IOSR Journal of Engineering (IOSRJEN)
ISSN: 2250-3021 ISBN: 2878-8719 PP 13-18
National Symposium on engineering and Research

Mobility and Security Management in the GSM System

[1]Mr. Yogesh S. Amle [2]Mr. Datta S. Shingate [3]Mr. Pramod C. Patil
[1]Comp/IT Dept MCOERC, Nashik [2] Comp/IT Dept MCOERC, Nashik [3]Comp/IT Dept MCOERC, Nashik

Abstract: - *Nowadays, the mobile industry has experienced an extreme increment in number of its users. The GSM network with the greatest worldwide number of users surrenders to several security vulnerabilities. Although some of its security problems are addressed in its upper generations, there are still many operators using 2G systems. This paper mainly focuses on the most important security flaws of the GSM network and its transport channels. It also provides some practical solutions to improve the security of currently available 2G systems.*

Important aspects of mobility and security in the Global System for Mobile communications system are discussed in this paper. Mobility management functions are categorized into three groups: a) Mobile turned on, b) Mobile turned off, and c) Mobile in conversation. The paper first outlines the mobile synchronization sequence followed by its mobility functions: mobile identification, authentication, international mobile station identity attach/detach, and its location update. The important role of security in the GSM system is fully explored, including authentication, encryption, and positive identification of mobile equipment before the user is provided with the service. The future of mobility management, with respect to subscriber identification module roaming, intersystem roaming, advancement in mobile service, and its impact on database requirements, is covered in subsequent paragraphs.

1. Introduction

Mobility management (MM) entails the Global System for Mobile communications (GSM) system's keeping track of the mobile while it is on the move. Basically, we have two different situations: mobile idle and mobile busy. These two cases lead to all the relevant cases we need to consider: a) mobile station (MS) is turned off, b) MS is turned on but is in the idle state, and c) MS is in the conversational mode.

a) *MS turned off:* In this case, the mobile cannot be reached by the network because it does not answer a paging message. It does not inform the system about possible changes of location area (LA), as it is simply inoperative. In this case, the MS is simply considered detached from the system [international mobile station identity (IMSI) detached].

b) *MS turned on, idle state:* In this state, the system can page the MS successfully. So IMSI attached procedure has to do for mobile registration. When mobile is moving, the MS has to check that it is always connected to the best range broadcast control channel (BCCH). This procedure is also called as roaming and the mobile must also inform the system about changes of LA, which is called as location updating.

c) *MS busy:* The radio network has traffic channels called as TCH allocated for the data flow to/from the MS. While moving, the MS must also be able to change to a new traffic channel as the signal on the traffic channel may reduced below an unacceptable level, which is called as handover process. In order to decide whether to hand over, the mobile switching center (MSC) base station controller (BSC

in some cases) interprets information received from the MS and base transceiver station (BTS) known as locating.

In view of the above, we shall discuss the complete mobility aspect of the system.

Another important aspect of the GSM system is security.

At an early stage in the development of the Pan-European

mobile radio system GSM, it was apparent that the weakest part of the system was the radio path, as this could be easily eavesdropped upon with radio equipment. There was also a need to authenticate users of the system so that the resources were not misused by nonsubscribers. It is easy to see that the public land mobile network (PLMN) needs a higher level of protection than traditional telecommunications networks. Therefore, to protect the system against the two cases mentioned above, the GSM system has been reinforced by the following four security techniques [1]–[3]:

- Temporary Mobile Subscriber Identification (TMSI);
- Authentication (A3algorithm);
- Encryption (A5 and A8 algorithm);
- Subscriber Identity Module (SIM) module and mobile equipment ID.

II. MOBILE INITIALIZATION

The MS must first acquire synchronisation with the GSM system. This process begins after the MS is turned on in a PLMN. The first step of the process is for the MS to search for and acquire a frequency control channel (FCCH) burst on some common control frequency channel.

The mobile will scan all or part of 124 RF channels and

calculate the average signal strength of each channel. During the scanning process.

