AN OVERVIEW OF THE GSM SYSTEM

Kousik Dasgupta
Lecturer, Dept. of C.S.E

The Global System for Mobile communications (GSM) is a digital cellular communications system. GSM was developed to provide a common second generation technology for Europe, so that the same subscriber units can be used throughout the country. It was designed for a digital (wide area) wireless network and made compatible with ISDN services.

1. History:

The idea of cell-based mobile radio systems appeared at Bell Laboratories (in USA) in the early 1970s. However, mobile cellular systems were not introduced for commercial use until the 1980s. But in the beginning, each country developed its own system, making it undesirable because the equipment was limited to operate only within the boundaries of each country and making its market limited.

To overcome this, the Conference of European Posts and Telecommunications (CEPT) formed, in 1982, the Groupe Spécial Mobile (GSM) in order to study and develop a pan-European mobile cellular radio system (the GSM acronym became later the acronym for Global System for Mobile communications). The criteria were to develop a standard to be common for the countries that created it. The standardized system had to meet certain criteria:

- Good subjective speech quality.
- Low terminal and base station cost.
- Support for international roaming – one system for all of Europe.
- Ability to support handheld terminals.
- Support for range of new services and facilities.
- Enhanced Features
- ISDN compatibility
- Enhance privacy
- Security against fraud

2. GSM System Architecture :

The GSM technical specifications define the different entities that form the GSM network. The GSM network can be divided into four main parts:

- The Mobile Station (MS).
- The Base Station Subsystem (BSS).
- The Network and Switching Subsystem (NSS).
- The Operation and Support Subsystem OSS).

The architecture of the GSM network is presented in figure 1.

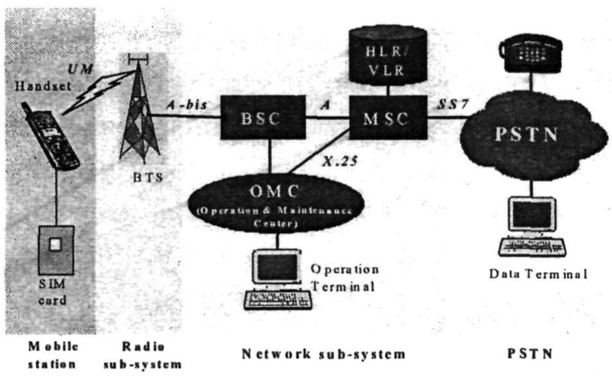

Figure 1 : GSM Architecture

2.1 Mobile Station (MS):

MS is used by the subscriber to access the GSM network via the air interface. It contains the hardware and software specific to the radio interface. Allows separation of user mobility from equipment mobility

The Mobile Station is made of two entities :

- Mobile Equipment (ME) or Mobile Terminal (MT).
- Subscriber Identity Module (SIM).

2.1.1 Terminal :

This is produced by many different manufacturers. Each of them must obtain approval from the standardization body. Each terminal is uniquely identified by an IMEI (International Mobile Equipment Identity).

2.1.2 SIM :

This is a removable plastic smart card. By inserting the SIM card into the terminal, the user can have access to all the subscribed services., without the SIM card, the terminal is not operational.

The SIM card is protected by a four-digit Personal Identification Number (PIN). In order to identify the subscriber to the system, the SIM card contains some parameters for the user such as its International Mobile Subscriber Identity (IMSI), short messages, billing information, telephone directory etc. Another advantage of the SIM card is it provides mobility to the users.

2.2 The Base Station Subsystem (BSS) :

The BSS connects the MS and the NSS through standardized Abis interface. It is in charge of the transmission and reception. The BSS can be divided into two parts:

- The Base Transceiver Station (BTS).
- The Base Station Controller (BSC).

2.2.1 The Base Transceiver Station (BTS):

The BTS corresponds to the transceivers and antennas used in each cell of the network. A BTS is present one per cell and usually placed in the center of a cell. Its transmitting power defines the size of a cell. Each BTS has between one and sixteen transceivers depending on the density of users in the cell. BTS separates the speech and control signaling associated with a MH and sends them to the BSC on separate channels. It performs channel coding/decoding and encryption/decryption.

2.2.2 The Base Station Controller (BSC) :

The BSC controls a group of BTS and manages their radio resource management. A BSC is principally in charge of call set up, handovers, frequency hopping etc.

2.3 The Network and Switching Subsystem :

Its main role is to manage the communications between the mobile users and other users (such as mobile users, ISDN users, fixed telephony users, etc.). It also includes data bases needed in order to store information about the subscribers and to manage their mobility.

