Notes

5 Wireless Systems

Syllabus

GSM system architecture, Radio interface, Protocols, Localization and calling, Handover, Authentication and security in GSM, GSM speech coding, Concept of spread spectrum, Architecture of IS-95 CDMA system, Air interface, CDMA forward channels, CDMA reverse channels, Soft handoff, CDMA features, Power control in CDMA, Performance of CDMA System, RAKE Receiver, CDMA2000 cellular technology, GPRS system architecture.

Contents

5.1 Global System for Mobile Communication (GSM) GTU : Summer-15

- GSM technique is most widely used for digital cellular radio. A GSM system has maximum 200 full duplex channel per cell. Each channel has different uplink and downlink frequency. GSM handles channel access using a combination of slotted ALOHA, FDM and TDM.
- The Global System for Mobile (GSM) communications is a feature rich, digital wireless technology. GSM provides subscribers with high-quality digital wireless phone service and clarity, as well as enhanced call security and privacy.

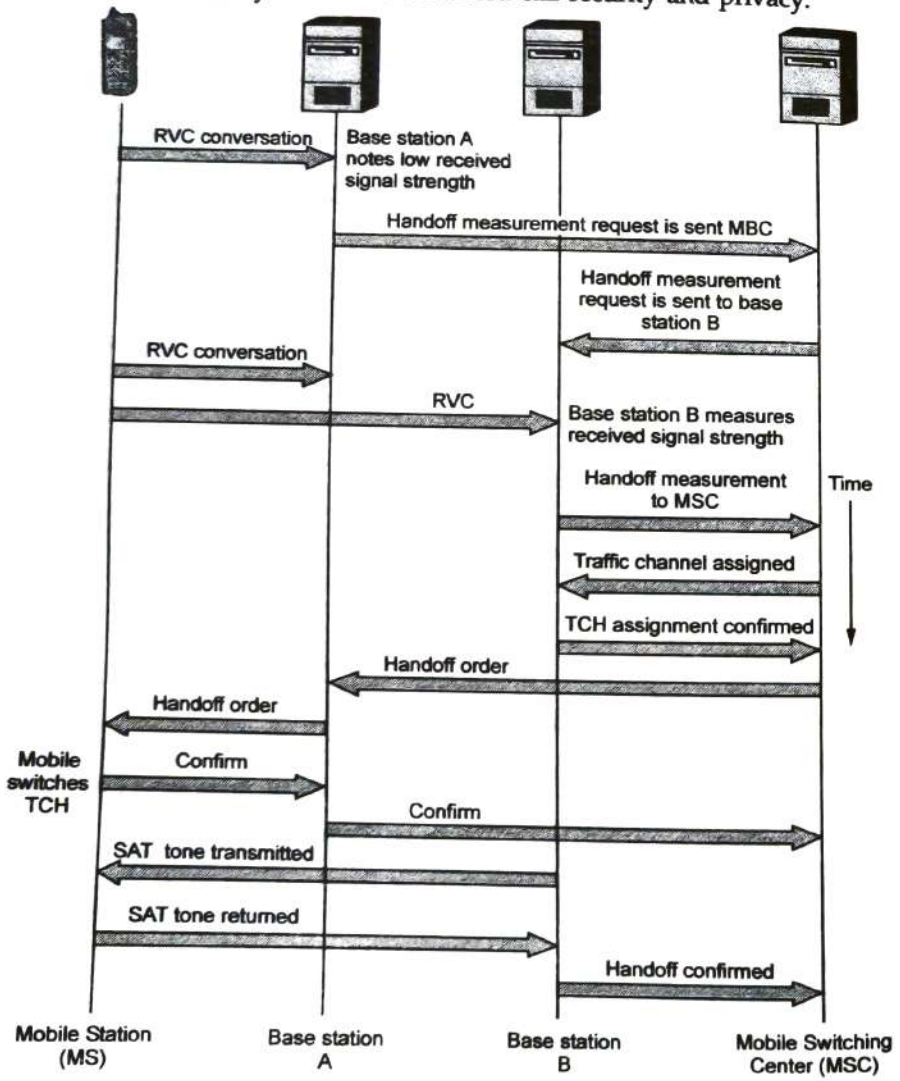


Fig. 5.1.1 Hand-off operation in AMPS

GSM is a second generation (2G) cellular system developed in Europe. It uses digital modulation and network level architectures and services. Commercial services of GSM was started in mid-1991.

GSM can handle both voice and data traffic, the voice waveform being digitally encoded before transmission. GSM transmission is done within frequency bands of 900 MHz, 1800 MHz and 1900 MHz.

5.1.1 Features of GSM

1. Short message service allows to send and receive 126 character text messages.
2. Ability to use same phone in different networks.
3. Allows data transmission and reception across GSM networks at 9600 bps speed.
4. FAX transmission and reception across GSM networks at 9600 bps.
5. Call forwarding, call on hold, conference facility.
6. Rapid call setup.
7. More subscriber capacity in the given spectrum.
8. Smaller handsets.
9. Encrypted conversions that cannot be tapped.
10. Calling Number Identification Presentation (CLIP).
11. Real time call costs.
12. Closed User Group - Allows a set of phones to be classed as PBX extensions.

5.1.2 Services Provided by GSM

Using ITU-T definitions, the telecommunication services of GSM can be divided into three categories

1. Bearer services or Data services 2. Teleservices 3. Supplementary services.

Bearer services or Data services

A variety of data services can be offered by GSM.

i) GSM users can send and receive data at rate upto 9600 bps.

ii) Access to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks and Circuit Switched Networks using a variety of access methods and protocols such as x.25 and x.32.

Since GSM is a digital network, a modem is not required between the users and GSM network, although an audio modem is required inside the GSM network to interwork with POTS.

iii) GSM supports Group 3 facsimile (FAX) service.

iv) Bidirectional SMS service, the messages are transported in a store-and-forward fashion. SMS can be sent on point-to-point and cell broadcast mode (traffic and

2. Teleservices

- The most basic teleservice supported by GSM is telephony. As with all other communications, speech is digitally encoded and transmitted through the GSM network as a digital stream.
- There is also an emergency service, where the nearest emergency-service provider is notified by dialling three digits (e.g. 911).
- GSM teleservice can also provide videotext, and teletext transmission.

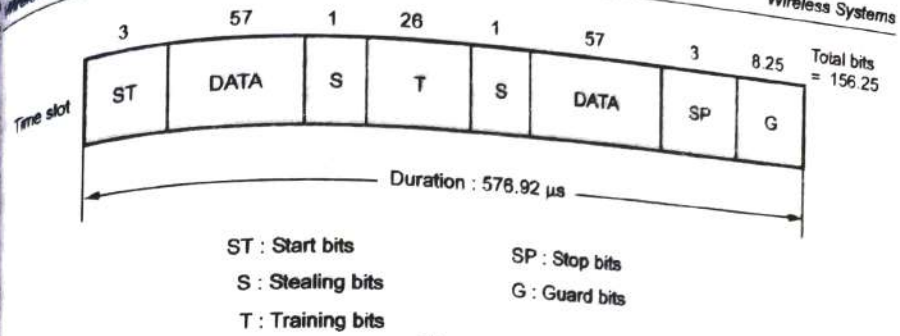
3. Supplementary services

- Supplementary services are provided besides teleservices or bearer services. Supplementary services includes several forms of :
  a) Number identification services
  b) Call forwarding service c) Call completion services
  d) Multiparty service e) Call restriction services.

5.1.3 GSM Radio Link Aspect

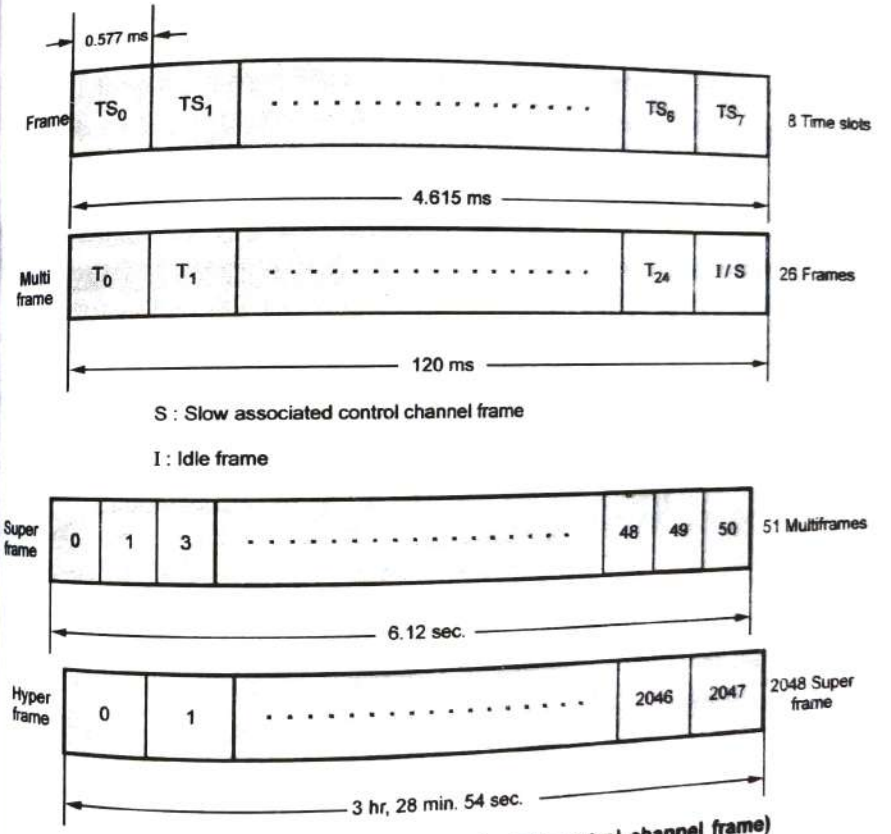
- GSM networks uses two 25 MHz bandwidth globally. This 25 MHz bandwidth is further divided into 124 carrier frequency channels each 200 kHz apart called "Absolute Radio Frequency Channel Numbers (ARFCN)".
  1. For subscriber to base transmission : 890-915 MHz (reverse link)
  2. For base to subscriber transmission : 935-960 MHz (forward link)
- The ARFCN indicates a pair of channel (forward and reverse) which are separated by 45 MHz. Each channel is time shared between 8 subscribers in TDMA scheme with a frame duration of 4.615 ms. Radio transmissions on both forward and reverse link are made at channel data rate of 270.833 kbps, using BT = 0.3 GMSK modulation. Therefore, signalling bit period = 3.692 μs and effective channel transmission rate per user is 33.854 kbps. But user data is sent at a maximum rate of 24.7 kbps because of GSM overload.
- Every Time Slot (TS) has 4156.25 bits, out of which 8.25 bits are used for guard time and 6 bits are used for start and stop bits to prevent overlap with adjacent time slots. Each time slot has duration of 576.92 μs.
- The GSM air interface specifications are summarized as under.

1.	Forward channel frequency	: 935 - 960 MHz
2.	Reverse channel frequency	: 890 - 915 MHz
3.	Forward and reverse channel bandwidth	: 25 MHz
4.	ARFCN	: 0 to 124 and 975 to 1023
5.	T_X /R_X frequency spacing	: 45 MHz



ST : Start bits SP : Stop bits
S : Stealing bits G : Guard bits
T : Training bits

Fig. 5.1.2



S : Slow associated control channel frame

I : Idle frame

Fig. 5.1.3 GSM frame (Speech dedicated control channel frame)

6.	T_X /R_X Time slot spacing	: 3 Time slots
7.	Frame / Burst period	: 4.615 ms

8. Voice transmission per RF channel	: 8
9. Time Slot (TS) period	: 576.9 μs
10. Bit period	: 3.692 μs
11. Modulation	: 0.3 GMSK (Gaussian Minimum Shift Keying)
12. Channel spacing	: 200 kHz
13. Interleaving delay	: 40 ms
14. Voice coder bit rate	: 13.4 kbps
15. Modulation data rate	: 270.8333 kbps
16. Frequency deviation	: 67.708 kHz
17. Slow frequency hopping	: 217 hops per second.

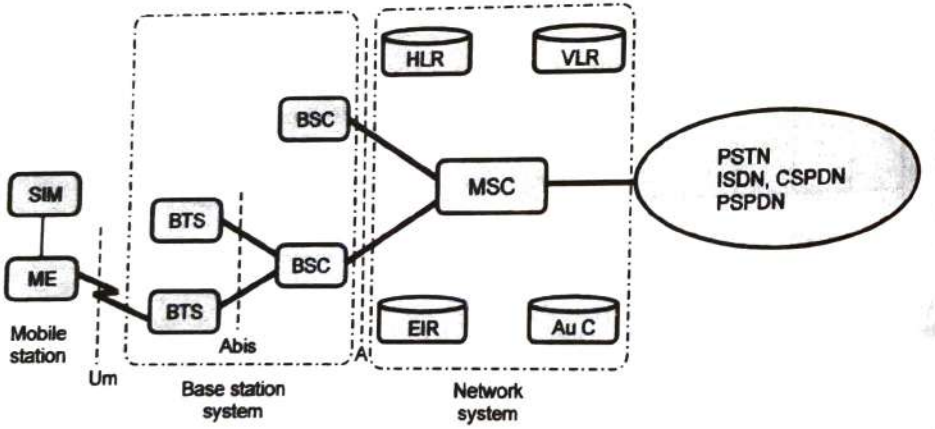
University Question

1. *How docs GSM radio subsystem work ?* **GTU : Summer-15, Marks 7**

5.2 GSM Network Architecture

GTU : Summer-15,16, Winter-15

- A GSM network consists of several functional entities, whose functions and interfaces are specified. Fig. 5.2.1 shows generic GSM network architecture.



SIM : Subscriber Identity Module
ME : Mobile Equipment
BSC : Base Station Controller
BTS : Base Transreceiver controller
EIR : Equipment Identity Register
HLR : Home Location Register
VLR : Visitor Location Register
MSC : Mobile Service Switching Center
Au C : Authentication Center

Fig. 5.2.1 GSM architecture

- The GSM network can be divided into three parts.
  1. Mobile station - Carried by subscriber
  2. Base station system - Controls the radio link with mobile station
  3. Network system - Performs switching of calls between mobile users.

5.2.1 Mobile Station (MS)

- The Mobile Station (MS) consists of mobile equipment (terminal) and a smart card called SIM (Subscriber Indentity Module). SIM provides personal mobility to have access to subscribed services irrespective of a specific equipment. By inserting the SIM card into another GSM equipment, the user can receive calls at that equipment, make calls from that equipment, and receive other subscribed services.
- The mobile equipment (terminal) is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication and other information. The IMEI and IMSI are independent, thereby allowing personal mobility. The SIM may be protected against unauthorized use by a password or Personal Identity Number (PIN).
- The power levels supported by GSM mobile station currently range from 0.8 to 8.0 W, and power saving techniques are used on the air interface to extend battery life.

5.2.2 Base Station Subsystem (BSS)

- The base station subsystem consists of two parts -
  1. Base Transceiver Station (BTS).
  2. Base Station Controller (BSC).
- Abis interface allows the operation between BSC and BTS. The interface comprises traffic and control channels.

BTS

- The Base Transceiver Station has radio transceivers that define a cell and handles the radio-link protocols with Mobile Station (MS).
- BTS serves one or more cells in the cellular network and contains more than one transceivers (TRXs). The transceiver serves full duplex communication to Mobile Station (MS).
- BTS contains the Transcoder Rate Adapter Unit (TRAU). In TRAU, the GSM specific speech encoding and decoding is carried out, as well as the rate adaption function of data.

BSC

- The Base Station Controller manages the radio resources for one or more BTSs. It handles radio-channel setup, frequency hopping and handoffs. The BSC is the connection between the mobile station and the Mobile Service Switching Center (MSC).
- The functions of BSC and BTS are listed below.

Sr. No.	Base Station Controller (BSC)	Base Transceiver Station (BTS)
1.	Control of BTSs.	Interleaving and deinterleaving.
2.	Radio resource management.	Radio link protocols handling.
3.	Handoff management and control.	Full duplex communication to MS.

5.2.3 Network Switching System (NSS)

- The central component of network subsystem is the Mobile Services Switching Center (MSC). It acts as switching node of PSTN and provides the function needed to handle a mobile subscriber such as - Registration, authentication, locating updating, handovers and call routing to roaming subscriber.
- Network subsystem includes data bases required for subscribers and mobility management. The Network subsystem also includes four different data bases -
  1. Home Location Register (HLR) 2. Visitor Location Register (VLR)
  3. Equipment Identity Register (EIR) 4. Authentication Center (AuC)

5.2.3.1 Mobile Switching Center (MSC)

- The MSC provides the connection to the fixed networks (PSTN or ISDN) with additional capabilities to support mobility management functions such as terminal registration location updating and handoff. These services are provided in conjunction with several functional entities which together form the network subsystem.
- The MSC does not contain mobile subscriber parameters. The major functions of MSC are listed below -
  1. Call setup, supervision, and release.
  2. Digit collection and translation.
  3. Call routing /call handling.
  4. Billing information collection.
  5. Mobility management
     - Registration
     - Location updating
     - Call handoff between BSC and MSC
  6. Management of radio resources during a call.

7. Echo cancellation.
8. Management of signalling protocol.
9. Interrogation of appropriate registers (VLR/HLR).

5.2.3.2 Home Location Register (HLR)

- The Home Location Register (HLR) and Visitor Location Register (VLR), together with MSC provide the call routing and roaming capabilities of GSM.
- The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with current location of Mobile Station (MS). The HLR database maintains unique International Mobile Subscriber Identity (IMSI) of each subscriber and VLR address. The location of the mobile station is typically in the form of the signalling address of the VLR associated with the mobile station.
- There is logically one HLR per GSM network, although it may be implemented as a distributed database.
- HLR database can be grouped into two types :

1. Dynamic database

a. Location information for each subscriber.

2. Permanent database

a. International Mobile Subscriber Identity (IMSI)
b. Service subscription information.
c. Service restriction.
d. Supplementary services.
e. Mobile terminal characteristics.
f. Billing/accounting information.

5.2.3.3 Visitor Location Register (VLR)

- The Visitor Location Register (VLR) contains selected administrative information from HLR, necessary for call control and provision of subscribed services, for each mobile currently located in the geographical area controlled by the VLR.
- The VLR is a temporary database that stores the IMSI and customer information for each roaming subscriber who is visiting the coverage area of a particular MSC. There is one VLR part MSC. When a roaming mobile enters in MSC area, the MSC informs the associated VLR about the mobile and this information is registered.
- The VLR also contains information about the locally activated features such as call forward on busy. The temporary subscriber information in VLR includes -
  1. International Mobile Subscriber Identity (IMSI and subscriber ID)
  2. Features currently activated

3. Temporary Mobile Station Identity (TMSI)
4. Current location information about MS
5. Location where mobile is registered
6. Directory number to route calls to roaming station
7. Copy of subscriber data from HLR
8. Mobile station ISDN number
9. HLR address.

5.2.3.4 Equipment Identity Register (EIR)

- The Equipment Identity Register (EIR) is a database that contains a list of all val mobile equipment on the network, where each mobile station is identified by International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if has been reported stolen or is not type approved.
- The EIR data is in the form of white, grey and black lists which is consulted b network when it wishes to confirm the authenticity of terminal requesting servic Different list types and their contents are given below.

Sr. No.	Type	Meaning	Contents
1.	White list	Valid IMEI numbers	List of valid mobile equipments.
2.	Grey list	IMEI under scanner	List of suspected mobile under observation.
3.	Black list	Prohibited IMEI numbers	List of mobile for which service is barred.

5.2.3.5 Authentication Center (AuC)

- The Authentication Center (AuC) is a protected database that stores a copy of th secret key stored in each subscriber's SIM card, which is used for authentication an encryption over the radio channel.
- Authentication center maintains authentication keys and algorithms and provid security triplets (RAND, SRES, and K_c) to the VLR. This ensures, user authenticatio and radio channel encryption procedures to carryout within visited network.
- The AuC contains security modules for authentication keys (K_i), authenticatio algorithms (A_3) and cipher key generation algorithms (A_8).

5.2.3.6 Operation and Support Subsystem (OSS)

- The Operations and Support Subsystem (OSS) is the command center used to moni and control the GSM system.

- The three areas of OSS are :
  i) Network operations and maintenance.
  ii) Subscription management (charging and billing etc.).
  iii) Mobile equipment management.
- If an emergency occurs at a base station, the OSS can determine where the BTS is located, what type of failure occurred and what equipment the site engineer will need to repair the failure.

5.2.4 GSM Network Interfaces and Protocols

- Different types of interfaces are used in GSM systems for interconnecting its subsystems.
  1. U_m interface 2. Abis interface 3. A interface

U_m interface :

- The U_m interface is radio or air interface. The U_m radio interface is used to communicate between Mobile Station (MS) with Base Transceiver Station (BTS).

Abis interface :

- The Abis interface is used for inter communication between BSC and BTS. This interface is defined by GSM equipment manufacturer. It carries traffic and control channel data.

A interface :

- The A interface allows the interconnection between BSC and MSC. These are physically connected by dedicated/leased lines or microwave links. The physical layer of A interface is a 2 Mbps CCITT digital connection.
- The A interface allows a service provider to use base stations and switching equipment made by different manufacturers.

B interface :

- The B interface exists between the MSC and the VLR. It uses a protocol known as the MAP/B protocol. As most VLRs are collocated with an MSC, this makes the interface purely an "internal" interface.
- The interface is used whenever the MSC needs access to data regarding a MS located in its area.

