A New Authentication Protocol Based on Pointer Forwarding for Mobile Communications*

Cheng-Chi Lee[†, ‡] Min-Shiang Hwang[§] I-En Liao[†]

Department of Computer Science[†]
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.

Department of Computer & Communication Engineering[‡]
Taichung Healthcare and Management University
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.
Email: cclee@cis.nctu.edu.tw

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

April 6, 2005

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC92-2213-E-005-027.

[§]Responsible for correspondence: Dr. Cheng-Chi Lee.

A New Authentication Protocol Based on Pointer Forwarding for Mobile Communications

Abstract

A frequently moving mobile user in GSM must re-register at the HLR frequently, and therefore the signaling traffic is overhead and HLR database update cost raised. In this paper, the authors propose a new authentication protocol based on pointer forwarding to reduce the HLR update cost and traffic load for the MS authentication protocol. The proposed protocol for GSM can achieve some objectives described in Introduction. Compared with other authentication protocols, our protocol is efficient.

Keywords: Authentication, GSM, Pointer Forwarding, Security.

1 Introduction

Mobile communications have exploded in recent years, especially the Global System for Mobile communication (GSM), a Pan-European digital cellular system standard [9, 16, 22]. Mobile communications bring convenience to people in their daily life, such that each user can communicate with others in any place at any time. In this busy age, people travel a lot for business. Therefore, more and more people need mobile communications equipment, such as cellular telephones. However, there are such problems with mobile telecommunications as privacy and authentication as discussed in [2, 3, 4, 5, 6, 8, 10, 13, 14, 19].

Due to the increasing requirement for mobile communications, an efficient system can be crucial. Its main objective is to reduce the signaling traffic and update the HLR/AuC (Home Location Register/Authentication Center) database when MSs (Mobile User) frequently change locations. In recent years, a good number of investigations have been conducted in reducing the update cost [7, 11, 15]. Lin and Tsai [15] proposed a location tracking system with distributed HLR pointer forwarding. This method reduces the HLR database update and location update costs. Although this method can reduce the location update costs, it does not address MS authentication for mobile communications. Authentication is an important issue in mobile communications. It can prevent a fraudulent user from obtaining access to the system.

Recently, a lot of research has been done and discussed to reduce signaling traffic [1, 12, 20, 21]. Lee, Hwang and Yang's authentication protocol [12] (named LHY-protocol) can reduce the sensitive information stored in a VLR (Visiting Location Register) and reduce the signaling traffic between the VLR and HLR. Compared with previously proposed researches, it is obvious that Lee, Hwang and Yang's authentication protocol is superior. However, up to now, the signaling traffic is still a major concern. The truth is, when each MS changes his/her VLR location frequently, the signaling traffic cannot actually be reduced because the MS must re-register at the HLR frequently. Under such circumstances, the signaling traffic problem becomes at best a matter of trade off. To overcome the problem even more constructively, a new authentication protocol based on pointer forwarding for mobile communications is to be proposed in this paper. Our protocol can turn the trade off problem into reducing both the update costs and the signaling traffic as well as achieve the following objectives:

1. To remove unnecessary sensitive information stored in VLR.
2. To require no additional computation.
3. To perform the authentication of mobile users at the VLR instead of the HLR, even if the VLR does not know the subscriber's secret key K_i and algorithm A3.

4. To improve the performance without changing the architecture of the original GSM system.

5. To empower the VLR TK_i to authenticate mobile users within the time limit instead of empowering the VLR indefinitely as in the LHY-protocol [12].

6. To lay no limit to the authentication process, even if the mobile user does not stay within the current VLR coverage.

7. To reduce the signaling traffic load for authentication between the VLR and HLR when mobile users change locations.

8. To reduce the database updating cost of HLR by not requiring the MS to re-register at the HLR.

The content of this paper is organized as follows. In the next section, we shall review the GSM authentication protocol. In Section 3, we shall introduce location tracking and pointer forwarding. Then, a better authentication protocol based on pointer forwarding is to be proposed in Section 4. In Section 5, we shall compare our new scheme with three other authentication protocols. Finally, the conclusion will be presented in the last section.

2 GSM Authentication Protocol

In a GSM network, the authentication process is the most important procedure before network accessing. The GSM authentication process, where mobile users are identified and verified, ensures that the services are not obtained fraudulently [17, 18, 24]. Basically, the authentication process is a challenge/response mechanism; the GSM server asks a question that only a legal mobile user can answer correctly during each communication session. In Figure 1, $RAND$ and $SRES$ are the question and answer, respectively. The random number $RAND$ is generated locally by the HLR/AuC along with K_i

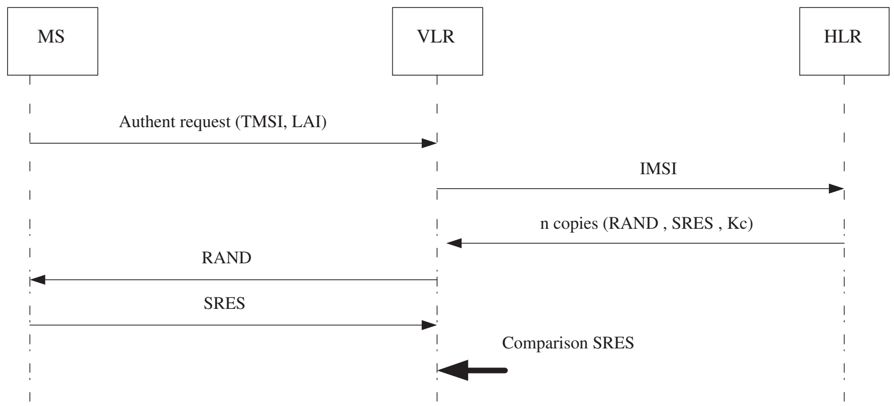

Figure 1: The GSM challenge/reponse signaling flow

to compute the $SRES$ and K_c, respectively, using algorithms A3 and A8, as shown in Figure 2.

