J Inf Process Syst, Vol.13, No.1, pp.152~173, February 2017
https://doi.org/10.3745/JIPS.03.0064

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Secure Authentication Approach Based New Mobility Management Schemes for Mobile Communication

Ghazli Abdelkader*, Hadj Said Naima*, and Ali Pacha Adda*

Abstract

Mobile phones are the most common communication devices in history. For this reason, the number of mobile subscribers will increase dramatically in the future. Therefore, the determining the location of a mobile station will become more and more difficult. The mobile station must be authenticated to inform the network of its current location even when the user switches it on or when its location is changed. The most basic weakness in the GSM authentication protocol is the unilateral authentication process where the customer is verified by the system, yet the system is not confirmed by the customer. This creates numerous security issues, including powerlessness against man-in-the-middle attacks, vast bandwidth consumption between VLR and HLR, storage space overhead in VLR, and computation costs in VLR and HLR. In this paper, we propose a secure authentication mechanism based new mobility management method to improve the location management in the GSM network, which suffers from a lot off drawbacks, such as transmission cost and database overload. Numerical analysis is done for both conventional and modified versions and compared together. The numerical results show that our protocol scheme is more secure and that it reduces mobility management costs the most in the GSM network.

Keywords

Authentication, GSM, Location Update, Mobility Management, Paging, Security

1. Introduction

The global system for mobile communication (GSM) is a digital mobile telephony system that is widely used in Europe and other parts of the world.

In addition to telephony, in modern mobile phones like smartphones, a large variety of services are supported such as Short Message Service (SMS), Multimedia Message Service (MMS), email, Internet access, business applications, and online gaming.

To better ensure theses functionalities, mobile phones require a good protocol to manage their mobility because these services must be available at any time where the mobile is moving anywhere in the network. The mobility management protocol provides the continuous location of the mobile station. It also includes two security features: user authentication, which allows the network to verify the accuracy of the identity of the MS, and keeping their identity confidential in order to prevent a hacker who is listening to the radio interface to follow the movements of a mobile subscriber.

Manuscript received July 27, 2015; first revision November 11, 2015; accepted January 6, 2016.

Corresponding Author: Ghazli Abdelkader (abdelkader.ghazli@univ-usto.dz)

* Dept. of Mathematics and Computer Science, University of Science and Technology (USTO), Oran, Algeria (abdelkader.ghazli@univ-usto.dz, nim_hadj @yahoo.fr, a.alipacha@gmail.com)

Location management schemes are based on users' mobility and incoming call rate characteristics. The network mobility process has its two basic procedures: location update (or registration) and paging. The location update procedure allows the system to more or less keep the exact location of the user. Location registration is also used to bring the user's service profile near its location. The paging process by the system sends paging messages to all cells where the mobile terminal can be located. A network must retain information about the locations of end points in the network in order to route traffic to the correct destinations. Location management refers to the problem of updating and searching for the current location of a mobile station in a GSM network. To make it efficient, the sum of the update costs for the location database must be minimized. The mobile station must be authenticated by the network before registering its location in the network even is switching on or moving in each cellule in the network. The GSM security issue covers three main aspects: authentication, confidentiality, and anonymity. Confidentiality is achieved by encrypting the radio channel. However, anonymity is achieved by using temporary identities, such as TMSI. In the GSM network, the unilateral authentication protocol is supported so that the network cannot be authenticated by the mobile station where the network sends a challenge to the mobile station, which must use the A3 algorithm to send back an appropriate response called SRES. Several drawbacks have been found in the GSM authentication protocol, including not supporting mutual authentication between the mobile station and the network. Furthermore, there are the issues of vast bandwidth consumption between VLR and HLR, storage space overhead in VLR, and high computation costs in VLR and HLR.

The study presents a secure authentication process to enhance the disadvantage of the current GSM authentication protocol based on an intelligent location management scheme to reduce the transition between the VLR and HLR by proposing a new location registration and call delivery procedures.

2. Components in Mobility Management

The elements of mobility management in GSM network are as described below.

Mobile station (MS): The phone and SIM (Subscriber Identity Module) card are the only two elements that a user has direct access to. These two elements are sufficient for carrying out all of the functions necessary for transmissions and managing travel. The main function of the SIM card is to contain and manage a variety of information, like the secret key Ki that it used in the authentication process in the GSM network.

Base station: This is an antenna that transmits and receives radio signals over a cell in a wireless network.

Base station controller (BSC): This is an agent that performs functions on behalf of a group of base stations. The BSC handles the allocation of radio channels, controls handovers, performs paging, and interfaces with the central network and HLR.

Cell: This is a geographical area serviced by a base station in a wireless network that also used to refer to one or more collocated base stations. Cells are the building blocks of a cellular network, with overlapping cells defining the coverage area of a particular network.

Location area (LA): In the location areas approach, the service coverage area is partitioned into location areas, and each location area consists of several contiguous cells. The base station of each cell broadcasts the identification (ID) of location area to which the cell belongs. Therefore, a mobile station knows which location area it is in Fig. 1 illustrates a service area with three location areas.

A mobile station will update its location whenever it moves into a cell that belongs to a new location area. For example, when a mobile station moves from cell B to cell D as we show in Fig. 1, it will report its new location area because cell B and cell D are in different location areas.

Handoff: This is the process of transferring an in-progress call from one cell or base station to a neighboring cell without interruption.

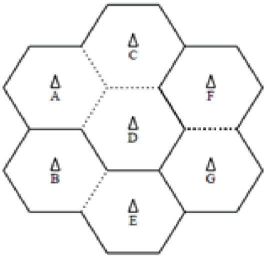

Fig. 1. Three location areas.

Home location register (HLR): This is the central database that contains the details of each mobile subscriber that is authorized to use the GSM core network. HLRs store the information of every SIM card issued by the mobile network operator. SIM cards have a unique identifier called an IMSI, which is the primary key to each HLR record. MSISDN (telephone number) information is also kept within the SIM and is a primary key in the HLR database.

Paging: Under a LA scheme, the network does not know the precise location of a device, only its general area. Paging is performed on an incoming call and involves sending a message to all cells in the LA to determine which one contains the destination device.

Visitor location register (VLR): The GSM VLR is a database that contains temporary information about subscribers, which is needed by the MSC in order to service visiting subscribers.

PSTN: This is the public switched telephone network, which is the world's collection of interconnected voice-oriented public telephone networks that are both commercial and government-owned [1,2].

3. Mobility and Authentication in a GSM Network

In a fixed network, the phone is always connected to the same switching center. However, in a mobile environment, a MS is not always attached to the same MSC. That is why the mobile must regularly inform the network of its current location. When a MS is placed under tensioned by the user, it is attached to the network, or when its location in the air is changed, it informs the MSC that controls the location area, in which it is present, of its current location [1,2].

To realize this action, a mobile uses a mobility management (MM) protocol, which provides the continuous location of the MS. It also includes two security features: authentication of the user, which allows the network to verify the accuracy of the identity of the MS, and keeping their identity confidential in order to prevent an attacker who is listening to the radio interface from being able to track the movements of a mobile subscriber [3,4]. The MS initiates a location update request when it detects that it has entered in a new location area by receiving a new location area number that is different from that which is stored on its SIM card. The network initiates an authentication and encryption message containing all of the necessary parameters for the calculation of results from authentication algorithms and encryptions. The mobile station returns the results to the MSC/VLR through the response. If the response is not valid, a rejection messages is sent to the mobile station [5,6].

3.1 Location Management in GSM Networks

The location management allows the system to know the position of a mobile at all moments. This function is necessary for the system to attach to a mobile station (Fig. 2).