C interface :

- The C interface is located between the HLR and a GMSC or a SMS-G. When a call originates from outside the network, i.e. from the PSTN or another mobile network it

has to pass through the gateway so that routing information required to complete the call may be gained.

- The protocol used for communication is MAP/C, the letter "C" indicating that the protocol is used for the "C" interface. In addition to this, the MSC may optionally forward billing information to the HLR after the call is completed and cleared down.

D interface :

- The D interface is situated between the VLR and HLR. It uses the MAP/D protocol to exchange the data related to the location of the ME and to the management of the subscriber.

E interface :

- The E interface provides communication between two MSCs. The E interface exchanges data related to handover between the anchor and relay MSCs using the MAP/E protocol.

F interface :

- The F interface is used between an MSC and EIR. It uses the MAP/F protocol. The communications along this interface are used to confirm the status of the IMEI of the ME gaining access to the network.

G interface :

- The G interface interconnects two VLRs of different MSCs and uses the MAP/G protocol to transfer subscriber information, during e.g. a location update procedure.

H interface

- The H interface exists between the MSC the SMS-G. It transfers short messages and uses the MAP/H protocol.

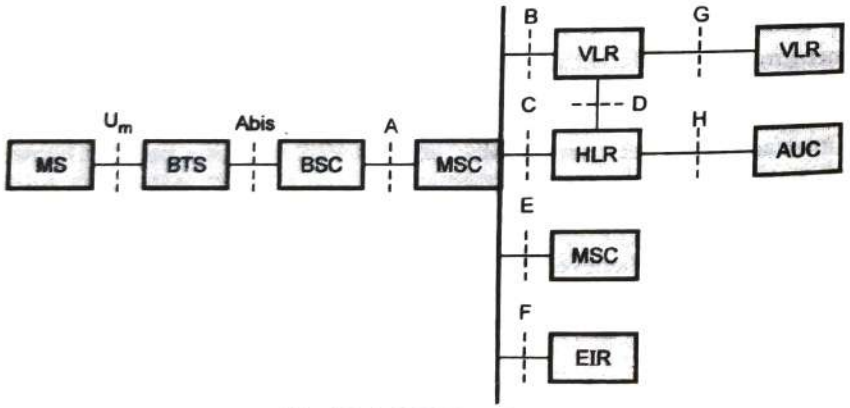


Fig. 5.2.2 GSM Interface

I interface :

- The I interface can be found between the MSC and the ME. Messages exchanged over the I interface are relayed transparently through the BSS.
- Various GSM interface standards are shown in Fig. 5.2.2.

University Questions

1. *Give differences between HLR and VLR functions.* GTU : Summer-15, Marks 7
2. *Draw GSM system architecture and explain it in detail.* GTU : Winter-15, Marks 7
3. *Describe in details GSM architecture with necessary block diagram and its various blocks.* GTU : Summer-16, Marks 7

5.3 GSM Signaling Protocol Architecture

GTU : Summer-16

- The MS communicates with MSC for providing system connection, mobility and radio resource management.

Layered structure/OSI model : The OSI model views the communications between user application processes as being partitioned into self-contained layers that contain tasks that can be implemented independently of tasks in other layers. A message sent between two network nodes travels downward in the protocol stack of the sending node. As the message propagates through the layer information is added to the original message at each layer. After transmission to the receiving network node, the message propogates upward through the receiving node protocol stack.

- Signaling model for GSM system is shown in Fig. 5.3.1.

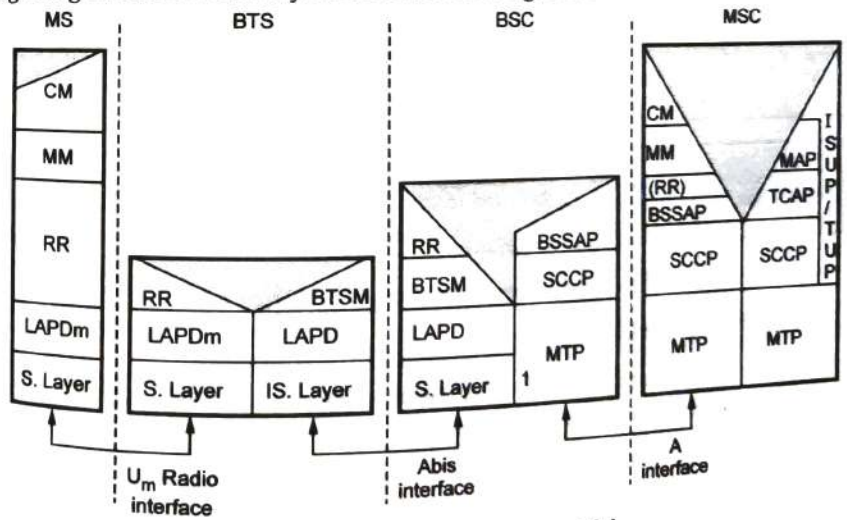


Fig. 5.3.1 GSM signalling model

- The signalling model shows various protocols used between the different GSM interfaces and at the OSI levels. The MSC communicates with the various networks connected to PSTN using various protocols.
- The GSM signaling protocol stack consists of three layers.
  1. Physical layer (Layer - 1)
  2. Data link layer (Layer - 2)
  3. Network or Messaging layer (Layer - 3)

5.3.1 Physical (Layer-1)

- Physical layer is defined for U_m air interface. The physical layer specifies :
  a) How the information from different voice and data are formatted in packets.
  b) Radio modem description.
  c) Varify of services.
  d) Modulation and control techniques.
  e) Power control methodology.
  f) Time synchronization.

5.3.2 Data Link Layer (Layer-2)

- Signaling and control data is communicated by layer-2 and layer-3 messages.
- The data link layer check the flow of data packets to layer-3.
- The data link control protocol is known as $LAPD_m$, where m indicates modified version of LAPD.

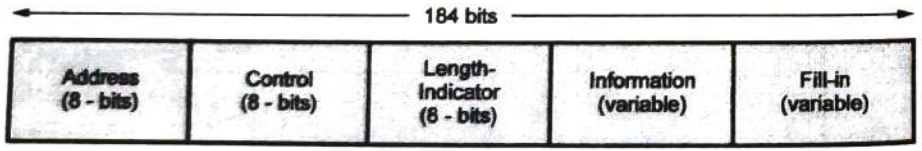


Fig. 5.3.2 Frame format of of $LAPD_m$

5.3.3 Networking (Messaging) Layer

- The networking or messaging layer is responsible for protocols to establish, maintain and terminate a mobile communication session.
- This layer specifies the messages on logical channels encapsulated in DLL frames.

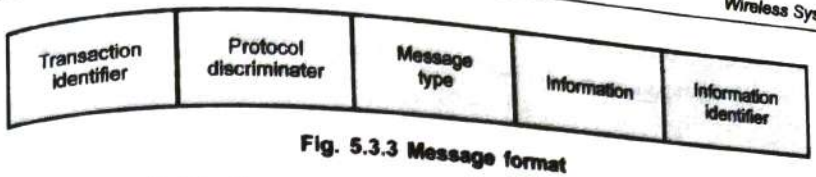


Fig. 5.3.3 Message format

- GSM standard divides the messages into sublayers as -
  a) Radio Resource Management (RRM)
  b) Mobility Management (MM)
  c) Communication Management (CM)

University Question

1. *Explain GSM network's hexagonal cellular concept and frequency reuse concept.*
   GTU : Summer-16, Marks 7

5.4 Identifiers in GSM System

- The MIN (Mobile Identification Number) is a number that uniquely identifies a mobile telephone subscriber. GSM uses a number of descriptors to identify subscribers, equipment, and fixed stations/areas. Many are temporary and used to maintain the confidentiality of fixed identities.
- There are basically three numbers that identify the mobile subscriber; these are IMSI, MS-ISDN, and the TMSI, which is a temporary identification number that is assigned by the serving MSC/VLR combination.
- The TMSI is mainly used for security reasons to avoid broadcasting the IMSI over the RF air interface, thereby making it harder for eavesdroppers. The TMSI is supposed to be changed on a per-call basis as recommended by GSM specific actions.

Subscriber Device Identification

- The mobile Subscriber Device (SD) can have different identification system depends on the type of networks such as TDMA, CDMA and GSM.

5.4.1 Mobile Station ISDN Identification (MSISDN)

- The MSISDN is a number which uniquely identifies a mobile telephone subscription in the public switched telephone network numbering plan. According to the CCITT recommendations, the mobile telephone number or catalogue number to be dialled is composed in the following way :
- MSISDN composed of :

$$\text{MSISDN} = \text{CC} + \text{NDC} + \text{SN}$$

CC = Country Code

NDC = National Destination Code

SN = Subscriber Number

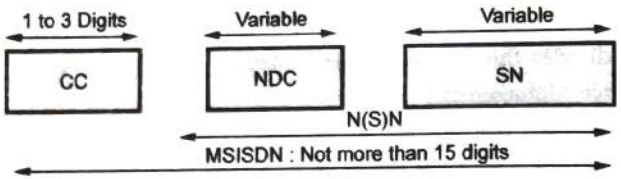


Fig. 5.4.1 MSISDN number

- CC (Country Code) is the country in which the VLR mobile station is registered.
- A National Destination Code (NDC) is allocated to each GSM PLMN. In some countries, more than one NDC may be required for each GSM PLMN. The international MSISDN number may be of variable length. The maximum length shall be 15 digits, prefixes not included.
- SN - is Subscriber Number
- N(S) N - National (Significant) Number consists of NDC and SN.
- The length of the MSISDN depends on the structure and numbering plan of each operator, as an application of CCITT recommendation E.164.

5.4.2 International Mobile Subscriber Identity (IMSI)

- The IMSI is the information which uniquely identifies a subscriber in a GSM/PLMN. An IMSI is assigned to each authorized GSM user. It consists of a Mobile Country Code (MCC), Mobile Network Code (MNC) and a PLMN unique Mobile Subscriber Identification Number (MSIN). The IMSI is not hardware-specific. Instead, it is maintained on a SC by an authorized subscriber and is the only absolute identity that a subscriber has within the GSM system.
- For a correct identification over the radio path and through the GSM PLMN network, a specific identity is allocated to each subscriber. This identity is called the International Mobile Subscriber Identity (IMSI) and is used for all signalling in the PLMN. It will be stored in the Subscriber Identity Module (SIM), as well as in the Home Location Register (HLR) and in the serving Visitor Location Register (VLR).
- According to the GSM recommendations, the IMSI will have a length of maximum 15 digits. All network-related subscriber information is connected to the IMSI.
- The IMSI consists of three different parts :

IMSI = MCC + MNC + MSIN

MCC = Mobile Country Code (3 digits)

MNC = Mobile Network Code (2 digits)

MSIN = Mobile Subscriber Identification Number (max 10 digits)

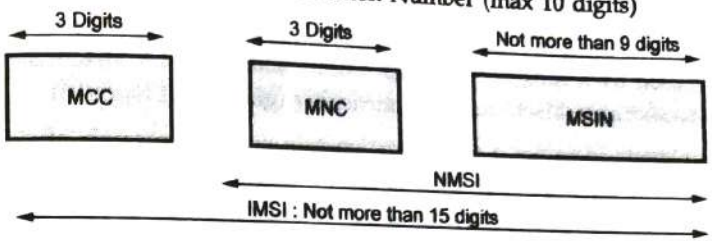


Fig. 5.4.2 IMSI number

- Mobile Country Codes (MCC) are used to identify mobile stations in wireless telephone networks.
- Mobile Network Code (MNC) uniquely identifies the home GSM PLMN of the mobile subscriber. It consists of 3 digits.
- Mobile Station Identification Number (MSIN) uniquely identifies the mobile subscriber within a GSM PLMN. The first 3 digits identify the logical HLR-ID of the mobile subscriber.
- National Mobile Station Identity (NMSI) consists of the MNC followed by the MSIN and is to be assigned by individual administration.

5.4.3 Temporary Mobile Subscriber Identity (TMSI)

- The TMSI is a temporary number used instead of IMSI to identify an MS. The TMSI is used for the subscriber's confidentiality on the air interface.
- The TMSI has only local significance (that is, within the MSC/VLR area) and is changed at certain events or time intervals.

5.4.4 Mobile Station Roaming Number (MSRN)

- A MSRN is used during the call setup phase for mobile terminating calls. Each mobile terminating call enters the GMSC in the PLMN. The call is then re-routed by the GMSC, to the MSC where the called mobile subscriber is located. For this purpose MSRN is allocated by the MSC and provided to the GMSC.
- The MSRN consists of -
  a. Country Code (CC)
  b. National Destination Code (NDC)
  c. Subscriber Number (SN)

MSRN = CC + NDC + SN

5.4.5 International Mobile Station Equipment Identity (IMEI)

- The IMEI is used for equipment identification. The IMEI is the unique identity of the equipment used by a subscriber by each PLMN and is used to determine authorized (white), unauthorized (black) and malfunctioning (gray) GSM hardware.
- An IMEI uniquely identifies a mobile station as a piece or assembly of equipment. In conjunction with the IMSI, it is used to ensure that only authorized users should be granted access to the system. An IMEI is never sent in cipher mode by a MS.

IMEI = TAC + FAC + SNR + sp

TAC = Type Approval Code (6 digits), determined by a central GSM body

FAC = Final Assembly Code (2 digits), identifies the manufacturer.

SNR = Serial Number (6 digits), an individual serial number of six digits uniquely identifying all equipment within each TAC and FAC.

sp = Spare for future use (1 digit)

According to the GSM specification, IMEI has the length of 15 digits.

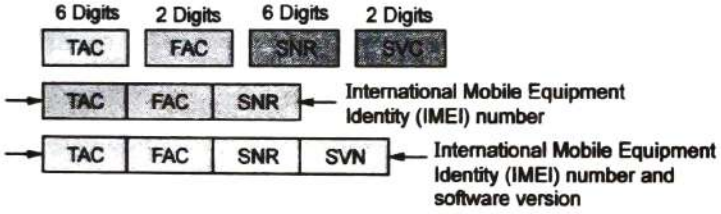


Fig. 5.4.3 Formation of IMEI number

5.4.6 Location Area Identity (LAI)

- LAI is used for location updating of mobile subscribers.

LAI = MCC + MNC + LAC

- MCC is Mobile Country Code (3 digits), identifies the country. It follows the same numbering plan as MCC in IMSI.
- MNC is Mobile Network Code (2 digits), identifies the GSM/PLMN in that country and follows the same numbering plan as the MNC in IMSI.
- LAC is Location Area Code, identifies a location area within a GSM PLMN network. The maximum length of LAC is 16 bits, enabling 65, 536 different location areas to be defined in one GSM PLMN.

5.4.7 Cell Global Identity (CGI)

- CGI is used for cell identification within the GSM network. This is done by adding a Cell Identity (CI) to the location area identity.

CGI = MCC + MNC + LAC + CI

- CI is Cell Identity, identifies a cell within a location area, maximum 16 bits

5.4.8 Base Station Identity Code (BSIC)

- BSIC allows a mobile station to distinguish between different neighbouring base stations.

BSIC = NCC + BCC

- NCC is Network Colour Code (3 bits), identifies the GSM PLMN. It does not uniquely identify the operator. NCC is primarily used to distinguish between operators on each side of border.
- BCC is Base Station Colour Code (3 bits), identifies the Base Station to help distinguish between BTS using the same BCCH frequencies.
- **Radio Base Station Identity Code (RBSIC)** - Used by the mobile operator to identify the RBS's within a wireless network.

5.4.9 Location Number (LN)

- Location number is a number related to a certain geographical area, as specified by the network operator by "tying" the location numbers to cells, location areas or MSC/VLR service areas.
- The location number is used to implement features like regional/local subscription and geographical differentiated charging.

5.4.10 Global Title (GT) and Global Title Translation (GTT)

- The GT is an address of fixed network element. The GT is used for the addressing of network nodes such as MSCs, HLRs, VLRs, AUCs and EIRs in accordance with E.164.
- The GTL is performed by SCCP translation function to provide the correct signalling point address information for the subsequent routing of the message to correct network node.

5.5 GSM Channel

GTU : Summer-15,16

- The GSM cellular system is based on the use of time division multiple access to provide additional user capacity over a limited amount of radio frequency spectrum.
- A single GSM RF carrier can support up to eight MS subscribers simultaneously. Each channel occupies the carrier for one eighth of the time. This technique is called Time Division Multiple Access (TDMA).
- Time is divided into discrete periods called timeslots. The timeslots are arranged in sequence and are conventionally numbered 0 to 7. Each repetition of this sequence is called a TDMA frame. Each MS telephone call occupies one timeslot (0 to 7) within the frame until the call is terminated, or a handover occurs. The TDMA frames are then built into further frame structures according to the type of channel.

  Frames - GSM system divides the radio link connection time into eight equal and repeating timeslots known as frames.

  Multi-frames - The system can use several different types of repeating framestructures known as multi- frames.
- For a system to work correctly, the timing of the transmissions to and from the MS is critical. The MS or BS must transmit the information related to one call at exactly the right moment, or the timeslot will be missed. The information carried in one timeslot is called a burst.
- Each data burst, occupying its allocated timeslot within successive TDMA frames provides a single GSM physical channel carrying a varying number of logical channels between the MS and BTS.
- Fig. 5.5.1 shows TDMA time frame structure

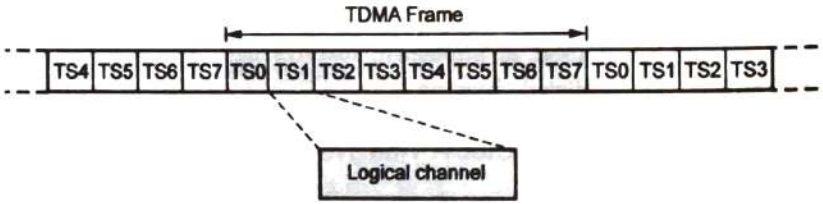


Fig. 5.5.1 TDMA time frame structure

5.5.1 Logical Channels

- There are two basic types of logical channels in GSM :
  1. Traffic Channels (TCH)
  2. Control Channels (CCH)
- Traffic Channels (TCH) are used to carry either digitally encoded user speech or user data in uplink and downlink directions. Initial GSM specification specifies full rate

speech channels (22.8 kB/s) and data channels (9.6, 4.8 and 2.4 kB/s) are defined as TCH.

Control Channels (CCH) carry signalling and synchronizing commands between the base station and mobile station. Three basic types of Control Channels (CCH) are :

i) Broadcast Control Channels (BCCH) ii) Common Control Channels (CCCH)

iii) Dedicated Control Channels (DCCH)

Each control channel is further subdivided. Fig. 5.5.2 shows different subcategories of traffic and control channels in GSM.

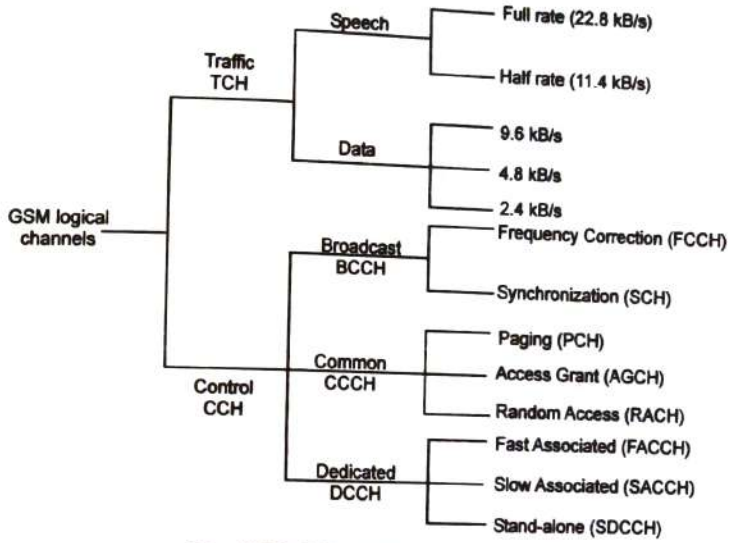


Fig. 5.5.2 GSM channel structures

5.1.1 Traffic Channels (TCH)

Traffic Channels (TCH) carry encoded speech and data. A TCH is a group of 26 TDMA frames, called multiframe. Each TDMA frame is having 120 ms duration. Out of 26 TDMA frames, 24 are used as TCH frames, one frame (13^{th}) is for SACCH and one frame (26^{th}) is unused or idle frame.

The TCH supports two information rates :

1. Full rate (TCH/F) . 2. Half rate (TCH/H).

When transmitted as full rate, the user data is occupied within one TS per frame. When transmitted as half rate, the user data is occupied into the same time slot but is sent in alternate frames.

The 26^{th} frame contains idle bits if full rate TCHs are used and contains SACCH data if half rate TCHs are used.