The current GSM authentication process must be carried out as follows (shown in Figure 1):

1. The MS sends an authentication request to the VLR. This request contains the Temporary Mobile Subscriber Identity (TMSI) and Location Area Identity (LAI) [1].

2. The VLR obtains the International Mobile Subscriber Identity (IMSI) of the MS from the old VLR through the TMSI. The VLR then sends the obtained IMSI to the HLR/AuC and asks for the authentication parameters for the MS.

3. For the IMSI of the MS, the HLR/AuC generates several triplets, ($RAND$, $SRES$, K_c), say n copies, at a time. Then HLR/AuC sends these copies to the visited VLR for storage and subsequent use.

4. The VLR then selects a pair, $(RAND, SRES, K_c)$ and sends the $RAND$ to the MS. The VLR then asks the MS to compute the $SRES$ and send it back.

5. When the MS receives the $RAND$, he/she computes $SRES$ and K_c with

his/her secret key K_i and the $RAND$ using algorithms A3 and A8. The MS keeps the K_c to communicate secretly and sends the $SRES$ back to the VLR.

6. Once the VLR receives the $SRES$ from the MS, the $SRES$ is compared with the stored select-$SRES$. If the two $SRES$s are equal, the MS passes the authentication process and is permitted to access the system; otherwise, the VLR rejects the MS.

The HLR/AuC must compute n copies of the $(RAND, SRES, K_c)$ for each MS in the HLR/AuC, and send them to the VLR that the MS is visiting. This results in some problems. Lee et al. [12] pointed out three drawbacks as follows:

- A space overhead occurs in the VLR when a set of authentication parameters is being stored in the VLR.
- The identification of an MS is performed in the VLR and must be aided by the HLR of the MS.
- When VLR needs another set of authentication parameters, a bandwidth will have to be consumed by the VLR and HLR.

3 Location Tracking and Pointer Forwarding

Location tracking is to find a mobile user where he/she is moving. When a mobile user changes his/her current VLR, he/she must send a message to update the HLR. Therefore, with a mobile user changing areas and receiving calls frequently, the HLR must get updated frequently so the traffic can move on. The algorithm is called pointer forwarding. The objective of pointer forwarding is to reduce the update cost in PCS [11].

When a mobile user moves to some new VLR, the forwarding pointer is created as shown in Figure 3. In this figure, PSTN is the abbreviation of Public

