

GSM BASICS

GSM HISTORY:

In 1982 the Nordic PTTs sent a proposal to CEPT (Conference of European Postal & telegraph Administration) to study and to improve digital cellular technology by forming a team called Group Special Mobile.

In 1989 GSM was moved to ETSI (European Telecommunication standards Institute) Organisation and was abbreviated as Global system mobile communication.

There are different types in GSM.

- 1) GSM 900
- 2) DCS 1800
- 3) PCS 1900

GSM 900:

- GSM 900 operates at 900MHz frequency.
- Up link operates on 890MHz to 915MHz Band.
- Down link operates on 935MHz to 960MHz Band.
- Uplink /Downlink separation: 45 MHz.
- GSM takes advantages of both FDMA & TDMA.
- In 25MHz BW, 124 carriers are generated with channel spacing of 200KHz(FDMA)
- Each carrier is divided into 8 time slots (TDMA)
- At any specific time 992 speech channels are made available in GSM 900.

DCS 1800:

- DCS 1800 operates at 1800 Mhz frequency
- Up link operates on 1715MHz to 1785MHz Band.
- Down link operates on 1805MHz to 1880MHz Band.
- Uplink /Downlink separation: 95 MHz.
- Channel spacing : 200khz
- Each carrier is divided into 8 time slots (TDMA)
- No. of carrier : 374

PCS 1900:

- DCS 1900 operates at 1900 MHz frequency
- Up link operates on 1850 MHz to 1910MHz Band.
- Down link operates on 1930MHz to 1990MHz Band.
- Uplink /Downlink separation: 80 MHz.

GSM ADVANTAGES:

- It is a wireless system. So mobile equipment (cell phone) can be on move.
- High secrecy in the system. So information cannot be tapped easily.
- Easy to carry MS. And consumes less power.
- GSM provides more voice channels in limited bandwidth.
- Cellular is based on concept of trunking. This allows large number of channels.

GSM CHANNELS:

1) Physical Channels:

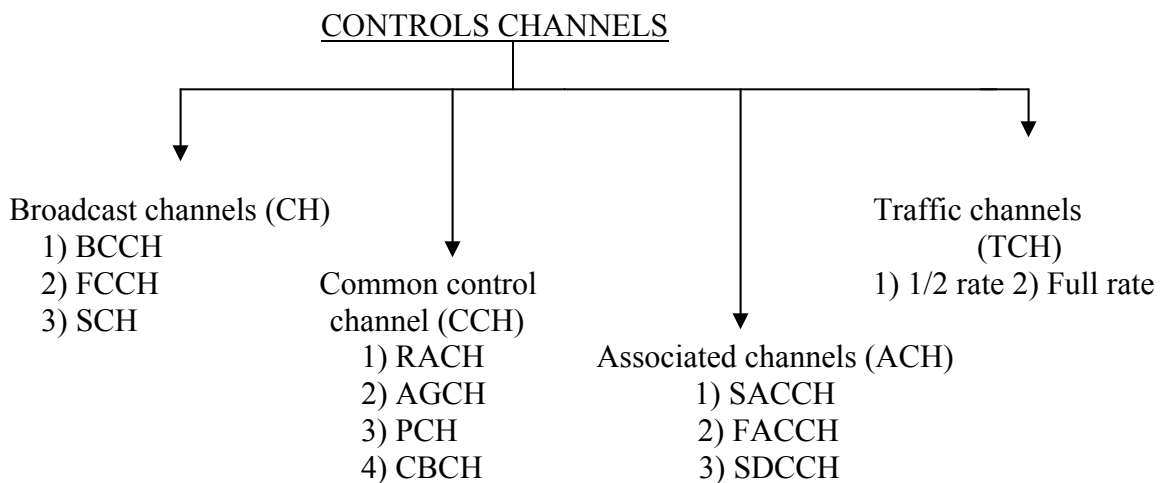
One time slot on one carrier is called physical channel.

2) Logical Channels:

Information carried by physical channels is called logical Channels.

Logical channels are:

FCCH, SCH, BCCH, PCH, RACH, AGCH, SDCCH, SACCH, FACCH, TCH.



CONTROLS CHANNELS

1) Broadcast CHannel (BCH) (downlink only)

- Broadcast Controls Channels (BCCH)
Broadcasts cell specific information to the MS.
- Frequency correction CHannel (FCCH)
Used for frequency correction of MS.
- Synchronization Channel (SCH)
Carrier information about TDMA frame number and the Base Station Identity code (BSIC) of the BTS.

2) Common Controls CHannel (CCH)

- Random Access Channel (RACH)
Is used by the mobile when making its first access to the system. By making that access, the MS is requesting a signalling. The reason for the access could be a page response or initiation. RACH is sent uplink, point to point.
- Access Grant Channel (AGCH)
It is used to assign dedicate resource to MS. It is sent downlink, point to point and grandly access the network.
- Paging Channel (PCH)
Used on the downlink to page the MS.
- Cell Broadcast Channel (CBCH)
It is used to transmit common message to the cell MS

3) ASSOCIATED CONTROLS CHANNELS (ACCH)

- Slow Associated Controls Channel (SACCH)
It is used Measurement reports from the MS to BTS are sent on the uplink. On the downlink the MS receives information from the BTS on what transmitting power to use and also instruction on Timing advance (TA).It is also used for the transmission of short text message in call connected (busy) mode. Controls channel associated with a TCH.
- Fast Associated control Channel (FACCH)
Controls channel associated with a TCH.It is mainly used handover information used on uplink and downlink.
- Standalone Dedicated Controls Channel (SDCCH)
Used for system signaling during call setup or registration, uplink and downlink, as well as the transmission of short message in idle mode.