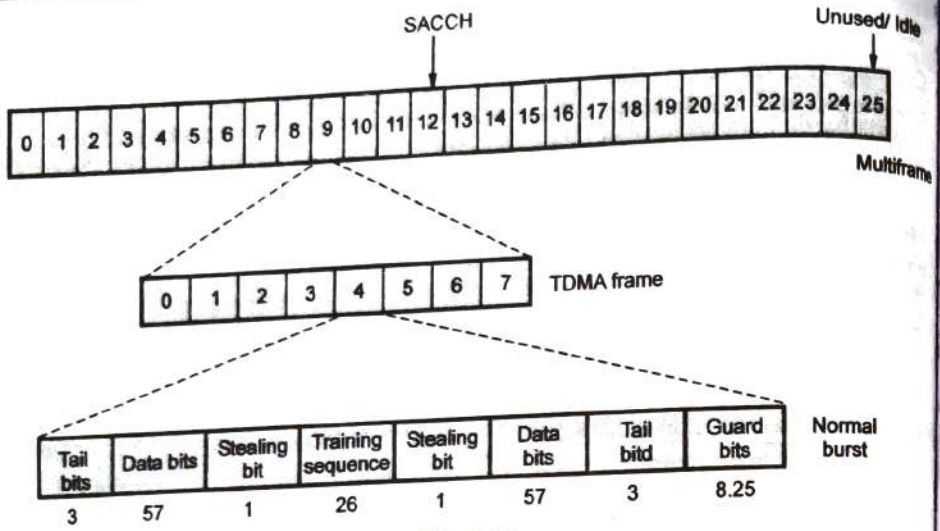


Fig. 5.5.3

Full Rate TCH

- Different full rate TCH for speech and data channels are as mentioned subsequently

1. Full Rate Speech Channel (TCH/FS) :

- The full rate speech is digitized at 13 kbps. After adding GSM channel coding digitized speech, the full rate speech channel carries 22.8 kbps.

2. Full Rate Data Channel for 9600 bps (TCH/F9.6) :

- The full rate traffic data channel carries raw user data which is sent at 9.6 kbps. A application of additional forward error correction coding using GSM standards, 9.6 kbps is sent at 22.8 kbps.

3. Full Rate Data Channel for 4800 bps (TCH/F4.8) :

- The full rate traffic data channel carries raw user data, which is sent at 4.8 kbps. W application of additional forward error correction coding using GSM standards, 4.8 kbps data is sent at 22.8 kbps.

4. Full Rate Data Channel for 2400 bps (TCH/F2.4) :

- The full rate traffic data channel carries raw data, which is sent at 2.4 kbps. W application of additional forward error correction coding using GSM standards, 2.4 kbps data is sent at 22.8 kbps.

Half Rate TCH

- Different half rate TCH for speech and data channels are as mentioned :

1. Half Rate Speech Channel (TCH/HS) :

- The half rate speech channel can carry digitized speech which is sampled at a rate half that of a full rate channel. GSM anticipate the availability of speech coders can digitize speech at about 6.5 kbps. After adding GSM channel coding to the digitized speech, the half rate speech channel will carry 11.4 kbps.

2. Half Rate Data Channel for 4800 bps (TCH/H4.8)

- The half rate traffic data channel carries raw user data which is sent at 4800 bps. After application of forward error correction using GSM standards, the 4800 bps data is sent at 11.4 kbps.

3. Half Rate Data Channel for 2400 bps (TCH/H2.4)

- The half rate traffic data channel carries raw user data which is sent at 2400 bps. After application of additional forward error correction using GSM standards, the 2400 bps data is sent at 11.4 kbps.

5.5.1.2 Control Channels (CCH)

Control Channels (CCH) are used, when mobile is idle or in dedicated mode. In idle mode, CCH exchange the signalling information needed to change dedicated mode.

The three basic control channels are : Broadcast (BCCH), Common (CCCH) and Dedicated (DCCH). Each control channel consists of several logical channels which are distributed in time to provide necessary GSM control functions.

roadcast Control Channel (BCCH)

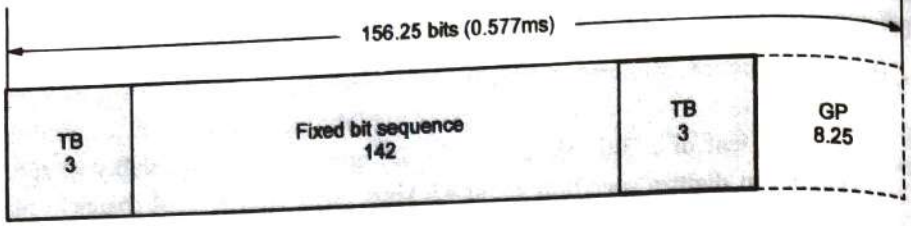
The Broadcast Control Channel (BCCH) is a unidirectional base to mobile channel which provides general information about the network, the cell in which the mobile is currently located and adjacent cells.

The BCCH includes two channels :

1. Frequency Correction Channel (FCCH) 2. Synchronization Channel (SCH)

Frequency Correction Channel (FCCH) :

FCCH is a base to mobile channel which provides information for carrier synchronization. The FCCH is a special data burst which occupies TS0 slot for the very first GSM frame (frame 0) and is repeated every ten frames within a control channel multiframe. The FCCH allows Mobile Subscriber (MS) to synchronize its internal frequency standard (local oscillator) with the frequency of Base Station (BS). In its first burst of FCCH, all zero bits are sent to indicate unmodulated carrier. Fig. 5.5.4 (a) shows Frequency Correction Burst (FCCH) structure.



TB : Tail Bits used to enhance demodulation
GP : Guard period, which allows for ramp up and down as the power is turned on and off.

Fig. 5.5.4 (a) Frequency correction burst

2. Synchronization Channel (SCH) :

- The Synchronization Channel (SCH) is a base to mobile channel which carries information for frame synchronization and identification of the Base Station (BS) transceiver. It also contains BSIC (Base Station Identity Code) and the frame number in relation to the hyperframe.
- In the frame following the FCCH, the BTS transmits with SCH in time slot 0. The SCH has a unique burst structure as well. It contains 64-bit binary (training) sequence that is same throughout all GSM networks and known to the MS. The BSIC is assigned to each BTS in GSM system. The SCH is transmitted once every ten frames within the control channel multiframe. Fig. 5.5.4 (b) shows synchronization burst structure.

TB	Coded data	Synchronization sequence	Coded data	TB	GP
3	39	64	39	3	8.25

TB : Tail Bits used to enhance demodulation
GP : Guard period, which allows for ramp up and down as the power is turned on and off.
Synchronization Sequence : Used for adaptive equalization and BTS identification
Coded Data : Encrypted user data or signalling control information.

Fig. 5.5.4 (b)

Common Control Channels (CCCH)

- The Common Control Channel (CCCH) includes : three different types of channels.
  1. Paging Channel (PCH) ; which is a forward link channel.
  2. Access Grant Channel (AGCH); which is a forward link channel.
  3. Random Access Channel (RACH); which is a reverse link channel.

1. Paging Channel (PCH) :

- The Paging Channel (PCH) is a part of CCCH and is a base to Mobile (forward link) channel used to alert a mobile to a call originating from the network.

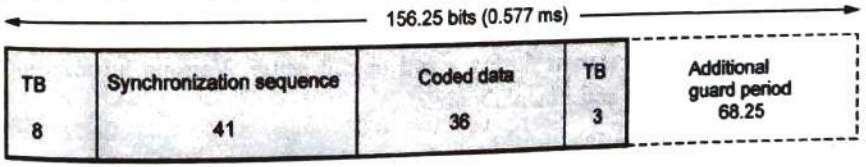
- The PCH generates paging signals from the base station to all Mobile Subscribers (MSs) in the cell and registers incoming call. The paging is done by transmitting IMSI of target subscriber along with request for acknowledgement on RACH.

2. Access Grant Channel (AGCH) :

- The Access Grant Channel (AGCH) is part of CCCH and is a base to mobile (Forward link) channel used to assign dedicated resources, such as Stand-alone Dedicated Control Channel (SDCCH) or Traffic Channel (TCH) to a mobile which has previously requested through RACH.
- AGCH is used to direct a mobile station to another type of control channel i.e. SDCCH or TCH, in order to complete the process of setting up a call and/or transferring information.

3. Random Access Channel (RACH)

- The Random Access Channel (RACH) is the reverse (mobile to base) channel. With the help of RACH, Mobile Station (MS) originates a call, sends signalling messages when not on call, acknowledges message from the BTS.
- The RACH uses the slotted ALOHA access scheme i.e. all mobiles requests access or respond to PCH alert within TS0 of a GSM frame. At BTS every frame will accept RACH transmissions from Mobile Station (MS). If RACH has been received successfully by the BTS, the network will direct the mobile station to the SDCCH-a two-way control channel designated just for this type of communication between mobile station and the network. Actually RACH carries very little information.
- The RACH burst has longer Guard Period (GP) to protect for burst transmission from an MS that does not know the timing advance when it first accesses the system. The additional guard time allows a distance upto 35 km between BS to MS. Random Access Burst Channel (RACH) structure is shown in Fig. 5.5.5.



TB : Tail bits used to enhance demodulation
Synchronization Sequence : Used for adaptive equalization and BTS identification
Coded data : Encrypted user data or signalling control information
GP : guard period

Fig. 5.5.5 Random access burst

Dedicated Control Channels (DCCHs)

The Dedicated Control Channels (DCCHs) come into play after call is established. These channels are bidirectional and have same formats and functions in both forward and reverse links.

- The DCCHs include three different types of channels :
  1. Fast Associated Control Channel (FACCH)
  2. Slow Associated Control Channel (SACCH)
  3. Stand-alone Control Channel (SDCCH)

1. Fast Associated Control Channel (FACCH) :

- The bidirectional FCCH is used for exchange of time critical information between mobile and base station during the progress of a call. A FACCH will spread over eight slots spread out over eight frames.
- The information in FACCH and SACCH is same. The FACCH is assigned whenever SACCH has not been dedicated to a Mobile Station (MS) and there is urgent message such as handoff is requested. The FACCH transmits control information by stealing capacity from the associated traffic channel. This is done by setting two special bits called stealing bits, in TCH forward channel burst. If stealing bit is set, the time slot is known to contain FACCH data for that frame. The normal burst with stealing bits is shown in Fig. 5.5.6.

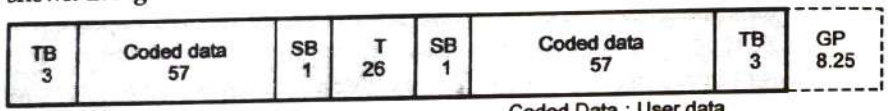


Fig. 5.5.6 Normal burst

2. Slow Associated Control Channel (SACCH)

- Slow Associated Control Channel (SACCH) is used to inform base of power measurements mode by the mobile of signal strength in adjacent cells. The SACCH is transmitted on every 26 bursts of every speech when half rate is used.
- The SACCH is a bidirectional channel. It exchanges control information between base station and mobile station during a call or call setup. Various information and control signals in uplink and downlink are :

Downlink (forward channel) :

i) Broadcast messages.

ii) Power control information.

iii) Timing advance in downlink.

Uplink (reverse channel) :

i) Measurement report.

ii) Acknowledged power control.

iii) Acknowledgement of timing advance.

iv) Received signal strength and quality of TCH.

3. Stand-alone Dedicated Control Channels (SDCCH) :

- The Stand-alone Dedicated Control Channel (SDCCH) is assigned for each mobile station. The SDCCH is a bidirectional logical channel, consisting of four time slots (carrying one massage) in every multiframe. This makes transmission speed slower, but it is sufficient for the information that needs to be sent.
- The SDCCH carries signalling data following the connection of the mobile with the Base Station (BS) and just before allocation of TCH by the Base Station (BS) to the MS. The SDCCH, ensures that the MS and BS remains connected whereas BS and MSC verify subscriber unit and allocate resources for the mobile. It is a channel which accepts a newly completed call from the BCH and holds the traffic while waiting for the BS to allocate to TCH channel.
- The SDCCH is used to send authentication and alert messages as the mobile synchronizes itself with the frame structure and waits for TCH. SDCCH may be assigned their own physical channel or may occupy TS0 slot of the BCH if there is low demand for BCH or CCCH traffic.
- GSM Logical Channels are summarized in Table 5.5.1.

Traffic Channels (TCH)		Control Channels (CCH)			
Speech	**Data**	**Broadcast CCH (BCCH)**	**Common CCH (CCCH)**	**Stand-alone Dedicated CCH (SDCCH)**	**Associated CCH (ACCH)**
Full-rate TCH/F	TCH/F9.6	Frequency correction	Paging channel		Fast (FACCH)
	TCH/F4.8 TCH/F2.4	(FCCH) Synchronization (SCH)	(PCH) Random Access (RACH)		Slow (SACCH)
Half-rate TCH/H	TCH/H4.8 TCH/H2.4		Access Grant (AGCH)		

Table 5.5.1 GSM logical channels

- Different bursts within time slots are used for data transmission illustrated at a glance in Fig. 5.5.7. (See Fig. 5.5.7 on next page)

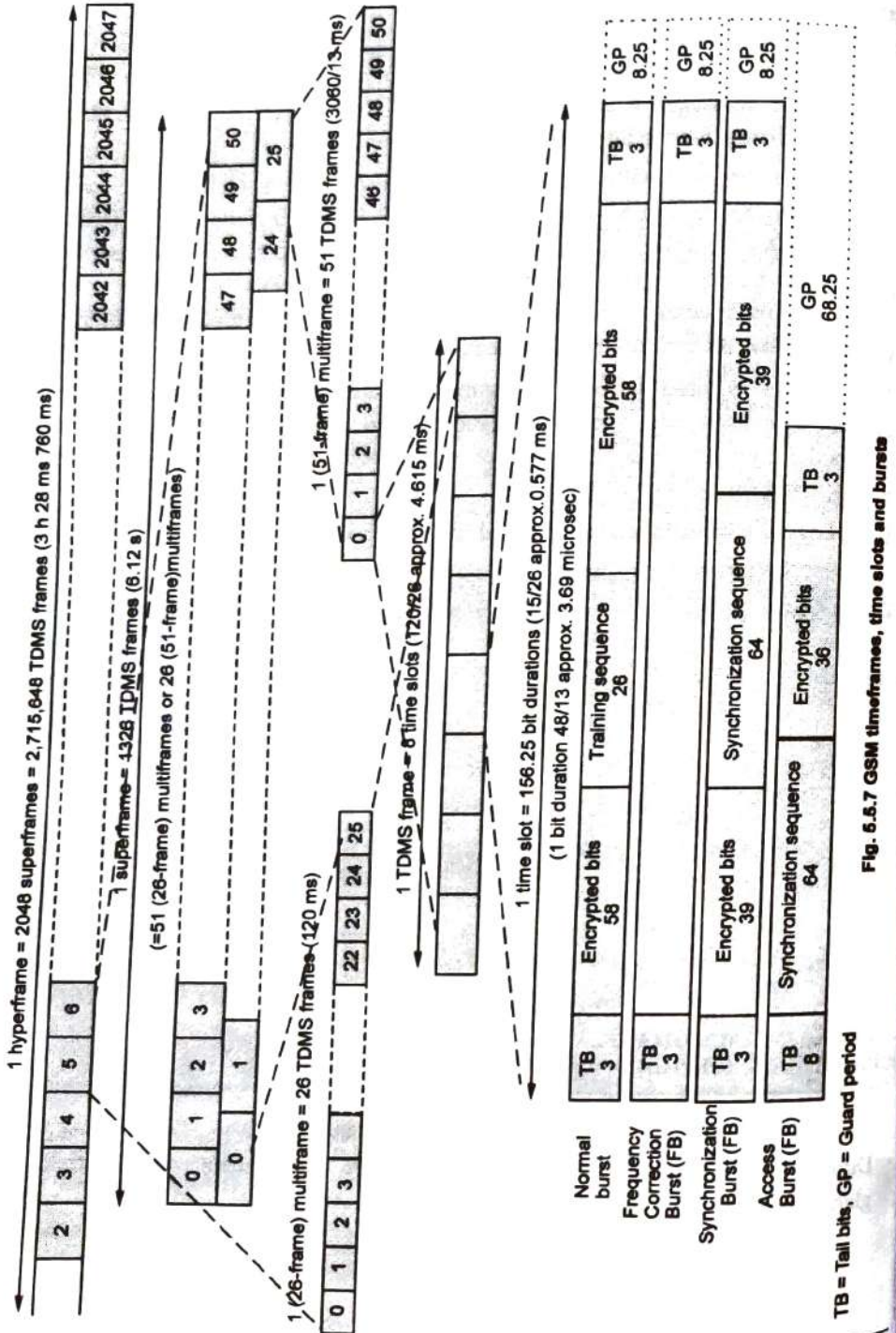


Fig. 5.5.7 GSM timeframes, time slots and bursts

University Questions

1. *Briefly explain GSM logical channels.* GTU : Summer-15, Marks 7
2. *Describe various GSM logical and physical channels.* GTU : Summer-16, Marks 7

5.6 GSM Frame Structure

GTU : Winter-14, Summer-15

- There are eight timeslots per TDMA frame. The frame period is 4.615 ms. A frame contains 1250 bits (8 × 156.25), some of them are not used.
- The 13th or 26th frame are not used for traffic but for control purposes. The frame rate is 216.66 frames per second or 270.833 kbps / 1250-bits / frame.
- Normal speech frames are grouped into larger structure called multiframes which forms multiframes, multiframes are grouped together to form superframes and superframes forms hyperframes. Fig. 5.6.1 shows GSM frame structure.

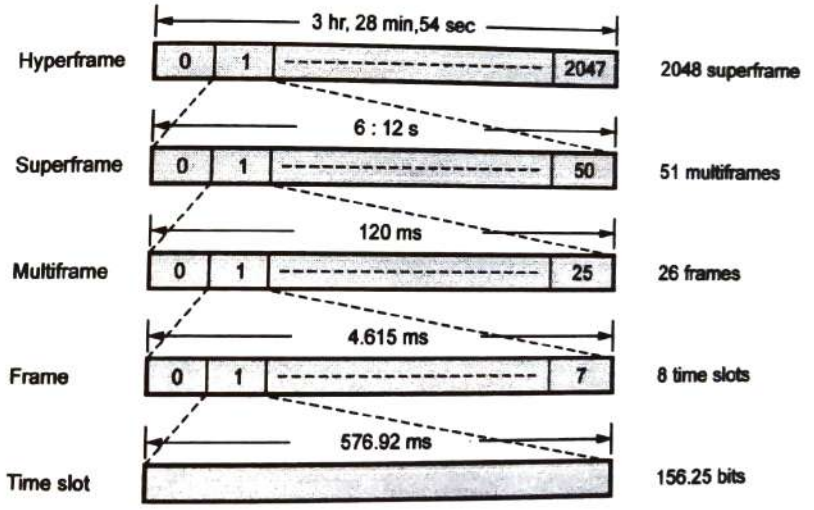


Fig. 5.6.1 GSM frame structure

- A multiframe contains 26 TDMA frames one superframe contains 51 multiframes (or 1326 TDMA frames). A hyperframe contains 2048 superframes or 2,715,648 TDMA frame. A hyperframe is sent for every 3 hours, 28 minutes and 54 seconds.

5.6.1 GSM Burst Structures

- Each logical channel is realized by transmission of a specific type of data packet (burst) in the assigned time slots. Such as frequency correction, synchronization and

broadcast logical channels are sent in the zero time slot of the broadcast carrier together with some other specific control channels.

- In order to realize all these channels, a normal burst, frequency correction burst and synchronization burst are emitted.
- There are 5 types of bursts :
  1. **Normal burst :** used to carry information on traffic and control channels.
  2. **Frequency Correction burst :** Used for frequency synchronization of the mobile.
  3. **Synchronization burst :** Used for Frame synchronization of the mobile.
  4. **Access burst :** Used for random and handover access.
  5. **Dummy burst :** Used when no other channel requires burst to be sent.

Fig. 5.6.2 shows various burst frame structures.

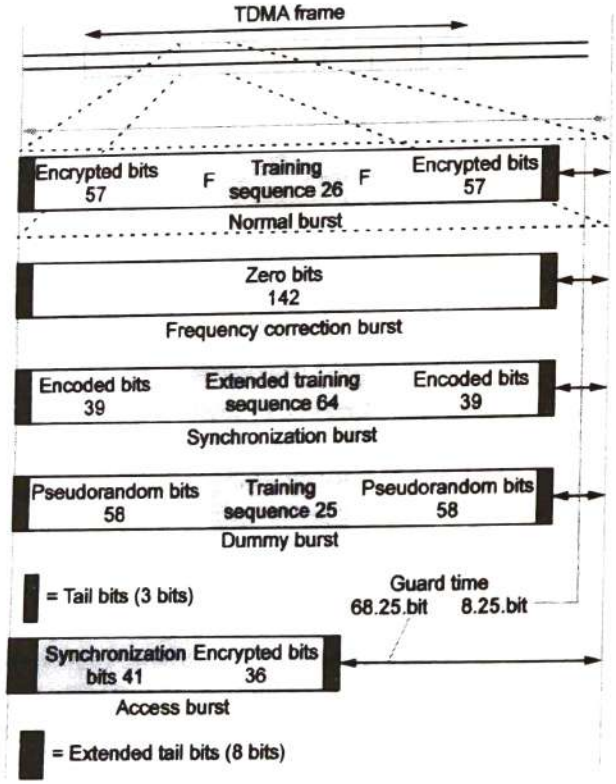


Fig. 5.6.2 GSM burst frames

- Table 5.6.1 summarizes the burst type, its purpose, used by channels and its content.