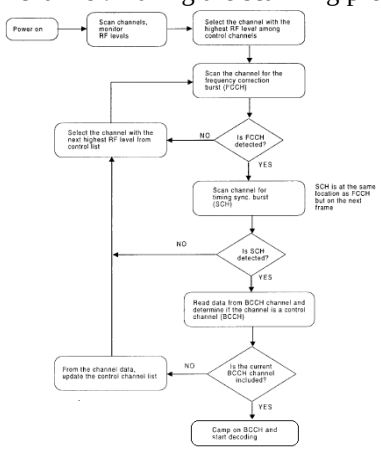

Fig 1.Initial Mobile Acquisition

For the complete scanning process may take several seconds. For each of the 124 channels, starting with the one of highest signal strength level, the mobile searches for the FCCH. This is the first step of the process known as frequency synchronization. The frequency correction burst is unique and easily recognizable. The FCCH burst is a long sine wave that is offset by 67.7 kHz from the carrier frequency. The cell transmits all zeros for the frequency correction signal. The mobile has to take out this offset before an estimate of the carrier frequency can be made. This process of frequency synchronization is shown as the first step in Fig. 1 [3]. If no frequency burst i0s detected, then the mobile can go to a channel with the next highest signal strength level.

After the frequency correction burst is detected, the MS will try to synchronize with the time synchronization burst synchronization channel (SCH). The SCH always occurs

in the next frame in the same time slot as the FCCH. This is eight burst periods later than the FCCH. The SCH contains precise timing information on the timeslot boundaries to permit refining the received slot timing. The SCH message also contains the current frame number to which the MS synchronizes. This time synchronization is generally carried out in two steps: coarse and fine. Here, the internally stored synchronizing pattern is correlated, and at the peak of correlation, the channel is considered to be synchronized. If synchronization does not occur, the process of frequency synchronization with the next highest channel in the list may start. If the synchronization is successful, the mobile will read the time division multiple access (TDMA) frame number and the BSIC.

The BCCH information also provides

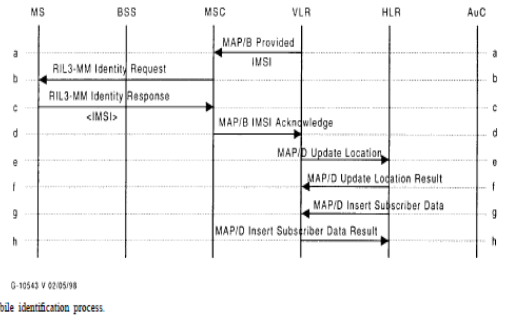

Fig. 4. Mobile identification process.

beacon frequencies of surrounding BTS cells, etc. All BCCH transmissions are at a standard power level, which permits the MS to compare received power from its own BTS as well as from adjoining BTS's. Therefore, when the BCCH information is correctly decoded, the mobile follows

one of the two paths discussed below.

a) If the BCCH information includes the present BCCH

channel, then the mobile will simply stay on the channel.

b) If the current channel is not in BCCH information

list, or the received signal strength level is below the desired level, the mobile will continue searching for the next control channel.

After the mobile has successfully synchronized to a valid

BCCH, the mobile is now ready to register, receive paging,

or originate an outgoing call.

III. MOBILITY FUNCTIONS

Among all functions that the mobile is at liberty to perform, we shall consider only those connected with the MM layer or the mobility aspect of the GSM system.

Those functions are [2]–[3], [5]–[8]:

- mobile identification;
- authentication;
- IMSI attach and detach;
- location update.

A. Identification Procedure

The identification procedure is used to identify the MS/SIM by its IMSI if the visitor location register (VLR) does not recognize the TMSI sent by the MS. This lack of
recognition can be the result of the mobile user's changing the MSC/VLR area from the last time he accessed the system or can be due to some other reason. If identification is required, the VLR first sends a MAP/B Provide IMSI message to the MSC, as shown in Fig. 4 [3]. As a result of this message, MSC sends an RIL3-MM Identity Request message to the MS. The MS responds by returning an RIL3-MM Identity Response message containing its IMSI to the MSC. The MSC then sends the MAP/B IMSI acknowledge to the VLR. If the IMSI is currently not in the VLR, then the VLR must get its file from the home location register (HLR) identified in the IMSI. To do this, the VLR sends