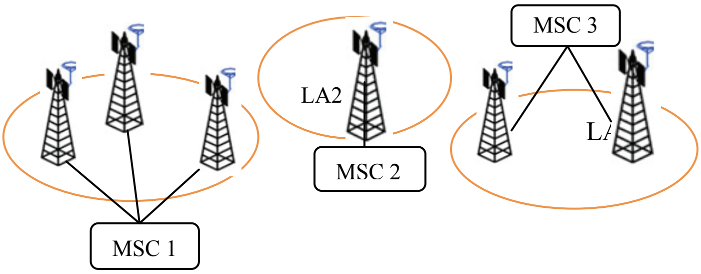

Fig. 2. Location areas.

The two basic mechanisms involved in the location management in GSM network are as listed below [3].

- Registration or location update when a MS informs the network of its location.
- Paging or tracking location, which is a mechanism initiated by the network to search for the location required when the network attempts to make a call to the MS.

The basic unit for location tracking in a GSM network is the LA, which groups a number of BTSs that communicate with MSC over radio links. The location updating procedures and subsequent call routing use the MSC and two location registers: the HLR and the VLR. When a mobile station is switched on in a new location area or when it moves to a new location area or different operators, it must register with the network to indicate its current location [2,4].

3.1.1 Location Update

In the GSM network, each BTS periodically send the related LA numbers to the MSs. Upon receiving it, the MS compares it with the location area address stored in its memory. If it's different it sends a message to the network to be registered. There are three cases of registration or location updates when MS moves from one LA to another LA: inter LA, inter MSC, or inter VLR [2] (Fig. 3).

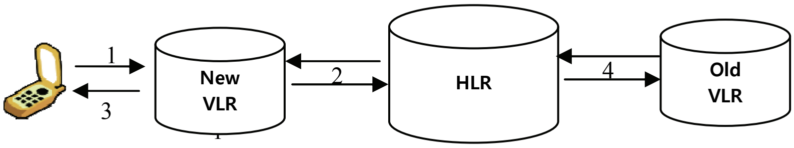

Fig. 3. GSM mobile station registration.

Inter LA location update: When the MS move from a LA to another belongs to the same MSC, the procedure for the location update follows these four steps:

- The MS sends a message to the MSC through its BTS to update its location.
- The MSC forwards the message to the related VLR.
- The VLR finds that the first LA and the second LA are in the same MSC.
- The VLR updates the location area and sends an ACK to the MS.

Inter MSC location update: This happens when a MS moves from the first LA to another LA that belongs to another MSC of the same VLR. The registration process is as follows:

- The MS sends a message to the MSC through its BTS to update its location.
- The VLR finds that the new LA and the old LA belongs to different MSCs of the same VLR.
- The VLR updates the location of the MS and sends a message to the HLR to update the location of MS.
- Upon receiving the message, the HLR updates the field of the MS and sends the ACK message to VLR.
- The VLR forwards the ACK message to the MS.

Inter VLR location update: Inter VLR registration takes place when a MS moves from a LA to another belongs to different MSCs which belong to different VLRs the process of registration is started as follow:

- The MS sends a message to the new MSC through its BTS to update its location.
- The new MSC forwards the message to the new VLR.
- The new VLR sends a message, including TMSI, to the old VLR for identifying the MS.
- The old VLR sends the IMSI of the MS to the new VLR.
- The new VLR updates the location of the MS in its database and sends a message to HLR to update the location of the MS.
- The HLR updates the field of the MS and sends an ACK message to the new VLR.
- The new VLR generates a new TMSI and send it to the MS.
- The old VLR deletes the field of the MS from its database.

3.1.2 Paging

The paging operation is performed by the cellular network when an incoming call arrives for a MS. The cellular network will page the MS in all possible cells to find the cell in which the MS is located so that the incoming call can be routed to the corresponding base station. This process is called paging [7,8].

The number of all possible cells to be paged is dependent on how the location update operation is performed. The location update operation is performed by an active MS (Fig. 4).

- Step 1: If a land line phone attempts to call a mobile subscriber, the call is forwarded to a switch, which is called the originating switch in the PSTN, which queries the HLR to find the current VLR of the MS. The HLR queries the VLR in which the MS resides to get a routable address.
- Step 2: The VLR returns the routable address to the originating switch through the HLR.
- Step 3: Based on the routable address, a trunk (voice circuit) is set up from the originating switch to the MS through the visited MSC [2].

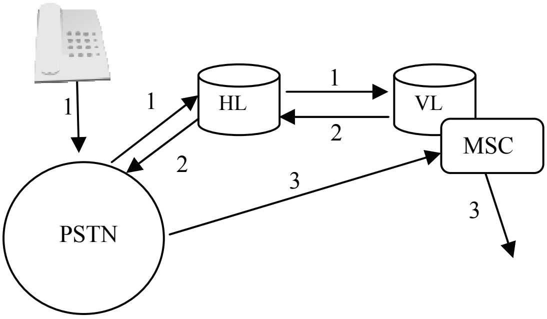

Fig. 4. GSM call delivery.

3.2 Authentication in the GSM Network

When a customer subscribes to a mobile subscription from an operator, it receives a unique identifier called IMSI, which is stored on the SIM card. Upon subscription, a Ki key is assigned to the user with the IMSI. It is stored in the SIM card of the subscriber and the AUC, which presents an essential part of HLR (Fig. 5).

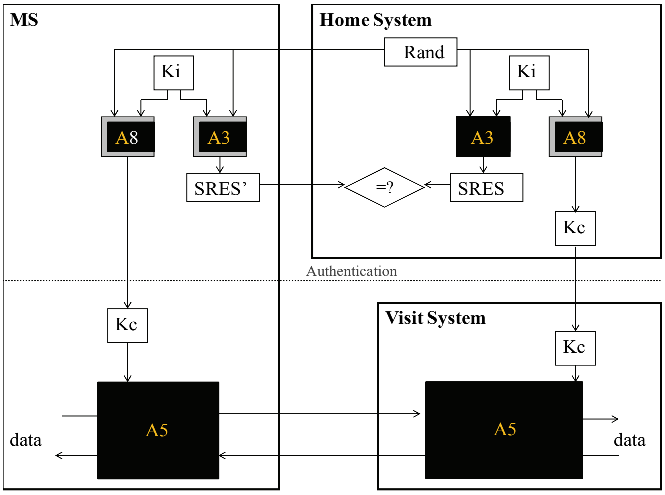

Fig. 5. GSM security algorithms.

The Ki is never transmitted over the radio interface or on the network [9,10].

Three security algorithms exist in GSM networks, namely the A3 authentication algorithm, the A5 ciphering/deciphering algorithm, and the A8 ciphering key generation algorithm [2,11].

The authentication center AuC has the authentication algorithm A3, the algorithm A8 to generate an encryption key, and the customer's key Ki of the network. BTS has the A5 encryption algorithm to encrypt user data and signaling data. A mobile SIM card has the authentication algorithm called A3, the A8 algorithm to generate an encryption key, and the individual authentication key of the user Ki. The A5 encryption algorithm is contained in the mobile equipment [12,13].

After the user has identified him/herself to the network using the IMSI or its TMSI, it must be authenticated. To do this, the individual authentication key Ki and the A3 authentication algorithm are used. To initiate the authentication process, the AuC generates a random number, RAND, of 128 bits in length. RAND and the key Ki of the mobile user are used as input parameters for the A3 authentication algorithm.

The result is called SRES. This is the result of the expected authentication. The HLR returns the MSC/VLR several triplets (RAND, SRES, Kc) [5,14] (Fig. 6).

The MSC/VLR uses the first triplet and requests the mobile authenticate from the RAND value. The mobile uses the same procedure as the AuC and calculates the SRES and an encryption key Kc from the RAND value received from the network and its key Ki that is stored in the SIM card.