4) TRAFFIC CHANNELS (TCH)

- Half rate channels
Used for half rate speech at 6.5kbps or data up to 4.8kbps.
- Full rate channels
Used for full rate speech at 13kbps or data up to 9.6kbps.

CHANNEL COMBINATIONS:

The different channels mentioned above are grouped into what are called channel combination.

The four most common type of combination are listed below:

Full rate Traffic channel combination –TCH8/FACCH

Broad channel combination – BCCH + CCCH

Dedicated channel combination – SDCCH8+SACCH8

Combined channel combination –
BCCH + CCCH + SDCCH4 + SACCH4

The channel combination pattern used us:

1. CELLS with single carrier:

Time slot 0 =BCCH+CCH+SDCCH4+SACCH4

Time slot 1-7 = TCH / FACCH + SACCH

2. CELLS with two carrier: for BCCH carrier

Time slot 0 =BCCH+CCCH

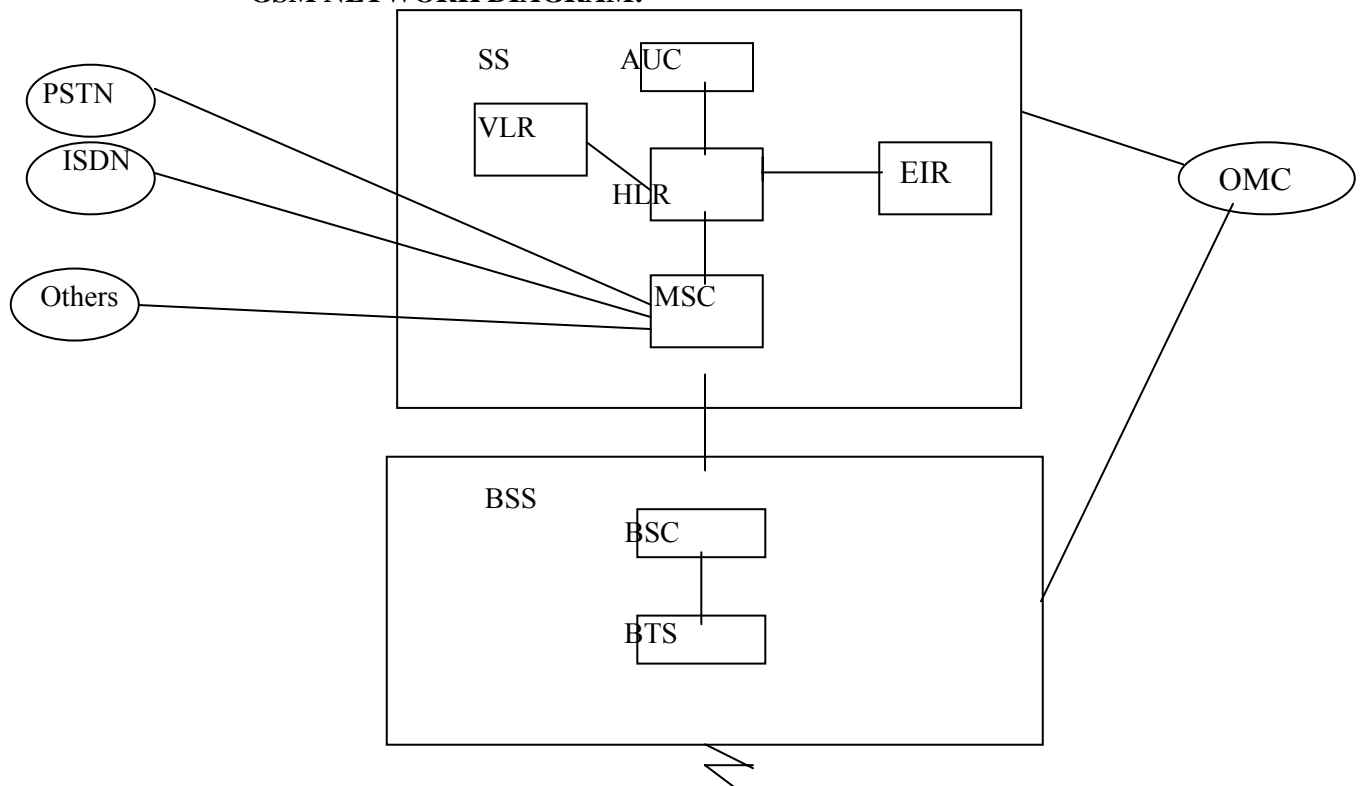
Time slot 1-7 = TCH / FACCH + SACCH

For non-BCCH carrier

time slot 0 = SDCCH8 +SACCH8

Time slots 1-7 = TCH / FACCH + SACCH

GSM NETWORK DIAGRAM:



MS

NETWORK NODES:

- 1) BSS (Base Station System)
- 2) SS (Switching System)
- 3) MS (Mobile Station)

BASE STATION SYSTEM (BSS):

The base station system is divided into the following functional units:

1) BASE TRANSCEIVER STATION (BTS):

The BTS is the radio equipment needed to serve one cell. It contains the antenna system, transmitters, receivers and digital signaling equipment.