Burst type	Purpose	Used by	Contents
Normal	Used to carry information on traffic and control channels.	BCCH, PCH, AGCH, SDCCH, CBCH, SACCH, FACCH, TCH	• Two blocks of 57 bits each for traffic. • Training sequence (26 bits) • Steal flags (1 bit each) to indicate that FACCH has temporarily stolen 57 bits. • Tail bits (always 000) • Guard period : 8.25 bit durations.
Frequency correction	Used for frequency synchronization of the mobile.	FCCH	• 142 frequency correction bits. • Tail bits. • Guard period : 8.25 bit durations.
Synchronization	Used for frame synchronization of the mobile.	SCH	• Two blocks of 39 bits for TDMA frame structure information. • 64 synchronization bits. • Tail bits. • Guard period : 8.25 bit durations.
Access	Used for random and handover access.	RACH FACCH	• 41 synchronization bits. • 36 bits of access information. • Tail bits. • Guard period : 68.25 bit durations. A longer GP is used because it is the first transmission from the mobile - no timing advance information is available.
Dummy	USed when no other channel requires a burst to be sent and carries no information.	All free TS on C0. (1-7)	• Pattern consists of training sequence and a mixed bits pattern.

Table 5.6.1

University Questions

1. *Determine frame efficiency of a TDMA frame structure used in GSM system.* **GTU : Winter-14, Marks 7**
2. *With the help of timing parameters. explain frame structure for GSM.* **GTU : Summer-15, Marks 7**

5.7 Authentication and Security in GSM

- GSM is a public system operating on radio frequencies. The information on the air interface needs to be protected to provide user data confidentiality (including speech) and to present fraudulent access and ensure subscriber privacy.
- The basic security mechanisms include :
  1. User authentication ; to prevent access by unregistered users.
  2. Radio path encryption ; to prevent unauthorized listening.
  3. User identity protection ; to prevent subscriber location disclosure.
- In GSM, the mobile station consists of two parts : One the hardware and software specific to radio interface and second part contains the user specific data known as Subscriber Identity Module (SIM).
- SIM has several functions and limited programs are possible by user. Most of the information contained in the SIM is protected against alteration. Because of security functions duplication of SIM is difficult as these provides a high degree of protection against fraudulent access to the network.
- The basic security aspects supported by the GSM SIM are :
  1. Authentication algorithm (A_3)
  2. Subscriber authentication key (K_i)
  3. Cipher key generation algorithm (A_8)
  4. Cipher key (K_c)
  5. Control of access to SIM stored data and functions performed in the SIM.
- SIM storage capability includes following data :

1. Administrative information	:	This indicates the SIM mode of operation (normal, type approval)
2. IC card identification	:	This is the number that uniquely identifies the SIM and the card issues.
3. SIM service table	:	This indicates optional services that are provided by SIM.
4. Information mobile subscriber identity	:	This unambiguously identifies subscriber.

5. Location information	:	This comprises the Temporary Mobile Subscriber Identity (TMSI) and Location Area Information (LAI).
6. Cipher key and cipher key sequence number	:	The cipher key is a sequence of symbols needed to encrypt or decrypt carried information.
7. Broadcast control channel information	:	This is the list of carrier frequencies to be used for call selection.
8. Forbidden PLMNs	:	These are held by the SIM to avoid unnecessary registration attempts.
9. Language preference	:	This indicates the Man-Machine Interface (MMI) languages preferred by subscriber.

5.7.1 Authentication

- In order to prevent fraudulent use of subscriber and mobile identities, GSM uses two methods.
  1. Use of personal identity number (typically 4-digit) which is stored in SIM. A user wishing to make a call enters the PIN which is checked by SIM, without transmission on the radio interface.
  2. In this stage, GSM interrogates the units. This is controlled from MSC/VLR and occurs at call set-up, location updating, handover etc.
- After the mobile user has made on access and service request, the network checks the identity of the user by sending a Random Number (RAND) of 128-bits to the mobile. The mobile uses the RAND, K_i and A_3 algorithm to produce 32-bit signed response (SRES). The network uses the same RAND, K_i and A_3 algorithm to produce a SRES which is then checked against the response from the mobile and

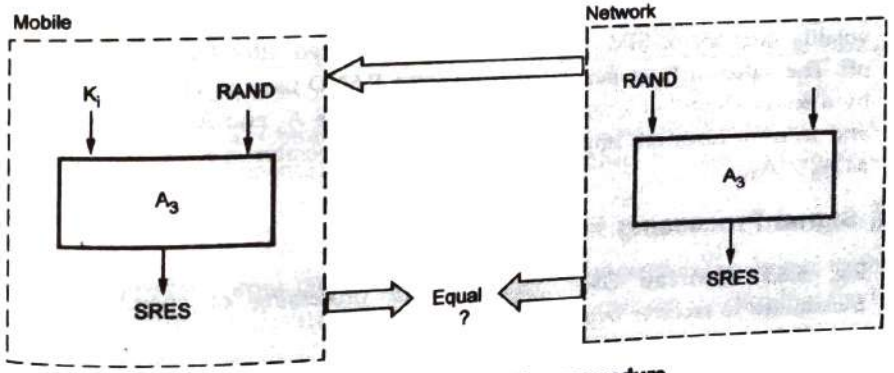


Fig. 5.7.1 GSM authentication procedure

access continues only if the two response match. The GSM authentication procedure is illustrated in Fig. 5.7.1.

- In order to maintain desired security level, A_3 is devised so that computation of SRES from RAND and K_i is straight forward but the computation of K_i from RAND and SRES is complex. A_3 is operator dependent, which is a further reason for performing the network SRES computation at mobile HLR.
- Authentication of mobile users can be carried out on both mobile originated call and mobile terminated call set-up, on location updating, and on activation of supplementary services. As the authentication sets are used up in VLR, further sets are requested from the HLR.

5.7.2 Ciphering / Encryption

- Ciphering or encryption is employed in GSM to prevent unauthorized listening. Encryption is used for all data transmitted between mobile and base station in dedicated state. It includes user information (voice, data), user related signalling (called numbers) and system related signalling (handover signalling).
- Ciphering is achieved by "exclusive OR-ing" the 114 data bits of each normal burst with a pseudo random sequence. Deciphering follows exactly the same operation and reproduces the original 114-bit data ("exclusive OR-ing twice with the same pseudo random reproduces the original data stream".) The algorithm employed for generating pseudo random sequence is known as A_5 and cipher key generation is algorithm is known as A_8.
- The A_5 algorithm generates the pseudo random sequence from two inputs one being the frame number (22-bits) and other being a key K_c (64-bits) between mobile and network. Two different pseudo random sequences are generated by A_5 both for uplink and downlink.
- K_c is actually computed during GSM authentication process. It is stored in non volatile memory of SIM. It is therefore remembered after the mobile is switched off. The value of K_c is generated from same RAND used in authentication process by a secret algorithm known as A_8. The algorithms A_3 and A_8 are always together and in most cases are implemented as a single operator specific algorithm known as A_3 / A_8.

5.8 Signal Processing in GSM

- Fig. 5.8.1 illustrates GSM operations for processing of speech signal from transmitter to receiver over logical traffic channels.

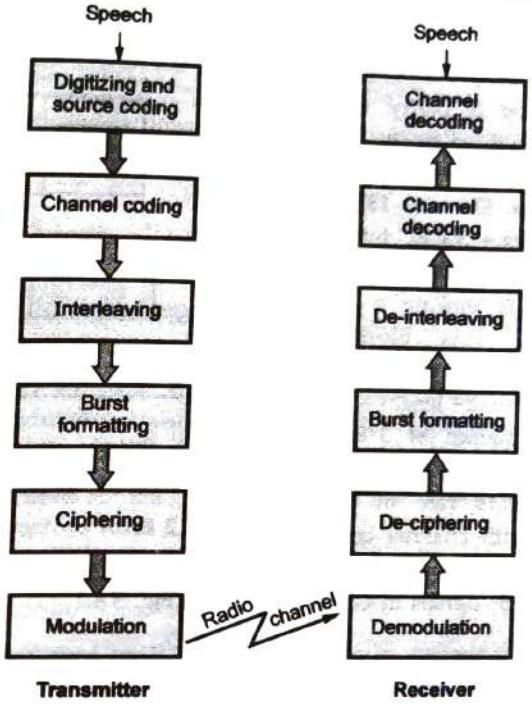


Fig. 5.8.1 GSM speech signal processing

Speech coding

- GSM speech coder uses Residually Excited Linear Predictive coder (RELP) along with LongTerm Predictor (LTP). The RELP provides 260-bits for each 20 ms blocks of speech which gives bit rate of 13 kbps.
- Normally a person speaks on average for less than 40 % of the time. Therefore, GSM system can operate in Discontinuous Transmission Mode (DTX) by incorporating Voice Acitivity Detection (VAD) in speech coder. This provides longer battery life for subscriber and reduces radio interference.
- At receiving end a Comfort Noise Subsystem (CNS) introduces background acoustic noise to compensate for the annoying switched muting occuring due to DTX.

Channel coding

- The speech coder output bits are grouped for error protection, according to their significance in speech quality. The quality of speech produced by encoding the bits in 260-bit block can be divided into three classes -

1. Class Ia : 50-bits (Most sensitive to bit errors)

2. Class Ib : 132-bits (Moderately sensitive to bit errors)
3. Class II : 78-bits (Least sensitive to bit errors)

- In class Ia type 3 parity check (CRC) bits are added to them to facilitate detection of noncorrectable errors at receiver. The next 132-bits with these 50-bits + 3 CRC bits are reordered and appended by four trailing zero bits making a total 189-bits block. This block is encoded using 1/2 convolutional encoder with constraint length K = 5, making this sequence of 378-bits. The error protection coding increases the data rate of GSM speech signal with channel coding to 22.8 kbps. The error protection scheme for speech signals in GSM is shown in Fig. 5.8.2.

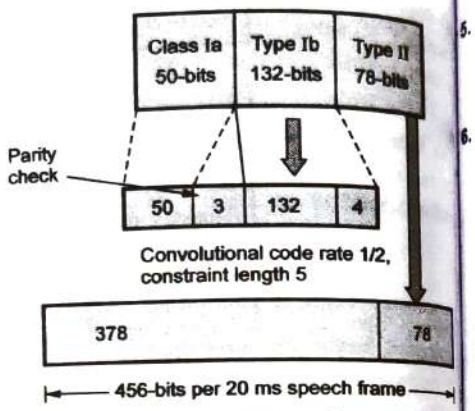


Fig. 5.8.2 Error protection scheme in GSM

3. Interleaving

- For minimizing the effect of sudden fades on received data, the total 456 encoded bits are broken into 8 sub-blocks of 57 bits each. These 8 sub-blocks are spread over eight consecutive TCH time slots.
- If any burst is lost due to interference or fading, channel coding ensures that enough bits will still be received correctly to allow error correction to work. A TCH time slot carriers two 57-bits of data from two different 20 ms speech segment. Fig. 5.8.3 shows diagonal interleaving of TCH/SACCH/FACCH data (speech frames) within time slots.

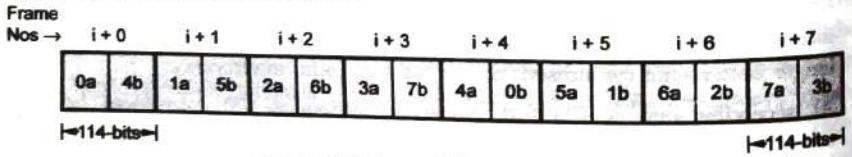


Fig. 5.8.3 Diagonal interleaving

4. Ciphering

- Ciphering modifies the contents of eight interleaved blocks by using encryption techniques. In order to enhance security, different encryption algorithms are used for different calls. Ciphering algorithms A3 and A5 are used to prevent unauthorized network access and radio privacy respectively. A3 algorithm provides authentication to each mobile by verifying passcode within SIM with

cryptographic key at MSC. A5 algorithm provides scrambling for 114 coded data bits sent in each TS.

5. Burst formatting

- Burst formatting adds binary digits to ciphered blocks in order to help synchronization and equalization of received signal.

6. Modulation

- GSM uses 0.3 GMSK modulation where 0.3 describes the 3 dB bandwidth of Gaussian pulse shaping filter with relation to the bit rate (BT = 0.3).
- GMSK is a special digital FM modualtion. Binary ones and zeros are represented in GSM by shifting RF carrier by ± 67.708 kHz. The GSM channel data rate is 270.833333 kbps, which is four times RF carrier shift. This minimizes the BW occupied by modulation spectrum which improves channel capacity.
- The MSK modulated signal is passed through Gaussian filter to eliminate rapid frequency transitions so that it will not spread energy into adjacent channels.

5.9 GSM Call Procedure

5.9.1 Call from Mobile

- A channel is requested on RACH and may be in contention with other mobile by using slotted ALOHA. If a request is received without a collision a dedicated control channel AGCH is assigned.
- On receiving access grant, mobile proceeds with call setup on the allocated dedicated control channel by sending setup message to network. The network accepts the call establishment on SDCCH .
- When called party alerting has been initiated, an alerting message is sent to the mobile over the FACCH and a ringing tone may be generated by the network and sent to mobile.
- When call has been accepted at the remote end, a connect message is transferred to the mobile, indicating that the connection is established in the network. The mobile station responds by sending connect acknowledge message and enters in active state.

.No	System activity	Channel	Mobile activity
1.	System overhead parameters and other overhead messages.	BCCH →	(Idle Updated) monitor BCCH and CCCH (PCH) for mobile control message.
2.	Receive channel request.	← RACH	Generate channel request.

3.	Assign stand alone dedicated control channel.	AGCH →	Receive stand alone dedicated control channel assignment and store in memory.
4.	Receive call establishment request.	← SDCCH	Send call establishment request.
5.	Request authentication from mobile.	SDCCH →	Receive authentication request.
6.	Receive and check authentication.	← SDCCH	Authentication response.
7.	Request mobile to transmit in ciphered mode.	SDCCH →	Receive cipher mode request.
8.	Receive acknowledgement.	← SDCCH	Acknowledge cipher mode request (all further transmission in cipher mode).
9.	Receive setup request.	← SDCCH	Send setup message and desired number.
10.	Send call proceeding indication to mobile and route call to desired number.	SDCCH →	Receive call preceeding indication.
11.	Assign traffic channel to mobile.	SDCCH →	Receive traffic channel assignment.
12.	Receive traffic channel acknowledgement on allocated channel.	← FACCH	Switch to traffic channel and send an acknowledgement.
13.	Send alert signal that called number is available and the phone is ringing.	FACCH →	Receive alert signal ringing sound.
14.	Send connect message when called party accepts.	FACCH →	Receive connect message.
15.	Receive connect accept response.	← FACCH	Acknowledge connect message and switch to traffic channel.
16.	Exchange of user data.	← TCH →	Conversation commences on TCH.

Table 5.9.1 Call establishment from a mobile

5.9.2 Call to Mobile

- A paging message is routed to the traffic area in while the mobile is registered and transmitted on paging channel.

- When access grant is received from the base station the mobile responds with call confirmed message on dedicated control channel. A traffic channel is then allocated and call proceeds.

Sr.No	System activity	Channel	Mobile activity
1.	System overhead parameters and other overhead messages.	SDCCH →	(Idle Updated) monitor BCCH and CCCH (PCH) for mobile control message.
2.	Receive incoming call, generate a paging message.	BCCH →	Receive paging message.
3.	Receive channel request .	PCH →	Generate channel request.
4.	Assign stand alone dedicated control channel.	← RACH	Receive stand alone dedicated control channel assignment and store in memory.
5.	Receive paging acknowledgement.	AGCH →	Answer paging message from network.
6.	Request authentication from mobile.	← SDCCH	Receive authentication request.
7.	Receive and check authentication.	← SDCCH	Authentication response.
8.	Request mobile to transmit in ciphered mode.	SDCCH →	Receive cipher mode request.
9.	Receive acknowledgement.	← SDCCH	Acknowledge cipher mode request, switch to cipher mode.
10.	Send setup message of incoming call.	SDCCH →	Receive setup message.
11.	Assign traffic channel to mobile.	SDCCH →	Receive traffic channel assignment.
12.	Receive traffic channel acknowledgement on allocated channel.	← FACCH	Switch to traffic channel and send an acknowledgement.

13.	Send alert signal.	FACCH	Receive alert signal and generate ringing sound.
14.	Send connect message when user off-hook.	FACCH	Receive connect message.
15.	Receive connect accept response.	FACCH	Acknowledge connect message and switch to traffic channel.
16.	Exchange of user data.	TCH	Conversation commences on TCH.

Table 5.9.2 Call establishment to a mobile

5.9.3 Call Setup

- Call setup in GSM consists of certain necessary operations. Some of the operations are -
  1. Interrogation phase
  2. Radio resource connection establishment
  3. Service request
  4. Authentication
  5. Ciphering mode setting
  6. IMEI check
  7. TMSI reallocation
  8. Call initiation procedure
  9. Assignment of a traffic channel
  10. Call confirmation, call accepted and call release

5.9.4 Radio Resource Connection Establishment

- The MSC/VLR initiates the call setup process by sending a message to the appropriate BSC. The BSC sends a paging command message to the appropriate BTS, finally BTS sends a paging request to the appropriate MS.
- Steps involved in radio resource connection establishment phase are-
  1. The MSC initiates the call setup process by sending paging message to BSC.
  2. The BSC sends paging command message to appropriate BTSs.
  3. The BTS sends a paging request message to MS on PCH.

4. The MS responds to paging request message by sending a channel request message to BTS on RACH.
5. BTS sends a channel required message to BSC.
6. BSC sends channel activation message to BTS.
7. BTS acknowledges the channel activation message.
8. BSC sends an immediate assignment command message to BTS.
9. The immediate assign command is sent by BTS to MS over AGCH.

- Fig. 5.9.1 illustrates steps involved in radio resource connection establishment.

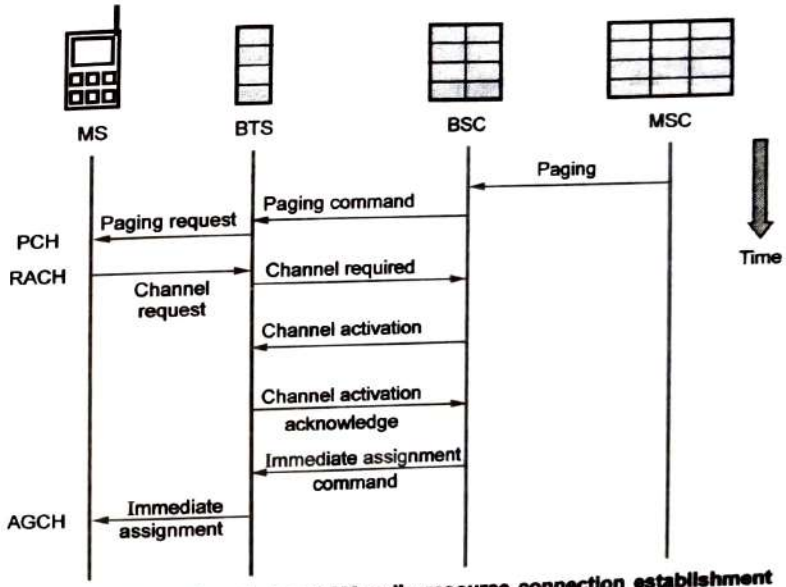


Fig. 5.9.1 Messaging during GSM radio resource connection establishment

5.10 GSM Handoff Procedure

GTU : Summer-16

- Handoff or handover occurs when an active MS changes cells. BSC of the location initiates handover. Several different types of handover scenarios are possible, such as
  1. Intra-BSC handover
  2. Inter-BSC handover
  3. Inter-MSC handover

5.10.1 Intra-BSC Handoff / Handover

- The intra-BSC handover process involves following steps.
  1. The intra-BSC handoff occurs between two cells controlled by BSC. During the call, MS will measure the strength and quality of the signal on the TCH and signal strength from the neighboring cells. MS will evaluate and assess the Received Signal Strength (RSS) average for each cell.
  2. The BTS will send the results of measurements on the TCH to the BSC. In the BSC, the function is activated when the placement is required to handover to another cell.
  3. When the handover is done, BSC will check whether the channel had requested be met by another cell, if not the BSC will be the new BTS to enable TCH.
  4. BSC will ask the BTS for a long time to send a message to MS with information about the frequency, time slot, and the output power for the change.
  5. MS choose a new frequency handover and access to the appropriate time slot.
  6. When the BTS to detect the handover, the BTS will send the information contains the physical "timing advance" (the distance between MS to the BTS) to MS over FCCH. BTS also sends a handover detection message to BSC.
  7. MS sends a handover complete message to BSC.

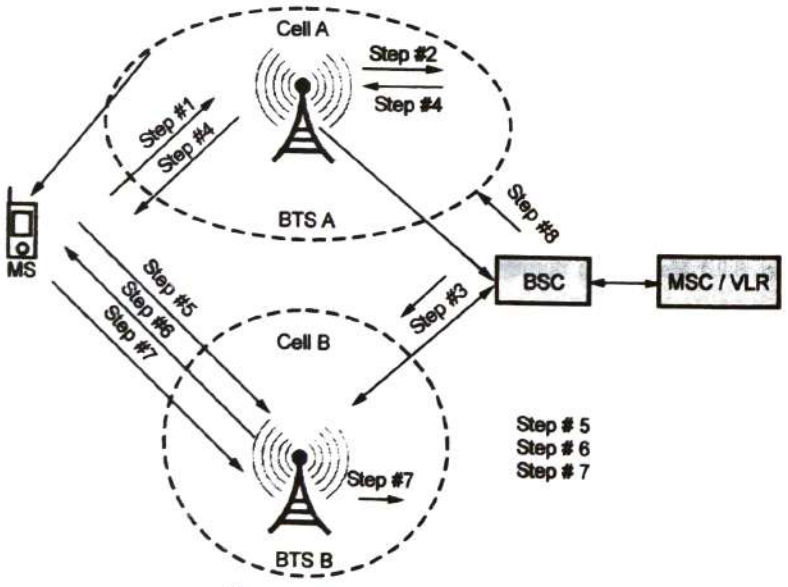


Fig. 5.10.1 Intra-BSC handover

8. BSC sends message to old BTS to deactivate the old TCH and its associated signalling channel SACCH.

- Fig. 5.10.1 illustrates intra-BSC handover process.

