Mobility management

Mobility management is one of the major functions of a GSM or a UMTS network that allows mobile phones to work. The aim of mobility management is to track where the subscribers are, allowing calls, SMS and other mobile phone services to be delivered to them.

OR

Mobility management is a functionality that facilitates mobile device operations in Universal Mobile Telecommunications System (UMTS) or Global System for Mobile Communications (GSM) networks. Mobility management is used to trace physical user and subscriber locations to provide mobile phone services, like calls and Short Message Service (SMS).

Explanation

UMTS and GSM are each made up of separate cells (base stations) that cover a specific geographical area. All base stations are integrated into one area, allowing a cellular network to cover a wider area (location area).
The ***location update procedure*** allows a mobile device to notify a cellular network when shifting between areas. When a mobile device recognizes that an area code differs from a previous update, the mobile device executes a location update, by sending a location request to its network, prior location and specific Temporary Mobile Subscriber Identity (TMSI). A mobile device provides updated network location information for several reasons, including reselecting cell location coverage due to a faded signal.

Location area includes a group of base stations assembled collectively to optimize signaling. Base stations are integrated to form a single network area known as a base station controller (BSC). The BSC manages allocation of radio channels, acquires measurements from cell phones, and handles handovers from one base station to another.

Roaming is among the basic procedures of mobility management. It enables subscribers to use mobile services when moving outside of the geographical area of a specific network.

Mobility management consists of two related functions:

- location management and
- call routing.

Location management is the process of identifying the physical location of the user so that calls directed to that user can be routed to that location. Location management is also responsible for verifying the authenticity of users accessing the network.

Routing consists of setting up a route through the network over which data directed to a particular user is sent, and dynamically reconfiguring the route as the user location changes.

In cellular systems location management and routing are coordinated by the base stations or the central mobile telephone switching office (MTSO), whereas on the Internet these functions are handled by the Mobile Internetworking Routing Protocol (Mobile IP).

Mobility management enables the serving networks to locate a mobile subscriber's point of attachment for delivering data packets (i.e. location management), and maintain a mobile subscriber's connection as it continues to change its point of attachment (i.e. handoff management).

2.1. Location management

Location management enables the networks to track the locations of mobile nodes. Location management has two major sub-tasks:

(i) *location registration*,
(ii) *call delivery* or *paging*.

In location registration procedure, the mobile node periodically sends specific signals to inform the network of its current location so that the location database is kept updated. The call delivery procedure is invoked after the completion of the location registration. Based on the information that has been registered in the network during the location registration, the call delivery procedure queries the network about the exact location of the mobile device so that a call may be delivered successfully. The design of a location management scheme must address the following issues:

- minimization of signaling overhead and latency in the service delivery,
- meeting the guaranteed quality of service (QoS) of applications, and
- in a fully overlapping area where several wireless networks co-exist, an efficient and robust algorithm must be designed so as to select the network through which a mobile device should perform registration, deciding on where and how frequently the location information should be stored, and how to determine the exact location of a mobile device within a specific time frame.

2.2. Handoff management

Handoff management is the process by which a mobile node keeps its connection active when it moves from one access point to another. There are three stages in a handoff process.

- First, the initiation of handoff is triggered by either the mobile device, or a network agent, or the changing network conditions.
- The second stage is for a new connection generation, where the network must find new resources for the handoff connection and perform any additional routing operations.
- Finally, data-flow control needs to maintain the delivery of the data from the old connection path to the new connection path according to the agreed-upon QoS guarantees.

Depending on the movement of the mobile device, it may undergo various types of handoff. In a broad sense, handoffs may be of two types:

(i) intra-system handoff (horizontal handoff) and
(ii) inter-system handoff (vertical handoff). Handoffs in homogeneous networks are referred to as intra-system handoffs. This type of handoff occurs when the signal strength of the serving BS goes below a certain threshold value.

An inter-system handoff between heterogeneous networks may arise in the following scenarios

- when a user moves out of the serving network and enters an overlying network,
- when a user connected to a network chooses to handoff to an underlying or overlaid network for his/her service requirements,
- when the overall load on the network is required to be distributed among different systems.

Location Update Procedure

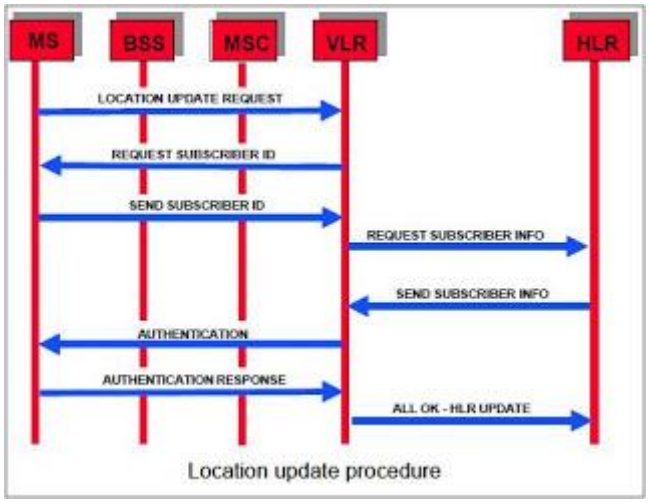
In order to make a mobile terminated call, The GSM network should know the location of the MS (Mobile Station), despite of its movement. For this purpose the MS periodically reports its location to the network using the Location Update procedure.