2.3.1 The Mobile services Switching Center (MSC) :

It is the central component of the NSS. The MSC performs the switching functions and connections of the network. The function of NSS are connecting call form sender to receiver, keeping call details, supervises operation of the network, handover and mobility.

2.3.2 The Gateway Mobile services Switching Center (GMSC):

A gateway is a node interconnecting two

networks. The GMSC is the interface between the mobile cellular network and the Public Switching Telephone Network (PSTN). It is in charge of routing calls from the fixed network towards a GSM user.

2.3.3 Home Location Register (HLR):

The HLR is important database that stores information of the subscribers belonging to the covering area of a MSC. It also stores the current location of these subscribers and the services to which they have access.

2.3.4 Visitor Location Register (VLR):

The VLR contains information from a subscriber's HLR necessary in order to provide the subscribed services to visiting users. When a subscriber enters the covering area of a new MSC, the VLR associated to this MSC will request information about the new subscriber to its corresponding HLR. The VLR will then have enough information in order to assure the subscribed services without needing to ask the HLR each time a communication is established.

2.3.5 The Authentication Center (AuC):

The AuC is a protected database used for security purposes. It provides the parameters needed for authentication and encryption. These parameters help to verify the user's identity.

2.3.6 The Equipment Identity Register (EIR):

The EIR database is used for security purposes. It contains information about the mobile equipments. More particularly, it contains a list of all valid terminals. A terminal is identified by its International Mobile Equipment Identity (IMEI). The EIR can block calls to a particular MH not a subscriber.

2.4 The Operation and Support Subsystem (OSS):

The OSS is connected to the different components of the NSS and BSC, in order to control and monitor the GSM system. It is also in charge of controlling the traffic load of the BSS. It is also responsible for providing GSM network add-on services.

3. The geographical areas of the GSM network:

The figure 2 presents the different areas that form a GSM network.

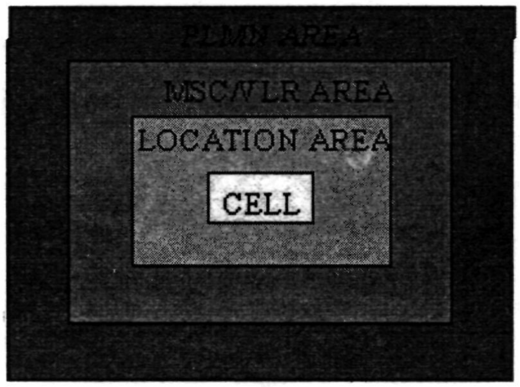

figure 2: GSM network areas

At innermost is a cell, identified by its Cell Global Identity number (CGI), corresponds to the radio coverage of a base transceiver station. A Location Area (LA), identified by its Location Area Identity (LAI) number, is a group of cells served by a single MSC/VLR. This number is based on international ISDN numbering plan Country Code (CC) of 3 decimal digits,

Mobile Network Code (MNC) of 2 decimal digits, Location Area Code (LAC) of maximum 5 decimal digits. A group of location areas under the control of the same MSC/VLR defines the MSC/VLR area. A Public Land Mobile Network (PLMN) is the area served by one network operator.

4. Features Provided by GSM:

4.1 Basic Features :

- ***Call Waiting :*** Notification of an incoming call while on the handset.
- ***Call Hold :*** Put a caller on hold to take another call.
- ***Call Barring :*** All calls (outgoing calls, or incoming calls) stopped.
- ***Call Forwarding :*** Calls can be sent to various numbers defined by the user
- ***Multi Party Call Conferencing :*** Link multiple calls together

4.2 Advanced Features :

- ***Calling Line ID (CLI) :*** Incoming telephone number displayed.
- ***Alternate Line Service :*** One line for personal calls and other for business calls.
- ***Closed User Group :*** Call by dialing last four numbers.
- ***Roaming :*** Services and features that can follow customer from one area to another.
- ***Advice of Charge :*** Provides the user with online charge information.

5. The GSM radio interface:

The radio interface is the interface between the mobile stations and the fixed infrastructure. One of the main objectives of GSM is roaming. Therefore, in order to obtain a complete compatibility between mobile stations and networks of different manufacturers and operators, the defining radio interface becomes important.

5.1 Frequency allocation :

Two frequency bands, of 25 MHz, have been allocated for the GSM system:

- The band 890-915 MHz has been allocated for the uplink direction (transmitting from the mobile station to the base station).
- The band 935-960 MHz has been allocated for the downlink direction (transmitting from the base station to the mobile station).