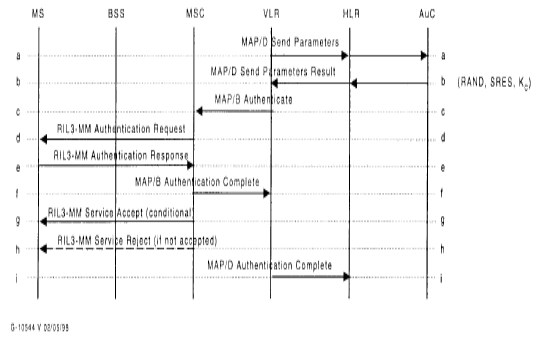

Fig. 5. MS authentication process [3, p. 119].

the HLR a MAP/D Update Location message. Assuming that the IMSI is in fact registered in the HLR, the HLR responds with a MAP/D Update Location Result message, followed by a MAP/D Insert Subscriber Data message containing other pertinent data needed by the VLR. The VLR acknowledges the data transfer with a MAP/D Insert Subscriber Data result message to the HLR.

B. Authentication

The authentication process may be run at each and every location update and at the initiation of every new service request. The process starts at VLR. If the VLR determines that authentication is required, it sends a MAP/D Send Parameters message to the HLR, which relays this message to the authentication center (AuC). The AuC then draws a value for the random challenge random number (RAND) and applies algorithms A3 and A8 to generate the signed response (SRES) and the cipher key. The complete process of authentication is discussed in section 4.0. The AuC then returns the triplet (RAND, signed response, K_c) value to the VLR in a MAP/D Send Parameters Result message. Actually, the AuC normally calculates and sends a few such triplets at a time for each requesting MS, so the VLR only has to request parameters from the AuC if it has no stored unused triplets for the particular MS [10]–[12].

The VLR then sends a MAP/B Authenticate message to the MSC, which in turn sends an RIL3-MM Authentication Request message containing RAND to the MS over the air. The MS calculates the required signed response challenge (SRESc) using the algorithm A3 and authentication key $K_i$stored in the SIM. The SRESc is returned to the MSC in a RIL3-MM Authentication Response message. The MSC compares the SRESc with the signed response, and if they agree, it sends the MS an RIL3-MM Service Accept message. The MSC also sends the VLR a MAP/B Authentication Complete message. The protocol for the authentication process is shown in Fig. 5. *C. IMSI* ***Attach and Detach***

The IMSI attach and detach procedures register and deregister the mobile to the system. If the mobile user is attached, he will be paged in the location area of the user's presence. If the mobile user is detached, the system will not waste its resources in paging for an incoming call.

1) IMSI Attach: The IMSI attach procedure is used by the MS to indicate that it has reentered the active state (power on). IMSI attach is invoked if the attach/detach procedures are required by the network and an IMSI is activated in an MS (i.e., activation of an MS with plugin SIM or the insertion of a card in a SIM card-operated MS, etc.) within the coverage area of the network or if an MS with an IMSI activated outside the coverage area enters the coverage area. The IMSI attached is marked in the MSC/VLR with an "attached" flag. The following
sequence of events describes the IMSI attach procedure, shown in Fig. 6 [2]–[3]. Upon turning on the power, the MS sends an RIL3-RR Channel Request message to the BSS on the random access channel (RACH). The network assigns the channel, and the BSS sends an RIL3-RR IMM Assignment message to the MS over the access grant channel (AGCH). This message assigns the stand-alone dedicated control channel (SDCCH) channel to the mobile.

After the channel is assigned, the MS sends an RIL3- MM IMSI Attach message over the SDCCH channel to the BSS, which is forwarded first to the MSC and then to the VLR as a MAP/B protocol message. The VLR sends an acknowledgment to the MSC, "IMSI Attach Acknowledge," as a MAP/B protocol, which is forwarded to the BSS and then to the MS. The MSC

also sends "Clear Command" for the channel release to the BSS as the BSSMAP protocol, which is then forwarded to the MS. Upon receiving the RIL3-RR Disconnect signal from the MS, a Clear Complete message is sent to the MSC as aBSSMAP protocol.