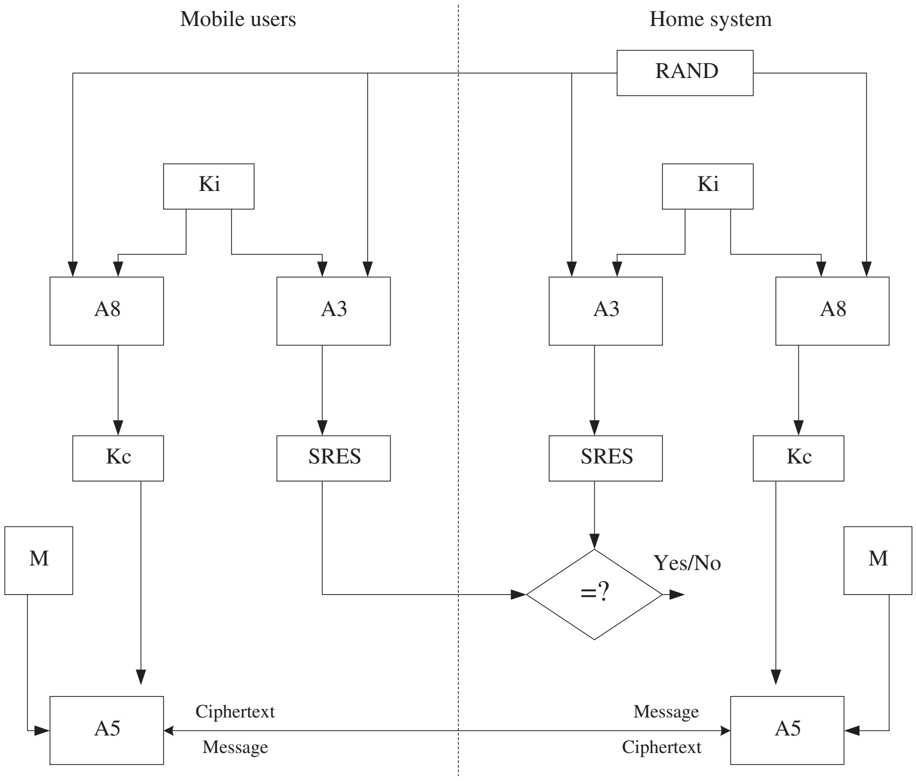

Figure 2: The GSM authentication architecture

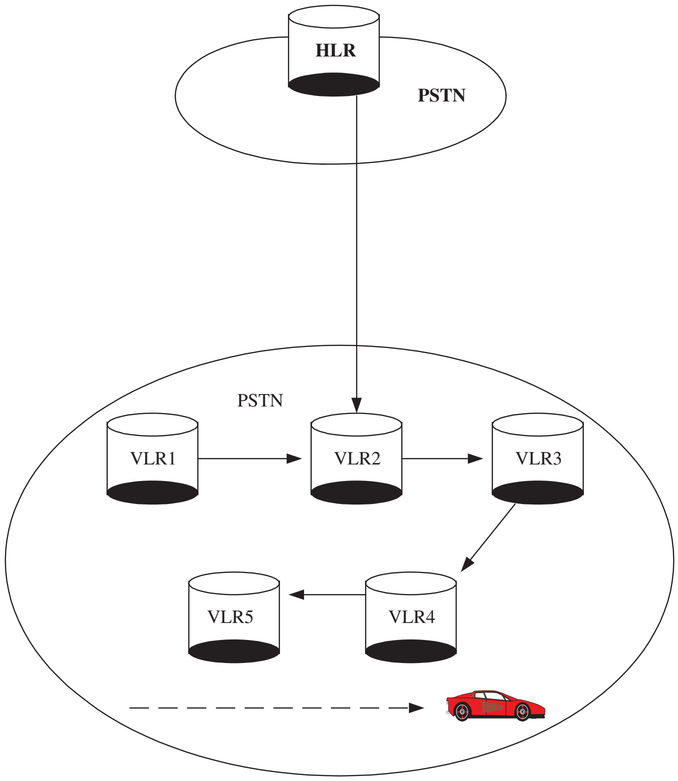

Figure 3: The registration of pointer forwarding

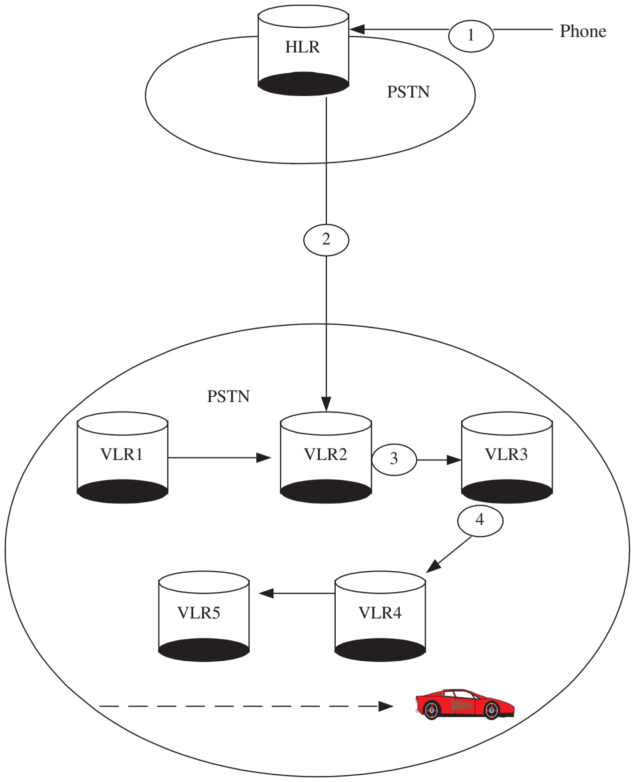

Figure 4: The find operation of pointer forwarding

Switched Telephone Network. Suppose the mobile user registers at HLR in VLR2 and moves all the way through VLR3 to VLR4. When he/she moves to VLR3, VLR3 sends a message to tell VLR2 that the mobile user is there. Once VLR2 receives the message from VLR3, VLR2 creates a forwarding pointer to VLR3. The same thing goes again when the mobile user moves to VLR4 from VLR3.

When a phone call is to be put through to the mobile user, the forwarding pointers will be traced until the location of the mobile user is found. The phone call reaches the HLR of the mobile user and first makes a query for the mobile user at where he/she was registered, and then a chain of forwarding pointers will be passed until the mobile user is located. The whole process is shown in Figure 4.

After the actual location of the mobile user is found, he/she is asked to register at the HLR in VLR4. Then the mobile user is delete-registered from