Location Area (LA)

A GSM network is divided into **cells**. A group of cells is considered a **location area**. A mobile phone in motion keeps the network informed about changes in the location area. If the mobile moves from a cell in one location area to a cell in another location area, the mobile phone should perform a location area update to inform the network about the exact location of the mobile phone.

The Location Update procedure is performed:

- When the MS has been switched off and wants to become active, or
- When it is active but not involved in a call, and it moves from one location area to another, or
- After a regular time interval.



Location update procedure

Location registration takes place when a mobile station is turned on. This is also known as **IMSI Attach** because as soon as the mobile station is switched on it informs the Visitor Location Register (VLR) that it is now back in service and is able to receive calls. As a result of a successful registration, the network sends the mobile station two numbers that are stored in the SIM (Subscriber Identity Module) card of the mobile station.

These two numbers are :-

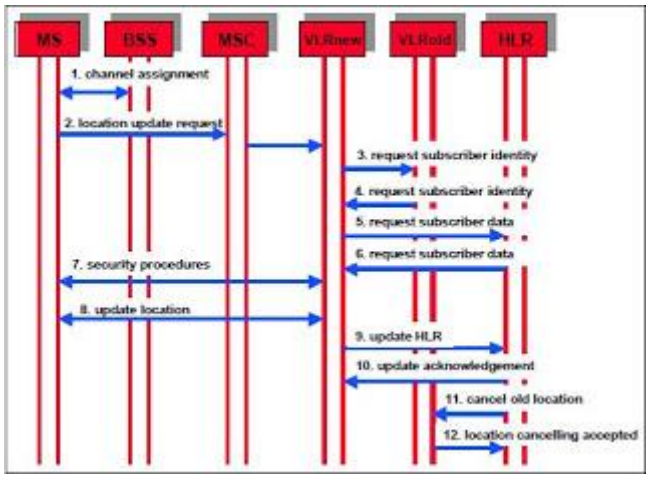
1. Location Area Identity (LAI)
2. Temporary Mobile Subscriber Identity (TMSI).

The network, via the control channels of the air interface, sends the LAI. The TMSI is used for security purposes, so that the IMSI of a subscriber does not have to be transmitted over the air interface. The TMSI is a temporary identity, which regularly gets changed.

- A Location Area Identity (LAI) is a globally unique number.
- A Location Area Code (LAC) is only unique in a particular network.

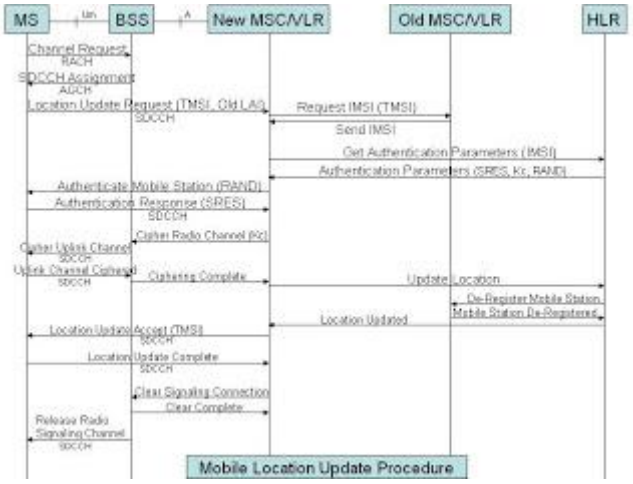
Every time the mobile receives data through the control channels, it reads the LAI and compares it with the LAI stored in its SIM card. A generic location update is performed if they are different. The mobile starts a Location Update process by accessing the MSC/VLR that sent the location data.
A channel request message is sent that contains the subscriber identity (i.e. IMSI/TMSI) and the LAI stored in the SIM card. When the target MSC/VLR receives the request, it reads the old LAI which identifies
the MSC/VLR that has served the mobile phone up to this point. A signalling connection is established between the two MSC/VLRs and the subscriber's IMSI is transferred from the old MSC to the new MSC. Using this IMSI, the new MSC requests the subscriber data from the HLR and then updates the VLR and HLR after successful authentication.