2) BASE STATION CONTROLLER (BSC):

The BSC controls and supervises a number of BTSs and radio connection in the system. It handles the administration of cell data, the locating algorithm and orders handovers.

SWITCHING SYSTEM (SS)

The SS contains the following functional units:

1) MOBILE SERVICES SWITCHING CENTER (MSC);

It is mainly performing switching function. The MSC is responsible for setting up, routing and supervising calls to and from the mobile subscriber.

2) VISITOR LOCATION REGISTER (VLR):

The VLR is the temporarily stores information about the MS currently visiting its service area.

3) HOME LOCATION REGISTER (HLR):

The HLR is a database for storing subscriber information specific to that PLMN. Subscriber information includes location information and on services assigned to the subscriber.

4) AUTHENTICATION CENTER (AUC):

AUC generates triplets used in the authentication of SIM card and used in the ciphering of speech, data and signaling over the air interface.

5) EQUIPMENT IDENTITY (EIR):

The EIR is database responsible for the validation of the mobile equipment.

MOBILE STATION (MS):

The MS allows the subscriber to access the network through the radio interface.

The MS consists of:

- **Mobile Equipment (ME):**

The ME consists of radio processing functions and interface to the user and to the terminal equipment.

- **Subscriber Identity Module (SIM):**

The SIM contains information on the user subscription and can be used with any ME.

OPERATION AND MAINTENANCE CENTRE (OMC)

The entity can be used for supervision and control of all the other entities in the network. Even though this part is not obligatory, it is highly needed.

PUBLIC LAND MOBILE NETWORK (PLMN)

A GSM PLMN is the complete GSM NETWORK belongs to one operator in one country. each country can have one or several PLMN.

GATEWAY MOBILE SERVICE SWITCHING CENTRE (GMSC)

A gate between the GSM and other network is necessary. At a call

To a subscriber in the GSM network, the call will first routed to GMSC. The GMSC is responsible for finding out in what part of the GSM network the questioning HLR and also for routing the call there.

SUBSCRIBER IDENTITY MODULE (SIM):

In order for the ME to operate in a GSM network for services other than the emergency services, a valid IMSI stored on it, must present. With the insertion of the SIM card the ME will become a fully functional Mobile Station. Certain subscriber parameter together with personal data used by the subscriber, e.g. frequently called number will be stored on the SIM.

There are three types of subscriber related information that is stored on the SIM.

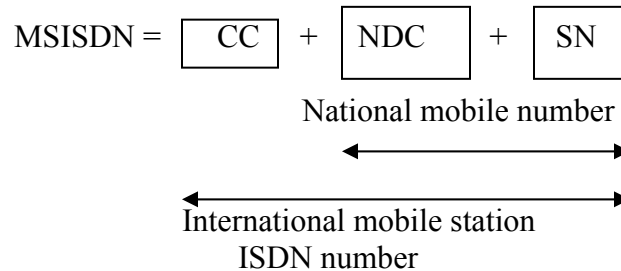
- Subscriber data – IMSI, authentication key (Ki) and access control class.
- Network data - TMSI, LAI, Kc, forbidden PLMNs
- Service related data – language preference, advice of charge.

GSM IDENTITIES

- **Mobile Station ISDN Number (MSISDN)**

The MSISDN is a number, which uniquely identifies a mobile Telephone subscription in the PSTN numbering plan.

In GSM 900/1800, the MSISDN consists of a following:



- **International Mobile subscriber Identity (IMSI)**

The IMSI is a unique identity allocated to each subscriber. It is used for correct identification over the radio path and through GSM PLMN network. All network-related subscriber information is connected to the IMSI. The IMSI is stored in the SIM, in the HLR and VLR.

The IMSI consists of three parts:

$$\text{IMSI} = \text{MCC} + \text{MNC} + \text{MSIN}$$

Where,

MCC=Mobile Country Code

MNC=Mobile Network Code

MISN=Mobile Station Identification Code

- **Temporary Mobile Subscriber Identity (TMSI)**

The TMSI is used to protect the subscriber's privacy on the air interface. The TMSI has only local signification (that is, within the MSC/VLR area) and hence Its structure can be determined by each operator. The TMSI should not consist of more than four octets.

- **International Mobile Equipment Identity (IMEI)**

The IMEI is used for equipment identification and uniquely identifies a MS as a separate piece or assembly of equipment. The IMEI consists of the following:

$$\text{IMEI} = \text{TAC} + \text{FAC} + \text{SNR} + \text{SVN}$$

Where,

TAC = Type Approval Code

FAC = Final Assembly Code

SNR = Serial Number

SVN = Software Version Number

- **Location Area Identity (LAI)**

The LAI is used for paging and it tells MSC in which location area the MS is located.

$$\text{LAI} = \text{MCC} + \text{MNC} + \text{LAC}$$

Where,

MCC = Mobile Country Code

MNC = Mobile Network Code

LAC = Location Area Code

- **Cell Global Identity (CGI):**

This is used for cell identification, within the location area. This is done by adding a cell identity.

$$\text{CGI} = \text{MCC} + \text{MNC} + \text{LAC} + \text{CI}$$

Where

CI = cell Identity (16 Digits Maximum).