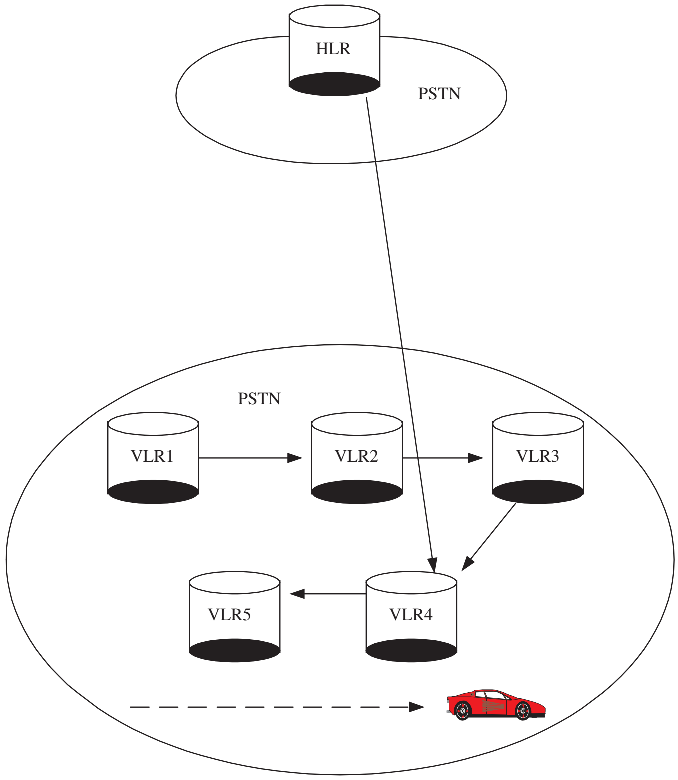

Figure 5: After the find operation of pointer forwarding

VLR2. It is shown in Figure 5. Therefore, the incoming call can be directly put through to VLR4. Next time, when the mobile user moves to another location from VLR4 and a phone call reaches the HLR of VLR4 for the mobile user, it can follow a chain of forwarding pointers to find the actual location of the mobile user the same way.

Therefore, with pointer forwarding, when the mobile user moves to a new VLR, the HLR can be updated one time less, and that means the update cost can be reduced. However, the HLR may become a bottleneck in virtue of the heavy signaling traffic generated by location tracking. Recently, one solution to the problem, namely to distribute the HLR in several locations, has been proposed by Lin and Tsai [15].

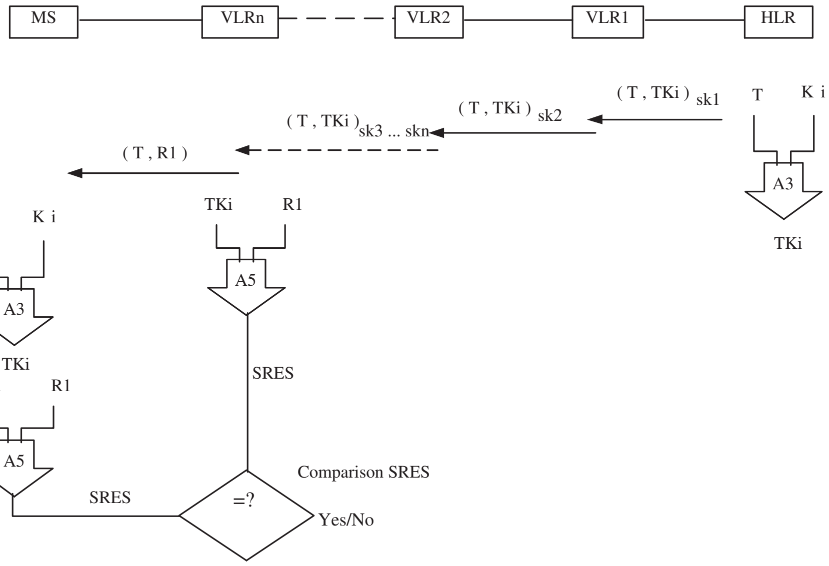

Figure 6: The new GSM authentication protocol

4 A New Authentication Protocol

Based on pointer forwarding, we propose a new authentication protocol in the following. The protocol can achieve our objectives as described in Section 1. The following notations are used:

T_s: starting time selected by HLR;

T_e: end time selected by HLR;

T: timestamp;

K_i: mobile user's secret key;

TK_i: temporary key;

R: random number generated by HLR and MS;

R1: random number selected by VLR;

sk: common session key;

A3, A5: one-way functions;

SRES: certificate of mobile user;

$||$: concatenated operator.

Our new authentication protocol is illustrated in Figure 6. In our authentication protocol, the last VLR into which the MS moves authenticates identity of the MS. No matter where the MS moves, the MS is not required to re-register at the HLR. Therefore, the new authentication protocol reduces not only the signaling traffic load but also the update costs between the HLR and VLR.

We assume that the MS moves from VLR1 to VLRn. The MS authentication process is described as follows:

1. HLR sends T and TK_i, which are encrypted with the session key $sk1$, to VLR1. VLR1 is where the MS is registered. T is computed as $(T_s||T_e)$, where T_s is the starting time for the temporary key TK_i and T_e is the ending time for TK_i. TK_i is generated through algorithm A3 using T and K_i as inputs.

2. Once VLR1 receives the message, VLR1 decrypts (T, TK_i) with the session key $sk1$ from the HLR. VLR1 then detects the location of the MS, finding out that the MS moves to VLR2. Since the forward pointer at VLR1 points towards VLR2 [15], VLR1 forwards the message (T, TK_i) which is encrypted with the session key $sk2$ to VLR2.

3. Once VLR2 receives the message, the step is similar to the above step. The session key sk_i is a common session key between the two parties. We assume that every party would have a table that stores the common session key between them or a secure channel between them.

4. After the message (T, TK_i) is forwarded to the last VLRn, namely MS's current location, VLRn decrypts the message with the session key. VLRn then checks whether the T is the correct time. If T is obsolete, the VLR requests the MS to re-register at the HLR. Otherwise, VLRn computes $SRES$ through algorithm A5 using TK_i and $R1$ as inputs. $R1$ is generated by VLRn for the first call by the MS. To verify the MS, VLRn sends $(T, R1)$ to the MS and asks him/her to reply with the correct $SRES$.