2) IMSI Detach Procedure: Similar to the IMSI attach procedure, the IMSI detach procedure may be invoked by an MS if the MS is deactivated or if the SIM is detached from the MS. A flag (ATTN) broadcasted in the System Information message on the BCCH is used by the network to indicate to the MS whether the detach procedure is required. The procedure causes the MS to be declared inactive in the network. Once the IMSI detach procedure is active, the MS can neither transmit nor receive. The system will also not page the MS. The IMSI detach procedure starts with the MS's sending an RIL3-RR Channel Request message on RACH to BSS.

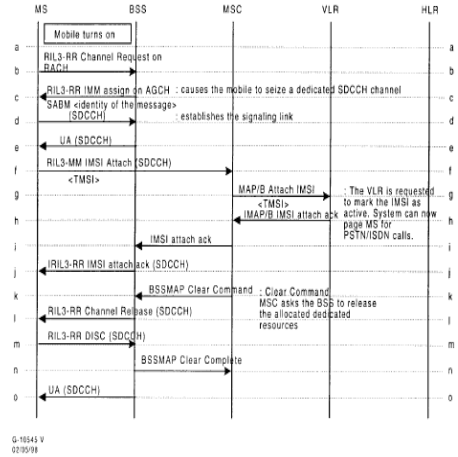

Fig. 6. IMSI attach.

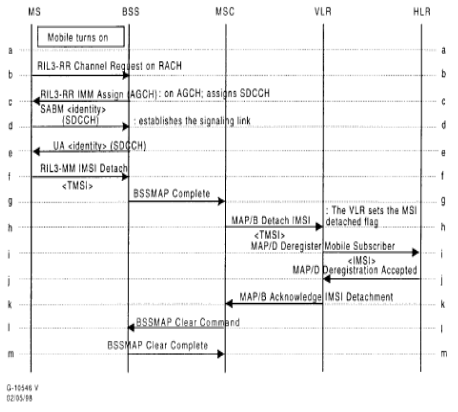

Fig. 7. IMSI detach.

The BSS assigns an SDCCH channel and notifies the channel assignment to the MS over the AGCH. The MS then sends an RIL3-MM IMSI Detach Indication message to the BSS. The message identifies the MS (indicated here as TMSI) and contains an 8-bit code indicating IMSI detach. After receiving an IMSI Detach Indication message from MS, the BSS forward this message in a BSSMAP complete layer 3 information message to the MSC. The MSC in turn updates the state of the MS in the VLR with a MAP/B Detach IMSI message. At this stage, all terminating calls to the MS are rejected, and the system does not page the mobile anymore. The VLR forwards this message to the HLR as a MAP/D Deregister Mobile Subscriber, and the HLR marks the MS as deregistered. The HLR forwards a MAP/B Deregistration Accepted message to the VLR, which, in turn, sends a MAP/B

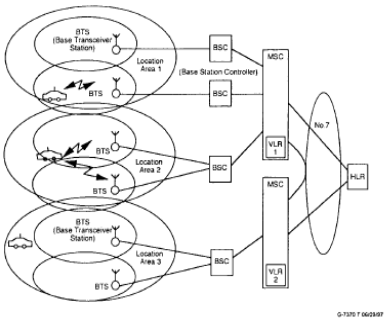

Fig. 8. Location updating [10, p. 303].

Acknowledge IMSI Detachment message to the MSC. No response is returned to the MS, as shown in Fig. 7 [2]–[3], [8]–[10]. This is correct because the mobile would be switched off before the return message is sent from the BSS to the MS. The MSC sends a BSSMAP Clear Command to the BSS to clear the SDCCH channel assigned to the MS. The BSS acknowledges with a BSSMAP Clear Complete message to the MSC.

3) Location Update: The MS location updating is performed to tell the system where to search for the MS during paging for an incoming call. If the location is known to a definite subregion of a particular PLMN, this will reduce the number of cells where the mobile has to be paged, thereby reducing the load on the system. The MS location is determined from the cell identification of the strongest BCCH signal received by the MS. The MS regularly measures the received signal strengths of the

BCCH's for all surrounding cells at least once every six seconds (superframe cycle). It stores at least the six strongest BCCH measurements and their identifications in the SIM, which can subsequently be used for handover decisions. The MS also transmits the location area of the strongest cell to the MSC during location updating. The location area may be a single cell or a contiguous

group of cells under the control of one BSC, as shown in Fig. 8 [3]–[4].

