An Efficient Authentication Protocol for Mobile Communications *

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

Department of Management Information Systems[‡]
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Tel: 886-4-22840864 ext. 670
Fax: 886-4-23608845
Email: mshwang@nchu.edu.tw

Department of Computer Science[†]
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Email: ieliao@nchu.edu.tw

Department of Photonics and Communication Engineering [§]
Asia University
No. 500, Lioufeng Road, Wufeng Shiang, Taichung, Taiwan, R.O.C.
Email: cclee@asia.edu.tw

August 18, 2009

An Efficient Authentication Protocol for Mobile Communications

Abstract

In this paper, a new Global System of Mobile Communications (GSM) authentication protocol is proposed to improve some drawbacks of the current GSM authentication protocol for roaming users including: (a) communication overhead between VLR; (b) huge bandwidth consumption between VLR and HLR; (c) storage space overhead in VLR; (d) overloaded in HLR with authentication of mobile stations; and (e) not supporting bilateral authentication. The main contribution of this paper is that it does not only improve the drawbacks listed above but also fits the needs of roaming users. In addition, the proposed protocol does not change the existing architecture of GSM, and the robustness of the proposed protocol is the same as that of the original GSM, which is based on security algorithms $A3$, $A5$, and $A8$.

Keywords: Authentication, GSM, Mobile Communications, Security.

1 Introduction

Since the 1980s, the Global System of Mobile Communications (GSM) has been the most popular standard, e.g. the standard of the Pan-European digital cellular system [8, 28, 32], for mobile phones in the world. It has become the worldwide wireless communication standard and is used by over 1.8 billion people across more than 210 countries, since it has been offering higher digital voice quality at a lower cost. More and more people use it to communicate with others in almost any place at any time. However, security is another major issue as far as wireless communication is concerned [9, 24, 29, 31, 33, 38, 39, 40].

*Responsible for correspondence: Prof. Min-Shiang Hwang

Two security problems, confidentiality and subscriber identity authentication [3, 4, 6, 13, 14, 17, 37], are main security issues in mobile communications. Confidentiality means the protection of the messages from interception or any other improper kind of access. Communications between the mobile user and home subsystem can be encrypted by using a longer shared authentication key and may not be divulged to third parties. On the other hand, a good identity authentication system can guarantee that no unauthorized user fraudulently gets required services from the home system. It verifies the claimed identity of a participant in mobile communications. In the original design, mobile users are authenticated by using a shared-secret cryptographical system. GSM only authenticates the mobile user to the network (not vice versa). To equip the GSM system with better power of security, in this paper, we shall focus on the development of solutions to possible user authentication problems.

1.1 GSM Network

In the GSM network, as GSM recommendation 02.09 [7] has defined, the three subsystems involved are the mobile station (MS) subsystem, the base station subsystem, and the home subsystem. The mobile station subsystem consists of the mobile equipment (ME) and a smart card called the Subscriber Identity Module (SIM). The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. The SIM card may be protected against unauthorized use by a personal identity number (PIN). The base station subsystem consists of the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These are the connections between the mobile stations and the Mobile Switching Center (MSC). The home subsystem is composed of five parts, the Mobile Switching Center (MSC), the Home Location Register (HLR), the Visitor Location Register

(VLR), the Authentication Center (AuC), and the Equipment Identity Register (EIR). We explain the difference between HLR and VLR as follows. The HLR is a database that stores complete local customer information. It is the main database. Your carrier puts your information on its nearest HRL, or the one assigned to your area. That info includes your IMEI, your directory number, and the class of service you have. It also includes your current city and your last known "location area" the place you last used your mobile. The VLR contains roamer information. Once the visited system detects your mobile, its VLR queries your assigned HLR. The VLR makes sure you are a valid subscriber, then retrieves just enough information from the now distant HLR to manage your call. It temporarily stores your last known location area, the power your mobile uses, special services you subscribe to and so on. The AuC stores a copy of the secret key kept in each subscriber's SIM card and generates authentication parameters for the authentication protocol on the request of HLRs. The EIR is a database that contains a list of all the valid mobile devices on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). The mobile stations communicate through radio links with the base stations, which are in turn connected to the MSC. The MSC is responsible for transiting signals between radio links and wire-lined networks. The network is illustrated in Fig. 1

1.2 GSM Security

The security of GSM is based on algorithms $A3$, $A5$, and $A8$. The architecture of GSM is shown in Figure 2 [1, 16, 28, 32]. It contains two aspects, privacy and authentication. To achieve privacy, the KC (Cipher Key) is output as a session key between the mobile station and the home subsystem to encrypt/decrypt the communication messages on the safety basis of algorithm $A5$ against interception by an eavesdropper. As for authentication, the $SRES$ (Signed RESponse) is output as a certificate to authenticate mobile stations.

The $SRES$ and KC are computed, respectively, by using K_i and $RAND$ as inputs through algorithms $A3$ and $A8$, where K_i is the mobile station's secret key shared between the mobile station and the HLR and saved in the SIM card and HLR's database, and $RAND$ is a random number generated by the home subsystem.

In a GSM network, authentication is important [30] in ensuring that the network services will not be obtained fraudulently. It works through a challenge/response mechanism. However, some drawbacks of the current GSM authentication protocol can be found as follows [23]:

(1) It lacks the capability of authenticating the home subsystem (VLR).

(2) It increases the bandwidth consumption between VLR and HLR

(3) Space overheads in VLR occur.

(4) Overheads due to the authentication of the mobile stations in HLR occur.