5. Once the MS receives $(T, R1)$, he/she computes the $SRES$ through algorithm A5 using TK_i and $R1$ as inputs, where TK_i is computed through algorithm A3 using T and K_i as inputs. Then the MS sends the $SRES$ back to the VLRn.

6. When VLRn receives the $SRES$, VLRn checks if the $SRES$ is equal to the pre-computed $SRES$. If the two $SRES's$ are the same, then the MS passes the authentication process. Otherwise, he/she is rejected.

In our proposed protocol, two cases where mobile users are moving are discussed as follows:

Case 1:

If the MS always stays within the coverage of his/her current location VLRn, VLRn generates a different R_i for each call made by the MS. Even for subsequent calls, the value of R_i varies from call to call. Only one copy of the authentication parameters (T, TK_i) is transmitted from the HLR to the VLRn. Therefore, no sensitive information is stored in VLRn. Our MS authentication is empowered by VLR, so no aid is required from HLR. This results in a reduction in the signaling traffic load for transmitting authentication parameters.

Case 2:

If the MS moves to the next VLR (changes the current location VLR), the old VLR only needs to forward the message pair (T, TK_i) encrypted with the session key sk to the new VLR. To verify the identity of the MS, the authentication process is the same as in Steps 4 to 6. The new VLR only generates a new R_i to compute the SRES. Even though the MS changes the current location VLR, he/she does not have to register at the HLR. This eliminates the bandwidth consumption for transmitting authentication parameters. As long as the T is not obsolete, the VLR requests no other authentication parameters (T, TK_i) from the HLR. If the T is obsolete, the VLR requests another set of authentication parameters from the HLR. The HLR re-computes the temporary key TK_i and generates a new T for MS authentication.

Our protocol does not only achieve our objectives but is also better than other authentication protocols for mobile communications. In the next section, we shall make comparisons among the original GSM protocol, the protocol by Lee et al. [12] and our proposed protocol.

5 Comparison and Analysis

We have reviewed the GSM authentication protocol and its' weaknesses as examined by Lee et al. [12]. Although many researches have been proposed to solve these problems [1, 2, 3, 4], there has been no complete solution to date. We consulted an authentication protocol, proposed by Lee, Hwang and Yang [12], which managed to deal with these problems. Here are some comparisons we have made among the original GSM protocol, the protocol by Lee et al. and our proposed protocol. First, we shall briefly present LHY-protocol as follows and illustrate the protocol in Figure 7.

LHY-protocol:

1. The HLR empowers the VLR to compute the $SRES$ for authentication. The HLR sends only one parameter pair $(RAND, TK_i)$ to the VLR instead of sending n copies $(RAND, SRES, K_c)$ to the VLR. The pair $(RAND, TK_i)$ is encrypted with the session key sk between the HLR and VLR. $RAND$ is a generated random number by the HLR. TK_i is computed using K_i and $RAND$ as inputs through algorithm A3.

2. The VLR decrypts the pair $(RAND, TK_i)$ with the session key sk. The VLR then computes $SRES$ using TK_i and $RAND1$ as inputs through algorithm A5. $RAND1$ is a random number generated by the VLR for

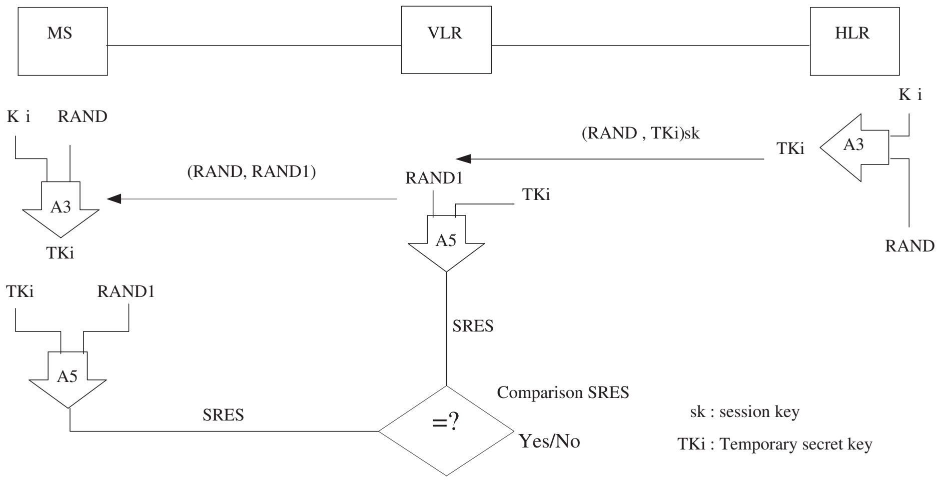

Figure 7: LHY's improved authentication method in GSM

the first call by the MS. The VLR then sends both $RAND$ and $RAND1$ to the MS.

3. The MS computes TK_i and $SRES$ and then sends $SRES$ back to the VLR for the identity check. TK_i is computed using K_i and $RAND$ as inputs through algorithm A3. $SRES$ is computed using TK_i and $RAND1$ as inputs through algorithm A5.

4. VLR compares the $SRES$ from the MS with the previously computed $SRES$. If the two $SRES's$ are equal, the MS passes the authentication process and proceeds to access the system; otherwise, the VLR rejects the MS.