SERVICES:

Service provision to a certain subscriber depends on three items;

- The subscription must include this service
- The mobile equipment must be able to handle the service
- The network must be able to offer service

There are different types of basic services available in the GSM system

TELESERVICES

This section describes the major Teleservices supported by all GSM network.

- Speech
- Emergency calls
- Facsimile group 3
- Short message services
- Short message services cell broadcast
- Voice mail fax mail
- Alternative speech/fax

BEARER SERVICES

All GSM network offer a wide range of bearer services. The GSM interworking unit (GIWU) supports all data services offered by the system. Asynchronous and synchronous data transmission rates up to 9.6 kbit/s are supported.

- Traffic to Public Switched Telephony Network (PSTN)
- Traffic to Integrated Services Digital Network (ISDN)
- Traffic to Packet Switched Public Data Networks (PSPDN)
- Traffic to Circuit Switched Public Data Networks (PSPDN)

SUPPLEMENTARY SERVICES

The supplementary services includes,

- Call forwarding
- Barring of outgoing and incoming calls
- Call hold

MOBILE MAXIMUM RANGE

$$\text{Range} = \frac{\text{Timing advance} \times \text{bit period} \times \text{velocity}}{2}$$

Range = Distance between Mobile to MS

Timing advance = Delay of Bits (0-63)

$$\begin{aligned}\text{Bit period} &= 577/156.25 = 3.693 \text{ } \mu\text{secs} \\ &= 3.693 \times 10^{-6}\end{aligned}$$

$$\text{Velocity} = 3 \times 10^5$$

$$\text{RANGE} = \frac{(63) \times (3.693 \times 10^{-6}) \times (3 \times 10^5)}{2}$$

$$\text{RANGE} = 34.9 \text{ Kms.}$$

LOCATION UPDATE

The process of mobile informing the MSC about its current Location area is called as Location update.

There exist three different causes for the MS to start the Location Updating Procedure.

There are,

- 1) Types of normal location update.
- 2) IMSI Attach.
- 3) Periodic Location update.

Types of normal Location update:

- Mobile turns on power
- Reads the new LAI
- If different, does a location update.

IMSI Attach:

- Mobile turns off and sends an IMSI detach to MSC
- Mobile turns on again and compares LAI
- If same, sends an IMSI Attach to MSC.

Periodic Location Update:

- Mobile coverage non-coverage zone
- MSC goes on sending pages
- Mobile has to inform MSC after set period.

HANDOVER

Handover is a processor by which the control/communication of a mobile is transferred from one cell to the another.

Criteria for Handover:

- Receive Quality (RX QUAL) on Uplink or Downlink
- Receive signal strength (RXLEV) on Uplink or Downlink
- Distance (Timing Advance)
- Interference level
- Power budget

Types of Handover:

- 1) Intra – Cell Handover
Handover between Channels / Time slots of same cell.
- 2) Inter – cell Handover
Handover between cells of same BTS.
- 3) Intra – BSC Handover
This type of Handover takes place if the cell to which Handover is to done belongs to the same BSC.
- 4) Inter – BSC Handover
This type of Handover, the mobile is handed over to a cell which belongs to another BSC.
- 5) Inter – MSC Handover
If the cell belongs to another MSC, then is Inter –MSC Handover.

LOSSES

Path Losses:

These losses occurred due to the transmission in air depends on Distance.

$$\text{Path losses} = 20 \log (4\pi d / \lambda)$$

Where,

$$\text{Frequency (f)} = 1/\lambda, \quad d = \text{Distance between MS and BTS.}$$

Shadowing losses:

These losses occurred due to the physical obstacles. (like one building)
It is also called as Long Term Fading.

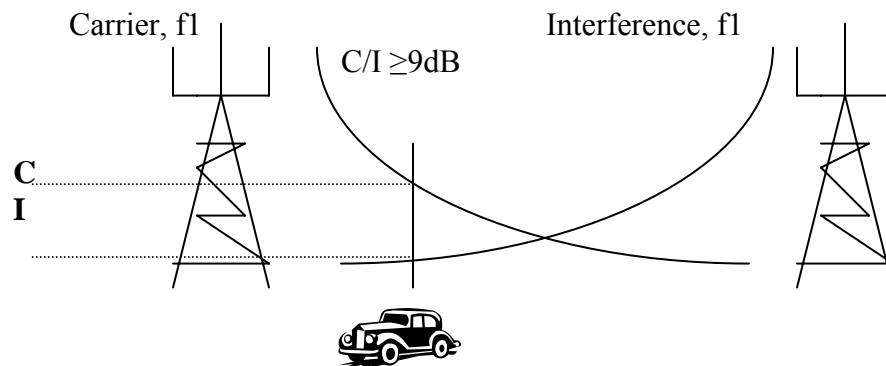
Multi-path (or) Rayleigh fading:

These losses occurred due to interference of direct and reflected the signals.

