GSM Call Flow Scenarios

1 Introduction

A mobile station (MS) can be in one of the following states:

- **Detached** – MS is powered off or the SIM card is deactivated
- **Attached** – MS power is on and the SIM card is activated. An attached MS can be:
    - **Idle** – MS has no dedicated channel allocated. It just listens to base stations broadcasted signals (called beacon signal) to remain attached
    - **Active** (dedicated) – MS has a dedicated connection to the network

There are some communications activities between the MS and the network when an MS changes its state. When it is switched-off its data in the VLR and the HLR get updated (detached state) so that no incoming call will try to page the MS. When an MS is switched-on it starts the initialization procedure in order to find the network and synchronizes itself to a right frequency (beacon frequency) and TDMA (Time Division Multiple Access) slot. After that the MS gets through the association procedure in order to anchor itself to the base-station (idle state).

When an MS is idle it still listens the paging channels for an incoming call, periodically re-synchronize itself and measures the signal strength of its own as well as its neighboring cells (for the purpose of location update).

An MS enters an active state when it requests for a service. At first it gets a dedicated data channel for a variety of authentication and security procedure. This channel is also used for SMS transfer (send/receive). If it is a voice call request then a dedicated voice channel is allocated before releasing the dedicated data channel.

The following list includes most of the categories of signaling on the GSM radio interface. Each of them is discussed in separate sections of this document.

1) MS initialization after switched-on
2) Service request
3) Authentication and security
4) MS attach and detach
5) Location update
6) Outgoing voice call
7) Incoming voice call
8) SMS and special services
9) Call hand over

2 Mobile Station Initialization

When a mobile station is switched on it starts initializing itself through the following three phases.

1. Frequency Synchronization
2. Time Synchronization
3. Network and cell information acquisition

All these happen by detecting the beacon signal (also called base frequency signal) which the network broadcasts from its radio base station (RBS). The beacon signal is a special signal that an RBS broadcasts in order to advertise its presence, identities (such as, which operator it is) and all the necessary initial information (such as, information about the paging channels).

2.1 Frequency Synchronization

The frequency synchronization is the process of finding the beacon frequency. The synchronization process has two 'logical' steps which are stated below.

Step 1: Find out a GSM signal

When a mobile station (MS) is switched on it starts scanning the GSM frequencies it supports. The GSM bands include 850 MHz and 1900 MHz (in North America) and 900 and 1800 MHz (Europe and rest of the world). Not all mobile stations support all the bands. Each band contains many 200 kHz frequency channels (called GSM frequency channels). The purpose of this scanning is to find if there is any radio signal in the GSM frequency band(s). The mobile station does this scanning by setting its receiver to a GSM frequency channel, measures radio signal strength and compares the signal strength with the threshold in order to make a decision if this signal level can be considered as 'enough'. Usually, an MS has two threshold power levels:

1. Lower power threshold: The power measurement below this level is not acceptable. In that case an MS continues frequency scanning.
2. Higher power threshold: The power measurement above this level is acceptable. In that case an MS will lock its frequency and proceed with next level of the synchronization.

When the measured signal falls in between those two power levels an MS accepts this 'conditionally' and moves to Step 2.

Step 2: Check if the frequency is a beacon frequency (Frequency Synchronization)

When an MS finds an acceptable GSM signal it checks if this frequency is the beacon frequency. A radio base station includes one GSM frequency which sends the beacon signal (and few more frequencies for user traffic and control signals).

- If the frequency is not a beacon the mobile station will reject that frequency and start searching for a new frequency (back to Step 1).
- If the frequency is a beacon frequency then the mobile station records this frequency and proceeds to the time-synchronization phase.

A beacon signal contains a time-slot filled with a pure carrier signal (called Frequency Correction/Correlation Channel or FCCH). This is the identity of a beacon that a mobile station searches for in order to make sure that this frequency is, indeed, a beacon frequency (base frequency). The pure carrier signal means unmodulated carrier (sinusoidal waveform). While the beacon frequency can be any valid GSM frequency the time-slot for the unmodulated carrier (that is, the slot for FCCH) has a fixed and specific location.

FCCH serves the following two purposes:

1. It indicates that this is the beacon channel
2. It helps synchronize with the carrier frequency (and phase)

The mobile station detects this unmodulated carrier sinusoid, locks itself with the carrier frequency (and phase), and proceeds to the time-synchronization phase.

2.2 Detect the start of a time-slot (Time Synchronization)

The time synchronization is the process of finding the bit and time-slot boundary. The FCCH channel (a time-slot in beacon frequency with pure carrier waveform) is immediately followed by a time-slot called Synchronization CHannel (SCH). This channel provides the means of time synchronization. The data packet (GSM call it 'burst') includes a training sequence (a known bit sequence) which help perform bit synchronization. Another purpose of the training sequence is to 'train' the receiver equalizer so that it can dynamically optimize itself for a better radio reception. The information in SCH channel includes:

- TDMA Frame Number (FN) – (to be discussed in another session)
- Base Station Identity Code (BSIC) which consists of
  - Network Color Code (NCC)
  - Base-station Color Code (BCC)

At this stage an MS already frequency and time synchronized, and it detected the operating company's identity. If the identity is its own service provider the MS will proceed to next phase (collection of further information about the cell and the network). Otherwise, it will go back to frequency synchronization phase and try with new frequencies.

2.3 Network and Cell Information Acquisition

When a mobile station is successful in synchronizations it reads four time-slot long Broadcast Control CHannel (BCCH) for the system information. This channel has a specific time-slot relative to the FCCH/SCH channels. The information in the BCCH channel includes:

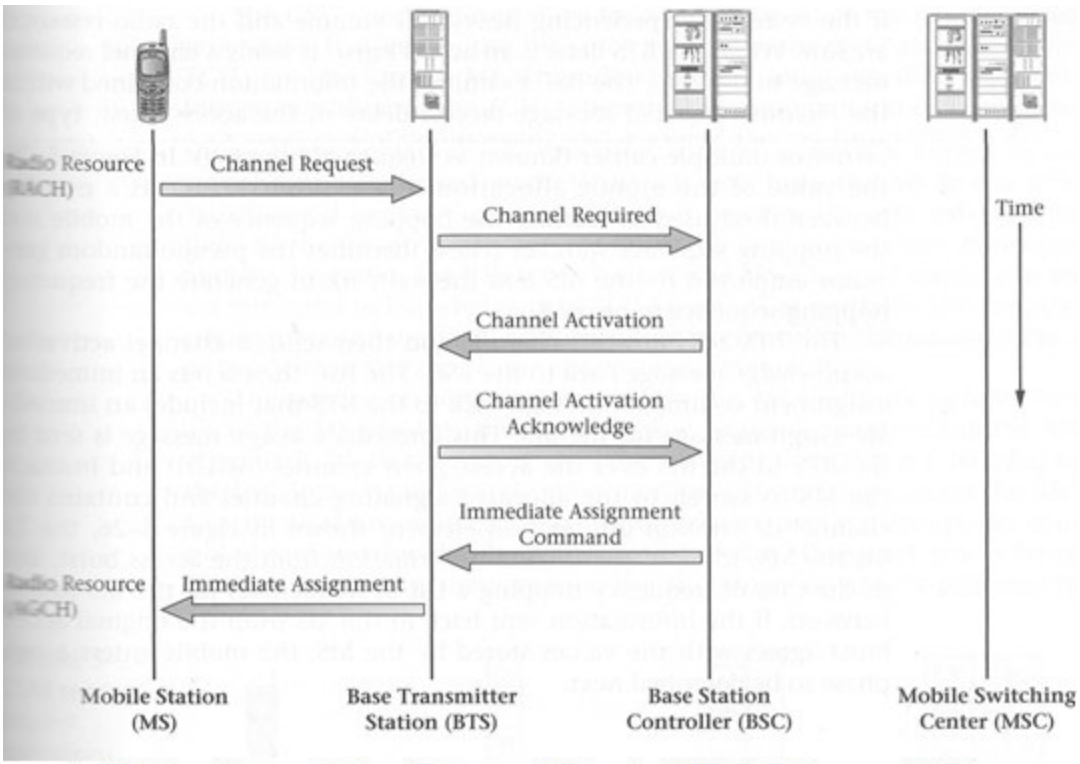
- Location Area ID (LAI)
  - Mobile Country Code (MCC)
  - Mobile Network Code (MNC)
  - Location Area Code (LAC)
- Cell ID (CID)
- BCCH Allocation List (BA list) – a list of neighboring cells' beacon frequencies
- Information about the locations of common control channels (paging, random access and access grant channels)
- Frequency hopping Sequence
- Maximum mobile station power limit (MSTXPwr)
- Base station's minimum received signal power to access the network (RxLevAM)
- Update period (location update)