But all countries can not use the whole GSM frequency bands principally due to military reasons and the existence of previous analog systems using part of the two 25 MHz frequency bands.

5.2 Multiple access schemes:

The multiple access scheme defines how simultaneous communications, between different mobile stations situated in different cells, share the GSM radio spectrum. A mix of Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA), combined with frequency hopping is used for this.

5.2.1 FDMA and TDMA:

Using FDMA, a frequency is assigned to a user. So larger the number of users, the larger is the requirement for the number of available frequencies. The limited available radio spectrum and the fact that a user will not free its assigned frequency until he does not need it anymore, explain disadvantage of using FDMA.

Using TDMA, several users can share the same channel. Each of the users, sharing the common channel, are assigned their own burst within a group of bursts called a frame. Usually TDMA is used with a FDMA structure.

In GSM, a 25 MHz frequency band is divided, using a FDMA scheme (as in figure 3), into 124 carrier frequencies spaced one from each other by a 200 kHz frequency band. Normally a 25 MHz frequency band can provide 125 carrier frequencies but the first carrier frequency is used as a guard band between GSM and other services working on lower frequencies.

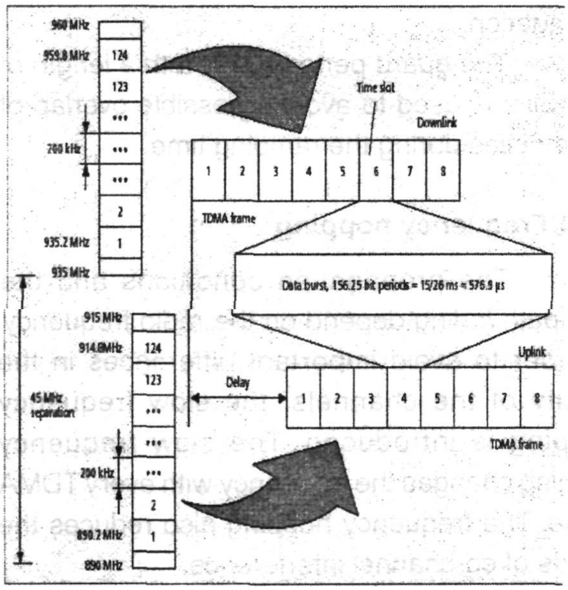

figure 4. GSM frequency band

Each carrier frequency is then divided in time using a TDMA scheme. This scheme splits the radio channel, with a width of 200 khz, into 8 bursts. A burst is the unit of time in a TDMA system, and it lasts approximately 0.577 ms. A TDMA frame is formed with 8 bursts and lasts, consequently, 4.615 ms. Each of the eight bursts, that form a TDMA frame, are then assigned to a single user.

5.2.2 Channel :

A channel corresponds to the recurrence of one burst every frame. It is defined by its frequency and the position of its corresponding burst within a TDMA frame. In GSM there are two types of channels (as in figure 5):

- The traffic channels used to transport speech and data information.
- The control channels used for network management messages and some channel maintenance tasks.

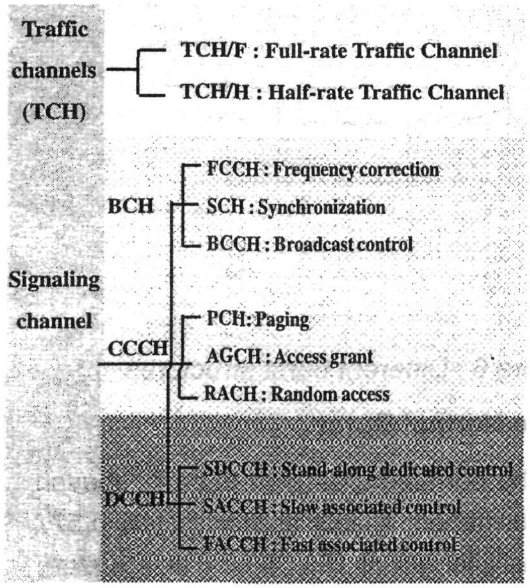

figure 5 Channels in GSM

5.2.3 Burst structure :

The burst is the unit in time of a TDMA system. Four different types of bursts can be are there in GSM:

- The frequency-correction burst is used on the FCCH. It has the same length as the normal burst but a different structure.
- The synchronization burst is used on the SCH. It has the same length as the normal burst but a different structure.
- The random access burst is used on the RACH and is shorter than the normal burst.
- The normal burst is used to carry speech or data information.

The different burst structure is as in figure 6.

