 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, 1993.

[7] M.S. Hwang, and C.H. Hwang, "Authenticated Key-Exchange in Mobile Radio Network," *European Transactions on Telecommunications*, Vol. 8, pp. 265-269, 1997.

[8] A. Peinado, "Privacy and Authentication Protocol Providing Anonymous Channels in GSM," *Computer Communications*, Vol. 27, pp. 1709-1715, 2004.

[9] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Comm. ACM*, Vol. 21, pp. 120–126, 1978.

[10] J. Hastad, "On Using RSA with Low Exponent in A Public Key Network," *In Advance in Cryptology - Crypto'85,* Vol. 218 *of Lectures Notes in Computer Science, Springer-Verlag*, pp. 403–408, 1985.

[11] M.S. Hwang, "A Remote Password Authentication Scheme Based on the Digital Signature Method," *International Journal of Computer Mathematics*, Vol. 70, pp. 657-666, 1999.

[12] M.S. Hwang, C.C. Lee, and Y.L. Tang, "An Improvement of SPLICE/AS in WIDE Against Guessing Attack," *Information*, Vol. 2, pp. 297-302, 2001.

[13] T. Hwang, "Scheme for Secure Digital Mobile Communications Based on Symmetric Key Cryptography," *Information Processing Letters*, pp. 35–37, 1993.

[14] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Comm. ACM*, Vol. 24, pp. 84–88, 1981.

[15] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," *J. Cryptology*, Vol. 1, pp. 65–75, 1988.

[16] S. P. Shieh, F. S. Ho and Y. L. Huang, "An Efficient Authentication Protocol for Mobile Networks," *Journal of Information Science and Engineering*, Vol. 15, pp. 505-520, 1999.

[17] H.Y. Lin, "Security and Authentication in PCS," *Computers and Electrical Engineering*, Vol. 25, pp.225-248, 1999.

[18] L. Harn and H.Y. Lin, "Modification to Enhance the Security of the GSM Protocol," *in Proc. of the 5th National Conference on Information Security*, pp. 74–76, 1995.

[19] C.H. Lee, M.S. Hwang, and W.P. Yang, "Extension of Authentication Protocol for GSM," *IEE Proceedings communications*, Vol. 150, pp. 91-95, 2003.

[20] C.H. Lee, M.S. Hwang, and W.P. Yang, "Enhanced Privacy and Authentication for the Global System for Mobile Communications," *Wireless Network*, Vol. 5, pp. 231-243, 1999.