Carrier to Interference (C/I):

It is also called as Co-Channel interference. It is the relation between the desired signal C and the undesired re-used signal I, both using the same carrier frequency.

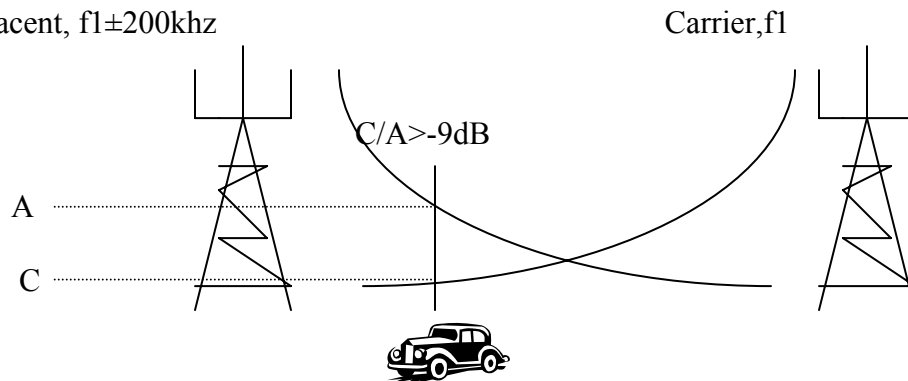
Carrier to Interference (C/I) $\geq 9\text{dB}$



Carrier to Adjacent (C/A):

The relation between the desired signals A from the correct carrier and the undesired signal A from the carrier 200khz away is called adjacent channel interference or C/A.

Adjacent, $f1 \pm 200\text{khz}$

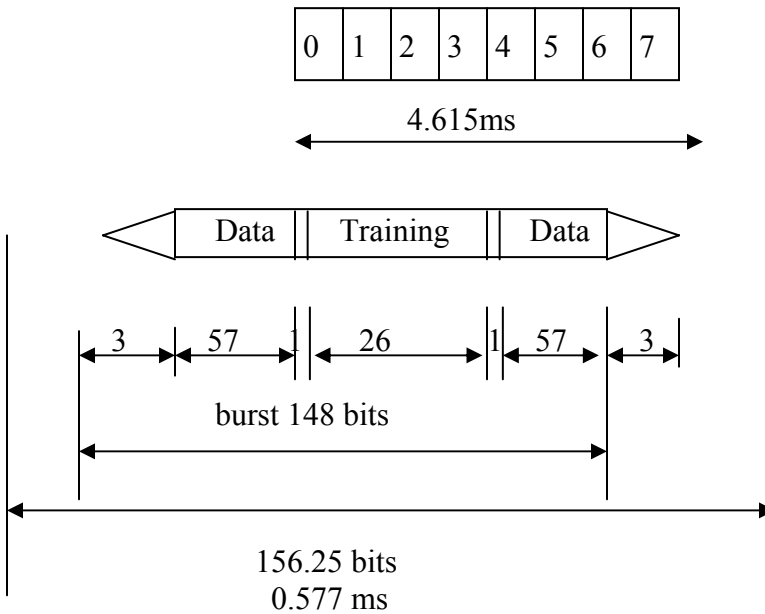


Carrier to interference (C/I) $\geq -9\text{dB}$

BURST AND FRAMES :

A Burst is a formatted sequence of bits during one-time slots.

Due to TDMA structure with time slots, we do not send continuously but only in the designated time slots. The information sent during one time slot is formatted into a Burst.



Types of Burst:

1) Normal Burst (NB):

It is used to carry information on traffic and control channels.

The normal burst contains;

- 2 information fields, each with 57 bits, used for encrypted speech or data
- One training sequence to be used by the equalizer in the receiver
- 2 bits to indicate whether the burst is “stolen” to be used as a FACCH
- 3 bits in each end to serve as start and stop bits.

TB 3	Encrypted 57	1	Training sequence 26	1	Encrypted bits 57	TB 3	GP 8.25
---------	-----------------	---	-------------------------	---	----------------------	---------	------------

2) Access Burst (AB):

It is for random access and handover access.

The Access burst is as short as possible, to allow a certain delay without interfering with the next time slots.

TB 8	INFORMATION	Guard period 68.25
---------	-------------	-----------------------

3) Synchronization Burst (SB):

It is used for frame synchronization of the mobile. To know the when certain information is broadcasted.

4) Frequency Burst (FB):

It is used for frequency synchronization of the mobile.

5) Dummy Burst (DB):

It is used when on other type of burst is to be sent.

THE RELATIONSHIP BETWEEN BURST AND FRAMES

There are two types of multiframes

- **26 TDMA frame multiframes** are used to carry TCH, SACCH and FACCH.
- **51 TDMA frame multiframes** are used to carry BCCH, CCCH, SDCCH and SACCH.

The superframe consists of 26 or 51 multiframes and hyperframe consists of 2048 superframes.

Authentication:

Security function for authenticating the SIM which is mandatory for any MS is based on the crypto graphical algorithm A3, and the secret subscriber authentication key Ki. Both A3 and Ki are located on the SIM.