Periodic location update is carried out when the network does not receive any location update request from the mobile in a specified time. Such a situation is created when a mobile is switched on but no traffic is carried, in which case the mobile is only reading and measuring the information sent by the network. If the subscriber is moving within a single location area, there is no need to send a location update request.
A timer controls the periodic updates and the operator of the VLR sets the timer value. The network broadcasts this timer value so that a mobile station knows the periodic location update timer values.
Therefore, when the set time is up, the mobile station initiates a registration process by sending a location update request signal. The VLR receives the request and confirms the registration of the mobile in
the same location area. If the mobile station does not follow this procedure, it could be that the batteries of the mobile are exhausted or the subscriber is in an area where there is no network coverage. In such
a case, the VLR changes the location data of the mobile station to **"unknown"**.



The **Location Update process** consists of the following phases

- Request for service; the MS detects that it has entered a new Location Area and requests to update its location. The new MSC/VLR identifies the MS.
- Authentication - The new MSC/VLR requests to the AUC for authentication parameters (SRES, Kc, RAND). Using these parameters the MS is authenticated.
- Ciphering - Using the parameters which were made available earlier during the authentication the uplink and the downlink are ciphered.
- Update HLR/VLR - The new MSC/VLR requests to update the MS location in the HLR. The MS is de-registered in the old VLR.
- TMSI re-allocation - The MS is assigned a new TMSI.



1. The MS detects that it has entered a new Location Area and transmits a Channel Request message over the Random Access Channel (RACH).
2. Once the BSS receives the Channel Request message, it allocates a Stand-alone Dedicated Control Channel (SDCCH) and forwards this channel assignment information to the MS over the Access Grant Channel (AGCH). It is over the SDCCH that the MS will communicate with the BSS and MSC.
3. The MS transmits a location update request message to the BSS over the SDCCH. Included in this message are the MS Temporary Mobile Subscriber Identity (TMSI) and the old Location Area Identification (oldLAI). The MS can identify itself either with its IMSI or TMSI. The BSS forwards the location update request message to the MSC.
4. The VLR analyzes the LAI supplied in the message and determines that the TMSI received is associated with a different VLR (old VLR). In order to proceed with the registration, the IMSI of the MS must be determined. The new VLR derives the identity of the old VLR by using the received LAI, supplied in the location update request message. It also requests the old VLR to supply the IMSI for a particular TMSI.
5. The new VLR sends a request to the HLR/AUC (Authentication Center) requesting the “authentication triplets” (RAND, SRES, and Kc) available for the specified IMSI.
6. The AUC, using the IMSI, extracts the subscriber's authentication key (Ki). The AUC then generates a random number (RAND), applies the Ki and RAND to both the authentication algorithm (A3) and the cipher key generation algorithm (A8) to produce an authentication Signed Response (SRES) and a Cipher Key (Kc). The AUC then returns to the new VLR an authentication triplet: RAND, SRES, and Kc.
7. The MSC/VLR keeps the two parameters Kc and SRES for later use and then sends a message to the MS. The MS reads its Authentication key (Ki) from the SIM, applies the received random number (RAND) and Ki to both its Authentication Algorithm (A3) and Cipher key generation Algorithm (A8) to produce an authentication Signed Response (SRES) and Cipher Key (Kc). The MS saves Kc for later, and will use Kc when it receives command to cipher the channel.
8. The MS returns the generated SRES to the MSC/VLR. The VLR compares the SRES returned from the MS with the expected SRES received earlier from the AUC. If equal, the mobile passes authentication. If unequal, all signaling activities will be aborted.
9. The new MSC/VLR requests the BSS to cipher the radio channel. Included in this message is the Cipher Key (Kc), which was made available earlier during the authentication.
10. The BSS retrieves the cipher key, Kc, from the message and then transmits a request to the MS requesting it to begin ciphering the uplink channel.

11. The MS uses the cipher key generated previously when it was authenticated to cipher the uplink channel, and transmits a confirmation over the ciphered channel to the BSS.
12. The BSS upon ciphering the downlink channel sends a cipher complete message to the MSC. At this point, we are ready to inform the HLR that the MS is under control of a new VLR and that the MS can be de-registered from the old VLR.
13. The new VLR sends a message to the HLR informing it that the given IMSI has changed locations and can be reached by routing all incoming calls to the VLR address included in the message.
14. The HLR requests the old VLR to remove the subscriber record associated with the given IMSI. The request is acknowledged.
15. The HLR updates the new VLR with subscriber data (mobiles subscriber's customer profile).
16. The MSC forwards the location update accept message to the MS. This message includes the new TMSI.
17. The MS retrieves the new TMSI value from the message and updates its SIM with this new value. The mobile sends then an update complete message back to the MSC.
18. The MSC requests from the BSS that the signaling connection be released between the MSC and the MS.
19. The MSC releases its portion of the signaling connection when it receives the clear complete message from the BSS.
20. The BSS sends a "radio resource" channel release message to the MS and then frees up the Stand-alone Dedicated Control Channel (SDCCH) that was allocated previously. The BSS then informs the MSC that the signaling connections has been cleared.