The mobile sends the SRES results to the network, which compares it with its SRES. If they are equal, the mobile authentication was successful [12,15].

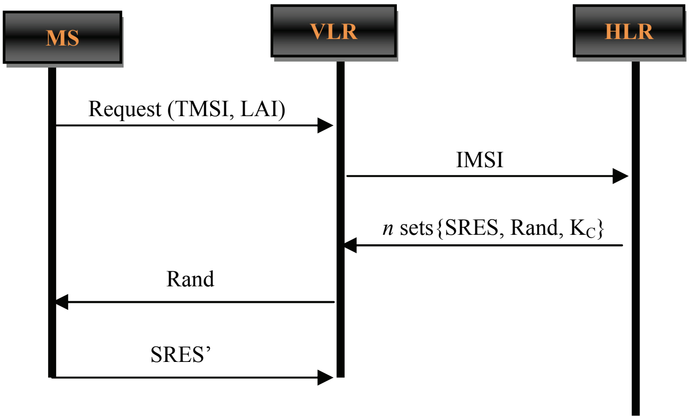

Fig. 6. GSM authentication protocol.

The authentication is performed between the mobile and the VLR and is realized when:

- The mobile is connected to the network
- The mobile initiates an outbound call.
- The mobile receives an incoming call.
- The mobile sends an SMS.
- The mobile receives an SMS.
- The mobile updates its location.

4. Limits of Mobility Management and the Authentication Mechanism in GSM Network

A cellular communication system must track the location of its users in order to forward calls to the related cell in a network. The mobile station must register its new location when moving between cells to allow the correct forwarding of data. Each location update is a costly exercise, involving the use of cellular network bandwidth and core network communication, including the modification of location databases VLR and HLR [16]. Different schemes have been proposed to reduce the cost of the location update and paging in wireless networks. In 2007, the authors [1] described and compared various location management schemes in the cellular networks. Their partitioned different schemes, as in [3] in

1995, into two categories of static and dynamic. A static scheme predetermines the set of cells at which location updates must be generated by a mobile station. However, this scheme is only dynamic if a location update can be generated by a mobile station in any cell depending on its mobility. Several dynamic techniques have been proposed to update the position of the mobile station in the network, which is generally based on thresholds, such as time-based, movement-based, and distance-based [8,16], or profile-based techniques, which are based on previous movements of the mobile station. In 2010, Singh and Karnan [7] proposed a novel intelligent technique for reducing the location update and paging cost. The technique uses an algorithm called a Cascaded Correlation Neural Network to find the called MS current cell within its registered LA in the most accurate and efficient way possible. The method represents a great reduction in location update and paging costs. Stephan et al. [17] in 2010, proposed a new mechanism that registers the location of the mobile station when it resides for a long fixed time in the cell. The mobile station location management scheme was proposed by Jie and Kadhim [14] in 2013, based on the history of movement. Their approach uses the database to predict the future location of the mobile station. In 2011, the authors [18] proposed a static method for the location management scheme. It uses a technique of Bloom filtering in the never update strategy of static location management to select the cells that to be paged and thereby helps to reduce the polling cost to a greater extent. Selvan and Shanmugalakshmi [19] in 2011, presented Location Management Techniques to improve QoS in mobile networks using an intelligent agent, which needs some adaptation with the existing protocols. In the GSM network, before the mobile registers its position in the network, the authentication procedure of the mobile is started. The GSM authentication algorithm is based on a protocol of challenge/response and does not provide mutual authentication. Only a client authentication is performed. The SIM card is not able to verify the identity of the network that the mobile is attached to. In theory, this leaves the door open to human middle attacks. Another problem has been found in the GSM authentication procedure, which is the bandwidth consumption between HLR and VLR because the VLR cannot authenticate the MS without the N triplets being sent from the HLR to the VLR.

The bandwidth consumption and the computational cost in the HLR will also increase when the mobile station moves in the new VLRs because each VLR will request a HLR for new N copies of triplet authentication parameters. Many authentication protocols have been proposed to solve the different drawbacks of the GSM authentication protocol. In 1999, Stach et al. [20] proposed a secure method for GSM by changing the GSM architecture, which can resolve some of the drawbacks mentioned above. In 2003, Lee and Hwang [21] proposed a new protocol based secret and public cryptosystem, which has a very high cost. In 2006, Ammayappan et al. [15] proposed an improvement protocol to the GSM authentication by using elliptic curve cryptography (ECC), but the model change to the GSM architecture and the computational cost is high. In 2009, Fanian et al. [9] proposed a new protocol, which can provide a bilateral authentication. Nevertheless, it changes the architecture of GSM network and is not suitable for roaming users. Later, Lee et al. [5] proposed a new method to solve all of the above drawbacks without changing the existing GSM architecture. However, the mutual authentication between MS and VLR is not provided in the second call [7]. In 2010, Khan and Ullah [22] have presented a new authentication and secure communication protocol for GSM, GPRS based on asymmetric cryptography for user/network authentication, and communication encryption in GSM/GPRS with reduced signaling overhead. However, the proposed protocol changed the architecture of the standard GSM and is computationally very extensive, which requires large processing power, battery, and memory [21]. In 2011, Lee et al. [5] proposed an efficient authentication protocol for mobile communication, which solves all of the drawbacks mentioned, but it can be adapted more to reduce bandwidth consumption between VLR and HLR [1].

5. Our Contribution

Every day, most subscribers do not change their location. They have a specific location during the crossbred from 8:00 to 12:00 (work period) and then move to another location before returning to work from 13:00 to 16:30. After work, a subscriber can usually move to specific locations (market ...) before returning home where he/she spends the majority of his/her time. So, the journey of each subscriber all the days of the week does not change except on the weekend where the subscriber will spend most his/her time at home or in public places, such as supermarkets, gardens, or forests. Our mobility management approach it based on safeguarding the percentage of presence of each subscriber in the VLR and HLR. The update process of this field is done every day. If the subscriber visits the same VLR in the same day and at the same time, his/her presence frequency will increase by 10%. After ten days, it will achieve 100%. If a subscriber is not present in a given period in the location area covered by the VLR, it will decrease the percentage of presence of this subscriber by 10%. If this presence reaches 30%, the VLR will remove the profile of this user from its database.

Table 1. Percentage of presence of mobiles in VLRs

Mobile	Saturday			Sunday			Monday			Tuesday			Thursday			Wednesday		
	VLR	**%**	**Period**	**VLR**	**%**	**Period**	**VLR**	**%**	**Period**	**VLR**	**%**	**Period**	**VLR**	**%**	**Period**	**VLR**	**%**	**Period**
M1	V1	70	P1	V1	60	P1	V1	70	P1	V1	90	P1	V1	90	P4	V1	90	P1
	V2	40	P4	V2	30	P4	V5	40	P4	V2	40	P4	V2	40	P2	V2	40	P3
	V3	40	P2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
M2	V5	10	P1	V1	60	P1	V1	70	P1	V5	70	P1	V1	70	P1	V1	90	P3
	V2	50	P3	V2	30	P4	V5	40	P4	V2	40	P4	V2	40	P2	V2	40	P4
M3	V1	70	P4	V1	60	P1	V1	70	P1	V1	90	P1	V2	90	P1	V1	90	P1
	V2	40	P2	V2	30	P4	V5	40	P2	V2	40	P4	V2	40	P4	V2	40	P4
	V3	40	P4	-	-	-	-	-	-	V4	20	P2	-	-	-	V6	30	P3

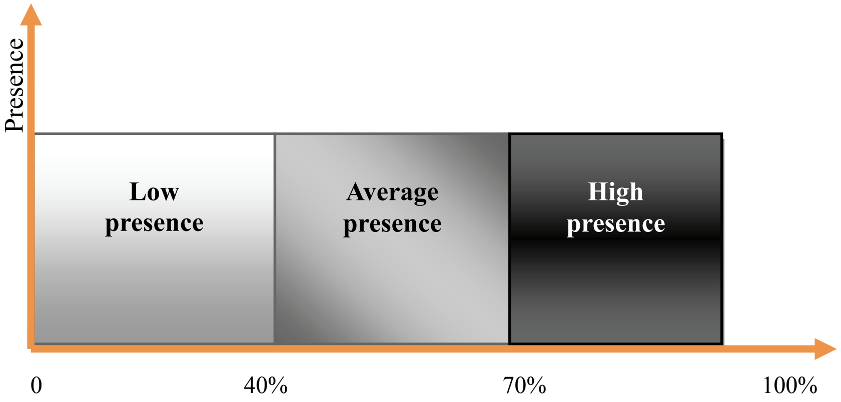

Fig. 7. Classes of presence according to the percentage.