In the LHY-protocol, regardless of the number of times the MS calls the VLR within a pre-defined period, only one $RANDi$ is needed for each ith call, where $RANDi$ is generated separately by the VLR for each call. In other words, there is only one set of authentication parameters from the HLR to the VLR. Therefore, the drawbacks of the original GSM authentication protocol are improved.

In the LHY-protocol [12], as long as the MS stays within the coverage of the current VLR, the VLR need not request the pair $(RAND, TK_i)$ from the

HLR and use a set of authentication parameters indefinitely. This does not only eliminate the unnecessary transmission of sensitive information but also reduces the signaling traffic from the HLR to the VLR. However, if a mobile user changes locations frequently, then the signaling traffic from the HLR to the VLR and the database updating cost of HLR will remain considerably high. When a mobile user changes his/her location from the old VLR to a new VLR, the new VLR will have to require another pair of authentication parameters $(RAND, TK_i)$ from the HLR. In other words, the MS will be required to re-register at the HLR. Hence, the updating cost will go up. To overcome these shortcomings, we have proposed a new authentication protocol based on pointer forwarding in above section.

In this section, the proposed authentication protocol will be compared with the original GSM and the protocol proposed by LHY. Our protocol achieves the same security requirement as the other two. The security is based on one-way function algorithms, A3 and A5. In addition to not changing the original GSM architecture, it also enhances the efficiency of the authentication protocol especially when a mobile user moves frequently, which is our major concern.

5.1 Computation and Storage Space

In the following, we shall make comparisons among the three authentication protocols in terms of computation and storage space in Table 1.

In order to authenticate the MS, each of the protocols verify the $SRES$ of the MS to determine if it is the correct authentication parameter. We compare the total computation costs and storage spaces for the three generated $SRES$'s from the three protocols during the period when the MS moves from VLR1 to VLRm. We assume that each user changes the current VLR location m times. In the original GSM protocol, we assume that the HLR generates n copies of SRES authentication parameters and then does $m \times n$ computations through algorithm A3. The MS computes the $SRES$ in each n sessions, and there is a

	Original protocol	LHY protocol	Our protocol
HLR	A3(R, Ki) = SRESj j = 1,2, . . . , n	A3(R, Ki) = TKi	A3(T, Ki) = TKi
MS	A3(R, Ki) = SRESj j = 1,2, . . . , n	A3(R, Ki) = TKi A5(Rj, TKi) = SRESj j = 1,2, . . . , n	A3(T, Ki) = TKi A5(Rj, TKi) = SRESj j = 1,2, . . . , n
Verification (by VLR)	SRESj	A5(Rj, TKi) = SRESj	A5(Rj, TKi) = SRESj
Total computations	2mnT(A3)	2mT(A3) + 2mnT(A5)	2T(A3) + 2nT(A5)
Total storage spaces	nS(SRES)	S(TKi)	S(TKi)

m: the times of MS moving to VLR, n: copies of authentication parameters,
T(): computation time, S(): storage space.

Table 1: Comparisons of authentication computations and storage spaces among the three GSM protocols

total of $m \times n$ computation. To verify the MS, VLR keeps the n copies of the authentication parameters. Therefore $nS(SRES)$ of the total storage space is required. The total number of computations is $2mnT(A3)$, where $S(\cdot)$ denotes the consumption of the storage space and $T(\cdot)$ denotes the consumption of the computation time.

The LHY GSM protocol is discussed in [12]. The difference between the LHY GSM protocol and ours is that we consider the MS moving from VLR1 to VLRm. With the LHY protocol, the total number of computations is $2mT(A3) + 2mnT(A5)$, and the total storage space is $S(TK_i)$.

In our protocol, the MS does not have to register at the HLR even though the MS changes the location from VLR1 to VLRm. This reduces much of the computation time. We empower the VLR TK_i to authenticate the MS within a limited time. As a result, the VLR does not have to request authentication parameters from the HLR each time MS changes locations. This also reduces the update cost in the HLR and the signaling traffic between the HLR and VLR. However, when the time limit T of TK_i is obsolete, the MS must re-register at the HLR. The HLR only generates 1 copy of the authentication parameter TK_i and then does $T(A3)$ computations through algorithm A3. The

	Original protocol	LHY protocol	Our protocol	m = 5 and n = 5			m = 10 and n = 10		
				Original	LHY	Our	Original	LHY	Our
MS register HLR	m	m	1	5	5	1	10	10	1
Generate Rand number	mn(R)	m(R) + mn(R1)	n(R1)	25	30	5	10	11	1
Total computations	2mnT(A3)	2mT(A3) + 2mnT(A5)	2T(A3) + 2nT(A5)	50	60	12	10	11	1.1
Total storage spaces	nS(SRES)	S(TKi)	S(TKi)	5	1	1	10	1	1

Table 2: Comparisons among the three GSM authentication protocols

MS computes TK_i to generate $SRES$ in each n sessions and then does $T(A3)+nT(A5)$ computations through algorithm A3. To verify the identity of the MS, VLR keeps TK_i and computes $SRES$, which takes $nT(A5)$ computations. The total number of computations is $2T(A3)+2nT(A5)$, and the total storage space is $S(TK_i)$.