5.10.2 Inter-BSC Handoff

- In inter-BSC handover, the mobile has moved to a cell that is in different location area and therefore has different BSC. The serving BSC decides that the call must be handed over to a new cell that belongs to different BSC.
- The inter-BSC handover process involves following steps.
  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 1 B.
  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 (1 B).
  8. Timing advance information is sent to the MS.
  9. BTS 1 B sends handover detection message to BSC B.

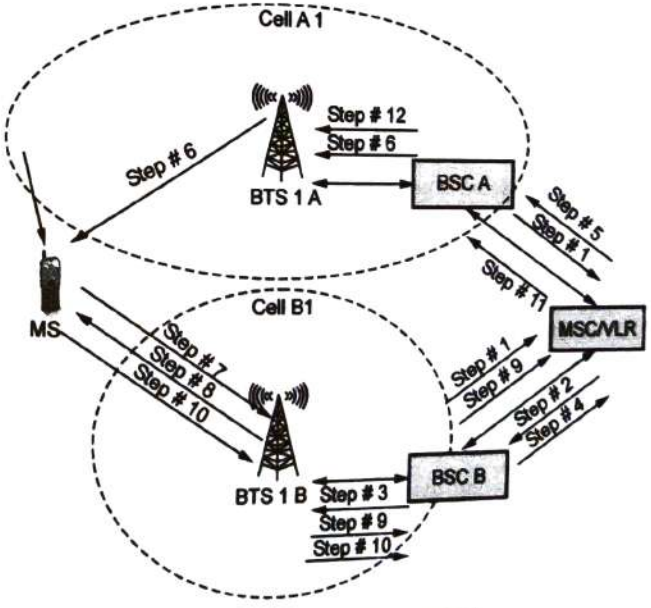


Fig. 5.10.2 Inter-BSC handoff

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 (1 A).

- Fig. 5.10.2 illustrates inter-BSC handover process.
- The basic difference between intra-BSC handover and inter-BSC handover is that two BSCs and the MSC are involved in an inter-BSC handover while the intra-BSC handover involves only two BTS connected to the same BSC.

University Question

1. *What is hand over in GSM? Give comparison of hard hand over and soft hand over.*
   GTU : Summer-16, Marks 7

5.11 GSM Speech Coding and Decoding

- Speech and data transmission in the GSM and associated control data signaling system require advanced digital signal processing and modern methods of coding.
- Speech coding is a process of waveform compression. Instead of generating quantized and processed samples of the input signal, the encoder determines the quantized parameters of the speech source model.
- Modern GSM uses three speech coding standards :
  1. Full Rate speech coding (FR) 2. Half Rate speech coding (HR)
  3. Enhanced Full Rate speech coding (EFR)

5.11.1 Full Rate Speech Coding (FR)

- Fig. 5.11.1 shows block schematic of GSM full rate speech encoder. Its major blocks are Long Term Prediction (LTP) filter, Regular Pulse Excitation (RPE) analysis block. (Refer Fig. 5.11.1 on next page)
- The bit rate of the codec is 13 kbit/s, or 1.625 bits/audio sample (often padded out to 33 bytes/20 ms or 13.2 kbit/s). The codec is widely used in networks around the world.

5.11.2 Half Rate Speech Coding (HR)

- The half rate speech coding uses analysis-by-synthesis procedure to find the best code word characterizing the excitation signal for each 20 ms signal frame.
- The best code word is found by applying each code word as an excitation for the Code-excited linear prediction (CELP) synthesizer.

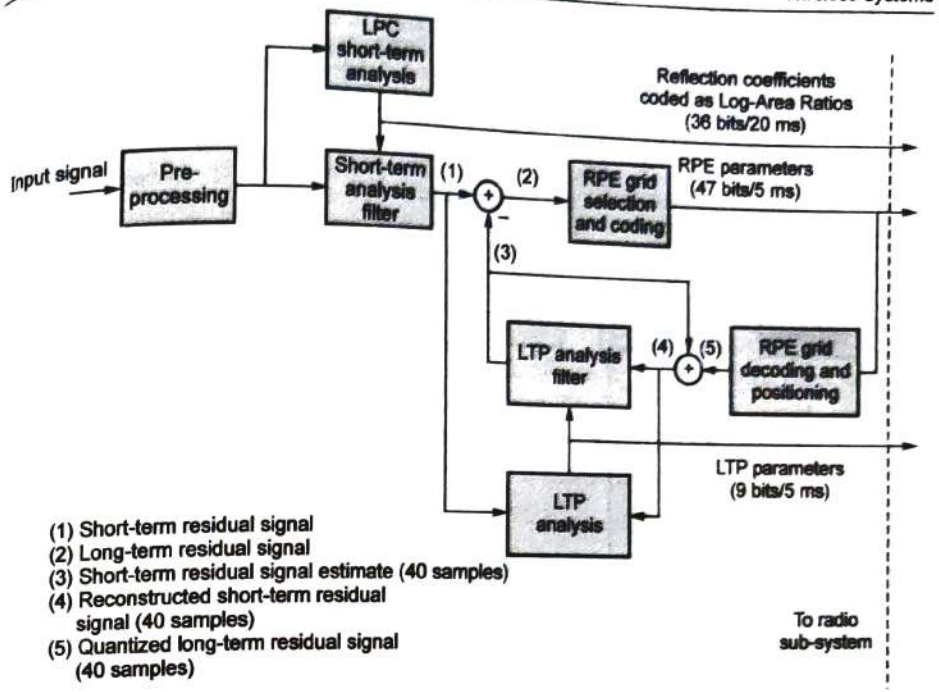


Fig. 5.11.1 GSM full rate speech coding

- The synthesized speech signal is then compared with the input speech signal and a difference signal is calculated. This difference signal is weighted by a spectral weighting filter with the characteristics W(z) and a second weighting filter C(z) generating error signal e(n). Fig. 5.11.2 shows block diagram of GSM half rate speech encoder. (Refer Fig. 5.11.2 on next page)
- The filter denoted by A(z) is a short-term spectral filter, whereas B(z) denotes the long-term filter with the lag L and filter coefficient β.
- In the process of speech analysis-by-synthesis, the encoder calculates 18 parameters characterizing each 20 ms frame. The parameters of a single frame are represented by 112 bits, which is equivalent to the 5.6 kbit/s data rate on the output, of the half rate encoder.

5.11.3 Enhanced Full Rate Speech Coding (EFR)

- The operation of Enhanced Full Rate (EFR) speech coding encoder is based on the Code-Excited Linear Predictive (CELP) coding model. Fig. 5.11.3 shows block diagram of enhanced full rate speech coding. (Refer Fig. 5.11.3 on next page)
- The speech encoder operates on 20-ms blocks of speech samples. The EFR encoder generates the data stream at the rate of 13 kbit/s.

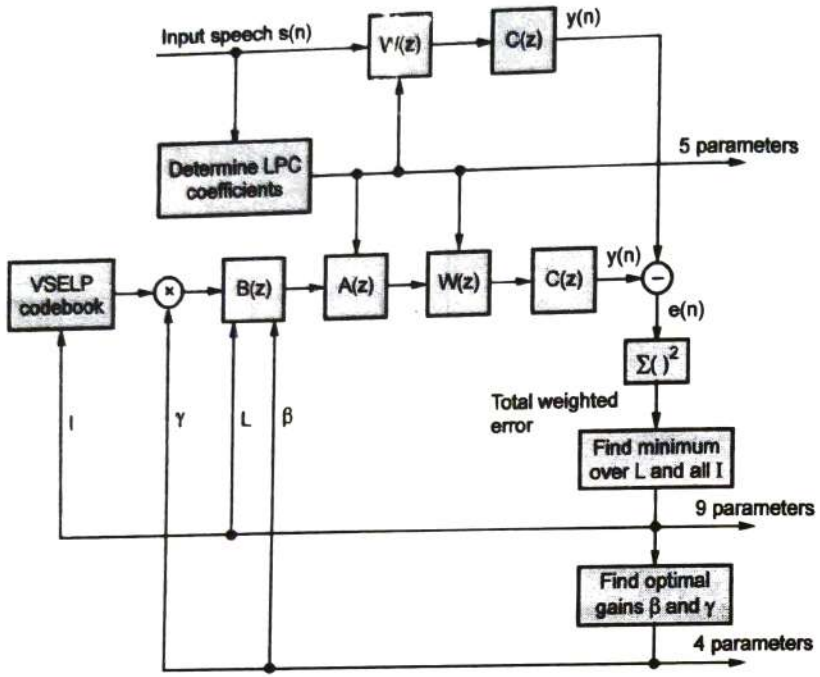


Fig. 5.11.2 GSM half rate speech encoder

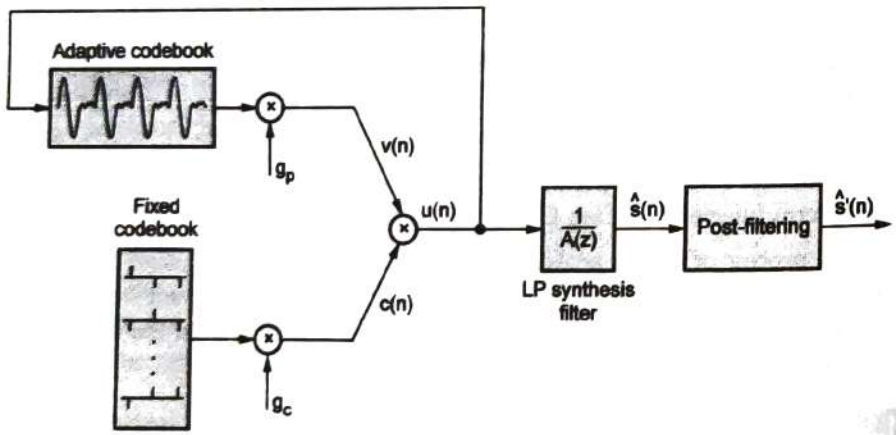


Fig. 5.11.3 GSM Enhanced full rate coder

5.11.4 Comparison of GSM Speech Coder

- Comparison of important parameters of various GSM speech encoders is summarised in Table 5.11.1.

Speech codec/Parameters	Full Rate speech coding (FR)	Half Rate speech coding (HR)	Enhanced Full Rate speech coding (EFR)
Coding Method	RPE-LTE	VSELP	ACELP
Bit Rate (Kbits/sec)	13	5.6	12.2
Compression	8	18.4	8.5

Table 5.11.1

5.12 Data Transmission in GSM

- GSM permits the integration of different voice and data services and the inter-working with existing network, offering 3 types of services :
  1. Bearer service
  2. Tele service
  3. Supplementary service
- In GSM system the protocol called Radio Link Protocol (RLP) is implemented in the terminal, mobile station or the **Terminal Adaptation Functions** (TAF) block. This protocol is based on the ARQ technique. Because of this, constant high transmission quality is assured but data rate and transmission delays are variable.
- The data rate substantially decreases during handover due to the repetition of the frames which are lost during the change of the serving base station.
- There are 21 different services associated with data transmission, starting from very slow asynchronous transmission at 300 bit/s and ending with direct packet access in synchronous mode at the data rate of 9.6 kbit/s.

5.12.1 Rate Adaptation

- In GSM data services the data rate has to be adjusted to the rate of 22.8 kbit/s used in GSM bursts and also to the data rate applied in the fixed circuits of the GSM network connecting BTS, BSCs and MSCs.
- To accommodate the data rates of GSM bursts and fixed networks, different adaptation functions are applied depending on the configuration of the actual data transmission. These adaptation functions are RA0, RA1, RA2

. RA0

- The RA0 adaptation function is used in asynchronous interface. This function realizes the transformation of the asynchronous stream generated by the user to a synchronous stream at the first allowable higher data rate.

- This operation is performed by adding or subtracting some stop bits contained in the asynchronous stream.

2. RA1

- The RA1 adaptation function used to adapt the data stream to intermediate rates. Its input is the output of a RA0 block or the synchronous data.

3. RA2

- The RA2 adaptation function used to convert the data stream at the output of RA1 block to a 64 kbit/s stream.
- The multiplexed data streams are placed in subsequent bit positions in the octets.

4. RA1'

- The RA1'adaptation function transforms the rates of data received from the terminal (DTE) to the rates used in a radio interface. The data stream is supplemented with control bits.
- The source of data for RA1' is either the output of RA0 or a synchronous stream.

5.12.2 Channel Coding

- Channel coding in data transmission depends on the data rate of the radio interface. In RA1' adaptation function the receive data stream rate is 3.6, 6.0 or 12 kbit/s. This data stream can be transmitted using the full- or half-rate traffic channel.
- All possible channel coding configurations can be possible. For different configuration, the level of protection can be very different, depending on the input data rate and required quality.

5.12.3 Radio Link Protocol (RLP)

- In order to ensure high quality of service, transparent data transmission requires data exchange protocol which is external to the GSM system. But it may not be feasible due to high time consumption and a large amount of system resources used because the block chain for transmitting the signaling information can be very long.
- The block chain consists of a data terminal (DTE), mobile station (MS), base station system (BSS), mobile switching center (MSC), interworking function (IWF) block, the external fixed network and the DTE of the second user.
- If the other user is also a subscriber of a mobile system the blocks listed above are again used in the transmission chain in the reversed order. Therefore,

non-transparent transmission using Radio Link Protocol (RLP) is more advantageous in many cases.

- If the RLP is applied, error protection is performed between Terminal Adaptation Functions (TAF) and IWF blocks using a kind of ARQ procedure. Fig. 5.12.1 shows RLP frame structure. The total length of RLP frame is 240-bits.

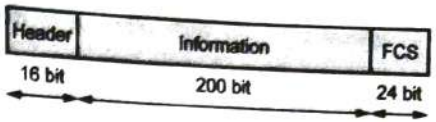


Fig. 5.12.1 RLP frame structure

Header

- The frame starts with a 16-bit header which performs control functions such as establishing or releasing an RLP link, counting the frames and signaling the presence of erroneous frames which have to be retransmitted.

Information

- The next field is information field .It has the length of 200 bits and contains user data.

Frame Check Sequence

- The frame is ended with a 24-bit Frame Check Sequence (FCS) calculated by dividing the frame contents by the cyclic code polynomial.

5.13 IS 95 / CDMA

GTU : Winter-14, Summer-15,16

- IS-95 system uses Code-Division Multiple Access (CDMA) by means of Direct Sequence Spread-Spectrum modulation (DS-SS).
- Code Division Multiple Access (CDMA) is one of the basis for many of the commercial 2 G cellular systems around the world and is also used in many other types of communications systems, including Personal Communication System (PCSs), fixed wireless (wireless local loop), Global Positioning System (GPS) and the OmniTRACS satellite system for transportation logistics. CDMA is also known as IS-95, which refers to original ITU IS-95 wireless Interface protocols.
- CDMA system users are distinguished from each other by a code rather than by alloted time slot as in GSM. A single physical link (channel) is 1.23 MHz wide and typically 12 subscribers share the same link simultaneously. An important feature of CDMA is that neighbouring cells or sectors in cells can use the same physical channel.

5.13.1 Principles of CDMA

- CDMA systems allow many data signals to be multiplexed and transmitted over a wireless channel at the same time and in same frequency band without interfering with each other. It is done by deliberately spreading the spectrum occupied by user with high speed codeword unique to that user. The spectrum spreading is done by multiplying the user data by identifying code and modulating a carrier with resultant waveform (spread spectrum). At the receiver original data is recovered by correlating the demodulated waveform by original spreading code.
- The spread spectrum technique used in CDMA is of direct sequence type. The data signals to be transmitted are modified through the use of pseudo-noise code (PN code). In time division systems, channels are separated by time slot they occupy but in code division systems, channels are distinguished according to which PN code they use.
- The PN codes used in a system are orthogonal means the codes should not correlate among themselves nor they be time shifted version of each other. Therefore, each signal with a unique PN code can be detected from other signals. When a PN code is auto-correlated, the result is high (1) but when cross-correlated with other PN code in the same set, the result is zero (0). PN coded sequence are generated by using one or more shift registers with specific feedback connections. This PN spreading code is often called as *chipping code*. An important characteristic of spread spectrum system is its processing gain G_P, which is proportional to the ratio of spreading code rate to the data rate.

$$G_P = \frac{R_{chip}}{R_{data}}$$

PN codes used in CDMA

- CDMA system uses three types of PN code.
  1. Walsh code
  2. Long PN code
  3. Short PN code

1. Walsh code : CDMA use of walsh code is of 64 different orthogonal codes used on

a. Downlink - For different user (spreading). It is a code channel.

b. Uplink - Not to differentiate users but for modulation.

2. Long PN code : 42-bit code

a. Down link - Used for data scrambling.

b. Uplink - For identifying mobile station (spreading).

3. Short PN code : 16-bit code

a. Down link - Used to identify base stations.

b. Uplink - Mobile uses this code for extra signal robustness without offset.

Features of CDMA

1.	Transmit rate of one channel	: 192 kbps
2.	Number of time slots in one CDMA channel	: 64
3.	Average data rate for each user	: 3 kbps
4.	Two voice coding schemes	: 8 kB/s, 13 kB/s
5.	Vocoder rate	: 1.25 Mbits/s
6.	Power updates of mobile user	: Every 1.25 ms
7.	Voice and data communication	: 1.25 MHz radio carrier

5.13.2 CDMA Architecture

- CDMA architecture is shown in Fig. 5.13.1.

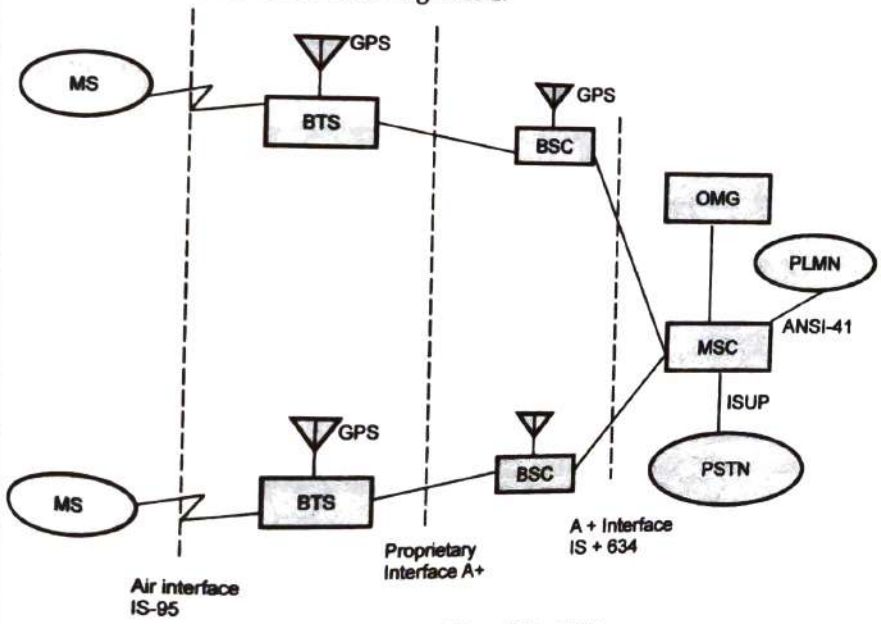


Fig. 5.13.1 CDMA architecture

- CDMA interfaces are as follows.
  1. A+ or A - bis : Interface between BSC and BTS (proprietary interface depends on vendor).
  2. IS + 634 : An open interface between MSC and BSC
  3. ANSI - 41 : An interface with other PLMNs.
  4. ISUP (ISDN user part) : Interface with user part.
  5. IS - 95 : This is an air interface between base station substation and mobile.

5.13.3 CDMA Frequency Reuse

- With CDMA all the frequency band can be used in all cells. In CDMA, an RF channel uses carrier of 1.2288 Mb/sec with QPSK modulation. The bandwidth of a channel is 1.25 MHz. Because of this system capacity is increased many fold.
- Spread spectrum technique used frequency diversity this is very useful in mobile environment with multipath fading. CDMA system uses full 1.25 MHz BW for voice transmission.
- Since the frequency is not changing when mobile is crossing the cell, handoff is not required. Instead, CDMA system uses **soft handoff**. In soft handoff, mobile communicates with two cells simultaneously instead of switching from one cell to other. This gives space diversity of antennas. The comparison of hard handoff and soft handoff is shown in Fig. 5.13.2 (a) and (b).

A] Hard Handoff

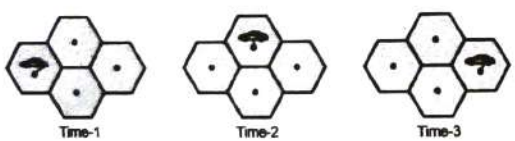


Fig. 5.13.2 (a)

Short blanking tones as mobile moves to cell.

B] Soft Handoff

Fig. 5.13.2 (b)

Mobile communicates with two base stations simultaneously hence no data lost.

5.13.4 CDMA Frequency Channels

- By using direct-sequence spread-spectrum, an RF channel at base station supports 64 orthogonal CDMA channels. The channels and their types are as under -

CDMA channels		
55	–	Traffic channels
07	–	Paging channels
01	–	Synch channel
01	–	Pilot channel

- The total BW of CDMA is 1.25 MHz to be used for 55 voice channels. Therefore 22.7 kHz BW is allocated to each channel.
- Since all channels can be used in all sectors of all cells therefore CDMA is more efficient in spectrum compared to any other system. In CDMA both forward and reverse channels are different.