Table 1 shows an example of the location management of different MSs in different periods P1, P2, P3, and P4 in different VLRs V1, V2, V3… every day of the week.

Our dynamic approach is based on the use of three linguistic variables of a low presence (if the presence of a subscriber is less than 40%), average presence (if the presence of subscriber is between 40% and 70%), and high presence (if it is greater than 70%) (Fig. 7).

5.1 Registration Procedure

After the registration of the subscriber in each VLR, fuzzy rules are applied to each profile when a mobile station is switched on in a new LA, or it moves to a new location area.

If the mobile changes its position to a new LA or exchanges its MSC but remains in the same VLR, the registration process will be as described below.

- The MS sends a message to the VLR to update its location.
- The VLR updates the location of the MS by modifying the percentage of presence if it is not 100% or by creating the subscriber profile if it does not exist in its dynamic table.

If the MS changes its position from the LA in the old VLR to another LA in the new VLR, the location update procedure is as listed below (Fig. 8)

- The new VLR checks its dynamic table for the presence of the MS profile by taking into consideration the day and period.
- If the profile of this MS exists in the new VLR, the new VLR updates the percentage of the presence of that MS in its table. If the percentage is less than 100%, then the percentage should increase by 10%.
- If the profile of the MS does not exist in the new VLR, the new VLR adds the profile of this MS to the dynamic table with a presence equal to 10% and sends an update request to the HLR.
- The HLR updates the location of the MS in its table and sends a message to the old VLR to update the profile of this MS.
- The old VLR decreases the percentage of presence of that MS in its table by 10% and checks the percentage of presence of this MS. If it is less than 40%, the old VLR removes his/her profile from its database.

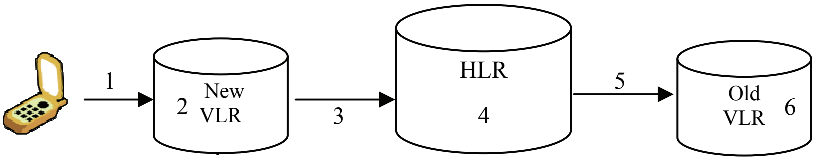

Fig. 8. GSM mobile station registration.

5.2 Call Delivery Procedure

When a mobile receives an incoming call, the network must identify the cell of the mobile station to transmit its call. In our system, the call delivery procedure is as follows:

- The originating switch queries the HLR for the current location of the MS.
- The HLR sends a message to the VLR to confirm the mobile's position.

- The VLR queries the MSC where is located to determine whether it can receive the call. Consequently, the MSC returns a routable address, Temporary Local Directory Number (TLDN), to the VLR.
- The VLR forward the TLDN to the HLR.
- The HLR forwards the TLDN to the originating switch.

5.3 Authentication

In this section, we propose our new secure authentication approach for GSM networks. Our proposed approach based key management mechanism is more efficient in terms of reducing storage space at the HLR and VLR, reducing the bandwidth consumption between VLR and HLR, and is more secure in order to overcome problems related to conventional GSM authentication process (Table 2).

This mechanism consists of two different phases, the first is when the mobile profile exists in the VLR and the second one is when the MS is present in a new LA covered by the VLR for the first time.

Table 2. Notation 1 [2,23,24]

Symbol	Definition	Bits
TMSI	The temporary mobile subscriber identity	128
IMSI	The international mobile subscriber identity	128
LAI	The location area identity	40
RAND	The random number generated by HLR/AuC	128
KI	The secret key shared between MS and HLR	128
SRES	The signed result	32
KC	The session key between MS and VLR	64
VLR ID	The identification of VLR	64
TKc	The temporary secret key	64
TC	The temporary value calculated	32
ACK	Acknowledgement	16
LU	Location update	128
TMSI-C	TMSI cancelation	16
N	Number of triplets sending to VLR by HLR to authenticate MS	-
INORM	Information message	32

5.3.1 Authentication for the first time (Fig. 9)

When a mobile is switching on or is presented in a new LA covered by a new VLR, which does not have the profile of this MS in its database it sends a request update to the network to register each new position in the VLR database. The network verifies the identity of this MS by applying the authentication process as follows:

- While the MS enters a new location area, it sends the TMSI and LAI to the visited VLR.
- The new VLR sends its identification VLR_{ID} and TMSI to the HLR through a secure channel.
- When HLR receives the information, it first checks whether the identity VLR_{ID} of the visiting VLR is legal or not. If the VLR_{ID} is not valid, the authentication process is terminated. Otherwise, HLR computes TC=A3 (VLR_{ID}, Ki) and TKc=A8 (RAND, Ki).

- After the success authentication of VLR, HLR sends TMSI to the old VLR to get IMSI of the mobile station and update the location of the mobile station in its dynamic database.
- Then the HLR sends IMSI, TC, RAND, and TKc to the VLR through a secure channel.
- Once the VLR receives the information from the HLR, it stores the TKc in the database and computes SRES=A5 (TKc, TC). After that, the VLR sends the VLRID, RAND, and TC to the MS and adds the profile of that MS with a percentage of presence equal to 10%
- When the MS receives the messages, it first authenticates the VLR by computing TC′=A3 (VLR_{ID}, Ki), and then compares it with the received TC. If they are not the same, the process is terminated; otherwise, the VLR is authenticated. The MS then computes TKc=A8 (RAND, Ki) and SRES′=A5 (TKc, TC). Finally, the MS sends SRES′ back to VLR.
- 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.

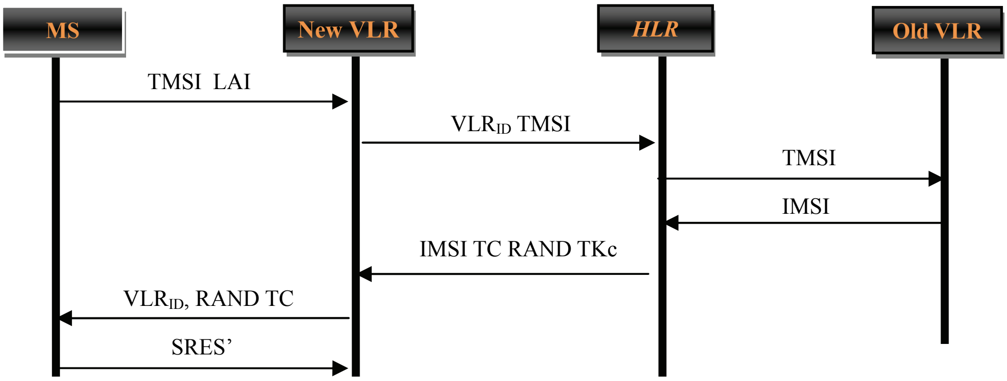

Fig. 9. Authentication for the first time.