At this stage an MS is fully furnished with necessary information and synchronization in order to communicate with the network. A mobile station is not yet to be attached to the network. It requires IMSI (International Mobile Subscriber Identity) attach and location update procedure. The IMSI attach procedure lets the network record that the mobile station is powered on and is ready to make or receive calls. The location update procedure lets the network record which location the MS is now anchored. To proceed with those tasks the mobile station must make a service request to the network (see the next section).

3 Request for Service

3.1 Channel Request for 'Start of a Communication'

For any calls (for example, voice, data stream, SMS, attachment/registration/association, and location updating) a mobile station requires sending a request to the network, and hence it needs a channel for that. This channel is called Random Access CHannel (RACH). All the RACH channels in a cell have specific 'locations' (frequency and time-slots). A mobile station, which is already initialized with the network (that is, it is already set with FCCH-SCH-BCCH channels), knows the location. Whenever a mobile station initiates a call it just sends a dedicated channel request using the RACH channel (see the figure below).



Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher

There is a possibility that more than one mobile station may try to send their requests at the same time using the same RACH. In that case there will be a collision and the information from the mobile stations are destroyed, and the mobile station must resend the request. The process of such sending and resending, if required, follows the Aloha random access procedure.

When the radio base station (GSM calls it Base Transceiver Station or BTS) receives a valid request it simply forwards the request to the Base Station Controller (BSC) for decision. The BSC selects an unused data channel, called Stand-alone Dedicated Control CHannel (SDCCH). This is a duplex data channel. As name suggests that it is a dedicated channel between the mobile station and the network; it is a data channel in order to carry further dialog between the mobile station and the network; and it is stand-alone channel as it is not associated to any traffic channel. The possible dialog includes:

- what type of service the mobile station wants (make a voice call, receive a voice call, send an SMS or just location update, for examples)
- authentication and security related dialog

The BSC sends the ID of the selected SDCCH to the BTS and asks to activate the channel. The BTS does so and sends back an acknowledgement to the BSC. The BSC then asks the BTS to assign the channel to the mobile station. The BTS uses another channel called Assignment Grant CHannel (AGCH) to let the mobile station know which SDCCH channel has been assigned.

When the BTS and BSC were exchanging the messages the mobile station listens to the AGCH channel for the reply to its request. Like RACH channel the AGCH channels have specific locations which were advertized by the network in its BCCH channel broadcast.

Note 1: In some traffic situations a new channel may be assigned using TCH (Traffic CHannel) instead of SDCCH. In that case, The AGCH message let the mobile station know that the allocated channel is a TCH channel in "signaling mode" instead of traffic mode. In such a case the TCH serves the function of an SDCCH. If the assignment process proceeds further to an assignment of "traffic TCH" then it is typical that the already assigned TCH will remain assigned, and the network simply sends a "channel mode modify command" to make it a traffic-mode TCH.

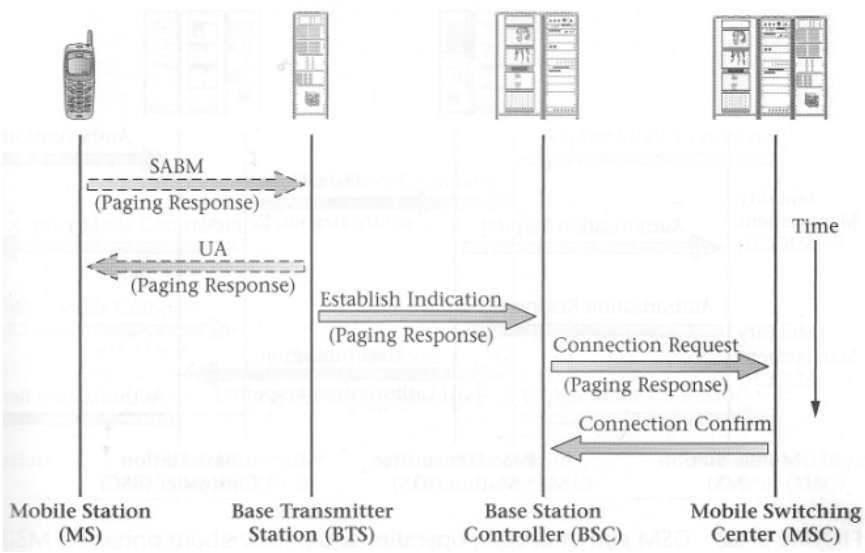
Note 2: The SDCCH and TCH have a supplementary channel, called Slow Associated Control CHannel (SACCH). This associated channel is used to carry the radio link related information such as current signal strength, power control signal and timing advance signal.

3.2 Service Request

As soon as a mobile station (that requested for a channel) receives a radio resource (SDCCH or TCH in signaling-mode) it sends a service request using the assigned channel. The message includes the code of the requested service which can be, for examples,

- Response to a paging
- New call initiation
- Location update or association after being powered on

The following diagram illustrates how a mobile station requests for an incoming call connection after being paged. The message SABM (Set Asynchronous Balance Mode) is a command to BTS that contains the code of the requested service. The UA (unnumbered acknowledgement) message is sent by the BTS to acknowledge the SABM. In this example it is a paging response, which typically means: extend the call to the mobile station. The likely result of this response is a ring to the mobile station, if everything goes well. The 'everything' includes a series of authentications and security check/setup (see the next section), and also the traffic channel (TCH) assignment. The following figure did not include the final response of the request.



Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher

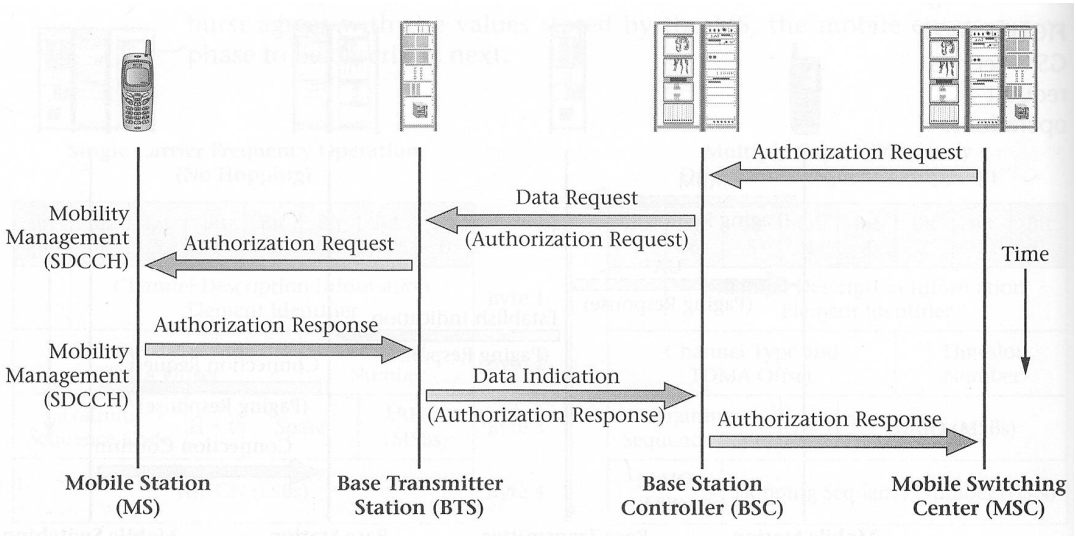
4 Authentication, Authorization and Security

When an MS requests for a service the network verifies authenticity, service profile, and then setup the encryption schemes, if required. All these dialogs between the mobile stations and network are carried by the allocated dedicated channel (SDCCH or TCH in signaling mode). The communications at this phase are in between the MS and the MSC. The BSC and the BTS forwards the messages transparently using appropriate protocol data unit (message format).