Authentication procedure

The authentication procedure is initiated from the MSC/VLR by sending RAND to the MS. the MSC/VLR has fetched the triplets from the HLR. Now the MS calculates the SRES and Kc using the same algorithms as the AUC. The calculated SRES will be sent to MSC/VLR which compares this SRES received from the MS with the one in the triplet from the AUC. if the two are same access will be granted . The calculated Kc will be stored in the SIM card.

Ciphering

The security function that ciphers the information sent and received by the MS required the cipher key Kc. The generation of the Kc is based on the crypto graphical algorithms A8, and the Ki. Also A8 is located on the SIM.

Ciphering start procedure

This ciphering start procedure is initiated from the MSC/VLR by sending the message a cipher mode command the Kc. The Kc will be removed from the message by the BTS before sending it on to the MS, so that the Kc will be never be sent on the air. When the MS receives this message it will be send the message cipher mode complete in the cipher mode using the calculated Kc stored on the SIM card. If the BTS can decipher this message it will be inform the MSC/VLR that ciphering has started.

DIVERSITY:

Diversity is actual used for to avoid the fading dip of receiving antenna. If the receiving antenna is located in a fading dip, there are only two ways of getting away from the dip,

- The receiving antennas are move away from the dip.
- The fading dip must be moved away from the antenna.

Types of diversity

1. Space diversity
2. Frequency diversity

Space diversity:

By using two receiving antennae at the base station, chances are that neither of them will be in a fading at the same time. A certain distances between the antennae are necessary, and 4-6 meters is recommended for GSM.

There are different methods of combining the two received signals.

- Either the system can alternate between the two antennae
- Always using the antennae with the highest signal strength
- Both receiving antennae can used all time

Frequency diversity:

Another effective way to multi-path fading is to change the frequency, thus changing the positions of dips. When frequency hopping is applied in GSM, each consecutive burst will be transmitted at a different frequency. The frequencies used are changed either according to a cyclic pattern or a pseudo-random pattern.

CHANNEL CODING:

The Different methods of channel coding used in GSM are,

- Block coding
- Convolutional coding

Block coding:

When the block coding is used, one or several check bits are added to the information block. The check bits only depend on the bits in that every block. A simple form of block coding is using parity coding. Block coding is mainly used for detecting errors.

Convolutional coding:

The Convolutional coder consists of a shift register into which the information bits are shifted one by one. Convolutional coding is not only good for detecting errors, but also for correcting them.

INTERLEAVING:

Interleaving is a method spreading the potential losses, so that they can be taken care of by “channel coding” thus minimizing the harm burst.

In GSM the channel coder produces a total of 456 bits for every 20 ms segment of speech. These are in blocks of 57 bits interleaved over the burst.

EQUALISER:

The equalizer will mainly address the problems of Inter Symbol interference, desired earlier. The problem is that the air interface affects the signals in some way that causes bit error in the receiving side.

In a normal burst, used for traffic, there is a 26 bits training sequence in the middle of the burst.

TB	Encrypted	1	Training sequence	1	Encrypted bits	TB	GP
3	57		26		57	3	8.25

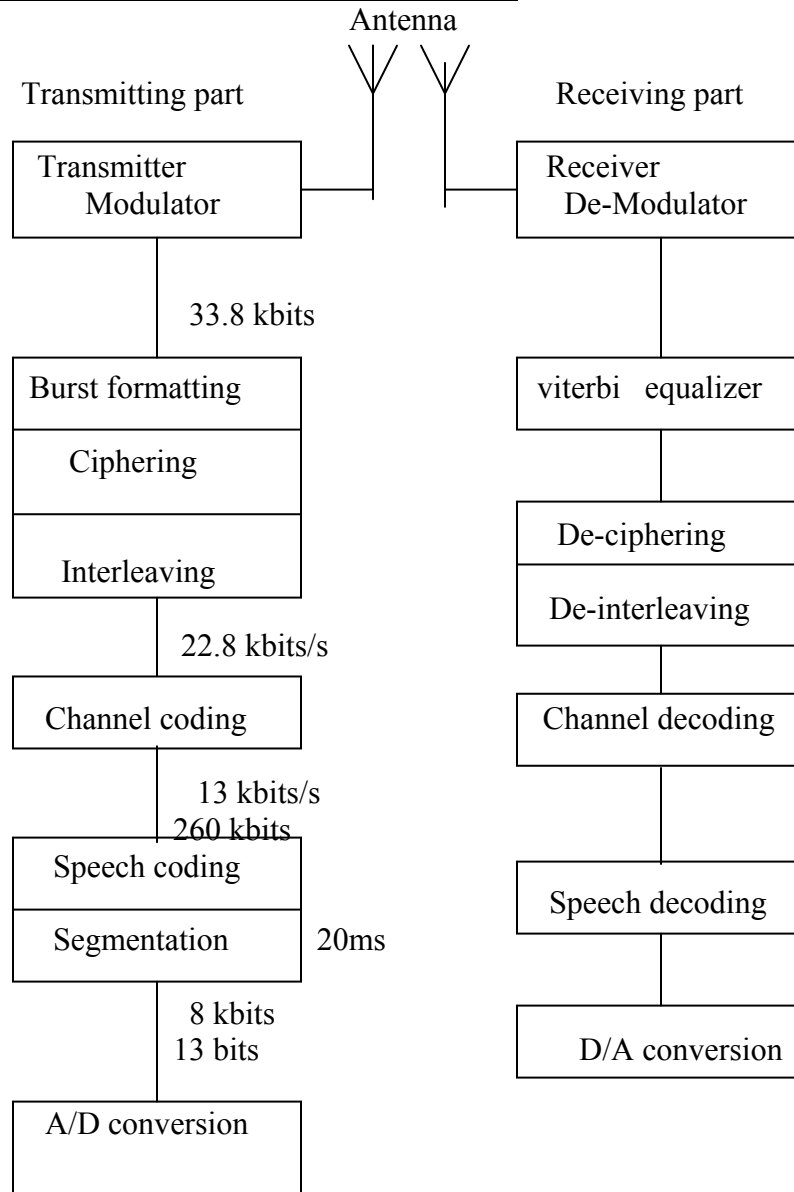
TIMING ADVANCE:

The radio signals take finite period of time to travel from the mobile station to the base station. it is called propagation delay.

The system will repeatedly send “timing advance” orders to the MS. The system will simply tell the MS how many bit times earlier, or later, to send. These decisions are based on an analysis of how the bursts are received in the base station.

- BSS calculates access delay from RACH in terms of bits.
- Informs mobile to delay its in terms of bits
- Maximum Timing advance of 63 bits.

SIGNAL PATH THROUGH THE NETWORK



AREAS:

1) PLMN SERVICE AREA

The Public Land Mobile network (PLMN) is a geographical area served by one network operator and is defined as the area in which an operator offers radio coverage and possibility to access its network.

2) MSC/VLR (SERVICE AREA)

If the system has more than one MSC, the PLMN is subdivided into several MSC/VLR service areas. To be able to route calls to the right MSC and eventually to the right MS, it is necessary to know in which MSC/VLR service area the MS is.

The HLR stores the data about which MSC/VLR service area the MS is in. The VLR contains detailed information about all the MS:s in the MSC/VLR service area.

3) LOCATION AREA

Location area is an identity, which specifies a group of cells as defined by the technicians is called as location area.

Each MSC/VLR service area is subdivided into a number of location area (LA). Information about, in which location area an MS is registered, is also stored in the VLR together with subscriber data of all the visiting subscribers in that MSC/VLR service area.

If an MS move within the location area, the system does not need to change the information in the subscriber register i.e. VLR and HLR. If the MS crosses over into a cell belonging to a new location area however, the system must be informed. This report done by the MS to the system is called "location updating".

One LA may include cells from different BSC: s, and cells belonging to one BSC may be subdivided into several LA: s.

CLUSTER

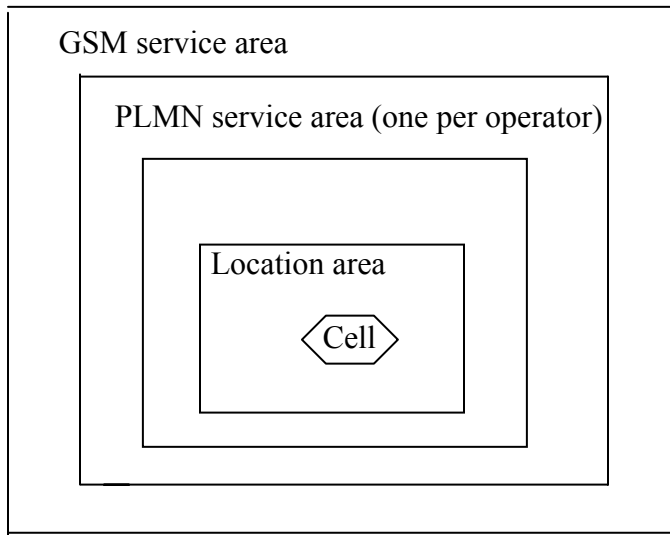
A group of neighboring cells using all the frequencies available in the system frequency band is called a cluster of cells.

4) CELLS

Location area subdivided into a number of cells. A cell is the geographical area covered by one Base Transceiver Station. A cell is the smallest geographical entity in a PLMN. A cell could be any size, from a radius of tens of kilometers down to a radius of tens or hundreds of meters.

GSM SERVICE AREA

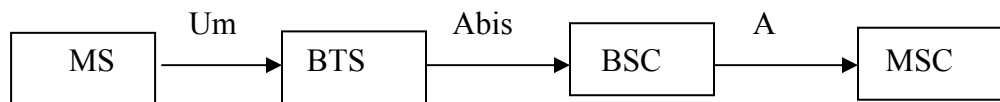
The GSM service area is the total geographical area in which subscriber can access the network. The more operators who sign contracts agreeing to work together, the more this area will increase.