To fix the above drawbacks, some revised GSM authentication protocols have been proposed [1, 12, 22, 26, 27, 35]. However, the architecture of GSM has to be changed in these protocols, and none of the protocols can fix all of the above drawbacks at a time. Furthermore, some protocols require that some additional hardware be added to the system, and others are changed to public-key cryptography, which means more computational costs. Recently, Lee et al. [23] and Chang et al. [5] proposed their separate authentication protocols in an attempt to fix all of the above drawbacks. The merit of their protocols is in being able to maintain the existing architecture of GSM and keeping its simplicity and efficiency. In 2004, Hwang et al. proposed an anonymous channel protocol where the mobile station could request services privately under the visit network [15]. The protocol uses tickets, secret key cryptosystem, and public key cryptosystem techniques. The architecture of the protocol is different from the GSM. Since the protocol uses a public key cryptosystem, the computational cost is very high. However, they cannot properly address the roaming users, furthermore their protocols are not suitable for roaming users. To a mobile user frequently roaming to another VLR, communication overheads occur. In 2004, Hahn et al. proposed an improved GSM authentication protocol for roaming users [11]. They improved the GSM authentication protocol to reduce the signaling load for a roaming user. The protocol exploits the enhanced user profile containing a few VLR IDs a mobile user is most likely to visit. However, the protocol cannot solve all of the above problems and is not flexible. Once the mobile user has changed its most likely location areas, the user profile has to be changed accordingly. In 2006, Kumar et al. proposed an efficient identity based mutual authentication scheme for GSM [21]. In their scheme, MS and VLR authenticate each other and establish a session key to communicate securely for every communication. Their scheme requires less bandwidth and storage. However, their scheme has changed the architecture of GSM and is not suitable for roaming users. In the same year, Ammayappan et al. proposed an improvement to the GSM authentication protocol, based on Elliptic Curve Cryptography (ECC) [2]. Their protocol provides mutual authentication, requires less storage, avoids replay attack and consumes smaller network bandwidth. However, the computational cost is very high, since their protocol is based on ECC. Their protocol also has changed the architecture of GSM and is not suitable for roaming users. In 2008, Kalaichelvi et al. [19] proposed a user authentication protocol for GSM which permits the use of weak secrets (e.g., passwords or PINs) for authentication, providing new flexibilities for GSM users. In 2009, Fanian et al. proposed a new mutual authentication protocol for GSM networks [10]. It can provide bilateral authentication. However, these protocols have changed the architecture of GSM and cannot properly address the roaming users, consequently these protocols are not suitable for roaming users. In this paper, we shall propose an efficient authentication protocol for roaming users that can not only solve all of the above problems but also be very suitable for roaming cases.

1.3 The Requirements of Our Authentication Protocol for Roaming Users

In this subsection, we set up the five goals that our new GSM authentication protocol for roaming users is aimed to achieve. The goals of this paper are listed as follows and will be discussed in detail later in Section 4.3.

- Roaming:

  The protocol should be suitable for roaming users. It should reduce the communication overhead.

- Reduction of bandwidth consumption:

  The protocol should reduce the bandwidth consumption between VLR and HLR.

- Reduction of storage of VLR database:

  The protocol should reduce the storage overhead in VLR.

- Reduction of overload of HLR:

  The protocol should reduce the overload of HLR.

- Mutual authentication:

  The protocol should be able to achieve mutual authentication between MS and VLR.

The existing GSM authentication protocol fails to do the above. The reasons will be detailed in Section 3.1.

1.4 Outline of This Paper

The rest of this paper is organized as follows. In the next section, we shall define the notations used throughout this paper and review the existing GSM authentication protocol for roaming users. In Section 3, we shall point out some drawbacks of the existing GSM authentication protocol for roaming users and then present our revised protocol. In Section 4, we shall present the quality of service analyses including security analysis, efficiency analysis, and goals analysis. Finally, Section 5 will conclude this paper.

2 A Review of GSM Authentication Protocol for Roaming Users

In this section, we shall briefly review the current GSM authentication protocol for roaming users. The notations to be used throughout this paper will be shown in Section 2.1, followed by the protocol in Section 2.2.

2.1 Notations

The notations to be used throughout this paper are in Table 1.

2.2 The Protocol

Let's first review the existing GSM authentication protocol in Figure 3. The details are described as follows.

(1) When MS enters a new visiting area and requires new communication services, he/she sends an authentication request to the visited VLR. The request contains the TMSI and the LAI.

(2) After receiving the TMSI, the new VLR can use the TMSI to get the IMSI from the old VLR. Then the new VLR sends the IMSI to HLR.

(3) The HLR/AuC then generates n copies of the triplet authentication parameters $\{RAND, SRES, KC\}$ at a time for the mobile station to use later for each call, and then the HLR sends them to the VLR through a secure channel.

Table 1: Notations

HLR	The home location register
VLR	The visitor location register
AuC	The authentication center
MS	The mobile station (mobile user)
TMSI	The temporary mobile subscriber identity
IMSI	The international mobile subscriber identity
LAI	The location area identity
ID_V	The identification of VLR
K_i	The secret key shared between MS and HLR
TK_i	The temporary secret key calculated by HLR
T_1	The timestamp generated by MS for the first time of the authentication
T_j	The timestamp generated by MS for the jth authentication request, $j > 1, j \in N$
T_y	The timestamp generated by MS for the yth authentication request, $y \in N$
$RAND$	The random number generated by HLR/AuC
A3, A5, A8	The three algorithms on which the security of GSM is based
A3/A5/A8(M, K)	Modification of the input M with the key K through A3/A5/A8
$SRES$	The signed result
$SRES_j$	The signed result computed for the jth authentication, $j > 1, j \in N$
$SRES_y$	The signed result computed for the yth authentication, $y \in N$
KC	The session key between MS and VLR
CERT_VLR	The certificate of the visited VLR
CERT_VLR$_j$	The certificate of the visited VLR computed for the jth authentication, $j > 1, j \in N$
CERT_VLR$_y$	The certificate of the visited VLR computed for the yth authentication, $y \in N$

(4) After receiving these authentication parameters, the VLR keeps them in its own database and then he/she selects a triplet $\{RAND, SRES, KC\}$ to authenticate the mobile station for each call. Then the VLR forwards the selected $RAND$ to the MS.

(5) When the MS receives $RAND$, he/she can compute $SRES'$ and KC' and send the computed $SRES'$ back to the VLR. Then the MS keeps KC' for secret communication.

(6) Once the VLR receives $SRES'$ from the MS, it compares it with the selected $SRES$. If they are the same, the MS is authenticated; otherwise, the MS is not a legal user.

As long as the MS stays in the area covered by this VLR, the VLR can use the n copies of the triplet authentication parameters to authenticate the MS for each call until the VLR uses up the set of parameters. Once the VLR uses up the set, she/he just makes a request for another set of parameters from HLR. When MS moves to an area covered by another VLR, Figure 4 illustrates the flow of signaling messages generated as the roaming MS performs either the location registration or update [11]. The details are described as follows.