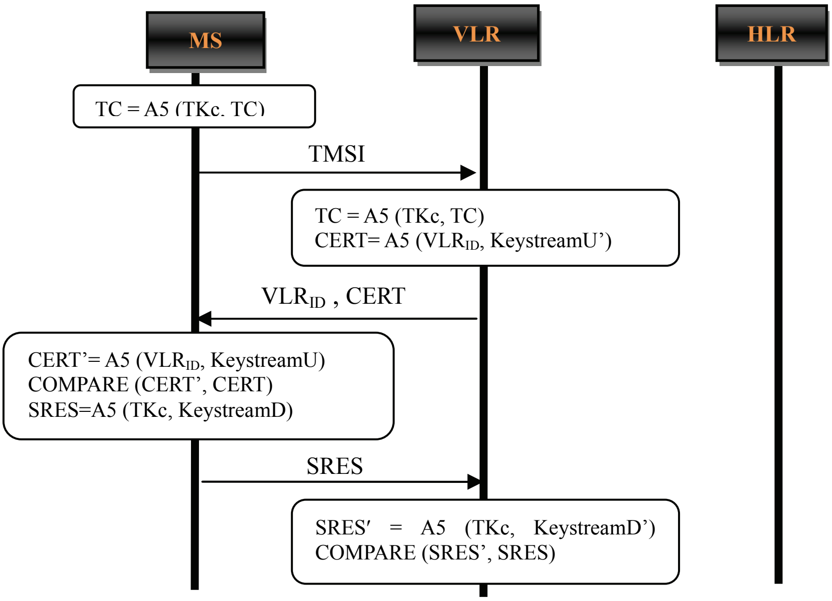
MS
VLR
HLR
TC = A5 (TKc, TC)
TMSI
TC = A5 (TKc, TC)
CERT= A5 (VLR_ID, KeystreamU')
VLR_ID , CERT
CERT'= A5 (VLR_ID, KeystreamU)
COMPARE (CERT', CERT)
SRES=A5 (TKc, KeystreamD)
SRES
SRES′ = A5 (TKc, KeystreamD')
COMPARE (SRES', SRES)

Fig. 10. Authentication for *n* time in the same VLR.

5.3.2 Authentication for *n* time in the same VLR (Fig. 10)

This procedure of authentication based mobility management is applied when the mobile station changes its location area that is covered by the same VLR

The details of the authentication are as described below.

- While the MS asks for new communication in the same service area of the same visiting VLR, it computes a new TC=A5 (TKc, TC)=KeystreamU+KeystreamD and sends a request that includes TMSI to the VLR, where KeystreamU is uplink Keystream generating by A5 and KeystreamD is the downlink one.
- The VLR receives the TMSI and computes the new TC=A5 (TKc, TC)=KeystreamU'+ KeystreamD'. After that, the VLR computes a CERT=A5 (VLR_{ID}, KeystreamU') and sends its VLRID and CERT to the MS.
- Once the MS receives the messages, it first authenticates the VLR by verifying its CERT, which must be the same as CERT'=A5 (VLR_{ID}, KeystreamU). Then, it computes the SRES=A5 (TKc, KeystreamD) and sends the value to the VLR.
- When the VLR receives the request from the MS, it computes SRES′=A5 (TKc, KeystreamD'), where TKc is the session key stored in its database for the previous authentication. Then, the VLR compares the SRES′ with the received one. If they are not the same, the process is terminated; otherwise the authentication process is successful.

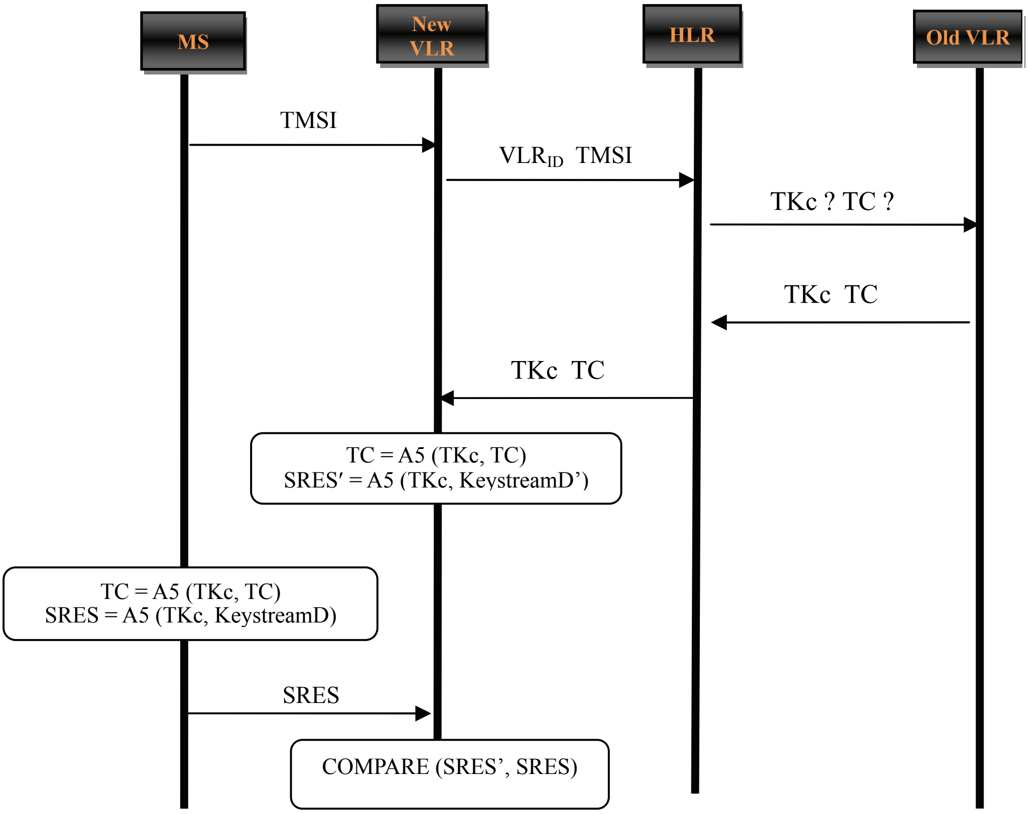

Fig. 11. Authentication for *n* time in different VLRs.

5.3.3 Authentication for n time in different VLRs (Fig. 11)

This kind of authentication is selected when the mobile station authenticated by an old VLR changes its location area to another location area covered by another VLR, which is called a new VLR.

The HLR can create a difference between the two types of authentication "in the first time" and "for *n* time in different VLRs" by verifying the profile of the mobile station in its dynamic table. If the mobile has a TC, the network knows that this mobile is already authenticated at least once by one VLR. The process of authenticating the MS for n time in different VLRs is as listed below.

- First, the MS sends its TMSI to the new VLR.
- The new VLR sends its identification $\mathrm{VLR_{ID}}$ and TMSI to the HLR through a secure channel.
- When the HLR receives the information, it first checks whether the identity $\mathrm{VLR_{ID}}$ of the visiting VLR is legal or not. If the $\mathrm{VLR_{ID}}$ is not valid the authentication process is terminated. Otherwise, the HLR requests the old VLR for the old TKc and the old TC values.
- The old VLR sends the old values of TC and TKc to the HLR.
- Once the HLR receives the message it forwards the TC and TKc to the new VLR, which computes the new TC=A5 (TKc, TC)=KeystreamU'+KeystreamD' and the SRES′=A5 (TKc, KeystreamD').
- After that, the MS computes new TC=A5 (TKc, TC)=KeystreamU+KeystreamD, and then it computes the SRES=A5 (TKc, KeystreamD') and sends the value to the VLR.
- When the VLR receives the request from the MS, it compares its SRES′ that have been calculated with the received one of the MS. If they are not the same, the process is terminated; otherwise, the authentication process is successful.