5.2 Comparisons Among The Three GSM Authentication Protocols

The comparisons among the three protocols are summarized in Table 2. We assume that each user changes VLR locations frequently, moving m times. That is, each user moves from VLR1 to VLRm. The details are discussed as follows:

- Ms register at HLR:

  Whenever MS moves to a particular VLR, he/she re-registers at his/her HLR. The original and LHY protocols require the MS to register at the HLR m times. This creates additional signaling traffic and update costs. In contrast, our protocol only requires the MS to register at the HLR once when the TK_i is within the time limit.

- Generate Rand number:

  For authentication in the original protocol, HLR generates n copies of the random number R to compute the $SRES_j$ for each n sessions. Therefore, the HLR generates $mn(R)$ for the MS that moves from VLR1 to VLRm. In the LHY protocol, HLR generates one random number R to compute the TK_i. The HLR empowers the VLR to use TK_i to derive $SRES_j$. VLR generates n copies of the random number $R1$ for each n sessions. Therefore, the HLR generates $m(R)$, and the VLR generates $mn(R1)$ for the MS that moves from VLR1 to VLRm. In our protocol, VLR only generates n copies of the random numbers $R1$ for each n sessions. Therefore, the total number of random numbers is $n(R1)$.

- Total computations:

  The total number of computations is discussed in the above subsection. The total computations in the original, LHY, and our protocol are $2mnT(A3)$, $2mT(A3) + 2mnT(A5)$, and $2T(A3) + 2nT(A5)$, respectively.

- Total storage space:

  The total storage space is discussed in the above subsection too. The total storage spaces in the original, LHY, and our protocol are $nS(SRES)$, $S(TK_i)$, and $S(TK_i)$, respectively.

We assume that $T(A3) \cong T(A5)$, $S(SRES) \cong S(TK_i)$, and $R \cong R1$. An example of the comparisons among the three protocols is shown in Table 2. We assume that $m = 5$, $n = 5$, $m = 10$ and $n = 10$. In the case of $m = 10$ and $n = 10$, the second and third columns are simplified. For example, the second column (100, 110, 10) is simplified to (10, 11, 1). Obviously, our protocol is better than the other two protocols for the MS moving from VLR1 to VLRm. Yet, if the MS always stays within his/her current location, that is, m is equal to 1. If m is equal to 1, the total computations in the original, LHY, and our protocol are $2nT(A3)$, $2T(A3)+2nT(A5)$, and $2T(A3)+2nT(A5)$, respectively, then the performance of our protocol will be worse than the original protocol in terms of the total number of computations. It just increased $2T$. However, most mobile users change their locations frequently. Therefore, m is not almost to be equal to 1. Today, there is still a very large population of users who in their daily lives do not usually move more than a few km. We had discussed it in Section 4. In Case 2, mobile users change their locations frequently. In this situation, our protocol is superior to other protocols. In Case 1, mobile users always stay within the coverage of his/her current location. In this situation, m is equal to 1. Although the total computation of the original protocol is better than taht of our protocol, the total storage space of our protocol is superior to that of the original protocol. In summary, for MS authentication, our protocol is the best in the long run.

Some way that there would be some hops in our proposed protocol (from HLR to VLR1...VLRm) before we can locate the actual VLR. This looks like a big overhead. However, in general, a limited pointer forwarding method only uses a very limited number of pointers, usually less than 5 as suggested in [11]. Hence, in our proposed protocol, m had better be set to be 5. Once the MS moves to a sixth VLR, he/she had better re-register at the HLR to acquire better efficiency.

5.3 Security Analysis

In this subsection, the security of our authentication protocol is examined. The security of our protocol is the same as that of the original GSM authentication protocol, which is based on one-way function algorithms A3 and A5. In addition, we also analyze the security of our protocol in terms of secrecy and examine the robustness against the replay attack.

Secrecy:

In our protocol, we assume that the HLR and all VLRs are trusted centers. All VLRs only forward the message pairs (T, TK_i); they cannot modify the pairs. To prevent the modification attack, the HLR can sign the pairs using his/her private key of asymmetric cryptosystem the way the digital signature is output in RSA [23]. All VLRs can verify the digital signature signed by the HLR using the HLR's public key of asymmetric cryptosystem. Hence, any VLRs can make sure of the accuracy of this (T, TK_i) sent by the HLR.

The secret key K_i between HLR and MS, as well as the common session key sk_i between two VLRs, must be kept secret. Each VLR does not really know the secret key of the MS. The VLR only knows the temporary key TK_i. The secret key is only known to the MS and the HLR. Based on one-way function algorithms A3 and A5, if an attacker does not have the secret key K_i, he/she cannot calculate TK_i to derive the $SRES$ to pass user authentication for mobile communications. Furthermore, using the common session key sk_i, two VLR's can transmit messages secretly. Therefore, our protocol is secure.

Replay attack:

The challenge/response mechanism is also used in our proposed protocol as in the original GSM authentication protocol. It can effectively prevent the replay attack. In our protocol, for MS authentication, the VLR generates a different R_i for each call session that prevents the replay attack. The pair $(R_i, SRES)$ is only valid for the user authentication of one call session, and then it expires. It is called a one-time password. An attacker cannot launch the replay attack even if he/she intercepts the message pair because in the next session a different pair of authentication parameters R_i and $SRES$ will be required for user authentication. Hence, our protocol can prevent the replay attack.