Step 2-1: When the MS moves to the area covered by VLR2, the MS sends a TMSI1 to VLR2.

Step 2-2: After receiving TMSI1, VLR2 forwards it to the area managed by VLR1.

Step 2-3: VLR2 receives an IMSI and a few remaining authentication triplets from VLR1 through a secure channel.

Step 2-4: VLR2 selects a triplet $\{RAND, SRES, KC\}$ to authenticate the mobile station with and then sends $RAND$ to the MS.

Step 2-5: MS computes a $SRES$ and sends it back to VLR2. Then VLR2 performs the user authentication procedure and compares it with the selected $SRES$.

Step 2-6: Once the MS is authenticated by VLR2 successfully, VLR2 sends a location update message to HLR. HLR will update the location of the MS.

Step 2-7: HLR returns an acknowledgement for the location update.

Step 2-8: VLR2 assigns a TMSI2 to the MS.

Step 2-9: HLR finally transmits a TMSI1 cancellation message to VLR1.

If the MS wants to move to the area covered by VLR3, similar steps will be taken for proper authentication. Note that when any visited VLR has used up the n copies of triplet authentication parameters, he/she must turn back to the HLR of the MS to ask for another set of authentication parameters.

3 The Proposed GSM Authentication Protocol for Roaming Users

3.1 Drawbacks of the GSM Authentication Protocol for Roaming Users

It is found that the above GSM authentication protocol for roaming users has some drawbacks as follows:

1. When the MS moves to another VLR frequently, the old VLR must repeatedly forward the remaining copies of n authentication parameters to the new VLR, and then communication overhead occurs.

2. Once the n copies of authentication parameters have been used up, the VLR should turn back to the HLR to ask for another set of authentication parameters, and then the bandwidth consumption between VLR and HLR rises [23, 34].

3. Each VLR must keep n copies of authentication parameters in its database, and that is why space overhead in VLR occurs.

4. To authenticate a MS, HLR must output n copies of authentication parameters. VLR then uses them to authenticate the MS. That is to say, it must be helped by the HLR of the MS for each communication session, but then overload in HLR occurs. This drawback is different from drawback 2. Drawback 2 increases the communication overhead between VLR and HLR. However, this drawback increases the computational cost in HLR. Hence, we hope that VLR can authenticate MS for each communication session.

5. A mutual authentication mechanism is not provided between MS and VLR. The current GSM authentication protocol only provides a one-way authentication channel for roaming users. It is therefore possible for an intruder to pretend to be a legal VLR and thus to get the MS's credentials [20].

3.2 Our Protocol

To fix the above drawbacks and to meet all the requirements covered in the Introduction part, an efficient authentication protocol of GSM for roaming users is proposed in this section. The proposed protocol is based on Lee et al.'s scheme [23] and Chang et al.'s scheme [5]. Its key concept is that the HLR of the MS gives the visited VLR authorization to authenticate the MS without knowing the secret key K_i of the MS. That is to say, the visited VLR only keeps a copy of TK_i to identify the MS and thus saves the space overhead in VLR. Furthermore, the VLR does not turn back to the HLR to require another set of authentication parameters and thus the bandwidth consumption between VLR and HLR is reduced.

Assume that an adversary is operating a device having the functionality of a VLR. Such a device is called a false VLR and is commercially available. Through the device, the adversary can impersonate a genuine VLR and entice a legitimate mobile user. To identify the legality of the visited VLR, the HLR of the MS gives the VLR a certificate CERT_VLR that will be authenticated by the MS. No one can pretend to be the legal VLR to fool the MS and get the MS's credentials. Therefore, our mechanism not only identifies the MS but also the legality of the visited VLR. It can achieve mutual authentication. In addition, the proposed protocol is suitable for roaming users. When the MS moves to another new VLR, the old VLR just forwards the TK_i instead of the remaining copies of n authentication parameters to the new VLR, and this way the communication overhead can be reduced.

Our protocol consists of three phases, namely, Phase 1, Phase 2, and Roaming Phase. Phase 1 is when the MS joins the new VLR and asks for the first authentication. In this phase, the HLR of the MS gives the VLR a TK_i to authenticate the MS without knowing the secret key K_i of the MS. The visited VLR will use it to authenticate the MS as long as the MS stays in the coverage of the visited VLR. In Phase 2, when the MS stays in the coverage of this visited VLR, the MS sends the jth authentication request to the VLR, where $j > 1$ and $j \in N$. Finally, the Roaming Phase happens when the MS moves to an area covered by another new VLR. In other words, Phase 1 is done only once when a MS joins the system. Then Phase 2 and the Roaming Phase are performed every time the MS uses the system services. Now, let's take a closer look at these three phases.

3.2.1 Phase1: The First Authentication With The Visited VLR

Firstly, we propose an efficient GSM authentication protocol for the first-time authentication which is shown in Figure 5. The details are as follows:

(1) While the MS enters a new area and requires new communication ser-

vices, the MS sends the TMSI, LAI, and T_1 to the visited VLR.

(2) After receiving the TMSI, the new VLR can use the TMSI to get the IMSI from the old VLR. Then the new VLR sends the ID_V, IMSI, and T_1 to HLR. Note that when there is no old VLR available, the new VLR can directly get the IMSI from the MS. Hence, the IMSI is revealed to the public network. A lot of anonymous schemes have been proposed to solve this problem. Here, our protocol including the original GSM protocol, does not discuss it.

(3) After that, the HLR checks whether the visited VLR is legal and whether T_1 is valid or not. If either of them is not valid, the authentication process is terminated; otherwise, HLR computes CERT_VLR=A3(T_1, K_i) and TK_i=A3($RAND$, K_i). Then the HLR sends CERT_VLR, $RAND$, and TK_i to the VLR through a secure channel.

(4) After receiving these authentication parameters, the VLR keeps TK_i in its own database and then computes $SRES$=A5(T_1, TK_i) and stores it in its own database. Then, the VLR sends CERT_VLR, $RAND$, and T_1 to the MS.

(5) When the MS receives theses messages, the MS first checks if T_1 is the same as it was before. If the result of the check is positive, the MS computes CERT_VLR'=A3(T_1, K_i) and then compares it with the received CERT_VLR. If they match, the VLR is authenticated. The MS then computes TK_i=A3($RAND$, K_i) and $SRES'$=A5(T_1, TK_i), and then sends $SRES'$ back to the VLR.