5.13.5 Forward Channel / Downlink

- The downlink (forward channel) refers to transmission from the mobile station to base station. On the downlink, the PN codes are used as follows :
  1. **Walsh codes** - To differentiate users (spreading),
  2. **Short PN code** - To identify the cell (base station),
  3. **Long PN code** - For data scrambling.
- Total downlink channels 64 for each carrier, out of which traffic channels are 55. The downlink traffic channels are used for information specific to MS during a call. It carries the control channels and user data (transmission and reception of speech, data and signalling). The basic user data rate is 9.6 kB/s and this is spread to a channel chip rate of 1.2288 Mchips/s using a combination of techniques.
- The forward CDMA channel comprises of pilot channel, synchronization channel, paging channel and speech channels. The direct sequence form is created by multiplexing these signals with different Pseudo-random Noise (PN) sequence. The orthogonal PN sequence can be recovered without any interference. When PN sequence are not orthogonal, there will be some mutual interference between signals.
- The use of orthogonal PN sequence is desirable. A Walsh code PN-sequence is used by base stations. The Walsh function consists of 64 orthogonal binary

sequences, each of length of 64-bits. It can provide 64 independent logical channels for all users on forward link.

- In Walsh code, channel '0' is assigned to the pilot channel to keep mobile receivers phase aligned with base station. Also a short code is used for synchronizing and a long code for encryption of voice and control data. Fig. 5.13.3 shows spreading in CDMA voice channel.

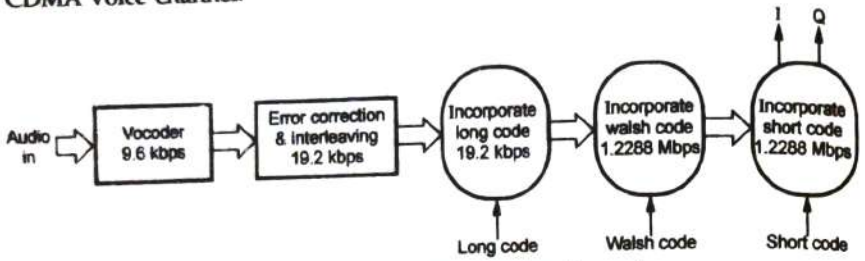


Fig. 5.13.3 CDMA forward voice channel

- The processing gain G_P, is given by -

$$G_P = \frac{B_{RF}}{B_{BB}} = \frac{\text{RF bandwidth}}{\text{Baseband bandwidth}}$$

$$G_P = \frac{1.2288 \times 10^6}{19.2 \times 10^3} = 64 = 18.06 \text{ dB}$$

Total spreading gain

$$G_P = \frac{1.2288 \times 10^6}{89.6 \times 10^3} = 128 = 21.1 \text{ dB}$$

- Such 64 orthogonal channels are transmitted on one RF carrier then QPSK modulator is used to modulate or single carrier. Fig. 5.13.4 shows multiplexing of CDMA channels.

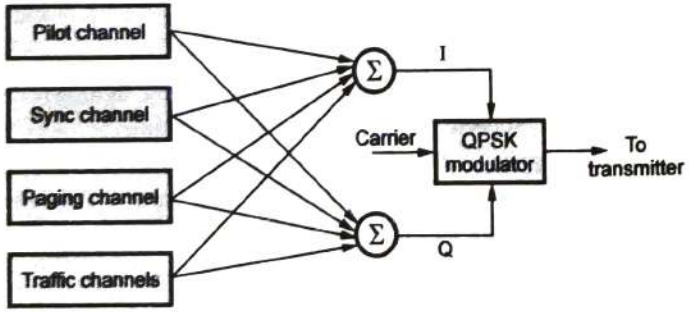


Fig. 5.13.4 Multiplexing CDMA channels

- The structure of downlink/forward channel is shown in Fig. 5.13.5.

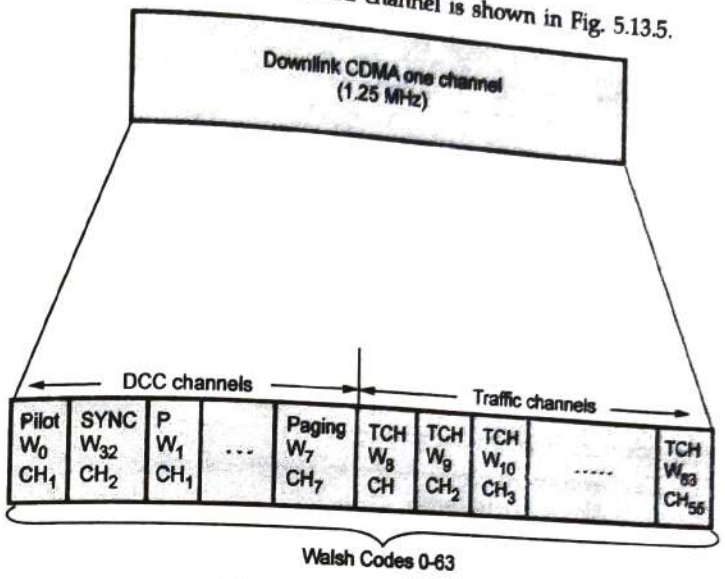


Fig. 5.13.5 Downlink structure

13.6 Reverse Channel / Uplink

- The uplink refers to transmission from base station to mobile station. The uplink frequency is built and arranged differently from downlink frequency. (45 MHz below forward channel frequency). The uplink (reverse channels) are coded with 1/3 rate convolutional PN long code. The unique MS equipment identifier is part of this PN code.
- On reverse channel, the PN codes are used as follows :
  1. Walsh codes are used for modulation (not to differentiate users).
  2. Short PN code is used by mobile for extra signal robustness without offset.
  3. Long PN code on uplink is used to identify the mobile station (spreading).

There are only two types of channels on reverse link, traffic channels and access channels. The access channels are almost identical to traffic channels. The data access channel occurs at a fixed rate of 4800 b/sec in 20 ms frames and contains information required by the network to properly log the mobile terminal into service.

A truly orthogonal channels cannot be used by mobile units, as there is no pilot channel (phase coherent). Assigning individual pilot channel to each mobile will require much larger bandwidth. Therefore error correction code used is more robust type. Fig. 5.13.6 shows CDMA reverse voice channel.

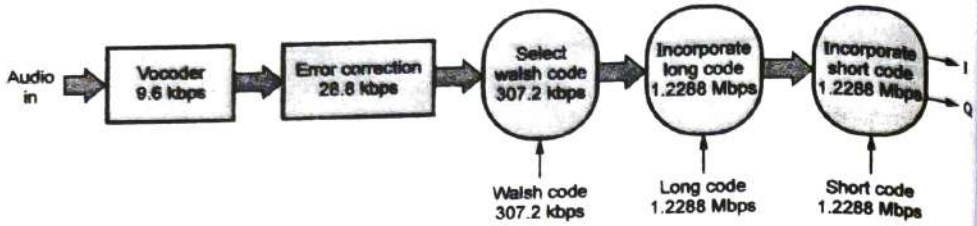


Fig. 5.13.6 CDMA reverse channel

- In reverse CDMA channel each code have different purposes. Long code is for distinguishing mobile, Walsh code is far decoding messages in presence of interference. The mobile unit uses offset QPSK modulation technique.
- The uplink structure is shown in Fig. 5.13.7.

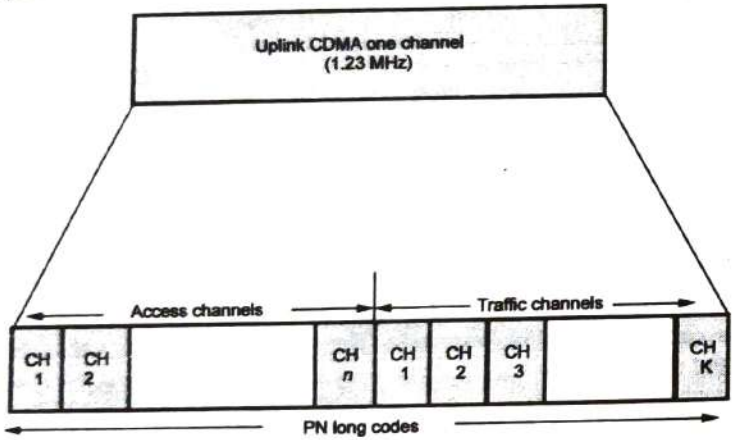


Fig. 5.13.7 Uplink structure

5.13.7 Voice Coding

- Variable rate vocoder is used for CDMA with 4 different bit rates i.e. 9600 bps, 4800 bps, 2400 bps and 1200 bps. When user is talking bit rate of 9600 bps is used and bit rate is reduced to 1200 bps during pauses.
- During a conversation, user actually talks for more than 50 %, during the pause the bandwidth allocated can be reassigned to other conversation.
- In FDMA or TDMA systems there exists two problems :
  1. When someone stops talking, the user assumes that the phone is disconnected. The reason is that there is always background noise even in quiet room. But CDMA system transmits this noise but codes it with lower rate (1200 b/sec) as it is not important.
  2. The vacated channel or time slots are not utilized for transmission. But CDMA system can do it efficiently hence the capacity of spectrum is increased.

5.13.8 Power Control

- Power control of mobile stations is important in CDMA systems.
- The power received at base station from mobile units must be within 1 dB.
- As mobile turns on it first measures power received from base station and then sets transmitter power assuming equal losses on reverse channel. This is known as open-loop power setting.
- The transmitted and received power are

$$P_T = -76 \text{ dB} - P_R$$

where, P_T is transmitted power in dBm

P_R is transmitted power in dBm

- If the mobile does not receives the acknowledgement from base station, it increases the power. The open-loop power setting is increased every 1.25 msec. This is called as **close-loop power control**. For a CDMA system it is necessary that all the received signal must have equal power. Otherwise it may not work properly as it suffers from near-far effect and weaker signal may last.
- The optimum power control also reduces draining of battery in mobile unit.

5.13.9 Soft Handoff

- In CDMA system, the multipath interference is reduced by combining direct and reflected signals in receiver.

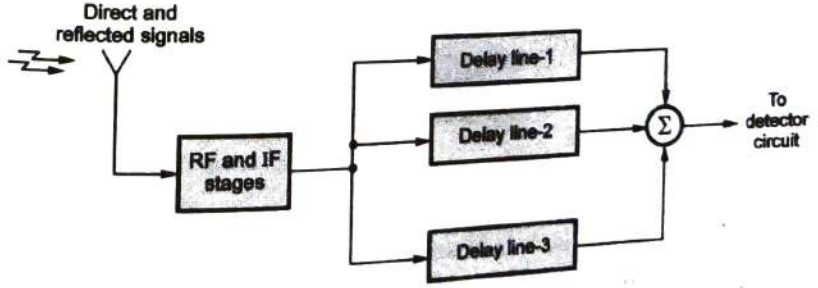


Fig. 5.13.8 Rake receiver

- The signals received with different time delays are compensated for propagation times by a receiver called rake receiver shown in Fig. 5.13.8.
- One of the signal is taken as base station signal and other two can be reflections or from neighbouring cell. After every 20 ms decisions about quality are made on frame-to-frame basis.
- In soft handoff two base stations communicating to a mobile simultaneously, this avoids dropping of calls. The only disadvantage is increased load in switching station.

5.13.10 CDMA Security

- CDMA channel is not easily decodable. In order to decode a call it requires a spread spectrum receiver and despreading code also.
- The chances of eavesdropping are also small. It uses private key encryption. Therefore CDMA offers excellent security.

5.13.11 Advantages of CDMA

- The CDMA have several advantages over other 2G systems.

1. Capacity

- One of major advantage of CDMA is its capacity. CDMA can accommodate more users per MHz of bandwidth than any other system of same generation. It has 4 to 5 times capacity than capacity of GSM and 8 to 10 times capacity than capacity of AMPS.

2. Call quality

- CDMA call quality is better with more consistent sound compared to GSM and AMPS. The handoff features reduces call drops and less interference.

3. Frequency

- CDMA uses one frequency per cell compared with maximum possible frequencies in TDMA. Therefore, the frequency reuse plan is much easier to manage.

4. Coverage

- CDMA gives better coverage and requires fewer antenna sites, consumes less power.

5. Multipath performance

- When radio signal is transmitted to a receiver, it can take direct route or it can take reflected path. This leads to multipath effect causing interference. CDMA has better multipath performance than AMPS and GSM.

5.13.12 Comparison of GSM and CDMA

Sr. No.	Parameters	GSM	CDMA
1.	Access mode	TDMA/FDD	CDMA/FDD
2.	Carrier (channel) spacing	200 kHz	1.25 MHz
3.	Time Slots (TS) in a frame-full-rate	8 TS	64 TS
4.	Time Slots (TS) in a frame-half-rate	16 TS	128 TS
5.	Downlink frequency (base station transmit to mobile subscriber)	925-960 MHz 1805-1880 MHz	869-894 MHz
6.	Uplink frequency (mobile subscriber transmit to base station)	880-915 MHz 1710-1785 MHz	824-849 MHz
7.	Frequency separation	45/95 MHz	45 MHz
8.	Carrier (channel) total bit rate	270.833 kbps	1228.8 kbps
9.	Full-rate coded traffic information (voice and data)-total sum of parameters : 10,11	22.8 kbps	About 77 kbps
10.	Error detection and correction bits	13 kbps	
11.	Full-rate, digitally coded speech	9.8 kbps	About 8/13 kbps
12.	Modulation technique	GMSK	QPSK/BPSK

University Questions

1. *Explain the following term with reference to CDMA*
   1. Power Control 2. Soft hand-off 3. Frequency hopping — GTU : Winter-14, Marks 7
2. *Explain how power control is achieved in CDMA.* — GTU : Summer-15, Marks 7
3. *Compare CDMA forward and reverse channel.* — GTU : Summer-16, Marks 7

5.14 Rake Receiver

GTU : Summer-16

- In order to combat fading, several innovative receiver implementations have been created. Rake receiver is used for the equalization of multipath.
- When multipath signals will arrive at the receiver over the mobile radio channel; these receivers exploit that fact by isolating the signal paths at the receiver.
- If the fading of multipath signals is different; then the isolation process yield the diverse signals needed to improve receiver performance.
- Typical RAKE receiver used in CDMA is shown in Fig. 5.14.1.

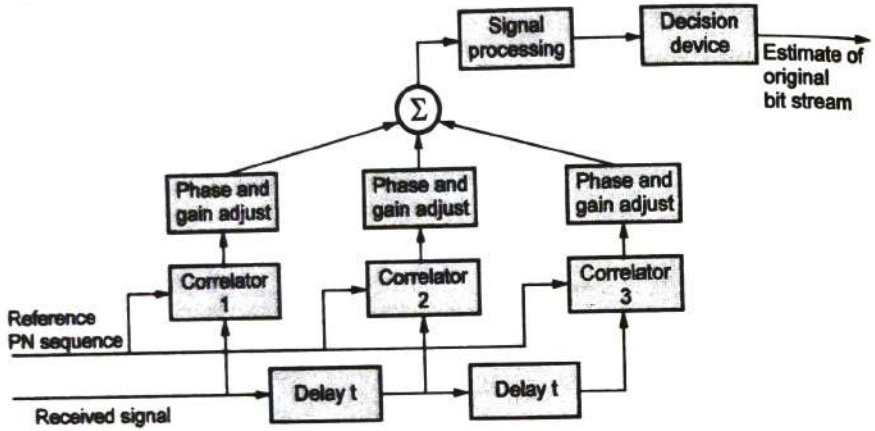


Fig. 5.14.1 RAKE receiver

- The usual implementation of space diversity for a wireless system is to use multiple transmitting and/or receiving antennas. These antennas must be physically some distance separate or apart from each other.
- Polarization diversity is implemented for a cellular wireless system by using several antennas with different polarizations.

University Question

1. *Describe RAKE receiver in CDMA.* GTU : Summer-16, Marks 7

5.15 CDMA2000

- Code division multiple access 2000 is the natural evolution of IS-95 (cdmaOne). It includes additional functionality that increases its spectral efficiency and data rate capability.

- Code Division Multiple Access is a method in which multiple users occupy the same time and frequency allocations and are channelized by unique assigned codes. The signals are separated at the receiver by using a correlator that accepts only signal energy from the assigned Code Channel. The channels are defined with codes (PN sequences). All other signals in that frequency band contribute only to the noise.
- Three main CDMA2000 standards are :
  1. cdma2000 1xRTT
  2. cdma2000 1xEV
  3. cdma2000 EV-DV
- cdma2000 1x supports both voice and data services over the standard 1.25 MHz CDMA channel. The 1x in the name signifies that it uses one 1.25 MHz channel. Due to improved modulation, power control, and overall design, it can achieve theoretical data transfer rates of 144 Kbps.
- There are two members of cdma2000 1x EV family :
  1. cdma2000 1x Evolution Data Optimized (cdma 1x EV-DO)
  2. cdma2000 1x Evolution Data and Voice (cdma 1x EV-DV)
- The cdma2000 1xEV-DO supports greater than 2.4 Mbps of instantaneous high-speed packet throughput per user on a CDMA channel, although the user data rates are much lower and highly dependent on other factors.
- cdma2000 EV-DV can offer data rates upto 144 kbps with about twice as many voice channels as IS-95B.
- Base station timing synchronization in cdma2000 can provide decreased latency and a reduced chance of dropping calls during soft handoff.
- Since both WCDMA and cdma2000 have been simultaneously adapted for the 3G standard, harmonization of these two systems becomes necessary to make IMT-2000 deployment successful.
- To create a single integrated 3G CDMA specification and process the separate W-CDMA and cdma 2000 proposals being developed by 3GPP and 3GPP2.

5.15.1 Network Components of CDMA2000

- Fig. 5.15.1 shows major components of CDMA 2000 wireless system.
(Refer Fig. 5.15.1 on next page)

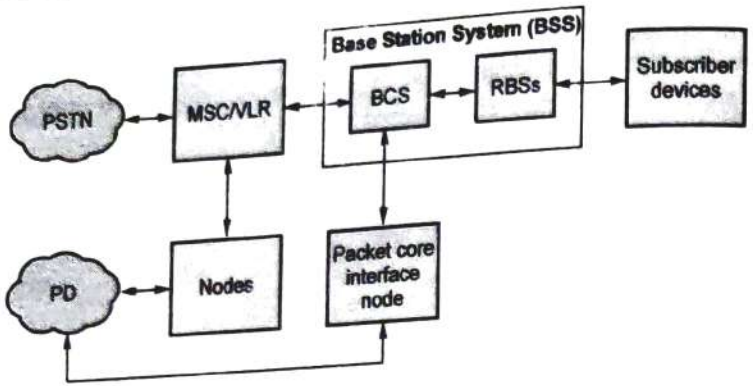


Fig. 5.15.1 Components of CDMA 2000

5.15.2 Network Nodes in CDMA2000

- Detail network nodes in a CDMA 2000 is shown in Fig. 5.15.2.

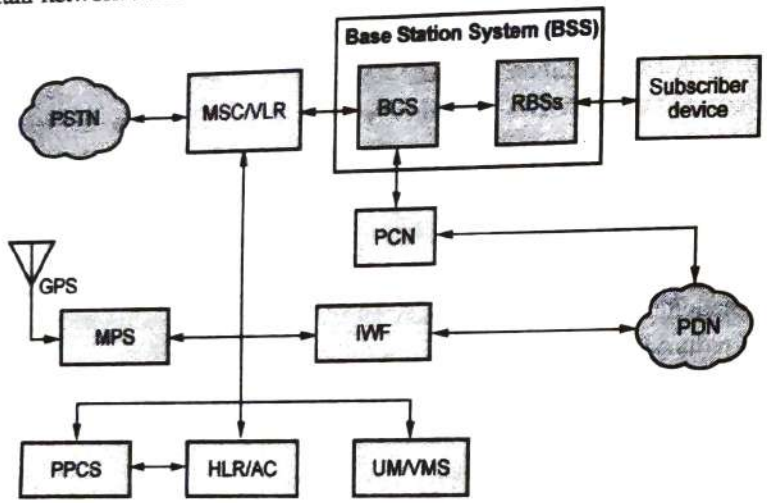


Fig. 5.15.2 Detail network nodes in CDMA 2000

Home Location Register/Authentication Centre (HLR/AC)

- The HLR holds the subscriber information in a database that is used by the system. It stores the ESN, subscribers service plan etc. AC provides secure database for authentication.

Base Station Subsystem (BSS)

- BSS consists of one BSC and all the radio base stations controlled by the BSC.

Base Station Controller (BSC)

- BSC interfaces between the MSC and the PCN, other BSS's in the system.

- It provides routing of data packets between the PCN and the RBS's, radio resource allocation, system and timing synchronization.

Radio Base Station (RBS)

- RBS interfaces between the BSC and the SD. Its functions include CDMA decoding and encoding of the subscriber, traffic and system overhead channels and the CDMA radio links to and from the subscriber.