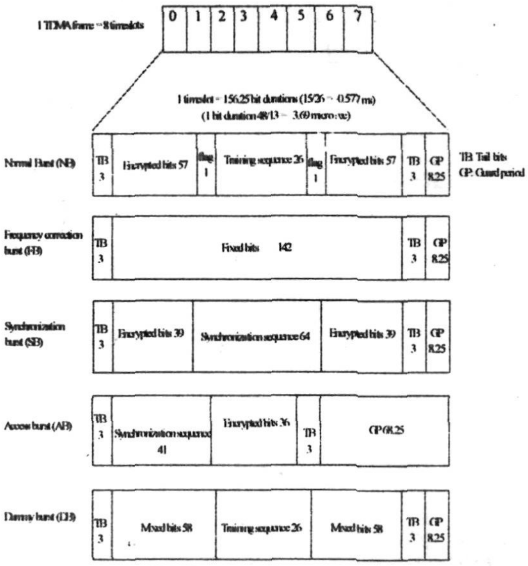

figure 6 : Different burst structures

5.2.3.1 The Normal Burst :

The normal burst used to carry speech or data information. It lasts approximately 0.577 ms and has a length of 156.25 bits. Its structure is presented in figure 7.

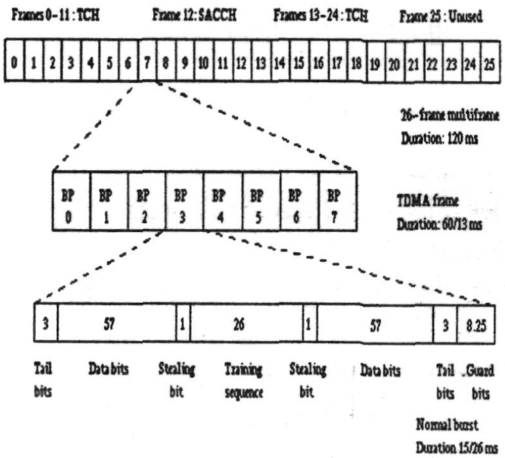

figure 7: Normal burst structure

The tail bits (T) are a group of three bits set to zero and placed at the beginning and the end of a burst. They are used to cover the periods of ramping up and down of the mobile's power.

The coded data bits correspond to two groups, of 57 bits each, containing signaling or user data. The stealing flags (S) indicate, to the receiver, whether the information carried by a burst corresponds to traffic or signaling data.

The training sequence has a length of 26 bits. It is used to synchronize the receiver with the incoming information, avoiding then the negative effects produced by a multipath propagation.

The guard period (GP), with a length of 8.25 bits, is used to avoid a possible overlap of two mobiles during the ramping time.

5.2.4 Frequency hopping :

The propagation conditions and the multipath fading depend on the radio frequency. In order to avoid important differences in the quality of the channels, the slow frequency hopping is introduced. The slow frequency hopping changes the frequency with every TDMA frame. The frequency hopping also reduces the effects of co-channel interference.

There are different types of frequency hopping algorithms. The algorithm selected is sent through the Broadcast Control Channels.

Even if frequency hopping can be very useful for the system, a base station does not have to support it necessarily On the other hand, a mobile station has to accept frequency hopping when a base station decides to use it.

6. GSM Layers :

GSM constitutes of three layers:

Layer 1: Physical layer

Responsible to provide physical transmission and channel quality measurements.

Layer 2: Data link layer

Responsible for providing Error detection (based on HDLC), Flow control, Transmission, quality assurance and Routing.

Layer 3: Network layer

Responsible for connection management

(air interface), Management of location data, Subscriber identification and Management of added services (SMS, call forwarding, conference calls, etc.).

Network layer consists of 3 sublayers

- Radio resource management (RR) : Establishment, maintenance and termination of radio channel connections
- Mobility management (MM): Registration, authentication and location tracking
- Call control (CC): Establishment, maintenance and termination of circuit-switched calls.

7. Incoming Call setup :

7.1 To MS which is known:

- Target MSC initiates a paging message.
- BSs forward the paging message on downlink channel in coverage area.
- If mobile is on (monitoring the signaling channel), it responds to BS.
- BS sends a channel allocation message and informs MSC.

7.2 To MS which is unknown :

1. Incoming call is passed from the fixed network to the gateway MSC (GMSC) as in figure 8.
2. Based on the IMSI numbers of the called party, HLR is determined.
3. HLR checks for the existence of the called number, then the relevant VLR is requested to provide a mobile station roaming number (MSRN).
4. Reply transmitted back to the GMSC.
5. Connection is switched through to the responsible MSC.
6. VLR is queried for the location range and reach ability status of the mobile subscriber.
7. If the MS is marked reachable, then a radio call is enabled.
8. Radio call is executed in all radio zones assigned to the VLR.
9. Reply from the MS in its current radio cell.
10. When mobile subscriber telephone responds to the page, then complete all necessary security procedures.
11. If this is successful, the VLR indicates to the MSC that call can be completed.
12. Call setup completed.