INTERFACES:

There are different types interfaces

- Air Interface (or) Um Interfaces]
Interface between the MS and BTS
- Abis Interface
Interface between the BTS and BSC
- A Interface
Interface between the BSC and MSC

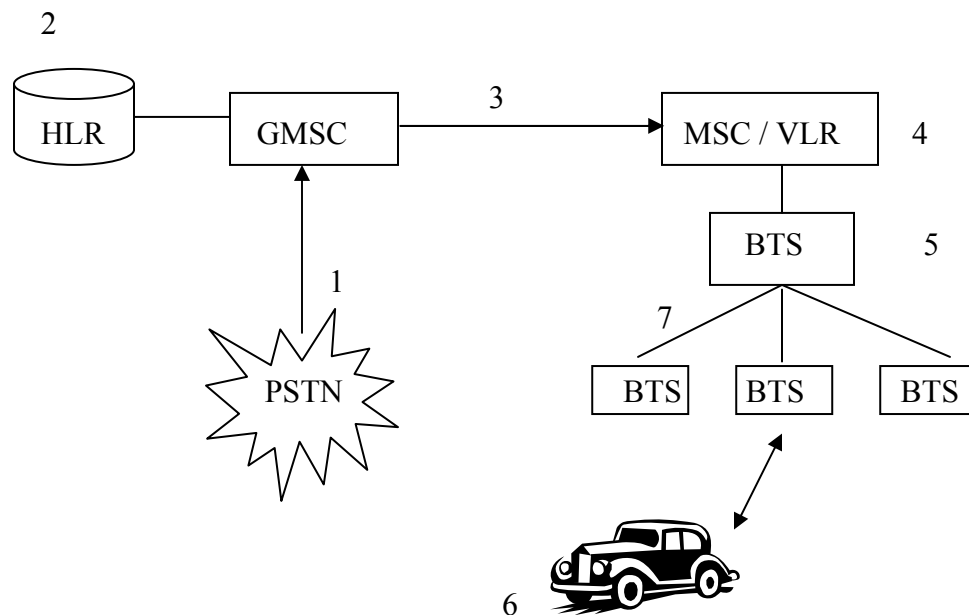


TRAFFIC CASES

CALL TO A MOBILE STATION

The difference between making a call to a mobile subscriber and a PSTN network subscriber is that the mobile subscriber's location is unknown. Therefore, the mobile station must be paged before a connection can be made. The steps in the call setup procedure from a PSTN subscriber to a mobile station are listed below. The numbers refer to figure

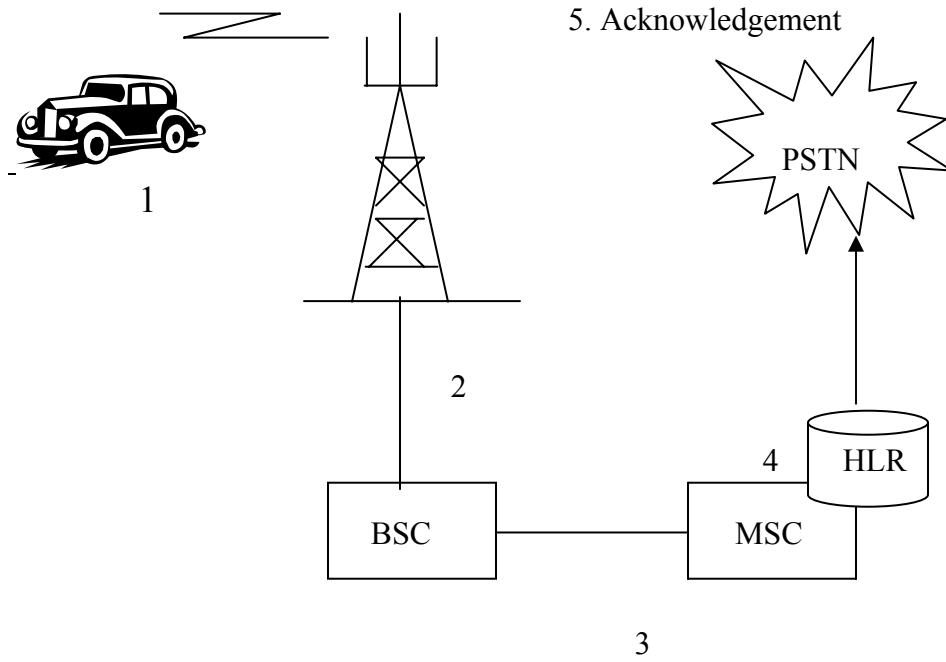
1. The PSTN subscriber dials the mobile subscriber's number. the Gateway MSC receives the call.
2. The Gateway MSC requires the HLR for the information needed to route the call to the serving MSC/VLR.
3. The GMSC routes the call to the MSC.
4. MSC checks VLR for the Location Area of the mobile station.
5. MSC contacts the mobile station via BSC and BTS by sending a page request.
6. The mobile station responds.
7. BSC selects a traffic channel and orders the mobile station to tune to this traffic channel. The mobile station generates a ringing signal and when the subscriber answers the speech-connection is established.



CALL FROM A MOBILE STATION

When a mobile station wishes to establish a speech call, the following steps are performed: the numbers refer to figure.

1. Mobile subscriber dials the number.
2. MSC /VLR receives a message requesting access.
3. MSC /VLR checks if the mobile station is authorized to initiates a call set up to the PSTN network.
4. the dialed number is analyzed by MSC /VLR , which in turn initiates a call set-up to the PSTN network.
5. MSC / VLR asks bsc to allocate a free traffic channel. This information is forwarded to BTS and the mobile station.
6. the person receiving the call answer and a connection is established.



BASE STATION SYSTEM