5.15.3 Comparison of WCDMA and CDMA2000

Sr. No.	Feature	WCDMA	CDMA2000
1.	Chip rate	4.096 MCps	3.6864MCps
2.	Forward Link Pilot Structure	Dedicated Pilot with TDM	Common Pilot with CDM
3.	Base Station Timing	Asynchronous	Synchronous
4.	Frame length	10 or 20 ms optional	20 ms
5.	Forward link RF channel structure	Direct spread	Direct spread or multicarrier
6.	Spreading factor	4.096 mcps	3.6868 mcps
7.	Spreading modulation	QPSK	Uplink m-ary PSK downlink-QPSK

5.16 GPRS

GTU : Summer-15

- General Packet Radio Service is an overlay on top of GSM physical layer and network entities. GPRS system is used by the GSM mobile phones.
- The GPRS network acts in parallel with the GSM network, providing packet switched connections to the external networks.
- A GPRS network must provide all of the functionality of a GSM network for packet switched networks and more.
- Frequency spectrum of GSM is used overlayed on the traffic channel of GSM.
- GPRS short packets of 500 - 1000 bytes have short access time.

GPRS Speed

- GRPS can theoretically use one to eight of the GSM timeslots for uplink and downlink traffic.
- The capacity ranges from 9.05 kbps to 21.4 kbps where the slower ones provide varying amounts of error correction.

GPRS Devices

- GPRS device are expected to be in many different kinds, shapes and functionality. However, all GPRS devices can be divided into three different categories :
  1. **Class A** devices can operate GPRS simultaneously with other GSM services (such as a normal voice call).
  2. **Class B** devices can operate both GPRS and GSM services but not at the same time. The device must shift between the two modes but can be registered in the network for both.
  3. **Class C** devices operate exclusively GPRS services.

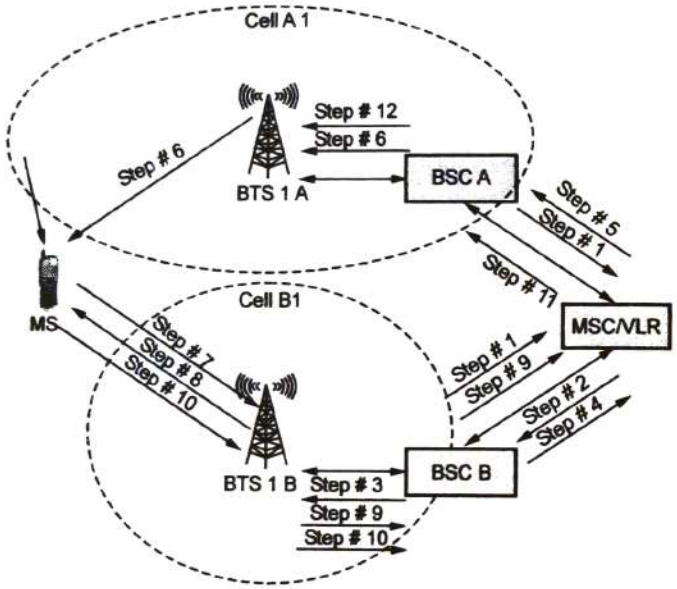


Fig. 5.16.1 Inter-BSC handoff

5.16.1 GPRS Functional Groups

- The functions defined in GPRS are as following.
  1) Network access function
  2) Packet routing and transfer
  3) Mobility management
  4) Logical link management
  5) Radio resource management
  6) Network management

1. Network Access Function :

- Main functions of network access function include :
  - Point to point data transfer,
  - Authentication and authorization
  - Admission control
  - Message screening
  - Registration of MS with packet data protocols,
  - Radio resources for MS communication and
  - Charging information about packet transmission.

2. Packet Routing and Transfer Function :

- Packet routing and transfer function route the data between an MS and the destination through the serving and gateway GPRS Support Nodes (GSNs).
  - Relay function
  - Routing
  - Address translation and mapping
  - Encapsulation and tunnelling
  - Compression and ciphering
  - Domain name service functions
  - Conversion of GPRS address to external address and forwarding of packets between an MS and GGSN, is provided by this function.

3. Logical Link Management Function :

- The communication between an MS and the GSM network is maintained by it. The main functions that are maintained are :
  - Logical link establishment
  - Logical link maintenance
  - Logical link release

4. Radio Resources Management Function :

- Radio communication paths are allocated by it. The main functions that are maintained are :
  - Um management
  - Cell selection
  - Um-tranx, which provides packet data transfer capability such as Medium access control, etc.
  - Path management

5. Mobility Management Function :

- Current location of an MS is kept by it. When an MS is entered to a new area, all routing and location in formations are also updated by it. The main functions that are maintained are -
  - ➤ Keeps track of the current location of an MS
  - ➤ Cell update, routing area update, combined
  - ➤ Routing area and location area update

6. Network Management Function :

- If provides mechanisms to support network functions related to GPRS. An important function performed is that it provides mechanism to support OA&M functions.

5.16.2 GPRS Architecture

- The GSM network still provides voice and the GPRS network handles data, because of this voice and data can be sent and received at the same time.
- GPRS is not a completely separate network to GSM. Many of the devices such as the base transceiver stations and base transceiver station controllers are still used. There are two new functional elements which play a major role in how GPRS works. The Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN). These two nodes are new to the network with the other changes being small if any. GPRS architecture is shown in Fig. 5.16.2.

5.16.2.1 Serving GPRS Support Node (SGSN)

- The Serving GPRS Support Node, or SGSN for short, takes care of some important tasks, including routing, handover and IP address assignment.
- The SGSN has a logical connection to the GPRS device. As an example, if you where in a car travelling on a long journey and were browsing the Internet on a GPRS device, you will pass through many different cells. One job of the SGSN is to make sure the connection is not interrupted as you make your journey passing from cell to cell. The SGSN works out which BSC to "route" your connection through.
- If the user moves into a segment of the network that is managed by a different SGSN it will perform a handoff of to the new SGSN, this is done extremely quickly and generally the user will not notice this has happened. Any packets that are lost during this process are retransmitted.
- The SGSN converts mobile data into IP and is connected to the GGSN via a tunnelling protocol.

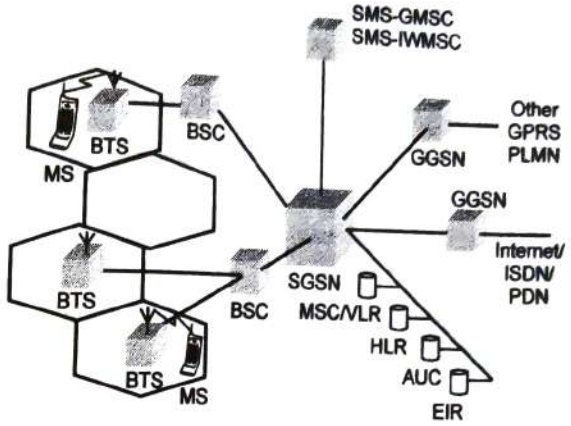


Fig. 5.16.2 GPRS architecture

5.16.2.2 Gateway GPRS Support Node (GGSN)

- The gateway GPRS support node is the "last port of call" in the GPRS network before a connection between an ISP or corporate network's router occurs.
- The GGSN is basically a gateway, router and firewall rolled into one. It also confirms user details with RADIUS servers for security, which are usually situated in the IP network and outside of the GPRS network.

5.16.2.3 Connectivity between the SGSN and GGSN

- The connection between the two GPRS support nodes is made with a protocol called GPRS. Tunnelling Protocol (GTP). GTP sits on top of TCP/IP and is also responsible for the collection of mediation and billing information.
- GPRS is billed on per megabyte basis unlike GSM. In practice the two GSN devices may be a single unit.

5.16.2.4 HLR

- The HLR or Home Location Register is a database that contains subscriber information, when a device connects to the network their MSISDN number is associated with services, account status information, preferences and sometimes IP addresses.

5.16.2.5 Air Interface

- GPRS is a packet switching data service, overlaid on the GSM infrastructure.
- GPRS service can be grouped into 3 classes :
  - a) **Class A :** Simultaneous use of data and voice services. Thus class A service allows a user to hold a conversation and transfer GPRS data at the same time.

b) **Class B** : Supports simultaneous GSM and GPRS attach but not simultaneous use of both services. Thus a class B user can be registered on both services at the same time, but cannot use both services at the same time.

c) **Class C** : Can attach to only one service at a time.

- As mentioned earlier, GPRS allows access to multiple slots. It is also asymmetric in the sense that downlink slots may be greater than uplink slots since higher data rates are needed during download operation. Table 5.16.1 shows common multi-slot class.

Multi-slot class	Download slots	Uplink
2	2	1
4	3	1
8	4	1
12	4	2

Table 5.16.1

- GPRS uses the same air interface as GSM i.e. 200 kHz RF Carrier and 8 Timeslots, however, at any given time, same of the slots may be carrying voice and same data. This is achieved by using a different logical channel allocation and coding scheme.

5.16.3 GPRS Network Service

- GPRS provides the following network services :

1. **Point-to-multipoint (PTM-M)** : Multicast services for subscribers in given area.
2. **Point-to-multipoint group (PTM-G)** : Multicast service to predetermined group that may be spread over geographic area.
3. **Point-to-point (PTP)** : Packet data transfer (connectionless and connection oriented)

- GPRS performance parameters are specified on the basis of different reliability cases and delay classes.
- Three reliability cases are defined as shown in Table 5.16.2.

	Probability for			
Class	Lost packet	Duplicated packet	Out-of-sequence packet	Corrupted packet
1	10^{-9}	10^{-9}	10^{-9}	10^{-9}
2	10^{-4}	10^{-5}	10^{-5}	10^{-6}
3	10^{-2}	10^{-5}	10^{-5}	10^{-2}

Table 5.16.2

- Delay classes are summarized in Table 5.16.3.

	128 Byte packet		1,024 Byte packet	
Class	Mean Delay	95 % Delay	Mean Delay	95 % Delay
1.	< 0.5s	< 1.5s	< 2s	< 7s
2.	< 5s	< 25s	< 15s	< 75s
3.	< 50s	< 250s	< 75s	< 375s
4.	Best effort	Best effort	Best effort	Best effort

Table 5.16.3

5.16.4 Mobility Supports in GPRS

- Similar to CDPD and GSM, GPRS also has mechanisms to support mobility.

5.16.4.1 Attachment Procedure

- Before accessing GPRS services, the MS must register with the GPRS network and become "known" to the PDN.
- The MS performs an **attachment procedure** with an SGSN that includes -
  1. Authentication
  2. Check with GR etc.
- It is allocated a Temporary Logical Link Identity (TLLI) by the SGSN.
- A PDP (Packet Data Protocol) context is created for the MS.
- A user may multiple PDP contexts at any time. The PDP address may be statically or dynamically assigned. This PDP context is used to route packet accordingly.

5.16.4.2 Location and Handoff Management

- The location and handoff management procedures in GPRS are based on tracking of MSs location and ability to route packets to it accordingly.
- The location management depends on three states of MS : IDLE, STANDBY and READY as shown in Fig. 5.16.3.
- In the IDLE state the MS is not reachable. Hence all PDP contexts are deleted.
- In the STANDBY state, movement across routing areas are updated to the SGSN but not across cells.
- In the READY state, every movement of the MS is indicated to the SGSN.

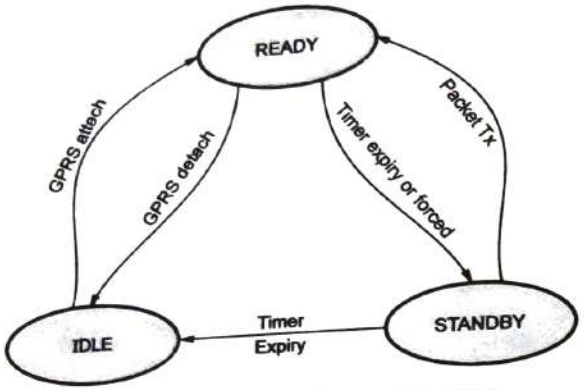


Fig. 5.16.3 Location management in GPRS

Why three states

- If the MS updates its location too often, it consumes battery power and wastes the air-interface resources.
- If it updates too infrequently, a system-wide paging is needed; this is also a waste of resources.
- A standby state focuses the area -chances of packets reaching are medium.
- A ready state pinpoints the area- chances of packets reaching are high.

Routing Area Updates

- Routing area updates are part of standby state.
- In intra-SGSN RA update, the SGSN already has the user profile. A new temporary mobile subscriber identity is issued as part of routing area update "accept". The home GGSN and GR (HLR) need not be updated.
- In inter-SGSN RA update, the new RA is serviced by a new SGSN. The new SGSN requests the old SGSN to send the PDP contexts of the MS. The new SGSN informs the home GGSN, the GR and other GGSNs about the user's new routing context.

5.16.4.3 Mobility Management in GPRS

1. Handoff Initiation

- The MS listens to the BCCH and decides which cell it has to select.
- Proprietary algorithms are employed that use RSS, cell ranking, path loss, power budget, etc.

- An option exists where the network can ask the MS to report its measurements and ask it to make a handoff (as in GSM).

2. Handoff Procedure

- The handoff procedure is very similar to Mobile IP.
- The location is updated with a routing update procedure as shown in Fig. 5.16.4.

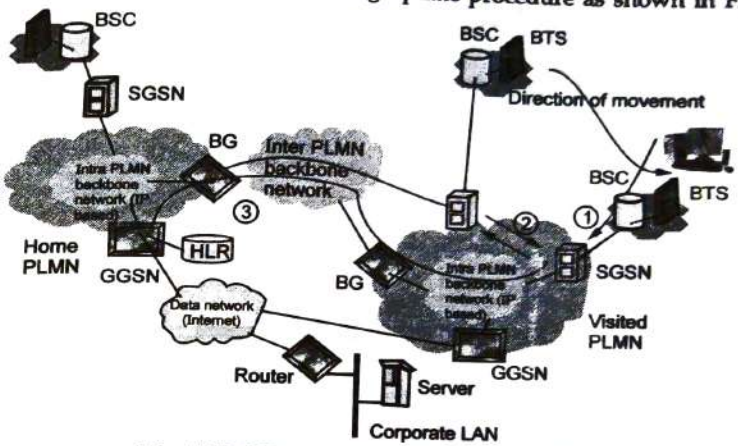


Fig. 5.16.4 Handoff management in GPRS

Steps in Mobility Management

i) When MS changes Routing Area (RA), it sends RA update to new SGSN.

ii) Communication between new and old SGSN.

iii) Communication between new SGSN and Home-GGSN/HLR.

iv) The Home GGSN "tunnels" packets to the new SGSN.

v) The HLR deletes old SGSN information and includes the new SGSN information in the database.

vi) The new SGSN decapsulates packets and forwards them to the MS.

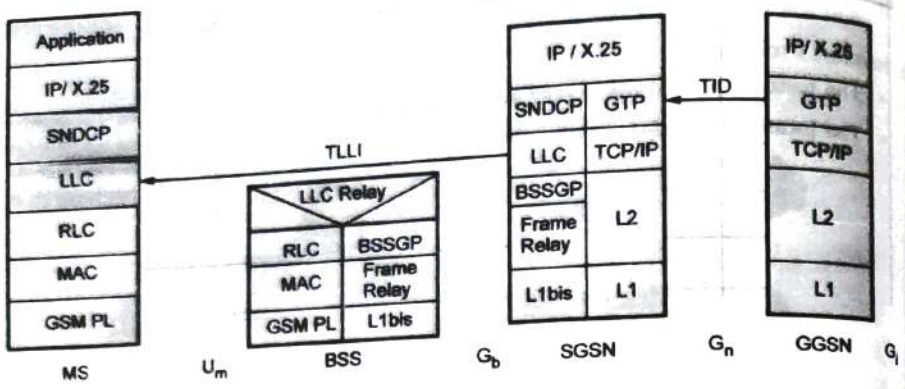
16.5 Transport Layers in GPRS

- GPRS protocol stack is shown in Fig. 5.16.5. This is the transport plane where data is transferred over GPRS/GSM infrastructure. (Refer Fig. 5.16.5 on next page)

5.5.1 GPRS Signaling Plane

GPRS signaling plane enables signalling between various elements of infrastructure.

GPRS employs out of band signaling in support of actual data transmission.



SNDCP : Subnetwork Dependent Convergence Protocol
BSSGP : BSS Gateway Protocol
GTP : GPRS Tunneling Protocol

Fig. 5.16.5 GPRS transport plane

- Signaling between SGSN, HLR, VLR, EIR is similar to GSM and extends only the GPRS related functionality. Therefore it is based on Signaling System -7.
- Between the MS and SGSN, a GPRS mobility management and session management (GMM/SM) protocol is used for signaling purposes.
- Over the air, physical layer is the same as GSM (uses GMSK). Its functionalities include -

1. Forward error correction and indication of uncorrectable code words
2. Interleaving of radio "blocks"
3. Synchronization
4. Monitoring of radio link signal quality
5. Other functions similar to GSM

5.16.5.2 Medium Access

- Uplink and downlink transmissions are independent.
- Medium access protocol is called "Master-Slave Dynamic Rate Access" or MSDRA.
- Organization of time-slot assignment is done centrally by the BSS.
- A "master" PDCH includes common control channels that carry the signaling information required to initiate packet transfer.
- The "slave" PDCH includes user data and dedicated signaling information.

5.16.5.3 Logical GPRS Channels

- The packet transfers are analogous to GSM, GPRS has certain traffic and control channels. Various packets are -

1. PDTCH → Packet Data Traffic Channel
2. PBCCH → Packet BCCH
3. PNCH → Packet Notification Channel
4. PRACH → Packet Random Access Control Channel
5. PAGCH → Packet Access Grant Channel
6. PACCH → Packet Associated Control Channel (Use to send ACKs for received packets)
7. PTCCH → Packet Timing-advance Control Channel is used for adaptive frame synchronization.

Uplink Channel

- The packet transfer on the uplink is shown in Fig. 5.16.6.

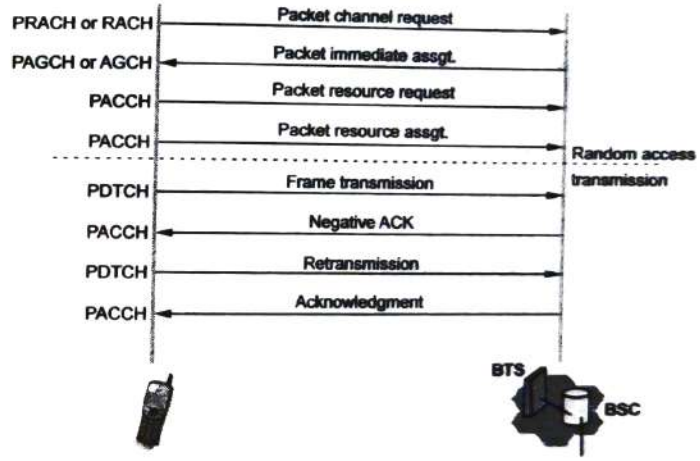


Fig. 5.16.6 Uplink data transfer

- If a MS does not get an ACK, it will back off for a random time and try again.
- The Master-Slave mechanism utilizes a 3 bit "uplink status flag" or USF on the downlink.
- A list of PDCHs and their USF are specified. The packet resource or immediate assignment message indicates what USF state is reserved for the mobile on a PDCH. Assignment can also be done so that a MS can send packets uninterrupted for a predetermined amount of time.

Downlink Channel

- The packet transfer on the downlink is shown in Fig. 5.16.7.

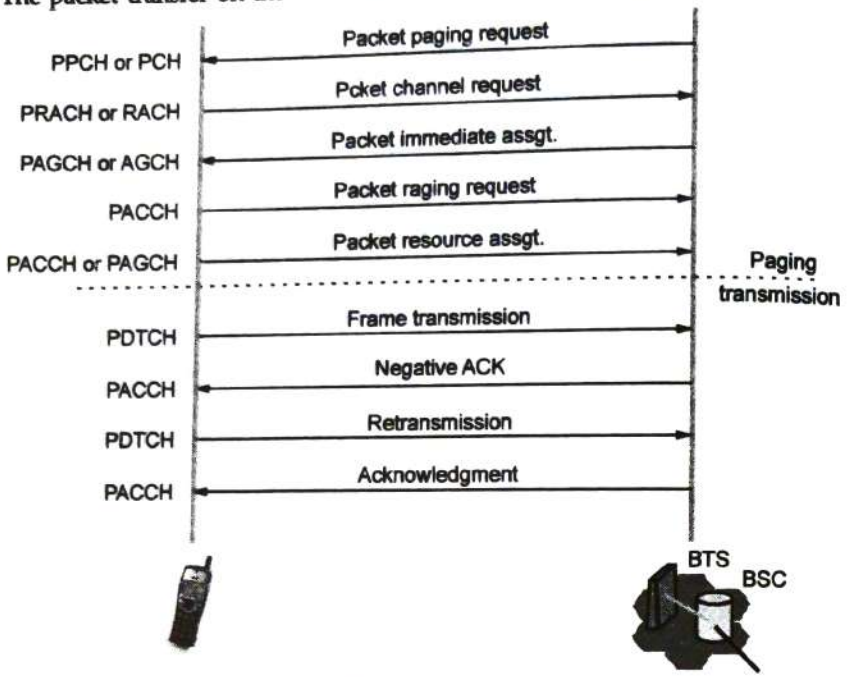


Fig. 5.16.7 Downlink data transfer

- Data transmission to a mobile can be interrupted if a high priority message needs to be sent.
- Instead of paging, a resource assignment message may be sent to the MS if it is already in a "ready" state.

Logical Link Control (LLC)

- The TLLI (Temporary Logical Link Identity) is used to identify a MS in the LLC header.
- A logical link is created between the MS and the SGSN.
- LLC performs sequence control, error recovery, flow control and encryption. It has an acknowledged mode (with retransmission for network layer payloads) and an unacknowledged mode (for signaling and SMS).
- LLC supports various QoS classes.