A cellular system requires that the user location of all active mobile units be known at all times as they roam. As
seen in Fig. 8, each cell is served by one BTS. Each location area is divided into many cells, which may be served by one or more BSC's. The VLR may serve one or more location areas. An inactive mobile is ignored by the system. As soon as the mobile switches its power, it retrieves its stored location-area identity and compares it with the one being broadcast within its present cell. If they match, the mobile does not have to do anything, as the subscriber is already correctly located; however, if it does not match, the mobile identifies itself by transmitting its IMSI together with the identities of the previous and present location areas. The BSS transmits this information to the associated VLR.

Each time an MS moves into a new location area, the corresponding VLR is informed. If both the present and previous areas are served by the same VLR, the mobile station is given a new TMSI, and its location is updated in the VLR memory. On the other hand, if the mobile enters a new VLR area, its HLR, the old VLR, and the new VLR are informed. The old VLR erases the data for the mobile, and the new VLR records relevant parameters needed to process calls.

The message sequence is shown in Fig. 9. The MS is switched on in a location area different from the previous one, or it moves across boundaries of a location area in the idle state RIL3-Location Updating Request message, which is sent from the MS to the BSS and is relayed to the MSC. The MSC in turn alerts the VLR by a MAP/B Update Location Area message. The message contains the old location area that the mobile had in its storage along with its TMSI (designated here as LAI , TMSI). The process of authentication, ciphering, and TMSI reallocation can now start. After completion of the ciphering process, the message is sent from the VLR to the MSC for reallocation of the TMSI if desired (Forward New TMSI). A TMSI Reallocation Complete message is sent from the MS to the BSS after reallocation of new TMSI. The HLR sends a MAP/D Location Update Result message to the VLR, which in turn sends a MAP/B Location Update Acknowledge message to the MSC. This message is subsequently forwarded to the MS as a RIL3-RR Location Update Accepted message. In the event that the HLR rejects the request, the VLR RIL3-MM Location Update Reject message is sent from the MSC to the MS (shown dotted). Either the accept or the reject message is initiated from MSC. Location area updating may not be accepted due to the following reasons:

- unknown subscriber;
- unknown location area;
- roaming not allowed;
- system failure.

After the location update accept or reject message, the MSC asks the BSS to release the allocated dedicated resource by sending a BSSMAP Clear Command message to the BSS, which then forwards it to the MS. A BSSMAP Clear Complete message follows from the BSS to the MSC,
which completes the location updating process.
In the next section, we shall discuss the most important
security aspects of the GSM system.

IV. SECURITY ASPECTS OF THE GSM SYSTEM

At an early stage in the development of the Pan European mobile radio system GSM, it was realized that security was an important issue that needed to be addressed. It was apparent that the weakest part of the system was the radio
path, as this could be easily eavesdropped upon with

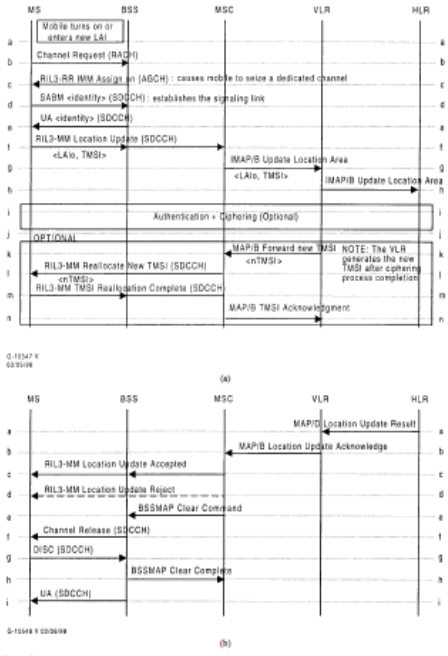

Fig. 9. Location update process.

radio equipment. There was also a need to authenticate users of the system so that the resources are not misused by nonsubscribers [3], [10]–[12].