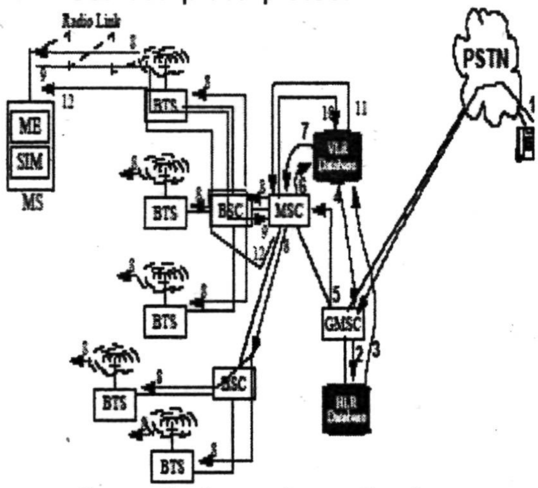

figure 8 : Incoming call setup

8. Outgoing Call setup :

- User keys in the number and presses send.
- Mobile transmits request on uplink signaling channel.
- If network can process the call, BS sends a channel allocation message.
- Network proceeds to setup the connection.

Network activity :

- Network completes the two halves of the connection.
- MSC determines current location of target mobile using HLR, VLR and by

communicating with other MSCs

- Source MSC initiates a call setup message to MSC covering target area

9. Call Routing :

The call routing is given as in figure 9.

1. A user dials the Mobile Subscriber ISDN (MISDN) to GMSC.
2. The GMSC asks the HLR for the information helping to route the call.
3. The HLR gives a Mobile Station Roaming Number (MSRN) for the call to the MSC.
4. The MSC sends this MSRN number to VLR which gives TMSI (Temporary Mobile Subscriber Identity) number.
5. With this TMSI the MSC routes the call to BSC.
6. The BSC pages this to BTs under it.
7. The Mobile with the TMSI responds.

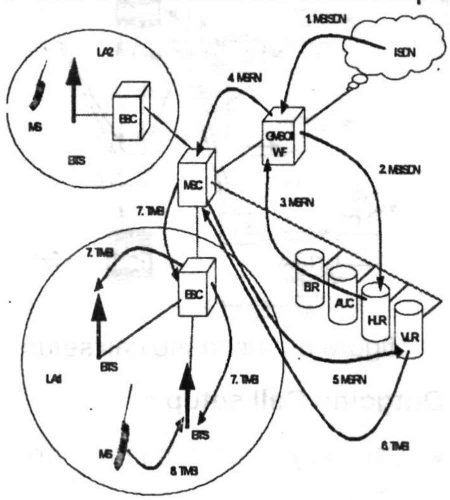

figure 9 : Call Routing

10. Handover :

The user movement often produces the need to change the channel or cell, especially when the quality of the communication is decreasing. This procedure of changing the resources is called handover. Four types of handovers are there :

- Handover of channels in the same cell.
- Handover of cells controlled by the same BSC.
- Handover of cells belonging to the same MSC but controlled by different BSCs.
- Handover of cells controlled by different MSCs.

Handovers are mainly controlled by the MSC. However in order to avoid unnecessary signaling information, the first two types of handovers are managed by the concerned BSC (the MSC is only notified of the handover).

The mobile station is the active participant in this procedure. In order to perform the handover, the mobile station controls *continuously its own signal strength and the signal* strength of the neighboring cells. The list of cells that must be monitored by the mobile station is given by the base station. The power measurements allow deciding the best cell is in order to maintain the quality of the communication link. Two basic algorithms are used for the handover:

- **The 'minimum acceptable performance' algorithm.** When the quality of the transmission decreases (the signal is deteriorated), the power level of the mobile is increased. This is done until the increase of the power level has no effect on the quality of the signal. When this happens, a handover is performed.
- **The 'power budget' algorithm.** This algorithm performs a handover, instead of continuously increasing the power level, in order to obtain a good communication quality.

11. Reference :

[1] Schiller, J. Mobile Communication 2nd Edition., Pearson.

[2] Yi-Bing Lin and Imrich Chalmatac Wireless and Mobile Networks Architecture, John Wiley & Sons .

[3] Pandya Raj,. Mobile and Personal Communication systems and services, Prentice-Hall of India.