4.1 Authentication and Key Generation Process

Typically a GSM network starts an MS (mobile station) authentication process right after the service request process. This is a dialog between MSC and MS (BSC and BTS are transparent) using the assigned dedicated channel (normally an SDCCH but can be TCH as well). This authentication process takes a full cycle if this is the first time the MS is sending a service request to this MSC after powered-on (attachment).

- When service request phase is complete the MSC checks for any existing security triple (RAND, SRES and K_C) in the VLR for this MS. If not available then the MSC requests the HLR for that, and the HLR works with AuC (authentication center) to provide (typically) five triples, which are then stored in the VLR and use one at a time.
- Authentication request message from MSC to MS includes 128-bit random number (RAND) and ciphering key sequence number (CKSN). The RAND is a random number to challenge the MS producing 32-bit SRES (Signed Response) equal to the one in the 'triple'. The CKSN is the ID of the triple saved in the VLR and to be saved in the MS (in the SIM) as well. This is useful for next authentication process (discussed later)
- The MS stores the CKSN and produces the SRES using the RAND and the Individual Subscriber Authentication Key (K_I) as the input to the MS authentication algorithm (A3). The algorithm is stored in the MS equipment as a part of the firmware.
- At this stage the MS also generates the ciphering key (K_C) using the RAND and K_I as the inputs to another algorithm A5 (The cipher key generation algorithm).
- The value of the SRES is returned to the MSC. The MSC verifies the SRES by comparing this one with its own one. The authentication process may have an additional phase, which is IMSI verification (subscription verification). Depending on the GSM operators setting the MSC may proceed with the verification of the current eligibility status of the MS for this call. In that case the MSC will consult with VLR (or HLR if VLR does not have any record, which may be the case for first time call after switch-on or location update under a new MSC). When the verification is complete the MSC updates the VLR record, and proceeds to the next step, which is typically the ciphering process.

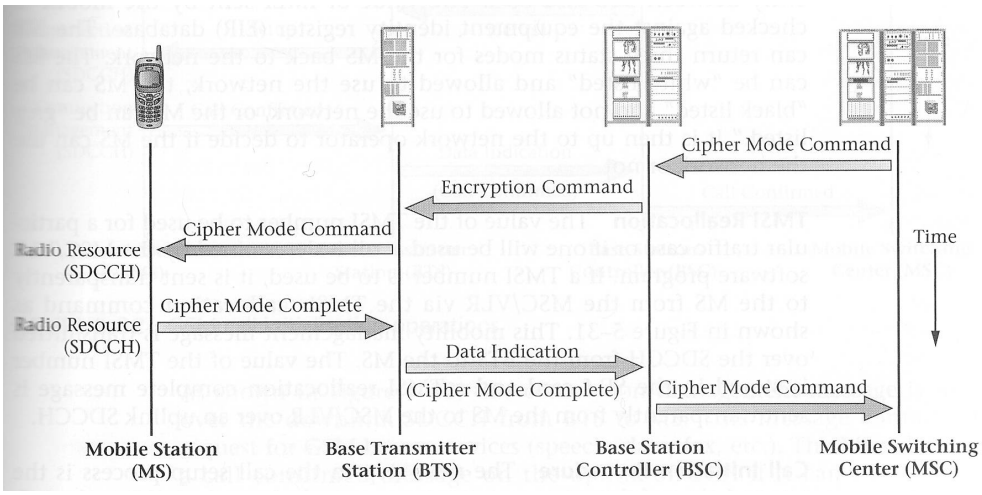


Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher

Once such an authentication process is successfully complete the network does not require repetition of the process for the subsequent call unless the MS is detached. In these cases the MS sends the CKSN in the service request message. The MSC checks this number with the VLR database. If it passes the check, the MSC bypasses the authentication process.

4.2 Ciphering Mode Setting

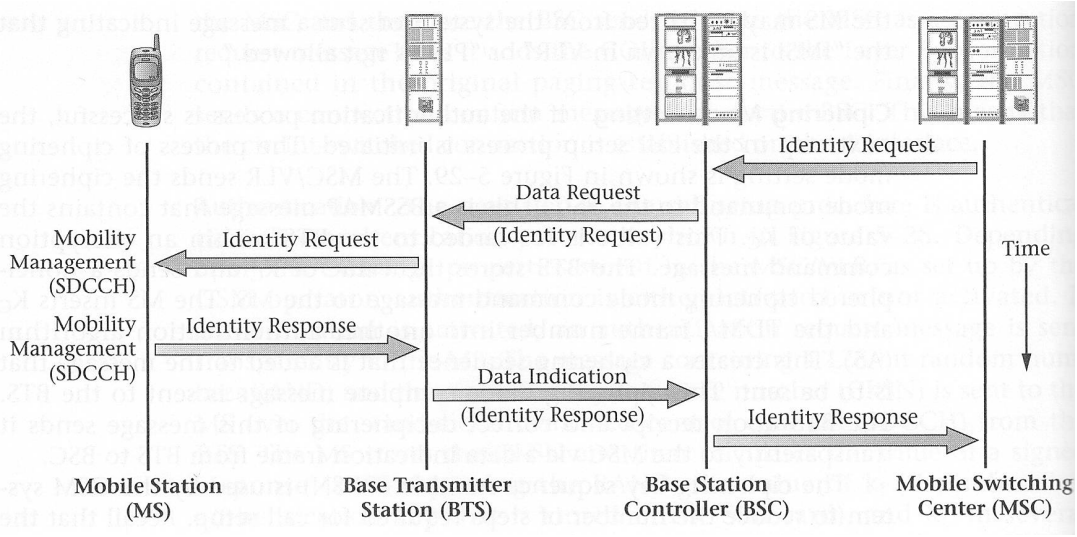
- If the ciphering is required, the MSC sends Cipher Mode Command to BSC to send the K_C (the cipher key).
- The BSC now sends the key and also the 22-bit TDMA-Frame# to the BTS.
- The BTS stores the values. The BTS also sends the encryption command to the MS. Note that BTS does not send K_C since it is not secured, and K_C is already computed by the MS during the authentication process.
- The K_C and the TDMA-Frame# are used as inputs to run the ciphering algorithm (A5) on the data/ digitized voice to produce encrypted payload. The MS and the BTS are the parties involved in the ciphering/deciphering process.



Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher

4.3 IMEI Number Check

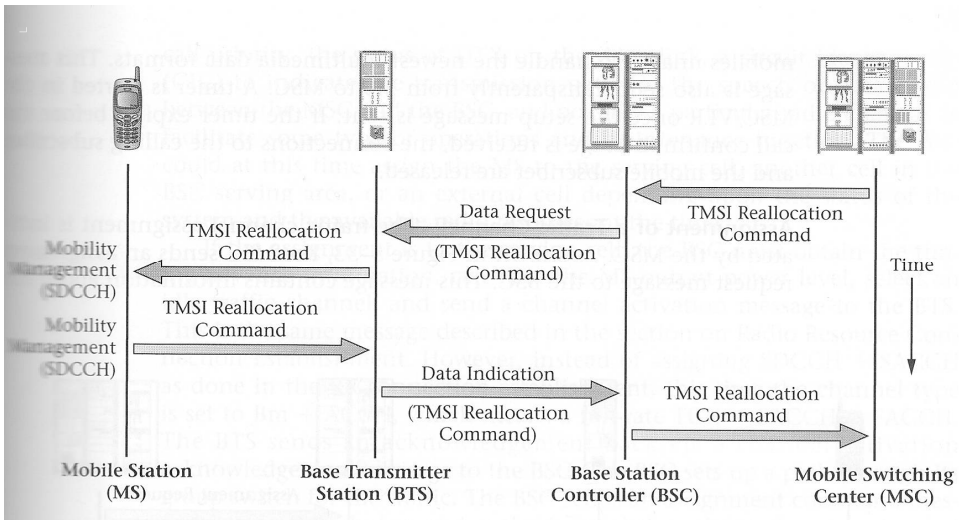
The network may perform IMEI (International Mobile Equipment Identity) check as illustrated in the following figure. After collecting the IMEI number of the MS the MSC verifies this with the White, Black and Grey list in the EIR (Equipment Identity Register). The white listed IMEIs are allowed to use the network; the black list IMEIs are not allowed; and the grey list IMEIs are those which are, for example, faulty or unapproved mobile stations, and under observation for probable problems. It is up to the network operator if any one IMEI in this list can (or can not) use the network.



Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher

4.4 TMSI Allocation

As an additional security measure the network allocates a TMSI (temporary IMSI) number to the MS. This happens when an MS passes the authentication phase for the first time under the MSC (powered on or location update). The MSC asks the AuC to generate a TMSI for the IMSI, and sends the newly generated TMSI to the MS. The MS stores it in the SIM card and MSC stores it in the VLR. Once it is assigned the MS uses TMSI instead of IMSI to identify itself when it requests for a service. The allocation process is illustrated in the following figure.



Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher

5 IMSI Attach and Detach

5.1 IMSI Attach

A mobile station can go switched-on or off. When switched on it gets initialized (frequency synchronization, time-synchronization and system information acquisition) and then gets attached to the network. This is a kind of status notification to the network so that it can accept MS's call request and page when there is an incoming call. This process of attachment is called IMSI attach. Note that IMSI is the primary ID that uniquely identifies a mobile station.

The IMSI attach procedure is as follows: Like all other service requests the MS gets an SDCCH data channel for this service. On the SDCCH the MS sends a message to inform the network that the MS is switched on. The MSC undergoes through the authentication procedure first. Then the MSC checks its VLR for information about this MS. If available (which means the MS was under this MSC before) the MSC updates the VLR entry (IMSI attached by removing IMSI detach flag). In some system the MSC may not inform any detach update to the HLR. In that case an attach update is also not required in this situation. Otherwise, the MSC will update the HLR as well. The MSC also updates the location of the MS according to the LAI (location area identity) sent by the MS. The MSC returns an acknowledgment message to the MS.

When the MSC finds the MS as a new MS (that is no entry for this MS in the VLR) the MSC queries the HLR and the HLR provides the detail about the MS. The MSC then create an entry into its VLR for the new MS with status "IMSI attached". The HLR updates its data for that MS and also sends a message to the MSC, where the MS was located before, asking to update its VLR.

5.2 IMSI Detach

The IMSI detach procedure may be used by the MS when it is powered off. The mobile station is marked as "detached" in the VLR and will not be paged when there is an incoming call. The system information, broadcast over the cell by BCCH, informs the MS whether IMSI attach and detach procedures are required or not.

The IMSI detach procedure is as follows: When the MS is powered off or the SIM card is taken out, the MS requests for IMSI detach service. Like all other service requests it gets an SDCCH data channel for this service. On the SDCCH the MS sends a message to inform the network that the MS is about to switch to detached mode. The VLR marks the IMSI as 'detached' (IMSI detached flag is set). The IMSI detach procedure is neither acknowledged nor authentication-performed. Optionally, The MSC informs the HLR about the IMSI detach state.

6 Location Update and Periodic Registration

A mobile station (MS) can move from place to place within the coverage area of the network. When it moves from a cell to another cell its location gets updated through a procedure of message transactions between the network and the MS. When an MS gets switched-on it gets change of state as well as location update.

The request for location updating can indicate one of three procedures.

- Location updating type normal
- IMSI attach
- Periodic registration

The MS listens to the beacon and checks if the LAI (location area identity) of the cell matches with the LAI stored in its SIM (from previous location update). The location update happens when they are different. In that case the MS requests for location update service. Like all other service requests it gets an SDCCH data channel for this service. On the SDCCH the MS sends a message to inform the network its new location (new LAI). The MSC undergoes through the authentication procedure first. Then the MSC updates its VLR. If the MS is new to this MSC (that is, location change causes the change of MSC) the MSC interacts with HLR to get all the required information about the MS, and gets its VLR a new entry for the MS. The HLR by that time updates its data for that MS and also sends message to the MSC, where the MS was located before, asking to update its VLR. The MSC returns an acknowledgment message to the MS. The network then releases the SDCCH channel.

The system also has a provision of periodic registration. This provision helps avoid unnecessary paging of the mobile in the case where the MSC never receives the IMSI detach message. The period of this registration is broadcasted in the beacon signal (BCCH message). After a registration the MS and MSC reset their timers. When the timer in the MS expires, the MS performs a location updating, and the timers in MS and MSC restart. If the MS does not register within the determined interval plus a guard time, then the MSC considers the MS detached, and it updates its VLR and optionally the HLR accordingly. The MSC sends an acknowledgment to the MS.