(6) Once the VLR receives $SRES'$ from the MS, it compares it with the $SRES$. If they are the same, the MS is authenticated; otherwise, the MS is not a legal user.

3.2.2 Phase 2: The jth Authentication Between The Same VLR And MS, $j > 1$

As long as the MS stays in the coverage area of the same VLR, the VLR can use the TK_i to authenticate the MS for each call. That is to say, as long as the MS stays in the coverage of the same VLR, the VLR does not need to go back to HLR to require another set of authentication parameters. The authentication process is depicted in Figure 6 and described as follows.

(1) When the MS requires a new communication, the MS computes $SRES_j$=A5(T_j, TK_i) and sends an authentication request to the VLR. The request includes TMSI, $SRES_j$, T_j.

(2) Upon receiving these messages from the MS, the VLR first checks whether T_j is valid or not. If it is not valid, the authentication is put to a stop; otherwise, the VLR computes $SRES'_j$=A5(T_j, TK_i), and then compares it with the received $SRES_j$. If they do not match, the process is terminated; otherwise, the MS is authenticated and the VLR can compute CERT_VLR$_j$=A3(T_j, TK_i), which is then sent back to the MS along with T_j.

(3) Once the MS receives CERT_VLR$_j$ and T_j from the VLR, the MS first checks if T_j is the same as it was before. If positive, the MS computes CERT_VLR$'_j$=A3(T_j, TK_i) and the MS compares it with the received CERT_VLR$_j$. If they are the same, the VLR is authenticated; otherwise, the process is terminated.

3.2.3 Roaming Phase

When MS moves to an area covered by another new VLR, as Figure 7 illustrates, the flow of signaling messages is generated while the roaming MS performs either the location registration or update. The details are described as follows.

Step 2-1: While the MS moves to the area covered by VLR2, the MS computes $SRES_y$=A5(T_y, TK_i) and sends a TMSI1, T_y, and $SRES_y$ to VLR2.

Step 2-2: After receiving these messages, VLR2 forwards TMSI1 to the area managed by VLR1.

Step 2-3: VLR2 receives an IMSI and a TK_i from VLR1 through a secure channel. Then VLR2 computes $SRES'_y$=A5(T_y, TK_i) and compares it with the received $SRES_y$. If they do not match, the process is terminated; otherwise, the MS is authenticated.

Step 2-4: VLR2 computes CERT_VLR$_y$=A3(T_y, TK_i) and sends it along with T_y to the MS. Once the MS receives CERT_VLR$_y$ and T_y from the VLR2, the MS first checks if T_y is the same as it was before. If positive, the MS computes CERT_VLR$'_y$=A3(T_y, TK_i) and compares it with the received CERT_VLR$_y$. If they are the same, the VLR is authenticated; otherwise, the process is terminated.

Step 2-5: VLR2 sends a location update message to HLR. HLR updates the location of the MS accordingly.

Step 2-6: HLR returns an acknowledgement for the location update.

Step 2-7: VLR2 assigns a TMSI2 to the MS.

Step 2-8: HLR finally transmits a TMSI1 cancellation message to VLR1.

If the MS moves to yet another area covered by VLR3, a similar authentication procedure will be performed. The security of our protocol for roaming users is also based on algorithms $A3$ and $A5$. In addition, the architecture of the existing GSM still remains the same. Note that the TK_i should not be used forever. A period of validity should be set, or it should stay active only before a certain maximum number of times of forwarding is reached. Furthermore, to reduce the location update cost for mobile communication, pointer forwarding [18] can be applied to our protocol. To keep track of the whereabouts of a mobile user, the HLR must get the location updated frequently so the traffic can move on. Therefore, the objective of pointer forwarding is to reduce the update cost. Our protocol can also reduce the location update cost in the same way.

4 Quality of Service Analyses

To evaluate our proposed protocol with respect to the protocol requirements listed in the Introduction section, in this section we shall analyze our protocol in terms of security, efficiency and goals.

4.1 Security Analysis

The proposed protocol does not change the architecture of the existing authentication protocol of GSM. Therefore, the robustness of the proposed protocol is the same as that of the original GSM, which is based on security algorithms $A3$, $A5$, and $A8$. As shown in Section 3.2.1, CERT_VLR is used to verify the visited VLR and the $SRES$ is used to verify the MS, where CERT_VLR=A3(T_1, K_i) and $SRES$=A5(T_1, TK_i). K_i is a secret key shared between MS and HLR, and TK_i is a temporary secret key shared between MS and VLR, where TK_i=A3($RAND$, K_i). Without knowing K_i and TK_i, no one can derive these values. That is to say, only a valid VLR can receive the certificate from the HLR, and only a valid MS can compute $SRES$. Furthermore, a timestamp T_1 used to help resist the replaying attack. The MS can check if it is the same as it was before. Even if an attacker gets to intercept the authentication parameters, the values cannot be used for later communications.

The CERT_VLR$_j$ is used to verify the visited VLR, and the $SRES_j$ is used to verify the MS, where $SRES_j$=A5(T_j, TK_i) and CERT_VLR$_j$=A3(T_j,

TK_i). Without knowing the TK_i, these values can not be computed. That is to say, only a valid VLR can compute the certificate, and only a valid MS can compute $SRES_j$. Furthermore, the timestamp T_j is also used to resist the replaying attack. In other words, without the knowledge of K_i and TK_i, no one can forge MS and VLR to fool others.

An issue such as the problem that a wrong VLR may try to cheat the HLR in order to get the TK_i and $CERT_{VLR}$ information can be prevented by the following assumption. In our protocol, we assume that the HLR and all VLRs are trusted centers. This assumption is the same as other protocols. When the VLR wants to get the authenticated parameters, the HRL first verifies the legitimacy of the VLR, and vice versa.

Our proposed protocol can overcome the following attacks:

- Replaying attacks: As shown above, our protocol uses a timestamp to resist the replaying attack. Since $SRES$ is used only once, an adversary cannot intercept it and replay it to the VLR. In addition, the timestamp is embedded in the authenticated parameters. Without the knowledge of K_i and TK_i, no one can compute the replayed messages and replay them.