6 Conclusions

Authentication is an important issue. The system must ensure that only legal users can access the resources. However, until now, the GSM authentication protocol has not yet gotten rid of its drawbacks such as signaling traffic overhead and database space overhead. In some researches [1, 12, 20, 21], a number of protocols have been proposed and discussed to improve GSM's drawbacks. On the other hand, *pointer forwarding* is an algorithm of location tracking to reduce the location update cost. With pointer forwarding, mobile users do not need to re-register at the HLR frequently in PCS, which leads to the reduction of the signaling traffic. In other researches [7, 11, 15], experiments have been conducted to find away to reduce the update cost.

In this paper, combining the advantages of the above two fields, we have proposed a new authentication protocol based on pointer forwarding. The protocol can achieve our proposed objectives. Compared with the original GSM authentication protocols and the LHY-protocol, the proposed protocol has more efficiency as our analysis of computation cost and storage space consumption have suggested. On the other hand, the proposed protocol can also be used in distributed HLRs [15].

References

[1] Khalid Al-tawil, Ali Akrami, and Habib Youssef. A new authentication protocol for GSM networks. *IEEE 23rd Annual Conference on Local Computer Networks (LCN'98)*, pages 21–30, 1998.

[2] A. Aziz and W. Diffie. Privacy and authentication for wireless local area networks. *IEEE Personal Communications*, 1(1):24–31, 1994.

[3] M. J. Beller, L. F. Chang, and Y. Yacobi. Privacy and authentication on a portable communications system. *IEEE Journal on Selected Areas in Communications*, 11(6):821–829, Aug. 1993.

[4] D. Brown. Techniques for privacy and authentication in personal communication systems. *IEEE Personal Communications*, pages 6–10, Aug.

1995.

[5] U. Carlsen. Optimal privacy and authentication on a portable communications system. *ACM Operation System Review*, 28:16–23, July 1994.

[6] C. W. Chen, C. C. Yang, and M. C. Chuang. An efficient authentication scheme between MANET and WLAN on IPv6. *International Journal of Network Security*, 1:12–21, July 2005.

[7] C. N. Lo et al. An estimate of network database transaction volume to support universal personal communication services. *8th ITC Specialist Seminar on Universal Personal Telecommunications*, pages 236–241, 1992.

[8] Min-Shiang Hwang and C. H. Lee. Authenticated key-exchange in mobile radio network. *European Transactions on Telecommunications*, 8(3):265–269, 1997.

[9] Min-Shiang Hwang, Yuan-Liang Tang, and Cheng-Chi Lee. An efficient authentication protocol for GSM networks. In *AFCEA/IEEE EuroComm'2000*, pages 326–330, Munich, Germany, May 2000.

[10] Min-Shiang Hwang and W. P. Yang. Conference key distribution protocols for digital mobile communication systems. *IEEE Journal on Selected Areas in Communications*, 13(2):416–420, Feb. 1995.

[11] R. Jain and Y. B. Lin. Performance modeling of an auxiliary user location strategy in a PCS network. *ACM-Baltzer Wireless Networks*, 1(2):197–210, 1995.

[12] C. H. Lee, Min-Shiang Hwang, and W. P. Yang. Enhanced privacy and authentication for the global system for mobile communications. *Wireless Networks*, 5:231–243, July 1999.

[13] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang. Extension of authentication protocol for GSM. *IEE Proceedings - Communications*, 150(2):91–95, 2003.

[14] Cheng-Chi Lee, Chou-Chen Yang, and Min-Shiang Hwang. A new privacy and authentication protocol for end-to-end mobile users. *International Journal of Communication Systems*, 16(9):799–808, 2003.

[15] Y. B. Lin and W. N. Tsai. Location tracking with distributed HLR's and pointer forwarding. *IEEE Transactions on Vehicular Technology*, 47(2):58–64, 1998.

[16] B. Mallinder. An overview of the GSM system. In *Proc. Third Nordic Seminar on Digital Land Mobile Radio Commun.*, pages 12–15, Copenhagen, Denmark, Sep. 1988.

[17] R. Molva, D. Samfat, and G. Tsudik. Authentication of mobile users. *IEEE Network*, 8(2):26–34, 1994.

[18] R. Molva, D. Samfat, and G. Tsudik. An authentication protocol for mobile users. *IEE Colloguium on Security and Cryptography Applications to Radio System*, pages 4.1–4.7, June 1994.

[19] A. Peinado. Privacy and authentication protocol providing anonymous channels in GSM. *Computer Communications*, 27(17):1709–1715, 2004.

[20] Gregory P. Polini and David J. Goodman. Signaling system performance evaluation for personal communications. *IEEE Communication Magazine*, pages 60–65, June 1995.

[21] Thomas F. La Porta, Malathi Veeraraghavan, and Richard W. Buskens. Comparison of signaling loads for pcs systems. *IEEE/ACM Transactions on Networking*, 4(6):840–855, 1996.

[22] Moe Rahnema. Overview of the GSM system and protocol architecture. *IEEE Communication Magazine*, 31(4):92–100, April 1993.

[23] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[24] Y. Zheng. An authentication and security protocol for mobile computing. *Mobile Communication - Technology, Tools, Applications, Authentication and Security (Proceedings of IFIP World Conference on Mobile Communications), Edited by J. L.Encarnacao and J. M.Rabaey,Chapman and Hall,Canberra, Australia.*, pages 249–257, Sep. 1996.