6. Efficiency Analysis

The main purpose of this paper is to present a new mechanism for mobility management in cellular networks and more specifically to the GSM network to solve different limits presented in classical GSM mobility management schemes, such as the security problem that is present in the authentication process between the MS and the network, and to reduce the bandwidth consumption between the VLR and HLR by minimizing the signaling message interchanging in the network. The computational cost is also taken into consideration to be minimized as much as possible to not overload the VLR by additional calculation.

6.1 Updating and Signaling Cost in the VLR and HLR

Our goal is to resolve the various drawbacks noted in the parrying classic mechanism of the GSM mobility management, where one of these drawbacks is the high computational cost.

To better evaluate our approach, we compared it with that of the GSM in each phase of the mobility management scheme's inter LA location updates, inter MSC location updates, or inter VLR location updates.

To evaluate the cost of our protocol we calculated the cost of each operation of location update inter LA, inter MSC, or inter VLR.

The values of registration procedures are shown in Table 3 by taking into consideration the notations mentioned in Table 4.

The paging cost is shown in Table 3 for our proposed protocol and the GSM, where *P* presents the probability that the profile of the MS exists in the database of the VLR and n the number of VLRs.

Table 3. Registration cost and call delivery cost

	GSM	Our
Registration cost		
Inter LA	$C_{\text{MS-BTS}}+ C_{\text{BTS-MSC}}+ C_{\text{MSC-VLR}}+ C_{\text{VLR}}+ ACK_{\text{VLR-MS}}$	$C_{\text{MS-BTS}}+ C_{\text{BTS-MSC}}+ C_{\text{MSC-VLR}}+ C_{\text{VLR}}+ ACK_{\text{VLR-MS}}$
Inter MSC	$C_{\text{MS-BTS}}+ C_{\text{BTS-MSC}}+ C_{\text{MSC-VLR}}+ C_{\text{VLR}}+ C_{\text{HLR-VLR}}+ C_{\text{HLR}}+ ACK_{\text{HLR-VLR}}+ ACK_{\text{VLR-MS}}$	$C_{\text{MS-BTS}}+ C_{\text{BTS-MSC}}+ C_{\text{MSC-VLR}}+ C_{\text{VLR}}+ACK_{\text{VLR-MS}}$
Inter VLR	$C_{\text{MS-BTS}}+ C_{\text{BTS-MSC}}+ C_{\text{MSC-VLR}}+ 2C_{\text{VLR-VLR}}+ C_{\text{VLR}}+ C_{\text{HLR-VLR}}+ C_{\text{HLR}}+ ACK_{\text{HLR-VLR}}+ ACK_{\text{VLR-MS}}+ D_{\text{VLR}}$	$C_{\text{MS-BTS}}+ C_{\text{BTS-MSC}}+ C_{\text{MSC-VLR}}+ P(C_{\text{VLR}})+ (1-p)(C_{\text{VLR}} +C_{\text{HLR-VLR}}+ C_{\text{VLR}})$
Call delivery cost	$C_{\text{HLR-PSTN}}+n{*}C_{\text{HLR-VLR}}+ C_{\text{HLR-VLR}}+ C_{\text{HLR-PSTN}} + C_{\text{PSTN-MSC}}$	$C_{\text{HLR-PSTN}}+ 2{*}C_{\text{HLR-VLR}}+ C_{\text{HLR-PSTN}} + C_{\text{PSTN-MSC}}$

Table 4. Notation 2

C_{HLR}	Cost for location update in HLR
C_{VLR}	Cost for location update in VLR
$C_{\text{MS-BTS}}$	Cost for transmitting a signaling message between MS and BTS
$C_{\text{BTS-MSC}}$	Cost for transmitting a signaling message between BTS and MSC
$C_{\text{MSC-VLR}}$	Cost for transmitting a signaling message between MSC and VLR
$C_{\text{VLR-MS}}$	Cost for transmitting a signaling message between VLR and MS
$C_{\text{HLR-VLR}}$	Cost for transmitting a signaling message between HLR and VLR
$C_{\text{VLR-VLR}}$	Cost for transmitting a signaling message between two VLRs
$C_{\text{HLR-PSTN}}$	Cost for transmitting a signaling message between HLR and PSTN
$C_{\text{PSTN-MSC}}$	Cost of establishing canal between PSTN and MSC
$ACK_{\text{HLR-VLR}}$	Acknowledgement HLR VLR
$ACK_{\text{VLR-MS}}$	Acknowledgement VLR MS
D_{VLR}	Deregistration cost in VLR

It is clearly seen that our protocol reduces the number of signaling messages and the updating cost in the VLR and HLR databases in the two procedures of registering the inter MSC and inter VLR.

In the registration cost inter MSC our approach release one update operation in each registration in the HLR network CHLR however in the second procedure of registration; inter VLR one update in each registration in the HLR network CHLR have been reduced and one deregistration operation in VLR $\mathbf{D_{VLR}}$ with some additional updating cost equal to (1–P)$\mathbf{C_{VLR}}$ in VLR database where P presents the probability that the profile of the MS exists in the database of the VLR.

The signaling messages are also more reduced, especially in the inter MSC location update procedure where we released two signaling messages—the first one between the HLR and VLR databases $\mathbf{C_{HLR\text{-}VLR}}$ and the second is the acknowledgement message between the VLR and HLR.

In the inter VLR registration procedure we released two signaling messages between the VLRs and two acknowledgment messages between the HLR, VLR, and the MS with the P **$C_{HLR-VLR}$** signaling message between the HLR and VLR, where P presents the probability that the profile of the MS exists in the database of the VLR.

Table 5 groups all numbers of signaling message reducing between MS, VLR and HLR by our protocol if we compared it with standard GSM where P presents the probability that the profile of the MS exists in the database of the VLR.

Table 5. Number of signaling messages reduced

Registration type	Number of signaling message reduced
Inter LA	0
Inter MSC	3
Inter VLR	3-P

The paging cost in our mobility management scheme is more efficient where we have a reducing (*n*–1) signaling message between the VLR and HLR where, *n* represents the number of VLRs.

6.2 VLR Storage Space

Since the VLR must save the N copies sent by the HLR in its database for every request of authentication, this overloads the VLR's database. However, in our proposed protocol for the first authentication, the VLR only must save the secret session key of TKc and its temporary identification TC. Even the MS stays in the same VLR for conducting mutual authentication between the MS and the network that was established by only using the two values stored in the VLR in the first authentication.

If the MS moves to the new VLR, the old VLR must send only the secret session key TKc and temporary identifier TC to the new VLR and delete the values from its database.

6.3 HLR Pre-computational Cost

In the GSM network, the HLR computes N copies of triplets before sending it to the VLR, which uses these copies that are stored in its database as the mobile station requires authentication from the same VLR. If the mobile changes the VLR before consuming the N triplets, the HLR have computed the unused triplets which are not using by the VLR, as a result the computational cost in HLR was increased. If the mobile station changes its location area to another VLR, the new VLR requests the HLR for new N copies of authentication parameters and does not use the unused triplets of the old VLR. Consequently, the computational cost in the HLR will increase.

In our proposed protocol, there is no pre-computational cost in the HLR, in the authentication for the first time the HLR compute just a certificate to authenticate the VLR by the MS. After that, the VLR can only use the secret sessions key TKc and its temporary identification TC, which are stored in its database, to authenticate the MS, which stays in the same VLR. If the mobile station changes its VLR, the old VLR transmits the old values of the TKc and TC to the new VLR to authenticate the MS without any pre-computational cost in the HLR.