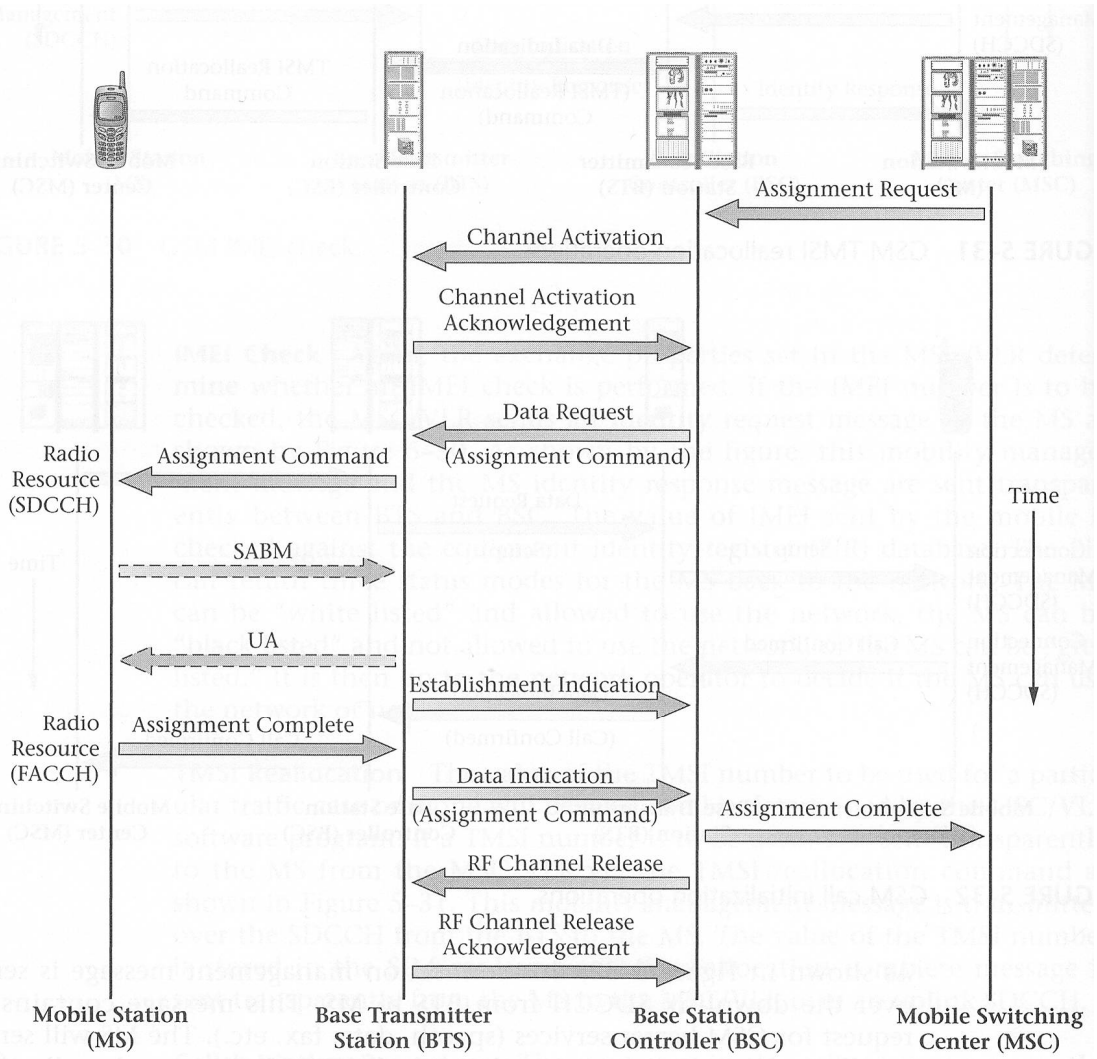
7 Outgoing Voice Call

7.1 Initiation Process

For initiating a voice call an MS sends a voice call request message. Like all other service requests the MS gets an SDCCH data channel for this service. On the SDCCH the MS sends a message to inform the network that its wants a voice connection. The MSC undergoes through the authentication procedure first. Then it sets the ciphering key for voice encryption, if enabled. Finally, the MS sends the call initiation message to the MSC including the dialled numbers. The MSC checks the subscription profile if the MS can make such a call. Then the MSC starts the voice channel (traffic channel) assignment procedure.

7.2 Assignment of Traffic Channel

When the MSC is set to establish a voice call it asks the network side (other MSC and/or PSTN switches) to establish a path to the called party (an MS or a PSTN telephone), and also asks the MS side (the BSC) to assign a traffic channel between the MS and MSC (see the figure below). The MSC also sets the MS's state 'busy' in order to handle an incoming call, if any, appropriately.



Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher

The selection of the voice channel between the BSC and MSC is decided by the MSC whereas the channel between the BTS and MS (the TCH channel) is up to the BSC. The BSC activates a free TCH channel preferably from the serving cell. If there is no free channel then the BSC may try to find one from the neighboring cell, if it works. In that case a location update is also required (it is like hand over before the call establishment). Finally, the activated TCH channel is assigned to the MS by sending an assignment command to the MS over the SDCCH channel.

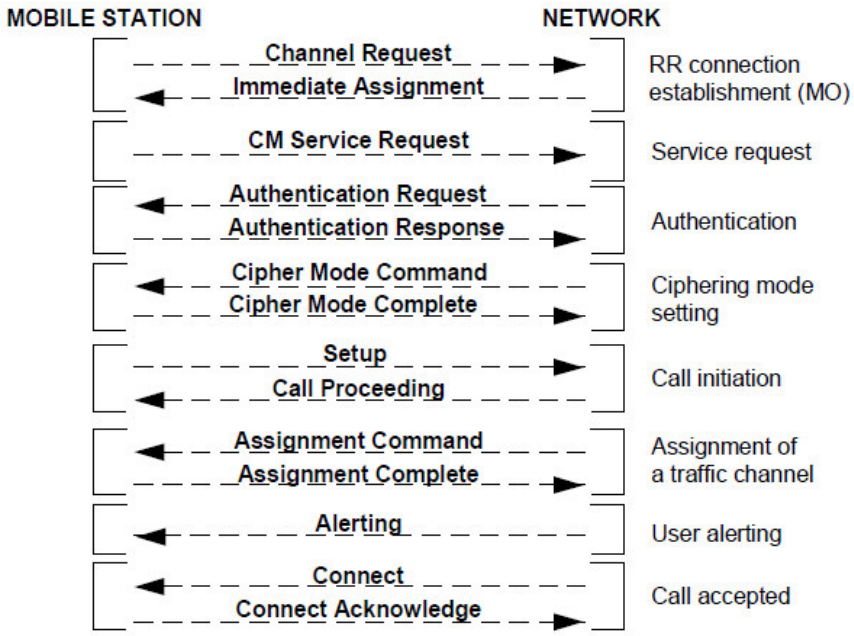
Not that the TCH channel accompanies SACCH (slow associated control channel) and FACCH (fast associated control channel). SACCH is a separate channel and used for dynamic performance adjustment of the link (such as timing advance and power control). The FACCH is, indeed, a TCH channel but momentarily turns as a signaling channel to quickly carry a control signal and backs to traffic mode. This FACCH is used for call setup, release and handover signaling since there is no SDCCH channel available anymore (released after TCH assignment).

When the TCH is assigned the MS in tunes its transmitter to the assigned TCH and sends SABM (Set Asynchronous Balance Mode) message which carries an indication of a successful seizure of the channel. The UA (unnumbered acknowledgement) message is sent by the BTS to acknowledge the SABM. Finally the SDCCH channel is released.

Note: If a TCH was assigned (with signaling mode) instead of an SDCCH channel during the service request phase then the same TCH may continue as the traffic channel. In that case no new TCH assignment or SDCCH release were necessary.

7.3 Call Confirmation, Acceptance and Release

When the caller MS successfully seizes the TCH channel it sends the assignment complete message to the network in the channel assignment phase. Then the MSC waits for an address complete message from the other end (the terminating-switch), which indicates that the called party is ringing. The MSC sends the caller MS an alert signal as soon as it receives the address complete message from the terminating switch. The MS now sends the connect request message to the MSC. The originating MSC returns an acknowledgement to the MS, and waits for an answer message (which confirms that the called party responded) from the terminating switch. The MSC completes the connection as soon as it receives that message. The following diagram depicts the message transactions between the caller MS and the network. The called side is covered in the next section



8 Incoming Voice Call

8.1 Interrogation

The interrogation is a process of allocating an MSRN (Mobile Station Roaming Number) to a visiting MS (mobile station) so that the switch (the MSC) can connect an incoming call to the visitor MS. The MSRN is a temporary telephone number (MS-ISDN) given to a visiting 'called-MS' in order to connect that call. The necessity of MSRN can be understood if we understand how a switch/MSC connects a call.