Therefore, the objective of this section is to outline clearly the most important security features adapted in GSM, including:

a) authentication;
b) ciphering; and

c) an equipment ID, which ensures that no stolen or unauthorized mobile equipment is used in the system.

A. Authentication

The authentication feature ensures that, to a very high level of probability, the user is the one he claims to be. The purpose of the authentication is to protect the network against unauthorized use. It also enables the protection of the GSM PLMN. Subscriber authentication is performed at each registration, at each call setup attempt (mobile originating or terminated), and before performing some supplementary services, such as activation or deactivation of the mobile (IMSI attach, IMSI detach).

Authentication is not mandatory prior to IMSI

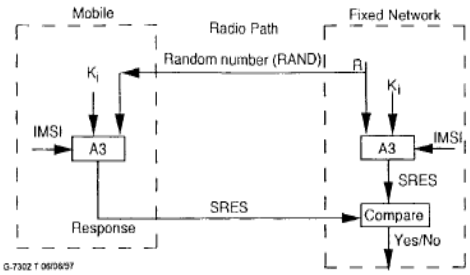

Fig. 10. Generic authentication process.

attach and detach procedures. The frequency with which a particular PLMN applies the authentication procedure to its own subscribers is their responsibility. However, a PLMN shall apply the authentication procedure to visiting subscribers as often as this feature is applied to those subscribers in their home PLMN.

GSM uses a sophisticated technique for authentication that consists of asking a question that only the right subscriber equipment (in this case, the SIM) can answer. The heart of this method is that a large number of such questions exist, and it is unlikely that the question can be answered correctly by the wrong MS. The generic process of authentication is shown in Fig. 10 [3], [10]. The authentication algorithm (called A3 in the GSM specifications) computes from a RAND, both at the MS and at the AuC, a signed response, using an individual secret key K_i attached to the mobile subscriber. The number RAND, whose value is drawn randomly between 0 and 2^{128} -1, is used to generate the response by the mobile as well as by the fixed part of the network. It should be noted that the authentication process is carried out both at the mobile and at the MSC simultaneously. The BSS remains transparent to this process. It should also be noted that the mobile only receives the random number over the radio path and in turn returns the signed response to the network. Thus, an air interface mobile designation is not disclosed. At subscription time, the subscriber authentication key K_i is allocated to the subscriber together with its IMSI. The key K_i is stored in the AuC and used to generate a triplet (K_c,signed response, RAND) within the GSM system. As stated above, the same K_i is also stored at the mobile in the subscriber ID (SIM). In the AuC, the following steps are carried out in order to produce one triplet. A nonpredictable RAND is produced. RAND and K_i are used to calculate the signed response and the ciphering key (K_c),using two different algorithms (A3, A8). This triplet (RAND, signed response, and K_c) is for each and every user and is then delivered to the HLR. This procedure is shown in Fig. 11 [3], [9]–[11].

VI. SUMMARY AND CONCLUSIONS

Protocols using the MM layer have been discussed. Important aspects of authentication, encryption, and the positive identification of mobile equipment before providing the user with service have been fully explored.

Authentication ensures that the network is accessed by the legitimate subscribers. The radio path is protected due to ciphering. Equipment ID ensures that the mobile is using the correct brand of transceivers. True mobility for the user can be achieved only by multiple entries on the SIM card ,by design of multimode terminals, and by the availability of fast and large data bases.

REFERENCES

[1] A. Mehrotra, GSM System Engineering. Norwood, MA: Artech House, 1997.

[2] C-C Lo, and Y-J Chen, "Secure Communication Mechanisms for GSM Networks," IEEE Transactions on Consumer Electronics, Vol.45, No.4, pp.1074-1080, Nov. 1999.

[3] S.M. Siddique, and M. Amir, "GSM Security Issues and Challenges," 7th IEEE International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD'06), pp.413-418, June 2006

[4] GSM World News - Statistics: http://www.gsmworld.com/news/statistics/index.shtml. Access: Jan. 23 2008