- Impersonating attacks: An adversary may try to impersonate one party to communicate with another party. If the adversary tries to impersonate the MS, the adversary cannot create the correct $SRES$ and cannot continue the protocol. If the adversary tries to impersonate the VLR, the adversary cannot create the correct certificate $CERT_{VLR}$ and cannot continue the protocol. Hence, without the knowledge of K_i and TK_i, no one can impersonate MS and VLR to fool others. In any case, the adversary is unable to obtain an advantage by active impersonation over what he/she could do by passive eavesdropping.

- Man-in-the-middle attacks: To resist this type of attack, a solution to establish mutual authentication is proposed in our protocol. In our protocol, the MS can verify the VLR by the received $CERT_{VLR}$. It can not be created unless the adversary knows K_i. On the other hand, the VLR can verify the MS by the received $SRES$. This also can not be created unless the adversary knows TK_i. Hence, our protocol can resist man-in-the-middle attacks. The legal identity of that user in the middle can not be replaced.

In addition, it is assumed that a secure channel between VLR and HLR is ready before mobile communications [5, 23].

4.2 Efficiency Analysis

The focus of our proposed protocol is on the user authentication schemes rather than on session key generation. Therefore, the protocol only needs to execute security algorithms A3 and A5 for user authentication. Of course, the protocol can involve session key generation so as to execute security algorithm A8. The number of algorithm combinations A3/A5 executed by each participant is listed in Table 2, Table 3, and Table 4. It is seen that the HLR only executes A3 twice in Phase 1. The load on HLR is very low. Our new protocol is more efficient than the current GSM authentication protocol for roaming users because the HLR no longer has to execute A3 at least n times. In addition, our protocol does not generate a random number for each communication request as Lee et al.'s protocol [23]. In our protocol, the VLR only keeps a TK_i to generate his/her certificate and MS's signed result. The efficiency of our protocol is approximately the same as that of Chang et al.'s protocol [5]. Only two rounds of mutual authentication are needed in Phase 2 and the Roaming Phase.

Table 2: The number of algorithm combinations A3/A5 executed by each participant in Phase 1

	MS	VLR	HLR
A3	2	0	2
A5	1	1	0

Table 3: The number of algorithm combinations A3/A5 executed by MS and VLR in Phase 2

	MS	VLR
A3	1	1
A5	1	1

Table 4: The number of algorithm combinations A3/A5 executed by MS and VLR in the Roaming Phase

	MS	VLR
A3	1	1
A5	1	1

4.3 Goals Analysis

In this subsection, we shall demonstrate that our protocol indeed can get rid of the drawbacks mentioned earlier in Section 3.1. The goals of our protocol are as follows:

- Roaming:

  The communication overhead between VLRs is increased because the MS roams frequently. To reduce the overhead, VLRs only forward TK_i instead of n copies of the authentication parameters. Thus, it is suitable for roaming users and reduces the communication overhead.

- Reduction of bandwidth consumption:

  The HLR gives the VLR a temporary secret key TK_i to authenticate MS with. As long as the MS stays in the coverage area of the same VLR or roams between VLRs, the VLR can use the TK_i to authenticate MS for each call. That is to say, the VLR does not turn back to the HLR to require another set of authentication parameters, and thus the bandwidth consumption between VLR and HLR is reduced.

- Reduction of storage overhead in VLR's database:

  The VLR only keeps a copy of TK_i instead of n copies of authentication parameters, and thus the storage overhead in VLR is reduced.

- Reduction of overload of HLR:

  In the proposed protocol, the HLR just outputs a copy of authentication parameters instead of n copies of authentication parameters. That is to say, the HLR gives authorization to the VLR, and then MS is authenticated by the VLR without the assistance of the HRL. Therefore, the overload of HLR can be reduced.

- Mutual authentication:

  In fact, we assume that the HLR is a trustworthy authority with the capability of identifying the VLR by using cryptographic techniques such as *digital signatures* [36]. Once the VLR can be verified, the HLR can assign a certificate, CERT_VLR, which will be sent to MS for authenticating the VLR. By authenticating the CERT_VLR, MS can ensure that the VLR is valid. When the MS stays in the coverage of the same VLR or roams between VLRs, only the valid MS and VLR can compute the signed result $SRES_j$ and the certificate CERT_VLR$_j$. Therefore, the proposed protocol can achieve mutual authentication between MS and VLR.

In Table 5, we compare the goals of our protocol with some other efficient GSM authentication protocols. The symbols used in Table 5 are defined as follows. RO means it is suitable for roaming users; RBC means it reduces the bandwidth consumption; RSO means it reduces the storage overhead in VLR's database; ROH means it reduces the overload of HLR; MA1 means it achieves mutual authentication for the first authentication; MA2 means it achieves mutual authentication for the rest of the authentication; AC means it changes the GSM architecture; N denotes no; Y denotes yes. It can be easily seen that our protocol can achieve all the goals defined in the previous section. The other protocols cannot achieve all these goals and are not suitable for roaming users. According to the comparison, our protocol is superior to the other GSM authentication protocols.

5 Conclusions

Nowadays, 3G and 4G mobile systems are becoming more and more dominant in the market. However, the cost for base station construction is still very high. Many telecommunication companies still use the old standard of Pan-European digital cellular system (GSM) or integrate the GSM system with their 3G/4G systems. Therefore, the GSM system is still popular and

Table 5: Comparisons among the GSM authentication protocols

	Original	Our	[5]	[23]	[1]	[12]	[22]	[11]
RO	N	Y	N	N	N	N	N	Y
RBC	N	Y	Y	Y	Y	Y	Y	N
RSO	N	Y	Y	Y	N	N	Y	N
ROH	N	Y	Y	Y	N	N	Y	N
MA1	N	Y	Y	Y	N	N	N	N
MA2	N	Y	Y	N	N	N	N	N
AC	-	N	N	N	Y	Y	N	N

widespread because of its simplicity and efficiency. Many authentication protocols have been developed to improve the original authentication protocol of GSM, but they have not taken the roaming users into account and mostly cannot solve the problems without modifying the architecture of GSM. In this paper, we have pointed out the drawbacks of the GSM authentication protocol for roaming users and presented a new authentication protocol that can fix all the drawbacks. The proposed protocol does not only inherit the advantages of Lee et al.'s and Chang et al.'s protocol, but also is very suitable and efficiency-increasing for roaming users. Of course, the concept of this protocol can also be applied to 3G/4G mobile systems.

Acknowledgment

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC 98-2221-E-468-002 and NSC 95-2221-E-005-051-MY3. Our gratitude also goes to Dr. Timothy Williams, Asia University.

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), pp. 21–30, 1998.

[2] K. Ammayappan, A. Saxena, and A. Negi, "Mutual authentication and key agreement based on elliptic curve cryptography for GSM," in *International Conference on Advanced Computing and Communications, 2006.*, pp. 183–186, Dec. 2006.

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

[4] 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.

[5] C. C. Chang, J. S. Lee, and Y. F. Chang, "Efficient authentication protocols of GSM," *Computer Communications*, vol. 28, pp. 921–928, January 2005.

[6] Alberto Peinado Dominguez, "Cryptanalysis of Parka's authentication protocol in wireless mobile communication systems ," *International Journal of Network Security*, vol. 3, no. 3, pp. 279–282, 2006.

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

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

[9] Vincenzo Falletta and Fabio Ricciato, "Detecting scanners: empirical assessment on a 3G network ," *International Journal of Network Security*, vol. 9, no. 2, pp. 143–155, 2009.

[10] A. Fanian, M. Berenjkoub, and T. A. Gulliver, "A new mutual authentication protocol for GSM networks," in *Canadian Conference on Electrical and Computer Engineering*, pp. 798–803, May 2009.

[11] G. Hahn, T. Kwon, S. Kim, and J. Song, "Design and analysis of improved GSM authentication protocol for roaming users," in *Lect. Notes Computer Sci. 3222*, pp. 451–458, 2004.

[12] L. Harn and H. Y. Lin, "Modification to enhance the security of the GSM protocol," in *Proceedings of the 5th National Conference on Information Security*, pp. 416–420, Taipei, May 1995.

[13] Min-Shiang Hwang, "Dynamic participation in a secure conference scheme for mobile communications," *IEEE Transactions on Vehicular Technology*, vol. 48, no. 5, pp. 1469–1474, 1999.

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

[15] Min-Shiang Hwang, Cheng-Chi Lee, and Ji-Zhe Lee, "A new anonymous channel protocol in wireless communications," *International Journal on Electronics and Communications*, vol. 58, no. 3, pp. 218–222, 2004.

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

[17] Min-Shiang Hwang and W. P. Yang, "Conference key distribution protocols for digital mobile communication systems," *IEEE Journal on Selected Areas in Communications*, vol. 13, pp. 416–420, Feb. 1995.

[18] R. Jain and Y. B. Lin, “Performance modeling of an auxiliary user location strategy in a PCS network,” *ACM-Baltzer Wireless Networks*, vol. 1, no. 2, pp. 197–210, 1995.

[19] V. Kalaichelvi and R. M. Chandrasekaran, “Secure authentication protocol for mobile,” in *International Conference on Computing, Communication and Networking, 2008*, pp. 1–4, Dec. 2008.

[20] Paual A. Karger, Y. Frankel, and A. Herzberg, “Security issues in a CDPD wireless network,” *IEEE Personal Communications*, vol. 2, pp. 16–27, August 1995.

[21] K. P. Kumar, G. Shailaja, A. Kavitha, and A. Saxena, “Mutual authentication and key agreement for GSM,” in *International Conference on Mobile Business, 2006.*, pp. 25–28, June 2006.

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

[23] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang, “Extension of authentication protocol for GSM,” *IEE Proceedings - Communications*, vol. 150, no. 2, pp. 91–95, 2003.

[24] Jing Li, Po Zhang, and Srinivas Sampalli, “Improved security mechanism for mobile IPv6,” *International Journal of Network Security*, vol. 6, no. 3, pp. 291–300, 2008.

[25] H. Y. Lin and L. Harn, “Authentication protocols with nonrepudiation services in personal communication systems,” *IEEE Communications Letters*, vol. 3, no. 8, pp. 236–238, 1999.

[26] Chi-Chun Lo and Yu-Jen Chen, "A secure communication architecture for GSM networks," in *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pp. 221–224, 1999.

[27] Chi-Chun Lo and Yu-Jen Chen, "Secure communication mechanisms for GSM networks," *IEEE Transactions on Consumer Electronics*, vol. 45, no. 4, pp. 1074–1080, 1999.

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

[29] Aikaterini Mitrokotsa, Nikos Komninos, and Christos Douligeris, "Protection of an intrusion detection engine with watermarking in ad hoc networks," *International Journal of Network Security*, vol. 10, no. 2, pp. 93–106, 2010.

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

[31] Animesh Patcha and Jung-Min Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *International Journal of Network Security*, vol. 2, no. 2, pp. 131–137, 2006.

[32] Moe Rahnema, "Overview of the GSM system and protocol architecture," *IEEE Communication Magazine*, vol. 31, pp. 92–100, April 1993.

[33] Wei Ren, "Pulsing RoQ DDoS attacking and defense scheme in mobile ad hoc networks," *International Journal of Network Security*, vol. 4, no. 2, pp. 227–234, 2007.

[34] Didier Samfat, Refik Molva, and Gene Tsudik, "Authentication of mobile users," *IEEE Network*, vol. 8, pp. 26–34, March 1994.

[35] J. F. Stach, E. K. Park, and K. Makki, "Performance of an enhanced GSM protocol supporting non-repudiation of service," *Computer Communications*, vol. 22, pp. 675–680, 1999.

[36] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Prentice Hall, second edition, 1999.

[37] Hsien-Chu Wu, Chi-Yu Liu, and Shu-Fen Chiou, "Cryptanalysis of a secure one-time password authentication scheme with low-communication for mobile communications ," *International Journal of Network Security*, vol. 1, no. 2, pp. 74–76, 2005.

[38] Christos Xenakis, "Security measures and weaknesses of the GPRS security architecture," *International Journal of Network Security*, vol. 6, no. 2, pp. 158–169, 2008.

[39] Cheng-Ying Yang and Cheng-Yeh Shiu, "A secure mobile IP registration protocol," *International Journal of Network Security*, vol. 1, no. 1, pp. 38–45, 2005.