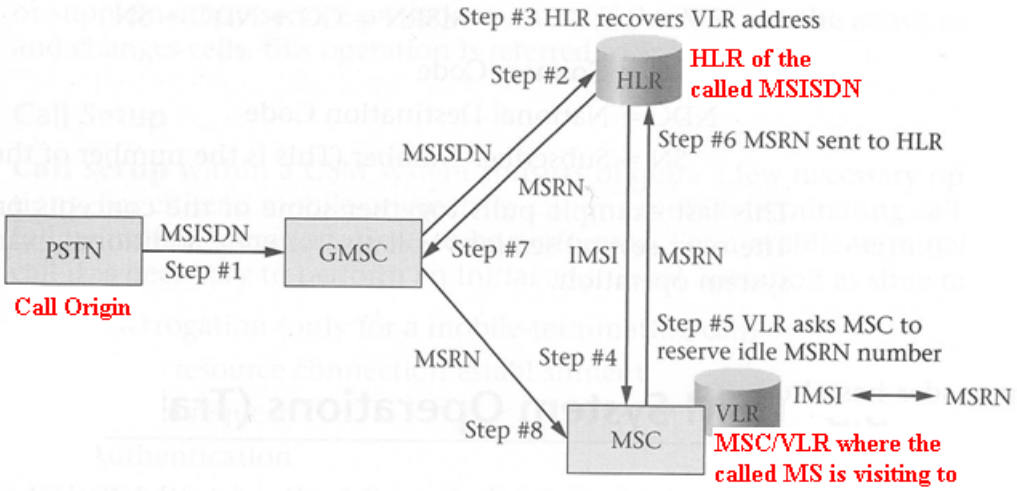
The fixed telephone systems (PSTN/ISDN) and cellular mobile systems, such as GSM, use the same number space (according to ITU E.164 format). For fixed telephony we call it PSTN/ISDN number and for GSM phone we call it MS-ISDN number.

The telephone numbering plan allocates a chunk of telephone numbers to a switch (PSTN and Cellular MSC alike). This is typically a fixed allocation. That is, an MSC has a fixed set of telephone numbers in its possession. When an MS is given a number from an MSC, that particular MSC becomes the 'home' for that MS. If an MS moves to the area of another MSC then that MS is a 'visitor' there. That is, an MSC can 'host' an MS of another MSC (the visitor or guest). If the MSC would follow the standard call-connection procedure then it could not connect an incoming call to a visitor MS since its Ms-ISDN is not one of its own.

When someone calls a visitor MS the system (with the help of HLR and VLR) locates the MSC who is currently hosting the visitor. The problem is that the hosting MSC can not connect the call using the original MSISDN of that visitor-MS since the number does not belong to that MSC. To get around this problem the following procedure is devised.

- The caller's MSC contacts the 'home HLR' of the called MS and asks for its whereabouts. If the call is from a PSTN/ISDN phone then the call request reaches to the Gateway MSC who contacts the home-HLR. Let us call this MSC an interrogator-MSC.
- The HLR determines the IMSI and VLR identity using the called-MSISDN number. The IMSI identifies the MS, and the VLR identity in effect locates the MSC (where the called-MS is currently visiting to) since VLR is always attached to an MSC.
- Locating the destination MSC/VLR is not enough to connect the call. The destination MSC can not connect the call since the called-MSISDN does not belong to it. HLR contacts the destination MSC/VLR to allocate one of its unused MSISDN number pool to that visitor-MS (which is the MSRN).
- The destination MSC/VLR makes that allocation and sends that MSRN to the HLR. The VLR also 'remembers' this assignment by entering this MSRN in its database.
- The HLR returns the MSRN to the interrogator-MSC.
- The interrogator-MSC replaces the original destination MSISDN with the MSRN and proceeds with standard call connection procedure.

The following figure illustrates the above procedure.



Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher

Notes:

- MSRN is required for a visitor-MS and for terminating call only.
- In the figure, the HLR is the home-HLR of the visitor-MS and the MSC/VLR is the one where the MS is visiting to.
- This process does not involve radio interface
- The above figure shows a call from PSTN. However, the call can be from another mobile. In that case GMSC is not involved. This will be just another MSC (the MSC from where the caller initiated the call).
- If the MS has LNP (Local Number Portability) service then there must be a process of consulting the FNR (Flexible Number Register) database of the GSM infrastructure.
- At the end of the MSRN allocation the VLR (of the visitor-MSC) and the HLR save the number for future use until the MS moves to another MSC or de-associates itself from the network. Thus the next call will not require another interrogation process.

8.2 Paging

For an incoming call the MSC/VLR require to page the MS. The MSC/VLR comes at a point of paging when it finds that:

- The called MS is in its area and currently associated and idle, or busy but has call waiting service
- MSRN is allocated for a visiting MS, if there is no MSRN already allocated

Otherwise, the MSC will not page, and the caller will get an appropriate message.

For the purpose of paging, an MSC finds the LAI (Location Area Identity) and the Paging Group Number (PGN) of the called-MS from the VLR. The LAI identifies the location area, which in turn, indicates which BTSs will broadcast the page. The PGN indicates what paging channel will be used for this page (since that is the paging channel the MS is listening to). It may happen that the MS moved to a new location area but the location is yet to be updated. In that case the, the location-area-wide paging will fail. When it fails the MSC goes for an MSC-wide paging before reporting a call connection failure.

The MSC sends a Paging Command (a Layer 3 SS7 command) to all the BSCs of a particular location area (if this is a LA-wide paging) or to all the BSCs of that MSC (if it is an MSC-wide paging). This paging message includes the IMSI/TMSI of the MS, the LAI and the paging group number.

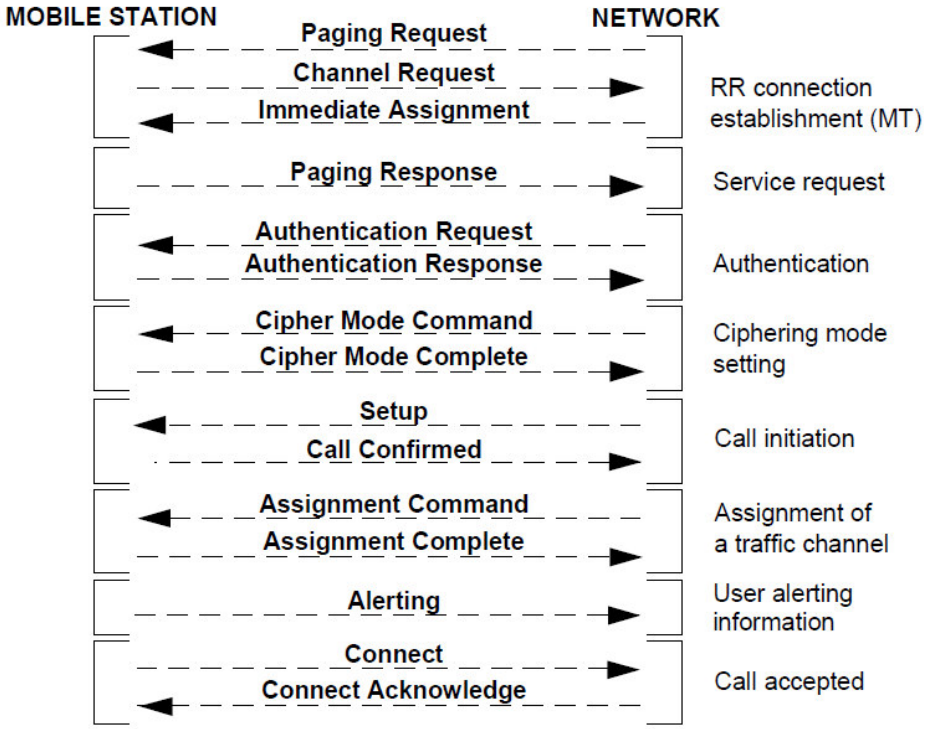
The BSC acts on the message:

- Using the LAI the BSC determines the CI (Cell Identity) of the cells involved.
- The BSC sends a paging command to the BTSs. The message includes the IMSI/TMSI, the PGN, and the Channel number. The channel number includes channel type (here it is downlink CCCH, which is the PCH) and the time slot number.

Each of the BTS sends the paging message over the designated PCH channel.

8.3 Call Receive

When an MS receives a page it sends a request of service message to the network and gets an SDCCH channel assigned. After passing through the standard authentication and security procedures the Ms receives a call initiation message from the network. This message informs the MS that it is a voice call. The MS sends call confirmed message to the network to tell that it is ready to accept the call. The network in return assigns the voice channel (the TCH channel) to the MS and sends the assignment command. The MS sends assignment complete message to confirm that it seized the channel. The MS also generates the ring tone for itself and sends alert message to the network. The terminating MSC then let the other side of the network (the caller side) know that the Ms is ringing. If the user of the MS answer the call the MS sends the connect message to the network. The network acknowledge the connect request. Finally the link is established between the two users.