6.4 Communication Overhead between the VLR and HLR

To evaluate the communication overhead of our protocol in the authentication process we calculated the total number of transmitted bits in each authentication phase. First authentication, authentication for *n* times in the same VLR and in the authentication for *n* time between two VLRs for our protocol, standard GSM and Lee's protocol [5]. All results are represented in Table 6 with the respect of values in Table 2, where *n* is the number of triplets sent by the HLR to the VLR for MS authentication.

Table 6. Communication overhead for first authentication and authentication for *n* time

	Our	[5]	GSM
First Authentication	416	512	2368 (N=10)
Authentication for *n* time in the same VLR	0	0	(n/N)*(128+N*(32+128+64))
Authentication for *n* time in different VLRs	416	544	416+N*224

In Figs. 12 and 13, we showed the communication cost generated by varying the number of mobiles used in each authentication process from 100, 200, and 500 to 1,000 mobiles.

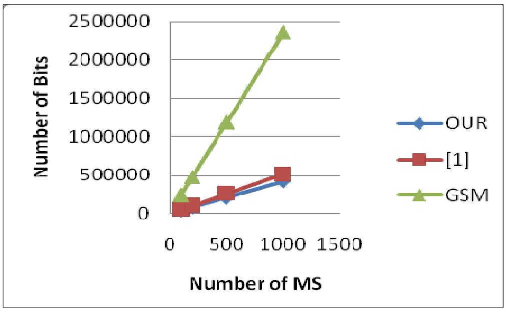

Fig. 12. Communication overhead for the first authentication.

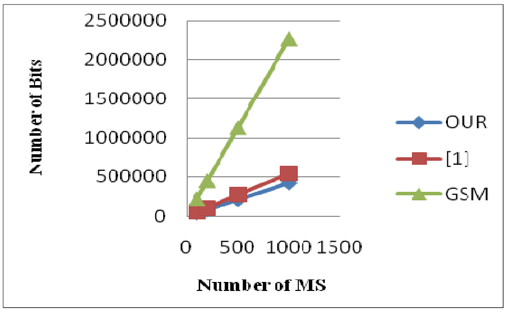

Fig. 13. Communication overhead for the authentication for *n* time in different VLRs.

As can be clearly seen, our protocol generates the minimum communication overhead between the VLR and HLR in each phase of authentication, as compared to Lee et al. [5] or the standard GSM protocol.

Furthermore, in our proposed protocol, as a long as MS stays in the covered area of the same VLR is authenticated by the VLR without need to the HLR. This process efficiently reduces the bandwidth consumption between the VLR and HLR to 0, as shown in Table 6.

6.5 The Computation Costs in the VLR and HLR

The standard GSM uses the two algorithms of A3 an A8 to update the location of the MS, especially in the authentication phase. In order to evaluate the computation costs in the VLR and HLR of our protocol, we calculated the number of using each function A3, A8, or A5 in each phase of the authentication process of our protocol and the related schemes, where *N* represents the number of triplets (SRES, Rand, KC) transmitted to the VLR by the HLR, and p is the probability that MS stays in the location area covered by the same VLR (Tables 7–9).

Table 7. Computation cost in the first authentication

	Our	[5]	**GSM**
A3	2	4	1+N
A8	2	0	1+N
A5	2	2	0
Total	6	6	2N+2

Table 8. Computation cost in the authentication for n time in the same VLR

	Our	[5]	**GSM**
A3	0	2	P*1+(1-P)*(N)
A8	0	0	P*1+(1-P)*(N)
A5	6	2	0
Total	6	4	2P+2N(1-P)

Table 9. Computation cost in the authentication for n time in different VLRs

	Our	[5]	**GSM**
A3	0	2	P*1+(1-P)*(N)
A8	0	0	P*1+(1-P)*(N)
A5	4	2	0
Total	4	4	2P+2N(1-P)

As already demonstrated, our protocol or Lee's can reduce the computation cost in the VLR and HLR in the first authentication process and in the authentication process for n time in different VLRs. However, Lee's protocol reduces the general computational cost by 33% in the second phase of the authentication process.

7. Security Analysis

In this section, we discuss the security of our proposed protocol to solve some security drawbacks that are present in the standard GSM mobility management mechanism, especially in the authentication phase, such as man-in-the-middle and impersonating attacks, which are practical in the existing GSM protocol.

7.1 Key Exchange

In our new protocol, an important secret session key TKc and a temporary identification TC were created to authenticate the VLR even the MS stay in the same; the secret session key TKc which is a variant of secret key Ki which is never exchanging over the air. Our protocols don't exchange this new Key in all authentication phases to be not intercepting and decrypting to save the secret of the mobile SIM card.

7.2 Algorithms Selection

Security in GSM networks is based on the following three cryptographic algorithms: A3, the authentication algorithm; A8, the key agreement algorithm; and A5, a stream cipher used for encryption. Our proposed protocol uses these algorithms to enhance a standard GSM authentication algorithm.

The choice of the GSM algorithm is for reducing the bandwidth consumption between the VLR and HLR. A lot of proposed protocols don't choose good algorithms, especially when using the A3 or A8 algorithms to authenticate the MS by the VLR. This is because these algorithms are implemented in the HLR/AUC, if we use one of them, necessary we will increase the bandwidth consumption between VLR and HLR. As a result, a VLR turn back up to the HLR in each authentication process.

Table 10. Percentage (%) of using A5 in the authentication process

	Our	[5]	GSM
First authentication	33	33	0
Authentication for *n* time in the same VLR	100	50	0
Authentication for *n* time in different VLRs	100	50	0

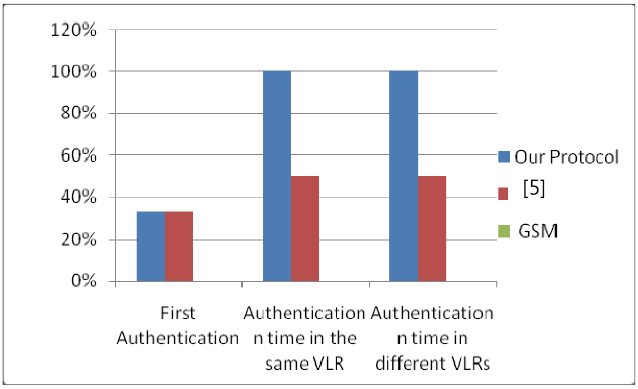

Fig. 14. Security level.

In our authentication process for each phase we used the A5 algorithm, which is for providing over-the-air communication privacy in the GSM and is more secure then A3 or A8. In Table 10 and Fig. 14, we calculated the percentage of times the A5 algorithm was used in each phase of authentication for each protocol.

In our protocol, we did not use the A5 algorithm in the first authentication because we needed to establish a certificate for the VLR that could be authenticated by the MS. This certificate is calculated by the HLR/AUC, which uses the A3 or A8 algorithm in the standard GSM network.

However, the second and third phases of authentication are only based on using the A5 algorithm, which is more secure than the other GSM algorithms of A3 and A8.

7.3 Impersonating Attack

The impersonating attack is invisible in our protocol. No one can impersonate the MS or the VLR in our proposed scheme because if an attacker tries to impersonate the MS he/she cannot generate the correct SRES. An attacker also cannot compute the certificate of the visiting VLR and cannot create the temporary identifier TC of the VLR without certifying its HLR.

7.4 Mutual Authentication

In our proposed protocol, mutual authentication is improved in each phase of our protocol, and the MS and the VLR will be authenticated in each phase.

In the first authentication mechanism, the VLR can get its authorization TC by computing the A3 algorithm, which is only implemented in the HLR/AUC and the SIM card of the mobile station. As such, the VLR can't get it without the help of its HLR.

The mobile station can authenticate the VLR when the visiting VLR sends a request for its authentication, which includes RAND, TC, and its identification VLRID.

When the MS asks the VLR for authentication for the n time, the VLR uses the TKC and TC as the inputs through A5 to compute the certificate CERT, and then the VLR requests the MS for a message, including the CERT and VLR_{ID}. The CERT is then used for the MS to authenticate the VLR. The VLR can authenticate the MS by comparing its SRES, which is calculated by the A5 algorithm.

In the authentication procedure in different VLRs, the new VLR cannot authenticate the MS without the secret session key TKC and its temporary identification TC. First, the new VLR is authenticated by its HLR, and then the old VLR transmits the TKc and TC to the new VLR through a secure channel. Finally, the new VLR stores the TKc and TC in its database for early authentication.

8. Conclusion

Unlike the fixed network, where the phone is always connected to the same switching center, in a mobile environment, a mobile subscriber is not always attached to the same MSC as it moves anywhere in the mobile networks, which need to update its location in order to route traffic to the correct destinations when the network attempts to deliver a call to the mobile station.

In this paper, we have proposed a strong protocol to enhance the standard GSM authentication protocol, which is executing before in the location update process by the mobile station. Our proposed solution, which is based on a new mobility management scheme, not only provides a secure bilateral authentication mechanism, but also decreases the bandwidth consumption between the VLR and HLR, the computation cost in the HLR, and increases efficiency by reducing the number of arguments being used in the authentication process. Our mobility management approach is based on safeguarding the percentage of presence of each subscriber in the VLR and HLR databases. To evaluate the performance of the proposed authentication protocol, we compared it to the GSM standard authentication algorithm and the protocol proposed in [5].

The result shows that our proposed mobility management protocol, including the new secure authentication process, are both secure and efficient.

References

[1] B. Sidhu and H. Singh, "Location management in cellular networks," *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, vol. 1, no. 1, pp. 49-54, 2007.

[2] EFORT, "GSM: Global System for Mobile Communications," 2008 [Online]. Available: http://www.efort.com.

[3] G. K. Patnaik, "GSM mobility management," 2013 [Online]. Available: https://pt.scribd.com/document/271708186/GSM-Mobility-Management-pdf.

[4] J. W. Lee, "Mobility management using frequently visited location database," in *Proceeding of International Conference on Multimedia and Ubiquitous Engineering (MUE)*, Seoul, Korea, 2007, pp. 159-163.

[5] S. Wanke, H. Saito, Y. Arakawa, and S. Shimogawa, "User location in picocells: a paging algorithm derived from measured data," *IEICE Transactions on Communications*, vol. 93, no. 9, pp. 2291-2298, 2010.

[6] C. H. Lee, M. S. Hwang, and W. P. Yang, "Enhanced privacy and authentication for the global system for the mobile communications," *Wireless Networks*, vol. 5, no. 4, pp. 231-243, 1999.

[7] J. A. P. Singh and M. Karnan, "A dynamic location management scheme for wirless networks using cascaded correlation neural network," *International Journal of Computer Theory and Engineering*, vol. 2, no. 4, pp 581-585, 2010.

[8] A. Bar-Noy, I. Kessler, and M. Sidi, "Mobile users: to update or not to update?," *Wireless Networks*, vol. 1, no. 2, pp. 175–185, 1995.

[9] A. Fanian, M. Berenjkoub, and T. A. Gulliver, "A new mutual authentication protocol for GSM networks," in *Proceedings of Canadian Conference on Electrical and Computer Engineering*, St. Johns, Canada, 2009, pp. 798-803.

[10] J. Al-Saraireh and S. Yousef, "Extension of authentication and key agreement protocol (AKA) for universal mobile telecommunication system (UMTS)," *International Journal of Theoretical and Applied Computer Sciences*, vol. 1, no. 1, pp. 109-118, 2006.

[11] 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*, Taipei, Taiwan, 1995, pp. 416-420.

[12] K. Al-Tawil, A. Akrami, and H. Youssef, "A new authentication protocol for GSM networks," in *Proceedings of IEEE 23rd Annual Conference on Local Computer Networks*, Boston, MA, 1998, pp. 21-30.

[13] B. Mallinder, "An overview of the GSM system," in *Proceedings of 3rd Nordic Seminar on Digital Land Mobile Radio Communication*, Copenhagen, Denmark, 1998, pp. 12-15.

[14] Y. Jie and D. J. Kadhim, "Performance evaluation of the mobility management towards 4G wireless networks," *International Journal of Electronics and Communication Engineering & Technology*, vol. 4, no. 5, pp. 1-10, 2013.

[15] K. Ammayappan, A. Saxena, and A. Negi, "Mutual authentication and key agreement based on elliptic curve cryptography for GSM," in *Proceedings of International Conference on Advanced Computing and Communication*, Surathkal, India, 2006, pp. 183-186.

[16] I. F. Akyildiz, J. McNair, J. S. M. Ho, H. Uzunalioglu, and W. Wang, "Mobility management in next-generation wireless systems," *Proceedings of the IEEE*, vol. 87, no. 8, pp. 1347-1384, 1999.

[17] C. C. Lee, I. E. Liao, and M. S. Hwang, "An efficient authentication protocol for mobile communications," *Telecommunication Systems*, vol. 46, no. 1, pp. 31-41, 2011.

[18] P. Acharya and S. S. Singh, "Mobile user's location management using bloom filter," *International Journal of Computer Science and Information Technology*, vol. 2, no. 3, pp. 1127-1130, 2011.

[19] C. Selvan and R. Shanmugalakshmi, "Location management techniques to improve QoS in mobile networks using intelligent agent," *International Journal on Computer Science and Engineering*, vol. 3, no. 1, pp 192-198, 2011.

[20] J. F. Stach, E. K. Park, and K. Makki, "Performance of an enhanced GSM protocol supporting non-repudiation of service," *Computer Communications*, vol. 22, no. 7, pp. 675-680, 1999.

[21] C. C. Lee, M. S. Hwang, and W. P. Yang, "Extension of authentication protocol for GSM," *IEE Proceedings - Communications*, vol. 150, no. 2, pp. 91-95, 2003.

[22] W. D. Lin and J. K. Jan, "A wireless-based authentication and anonymous channels for large scale area," in *Proceedings of the 6th IEEE Symposium on Computers and Communications (ISCC)*, Hammamet, Tunisia, 2001, pp. 36-41.

[23] N. Saxena and N. S. Chaudhari, "Secure-AKA: an efficient AKA protocol for UMTS networks," *Wireless Personal Communications*, vol. 78, no. 2, pp. 1345-1373, 2014.

[24] P. Ravi Kiran and Y. K. Sundara Krishna, "A study report on authentication protocols in GSM, GPRS and UMTS," *International Journal of Engineering Research and Development*, vol. 10, no. 6, pp. 42-48, 2014.

Ghazli Abdelkader

He is a PhD student in Computer Science University of Science and Technology of Oran (USTO), Algeria. He received the diploma of Engineering in Computer Science from the USTO, Algeria in 2005. He received the diploma of teaching in Computer Science from the USTO, Algeria, in 2009. He is a lecturer at the University of Tahri Mohamed of Bechar, Algeria, His research interests are in the cryptography, wireless networks and systems security.

Hadj Said Naima

She is a lecturer in Computer Science. She teaches at the University of Science and Technology of Oran (USTO), Algeria. His research interests are coding, cryptography and security.

Ali Pacha Adda

He is a lecturer in electronics and Computer Science. He is a teacher at the University of Science and Technology of Oran (USTO), Algeria. His research interests are coding, cryptography and security, FPGA.