[40] Aneta Zwierko, Zbigniew Kotulski, "Integrity of mobile agents: a new approach," *International Journal of Network Security*, vol. 4, no. 2, pp. 201–211, 2007.

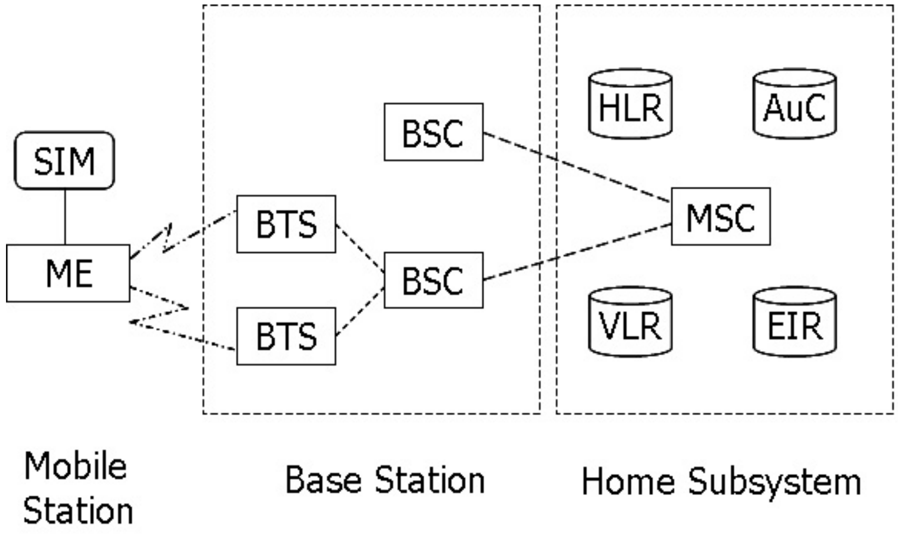

Figure 1: The GSM Network

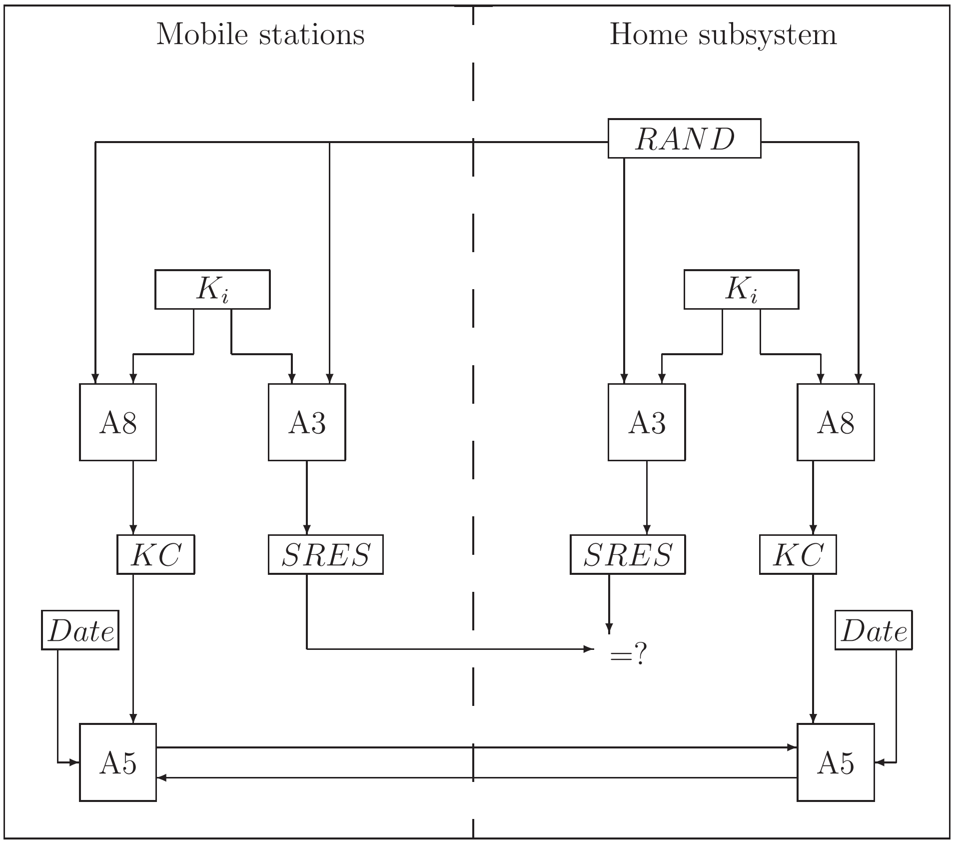

Figure 2: Architecture of GSM

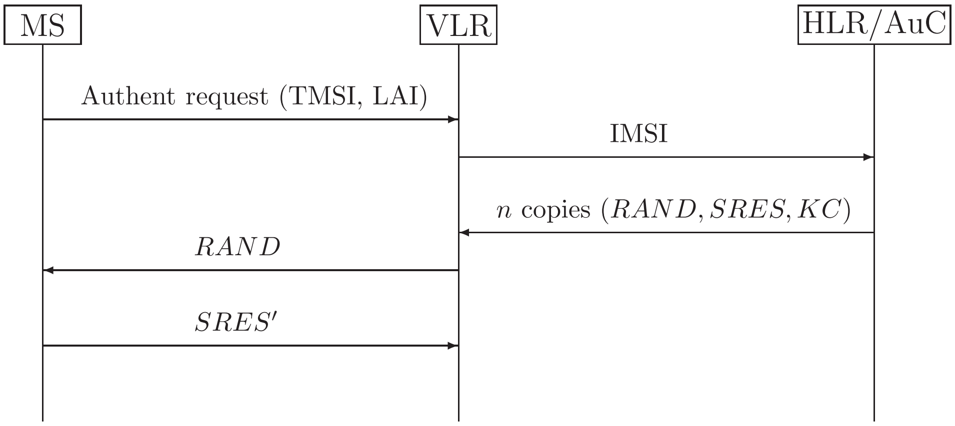

Figure 3: The authentication protocol of GSM

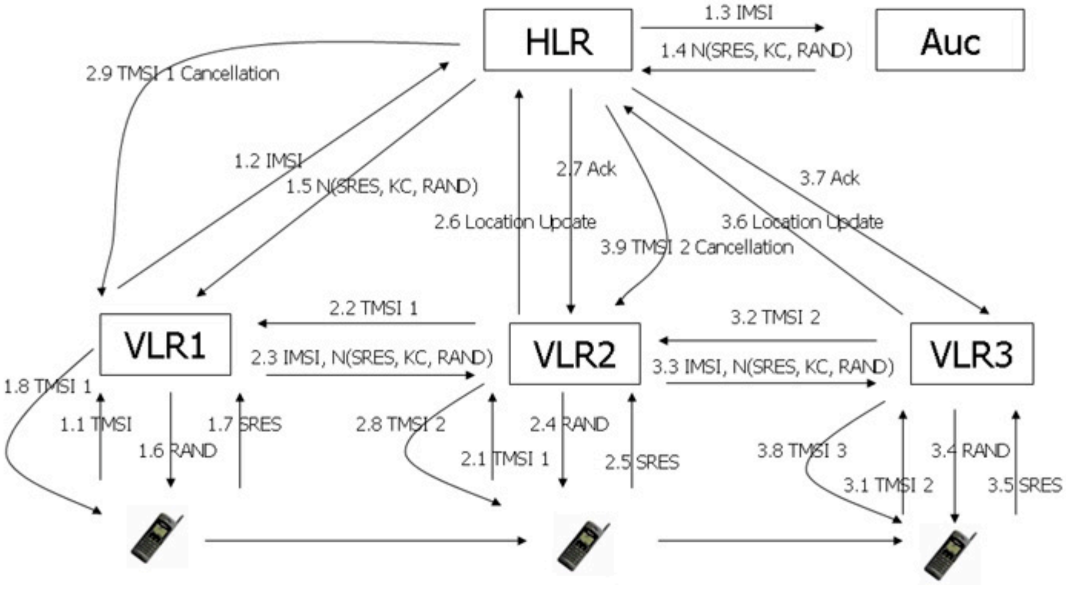

Figure 4: GSM authentication protocol for a roaming user

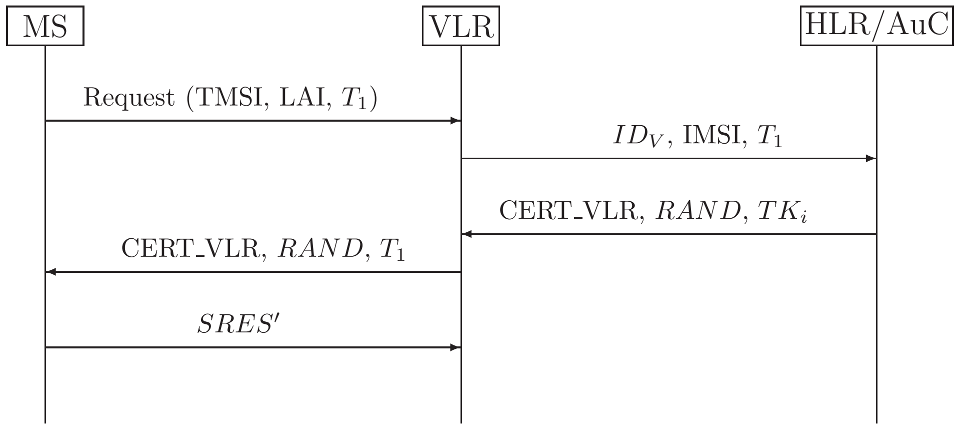

Figure 5: The proposed authentication protocol for the first authentication

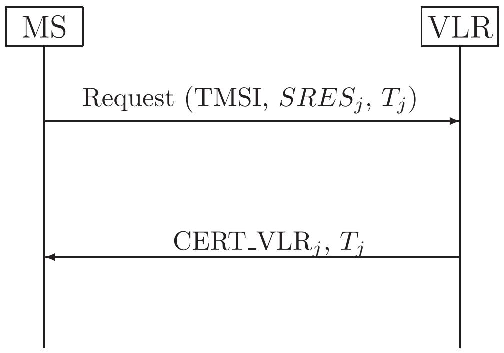

Figure 6: The proposed authentication protocol for the jth authentication

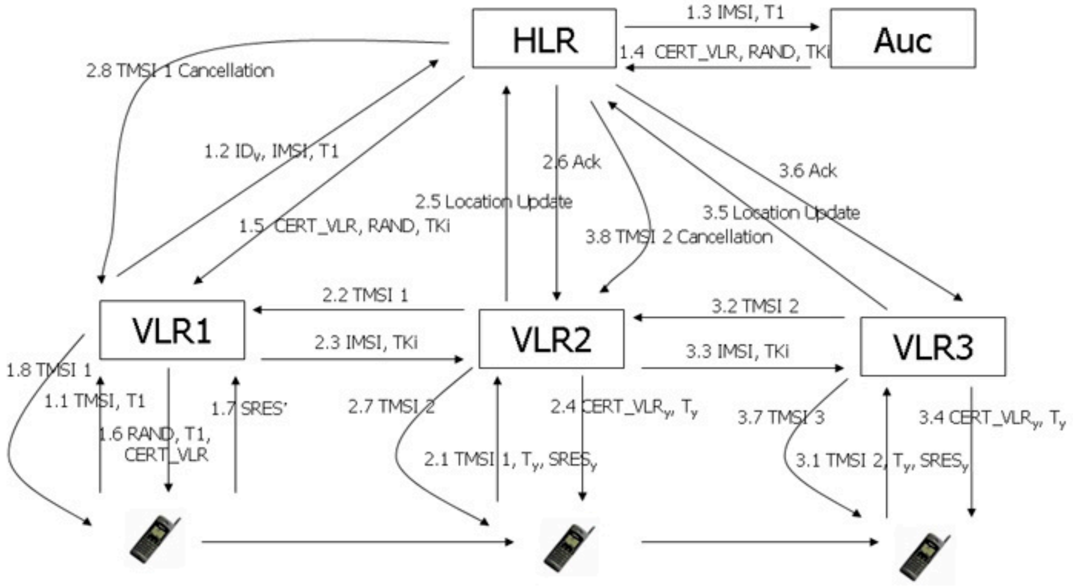

Figure 7: The proposed authentication protocol for a roaming user