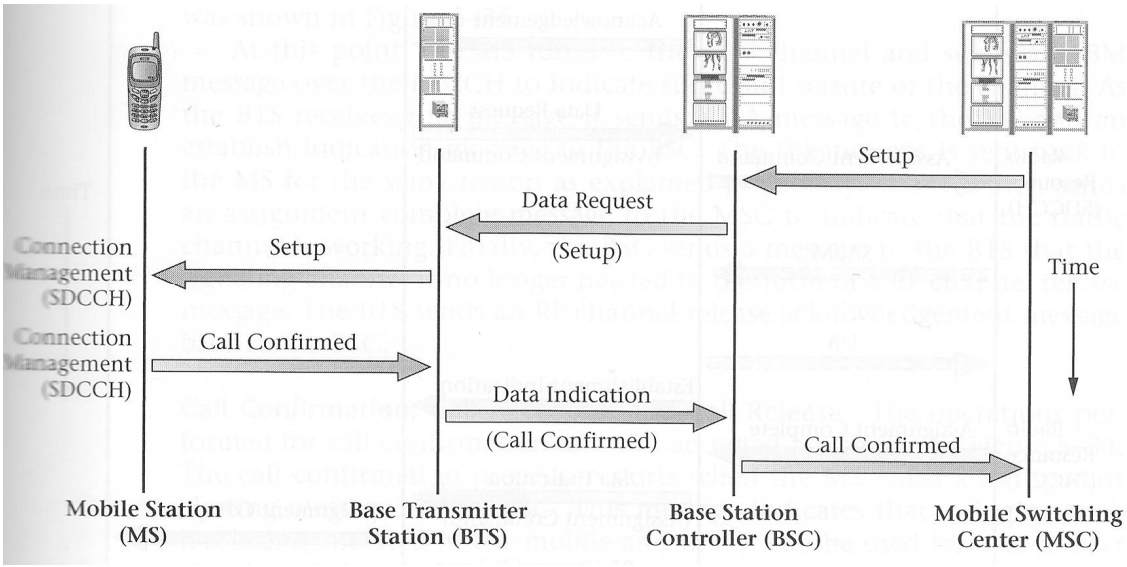


9 SMS and Special Services

The SMS (Short Message Service) message is sent over SDCCH channel. Note that this channel is allocated upon a service request. A SMS sender sends a SMS service request and gets an SDCCH channel. After all the authentication and security checks the sender finally forwards the message to the MSC. The MSC then forwards the message to the SMS service center to handle the rest. The MSC also send an acknowledgement to the MS. For an incoming SMS the MSC page the MS. The MS then requests for the service in order to receive the SMS. The rest of the transactions are similar to the case of outgoing SMS.

An SMS can be sent of receive while taking (that is, a TCH channel is assigned), In that case the SMS uses the FACCH channel, which is, indeed, the TCH channel but momentarily becomes a signaling channel to carry the signal (here it is an SMS message) before going back to be the traffic channel.

The cellular mobile system carries multimedia and other innovative services. Often these services require special feature for a mobile station. For example, an MS wants to send a picture to another MS but the receiver MS does not support this feature. To avoid this kind of problems the GSM system provides a feature to make a query to an MS if it has certain feature in order to communicate with the other end. The following diagram illustrates such a query.