SNDCP

- Fig. 5.16.8 shows how packets flow from higher layers, applications and signalling levels to SNDCP and the LLC.

- It supports a variety of network protocols (IP, X.25, CLNP etc.). It multiplexes and demultiplexes the network layer payload.
- It forms the interface between the LLC and the network layer. Also, handles packets based on QoS.
- The packet transformation data flow is shown in Fig. 5.16.8.
- The end result is blocks of 114 bits that are transmitted in burst similar to GSM.

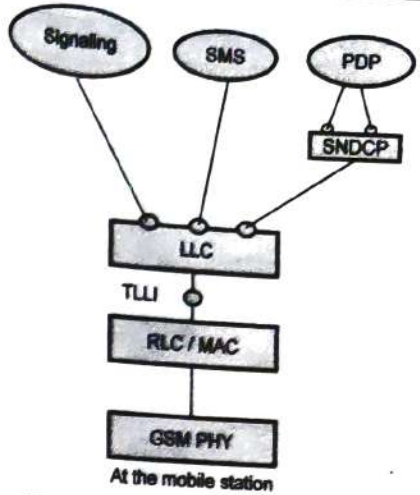


Fig. 5.16.8 SNDP and LLC in GPRS

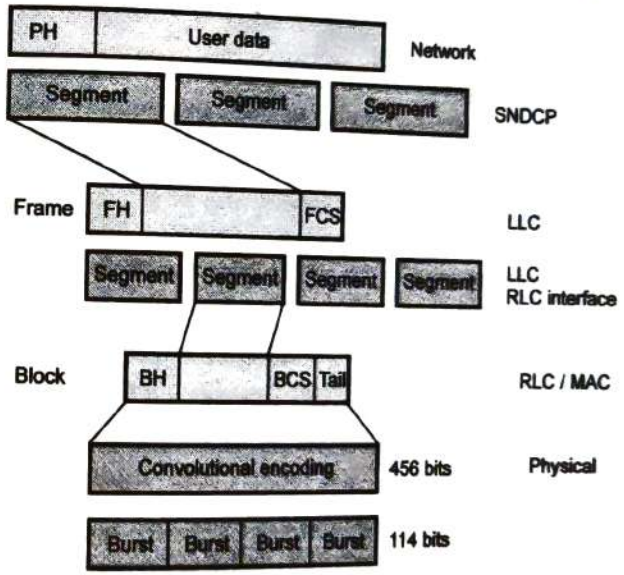


Fig. 5.16.9 Packet transformation data flow

GPRS Tunneling Protocol (GTP)

- GPRS Tunneling Protocol (GTP) allows multi-protocol packets to be tunneled through the GPRS backbone.
- A Tunnel ID (TID) is created using signaling plane that tracks the PDP context. GTP has capability of multiplexing different payloads.

- TID use in mobility management. Two level tunnelling mechanism implemented in GPRS is shown in Fig. 5.16.10.

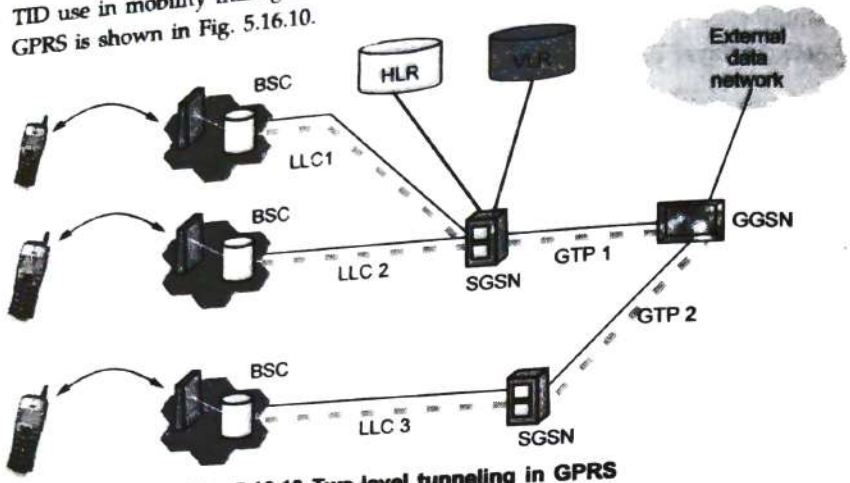


Fig. 5.16.10 Two-level tunneling in GPRS

- The two-level tunneling mechanism corresponds to a two level mobility. LLC "tunnels" (or virtual circuits) correspond to small area mobility, while GTP tunnels correspond to wide area mobility.

5.16.6 Call Routing in GPRS

- One of the main requirements in the GPRS network is the routing of data packets to and from a mobile user.
- The requirement can be divided into two areas :
  1. Data packet routing and
  2. Mobility management.

1. Data Packet Routing

- The main functions of the GGSN involve interaction with the external data network. The GGSN updates the location directory using routing information supplied by the SGSNs about the location of an MS.
- GGSN routes the external data network protocol packet encapsulated over the GPRS backbone to the SGSN currently serving the MS.
- GGSN also decapsulates and forwards external data network packets to the appropriate data network and collects charging data that is forwarded to a Charging Gateway (CG).

Fig. 5.16.11 illustrates three routing schemes.

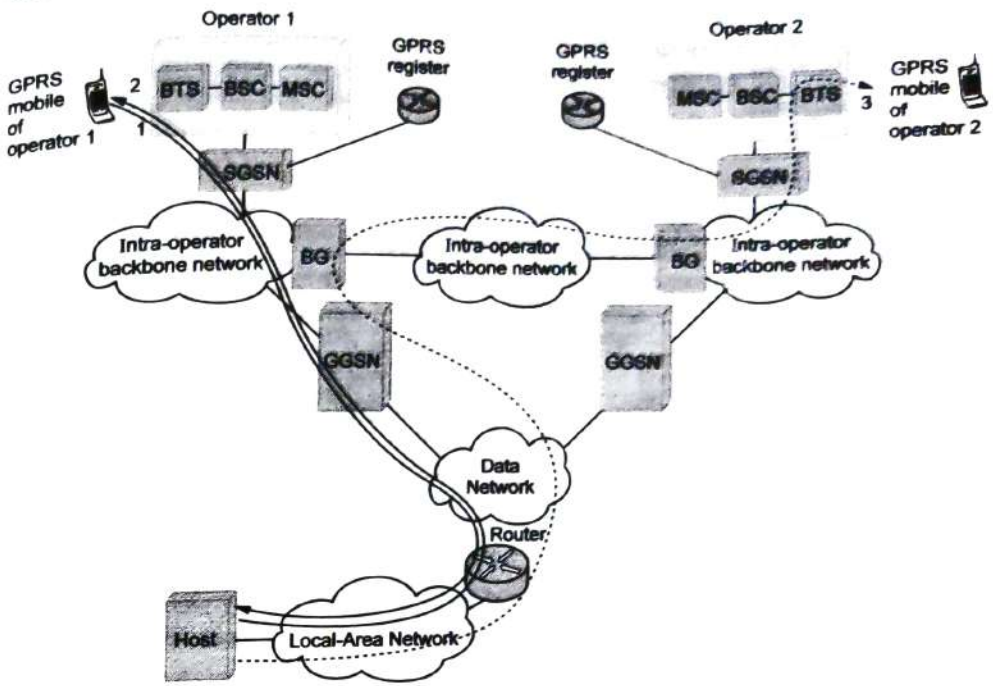


Fig. 5.16.11 Routing of data packets between a fixed host and a GPRS MS

1. Mobile-originated message (path 1)

- This path begins at the GPRS mobile and ends at the Host.

2. Network-initiated message when the MS is in its home network (path 2)

- This path begins at the Host and ends at the GPRS mobile.

3. Network-initiated message when the MS roams to another GPRS network (path 3)

- This path is indicated by the dotted line.
- The GPRS network encapsulates all data network protocols into its own encapsulation protocol called the GPRS tunneling protocol (GTP).
- The GTP ensures security in the backbone network and simplifies the routing mechanism and the delivery of data over the GPRS network.

2. Mobility Management

- The operation of the GPRS is partly independent of the GSM network. However, some procedures share the network elements with current GSM functions to increase efficiency and to make optimum use of free GSM resources (such as unallocated time slots).

- An MS has three states in the GPRS system.
  1. Active state
  2. Standby state
  3. Idle state
- The three-state model is unique to packet radio system whereas GSM uses a two-state model (idle or active).
- Fig. 5.16.12 shows GPRS states in a mobile station.

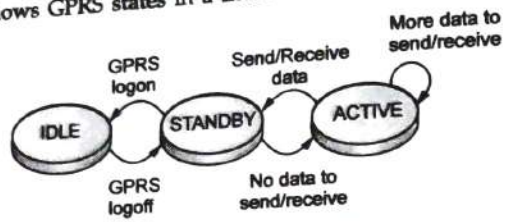


Fig. 5.16.12 GPRS states

State 1 : Active State

- Data is transmitted between an MS and the GPRS network only when the MS is in the active state. In the active state, the SGSN knows the cell location of the MS.
- Packet transmission to an active MS is initiated by packet paging to notify the MS of an incoming data packet. The data transmission proceeds immediately after packet paging through the channel indicated by the paging message.
- The purpose of the paging message is to simplify the process of receiving packets. The MS listens to only the paging messages instead of to all the data packets in the downlink channels. This reduces battery usage significantly.
- When an MS has a packet to transmit, it must access the uplink channel (i.e., the channel to the packet data network where services reside). The uplink channel is shared by a number of MSs, and its use is allocated by a BSS. The MS requests use of the channel in a random access message.
- The BSS allocates an unused channel to the MS and sends an access grant message in reply to the random access message. The description of the channel (one or multiple time slots) is included in the access grant message. The data is transmitted on the reserved channels.

State 2 : Standby State

- In the standby state, only the routing area of the MS is known. (The routing area can consist of one or more cells within a GSM location area).

- When the SGSN sends a packet to an MS that is in the standby state, the MS must be paged. Because the SGSN knows the routing area of the MS, a packet paging message is sent to the routing area.
- On receiving the packet paging message, the MS relays its cell location to the SGSN to establish the active state.
- The main reason for the standby state is to reduce the load in the GPRS network caused by cell-based routing update messages and to conserve the MS battery.
- When an MS is in the standby state, the SGSN is informed of only routing area changes. By defining the size of the routing area, the operator can control the number of routing update messages.

State 3 : Idle State

- In the idle state, the MS does not have a logical GPRS context activated or any Packet-Switched Public Data Network (PSPDN) addresses allocated.
- In this state, the MS can receive only those multicast messages that can be received by any GPRS MS. Because the GPRS network infrastructure does not know the location of the MS, it is not possible to send messages to the MS from external data networks.

Routing Updates

- When an MS that is in an active or a standby state moves from one routing area to another within the service area of one SGSN, it must perform a routing update.
- The routing area information in the SGSN is updated, and the success of the procedure is indicated in the response message.
- A cell-based routing update procedure is invoked when an active MS enters a new cell. The MS sends a short message containing the identity of the MS and its new location through GPRS channels to its current SGSN. This procedure is used only when the MS is in the active state.
- The inter-SGSN routing update is the most complicated routing update. The MS changes from one SGSN area to another, and it must establish a new connection to a new SGSN. This means creating a new logical link context between the MS and the new SGSN and informing the GGSN about the new location of the MS.

5.16.7 Billing and Charging in GPRS

- GPRS is essentially a packet switching overlay on a circuit switching network. The minimum charging information is collected in the Stage 1 service description. The stage 1 service description includes :
  - destination and source addresses,
  - usage of radio interface,

- usage of external packet data networks,
- usage of the packet data protocol addresses,
- usage of general GPRS resources
- location of the Mobile Station.

- GPRS network break the information to be communicated down into packets therefore it is needed to be able to count packets to charging customers for the volume of packets they send and receive.

The SGSN and GGSN register all possible aspects of a GPRS user's behavior and generate billing information accordingly. This information is gathered in so-called Charging Data Records (CDR) and is delivered to a billing gateway.

- The GPRS service charging can be computed on several parameters :

1. **Volume of data** : The amount of bytes transferred downloaded and uploaded.
2. **Duration of connection** : The duration of a PDP context session.
3. **Time of session** : Date, time of day, and day of the week (enabling lower tariffs at off-peak hours).
4. **Destination** : Subscriber could be charged for access to the specific network, such as through a proxy server.
5. **Location** : The current location of the subscriber.
6. **Quality of Service** : More charges for higher network priority.
7. **SMS** : The SGSN will produce specific CDRs for SMS.
8. **Served IMSI/subscriber** : Different subscriber classes (different tariffs for frequent users, businesses, or private users).
9. **Reverse charging** : Receiving subscriber is not charged for the received data; but the sending party is charged.
10. **Free data** : Specified data to be free of charge.
11. **Flat rate** : A fixed monthly fee.
12. **Bearer service** : Charging based on different bearer services (for an operator who has several networks, such as GSM900 and GSM1800, and who wants to promote usage of one of the networks). Or, perhaps the bearer service would be good for areas where it would be cheaper for the operator to offer services from a wireless LAN rather than from the GSM network.

5.16.8 Comparison of GSM and GPRS

Sr. No.	GSM	GPRS
1.	GSM has lower bandwidth compared to GPRS.	GPRS has a higher bandwidth and therefore a higher speed of data transmission.
2.	GSM service involves circuit switching channels.	GPRS networks use packet switching.
3.	In the circuit switched connection, the channel remains active even if there is no communication going on.	Much better and efficient use of bandwidth and other resources in the GPRS networks because here the bandwidth is used only when the data is being transferred.
4.	In GSM one timeslot is allocated to one MS.	In GPRS multiple timeslots are allocated to one MS.
5.	In GSM signaling and traffic follow different multi frame structure. 51 frame MF is used for signaling and 26 frame MF is used for traffic.	In GPRS signaling and traffic both follow common one multi frame structure i.e. 52 frame MF structure. Here 52 Multiframe composed of total 12 radio blocks, two idle slots and two slots are for PTCCH used for timing advance purpose. Each Radio Block spans over 4 consecutive TDMA frames of one time slot.
6.	In GSM time slot is allocated both in uplink and downlink hence in GSM radio resource allocation is called symmetric allocation.	While in GPRS it is asymmetric, for example it is possible to allocate time slot only in downlink and not in uplink when user is only downloading some file.
7.	In GSM location area concept is used.	In GPRS routing area concept is used.
8.	In GSM Mobile or UE will be in two states i.e. IDLE and READY.	In GPRS UE will be in three states i.e. IDLE, STANDBY and READY.

- GPRS requires the introduction of two new network elements in the GSM network :
  1. Serving GPRS Support Node (SGSN),
  2. Gateway GPRS Support Node (GGSN).

5.16.9 Applications of GPRS

1. Email
2. Web based application
3. Fax service
4. Text messages
5. Multimedia
6. File transfer
7. Database access
8. Telemetry

9. Point of sale credit card transactions (especially in a flea market or taxi payment where there is no modem).

5.16.10 Limitations of GPRS

1. Limited cell capacity for all users : Limited radio resources can be deployed. Also voice and GPRS share the same network resources.
2. Lower access speed in reality : Maximum GPRS transmission 172.2 kbps can be with single user over all eight time slots without error protection.
3. No support of GPRS mobile terminate connection for a mobile server.

University Question

1. *With the help of a neat sketch. describe GPRS archi tecture.* **GTU : Summer-15, Marks 7**

5.17 Multiple Choice Questions

Q.1 GSM provides only _____ data connection.

[a] 8.6 kbps [b] 9.6 kbps [c] 7.6 kbps [d] 8.8 kbps **[Ans. : b]**

Q.2 The uplink and downlink frequencies for GSM are different and therefore a channel has a pair of frequencies _____ apart.

[a] 70 MHz [b] 80 MHz [c] 90 MHz [d] 60 MHz **[Ans. : b]**

Q.3 The separation between uplink and downlink frequencies are called _____.

[a] duplex distance [b] double distance [c] triplex distance [d] none of these **[Ans. : a]**

Q.4 In a channel the separation between adjacent carrier frequencies is known as channel separation which is _____ in case of GSM.

[a] 100 kHz [b] 200 kHz [c] 300 kHz [d] 400 kHz **[Ans. : b]**

Q.5 The services supported by GSM are _____ .

[a] telephony [b] fax and SMS [c] call forwarding [d] caller ID [e] call waiting [f] all of these **[Ans. : f]**

Q.6 GSM supports data at rates up to 9.6 kbps on _____ .

[a] POTS(Plain Old Telephone Service)
[b] ISDN
[c] Packet Switched Public Data Networks
[d] Circuit Switched Public Data Networks
[e] All of these

[Ans. : e]

Q.7 The access methods and protocols for GSM may be from _____.

[a] X.25 [b] X.32 [c] Both a & b [d] None of these **[Ans. : c]**

Q.8 There are basic types of services offered through GSM are _____.

[a] telephony or teleservices [b] data or bearer services [c] supplementary services [d] all of these **[Ans. : d]**

Q.9 The supplementary services are used to enhance the features of _____.

[a] bearer [b] teleservices [c] both a & b [d] none of these **[Ans. : c]**

Q.10 Dual tone signals are used for various control purposes via the _____.

[a] telephone network [b] different from dual pulses [c] both a & b [d] none of these **[Ans. : c]**

Q.11 SMS (Short Message Service) is a message consisting of a maximum of _____ alphanumeric characters.

[a] 150 [b] 160 [c] 170 [d] 180 **[Ans. : b]**

Q.12 GSM supports _____ Group 3 facsimile.

[a] CCIIT [b] CCITT [c] CCCIT [d] CCTTI **[Ans. : b]**

Q.13 Call forwarding is a _____.

[a] telephony or teleservices [b] data or bearer services [c] supplementary services [d] all of these **[Ans. : c]**

Q.14 The other services of call forwarding are _____.

[a] cell broadcast, voice mail, fax mail
[b] barring of outgoing and incoming calls conditionally
[c] call hold, call waiting, conferencing
[d] closed user groups
[e] all of these **[Ans. : e]**

Q.15 GSM consists of many subsystems, such as the _____ .

[a] Mobile Station(MS) [b] Base Station Subsystem(BSS)
[c] Network and Switching subsystem(NSS) [e] All of these
[d] Operation Subsystem(OSS) **[Ans. : e]**

Q.16 Which forms a radio subsystem ?

[a] Mobile station [b] Base station subsystem
[c] Both a & b [d] None of these **[Ans. : c]**

Q.17 The generic GSM network architecture which is composed of three subsystem are_____ .

[a] radio subsystem (RSS) [b] network and switching subsystem
[c] operation subsystem [d] all of these **[Ans. : d]**

Q.18 The RSS is basically consisting of radio specific equipment such as _____ to control the radio link.

[a] Mobile Station(MS) [b] Base Station Subsystem(BSS)
[c] Both a & b [d] None of these **[Ans. : c]**

Q.19 The chief components of RSS are _____ .

[a] BSS [b] Cellular layout
[c] Base Station Controller(BSC) [d] All of these **[Ans. : d]**

Q.20 SIM stands for _____.

[a] System Identity Module [b] Subscriber Identity Module
[c] Subscriber Identity Modem [d] Subscriber Input Modem **[Ans. : b]**

Q.21 MS contains a SIM card in the form of a very _____ inside the equipment.

[a] large chip [b] small chip
[c] both a & b [d] none of these **[Ans. : b]**

Q.22 Cell site is defined as the location where _____ are placed.

[a] base station [b] antennas
[c] both a & b [d] none of these **[Ans. : d]**

Q.23 Cells are the basic constituents of a cellular layouts with _____.

[a] cell sites [b] cell systems
[c] cell forwarding [d] none of these **[Ans. : a]**

Q.24 A cell is simply represented by simple _____.

[a] pentagon [b] hexagon
[c] both a & b [d] none of these **[Ans. : b]**

Q.25 The size of cells in case of GSM and Personal Communication Service(PCS) are much smaller in the range of _____ .

[a] 5 kms [b] 10 kms [c] 15 kms [d] 20 kms **[Ans. : b]**

Q.26 The portions covered by the antenna are called _____ .

[a] portions [b] sectors [c] cell sector [d] none of these **[Ans. : b]**

Q.27 The BTS or Base Transceiver Station is also called _____ .

[a] RBS [b] PCS [c] GSM [d] SIM **[Ans. : a]**

Q.28 BTS are housed with all radio equipments such as _____ .

[a] antennas [b] signal processors
[c] amplifiers [d] all of these **[Ans. : d]**

Q.29 Base station may also be placed near center of cell and known as _____ .

[a] excited cell [b] center excited cell
[c] center cell [d] none of these **[Ans. : b]**

Q.30 Antenna always transmits inward to each cell and area served depends on _____ .

[a] topography [b] population
[c] traffic [d] all of these **[Ans. : d]**

Q.31 Network and switching subsystem is composed of the _____ .

[a] Mobile Services Switching Center(MSC)
[b] Home Location Register(HLR)
[c] Visitor Location Register(VLR) [d] All of these **[Ans. : d]**

Q.32 The mobile stations(MS) communicates only via the _____ .

[a] BTS [b] BSS [c] BSC [d] U_m **[Ans. : a]**

Q.33 A BTS is connected to a mobile station via the _____.

[a] BTS [b] BSS
[c] A_{bis} interface with BSC [d] U_m interface **[Ans. : e]**

[e] Both c & d