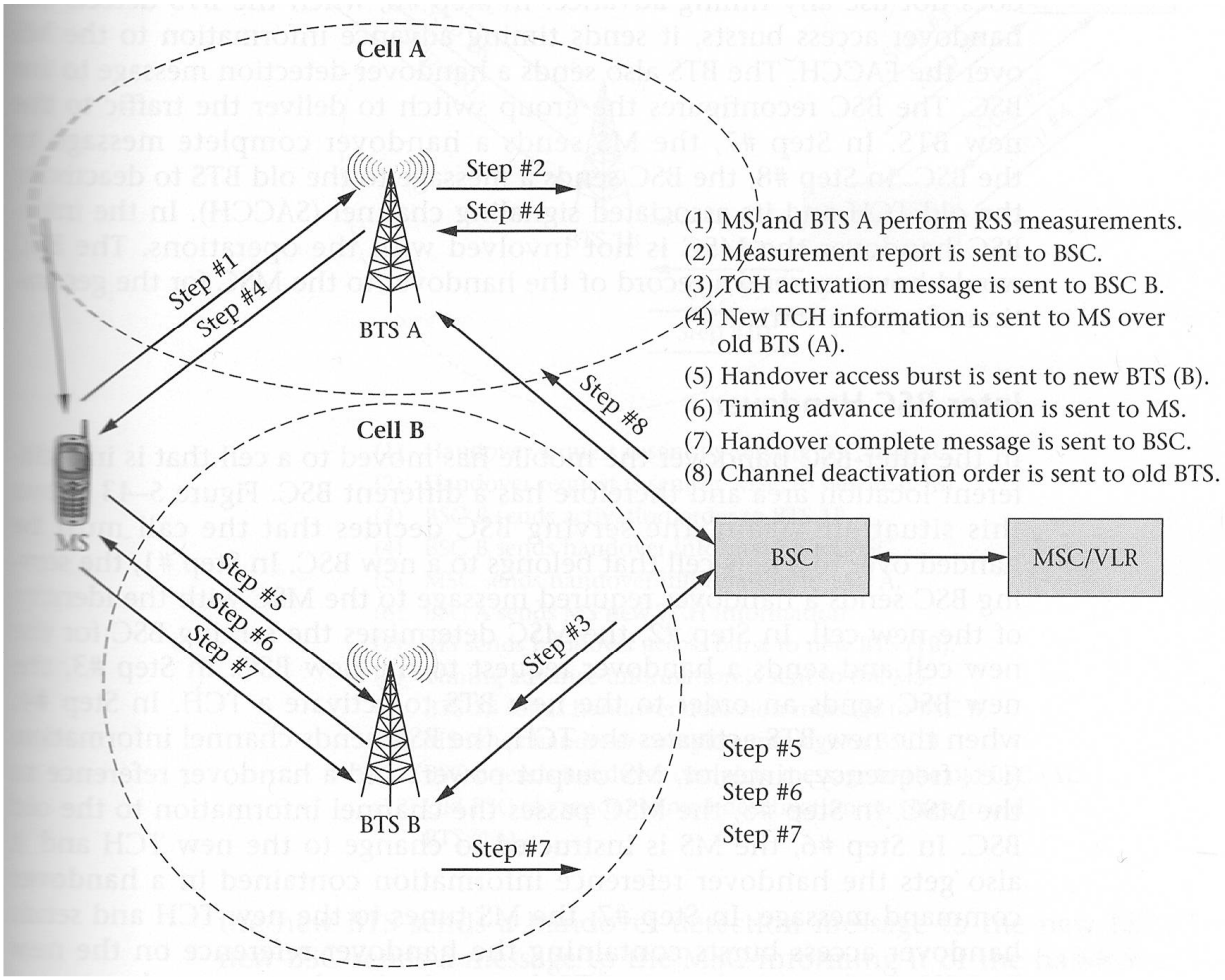


Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher

10 Call Hand-Over

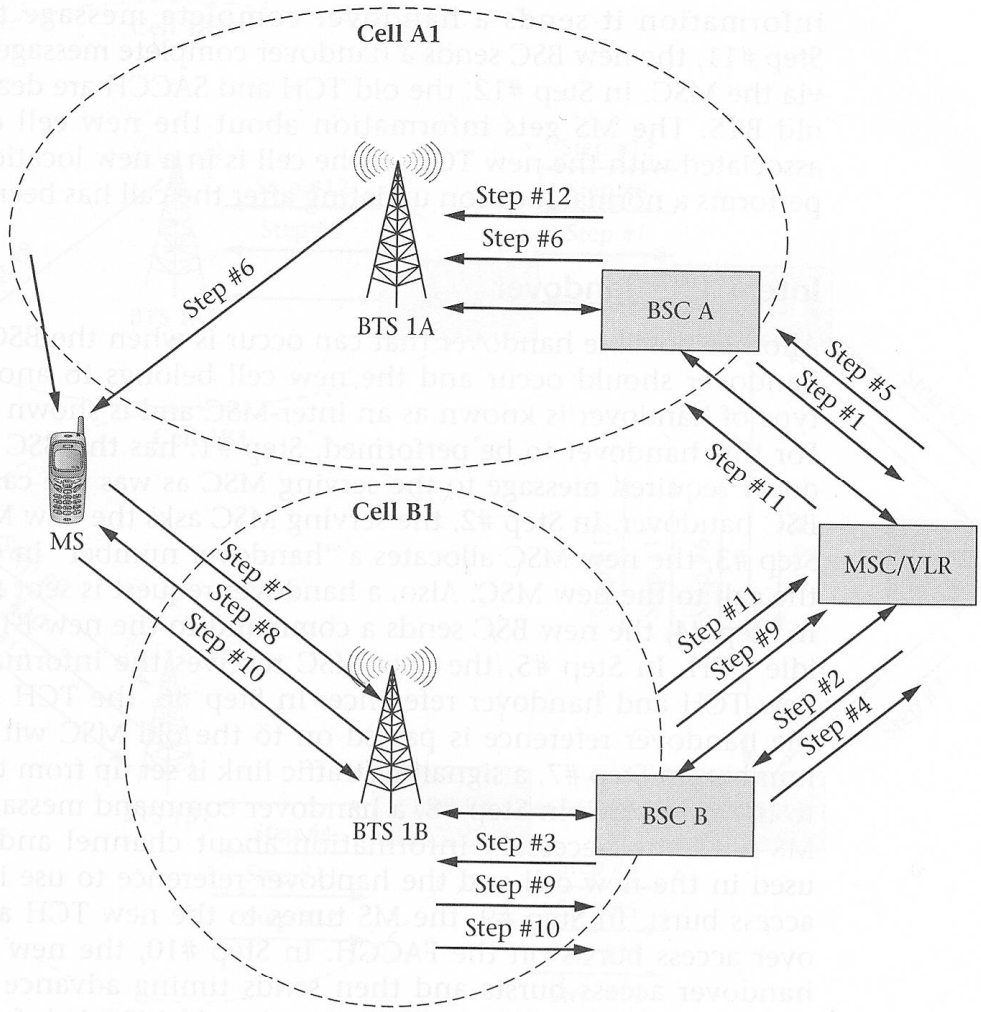
Hand-over can be Intra-cell, Intra-BSC, Inter-BSC and Inter-MSC. Intra-cell handover happens in case of poor channel quality for a particular channel. An inter-sector hand-over is also possible. The handover can happen on a TCH as well as on an SDCCH connection.

10.1 Intra-BSC Hand-Over



Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher

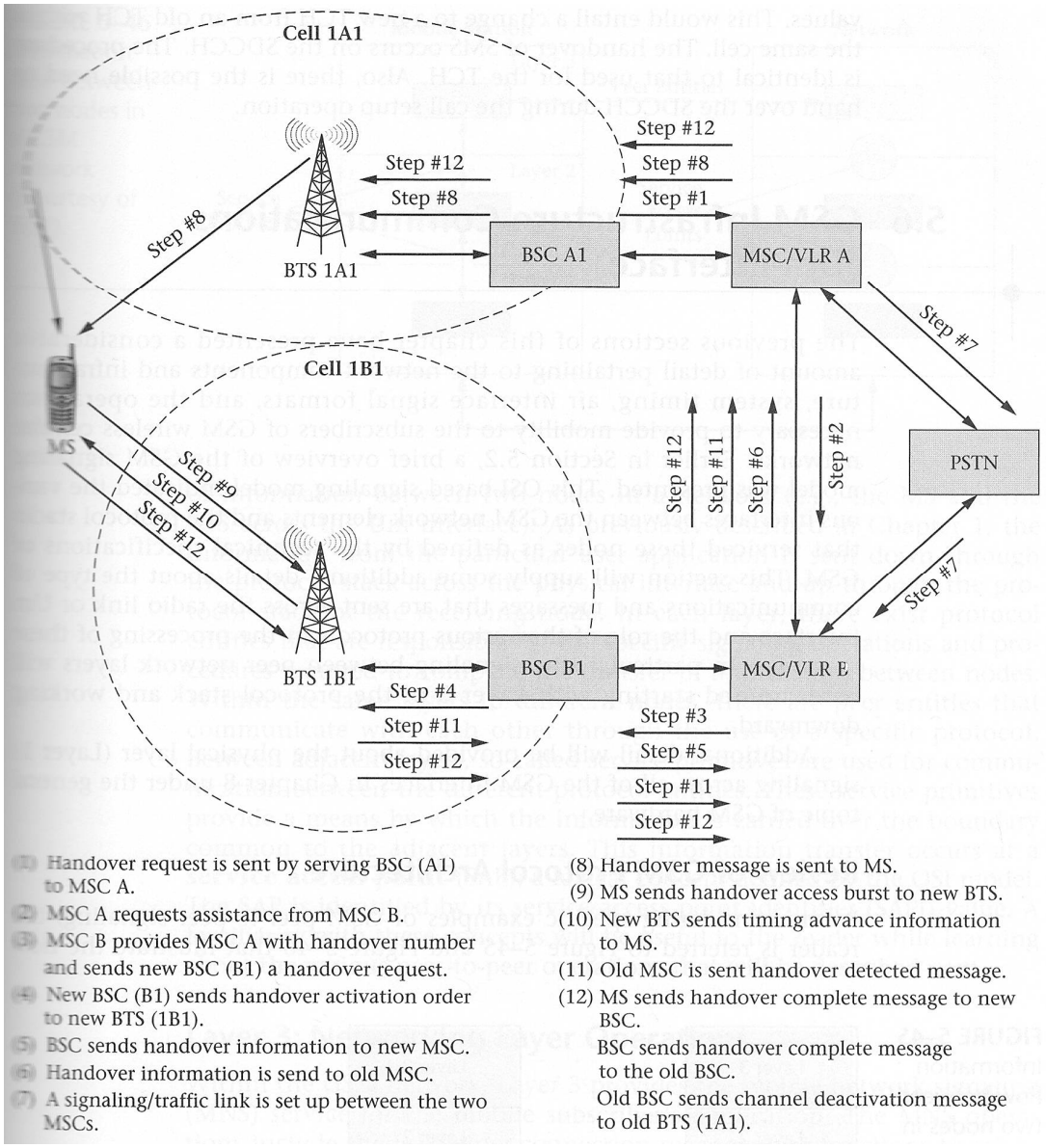
10.2 Inter-BSC Hand-Over



(1) Handover request is sent by serving BSC to MSC.
(2) Handover request is sent by MSC to new BSC (B).
(3) BSC B sends activation order to BTS 1B.
(4) BSC B sends handover information to MSC.
(5) MSC sends handover information to BSC A.
(6) BSC A sends MS new TCH information.
(7) MS sends handover access burst to new BTS (1B).
(8) Timing advance information is sent to the MS.
(9) BTS 1B sends handover detection message to BSC B.
(10) MS sends handover complete message to BSC B.
(11) BSC B sends handover complete message to the old BSC (A).
(12) Old BSC (A) sends channel deactivation message to old BTS (1A).

Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher

10.3 Inter-MSC Hand-Over



Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher