Mobile Computing UNIT-1

Mobile Communications : Overview

Communication is a two-way transmission and reception of data streams. Voice, data or multimedia streams are transmitted as signals which are recieved by a reciever. so communication is a basic procan of exchanging information.

This data or information can be in two forms i.e) Analog or Digital

- Analog data refers to information that is continous.
  For example, an analog clock that has hour minute and second hands give information in a continous form as the movements are continous.
  Analog signals have an infinite nomber of values in a range.
- Digital data refers to information that has discrete states.
  For example, a digital clock that reports the hours and minutes will change suddenly change from say. 3:01 to 3:02 AM
  A digital signal can have only a limited nomber of defined values.

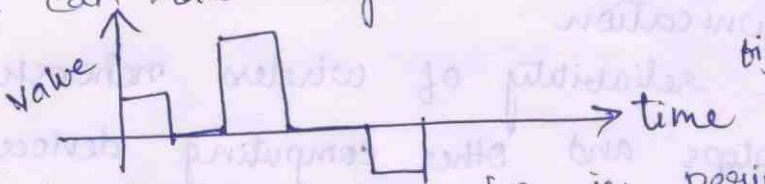
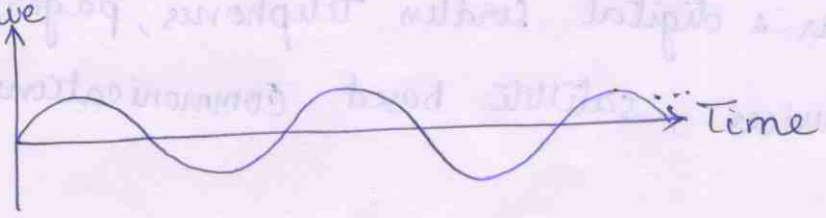


fig: Digital Signal

Both Analog and digital signals can be i.e) periodic or non periodic. where a periodic signal completes a pattern within a measureble time frame, called a period and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a Cycle.

A non periodic signal changes without exhibiting a pattern or cycle that repeats over time.

consider, a periodic Analog signal : Sine wave



Wired Communication:

- Wired communication requires cables to be connected to each and every computer in the network.
- Cost of the wired network is less as compared to wireless n/w as Ethernet - Cables, switches are not expensive.
- Wired LAN offers better performance.
- It is the most reliable form of communication.
- No data loss occurs in wired communications.
- Security considerations for a wired n/w connected to the internet are firewalls.

Wireless network:

- Wireless network can be configured in two ways, i) Adhoc or infrastructure mode.
- Cost of wireless network is high.
- In wireless communication performance drops when compared to wired communication.
- The reliability of wireless network is less.
- Laptops and other computing devices can be moved around freely within the wireless n/w because mobility of wireless n/w is better as compared to wired n/w.

Mobile communication is a wireless form of communication in which voice and data information is emitted, transmitted and recieved via. microwaves. This type of communication allows individuals to converse with one another and/or transmit and recieve data while moving from place to place.

Eg: cellular & digital cordless telephones, pagers, telephone answering devices, satellite based communications.

Before going in Guided and Unguided Transmissions in detail let us study the basics of what a signal is and its other properties.

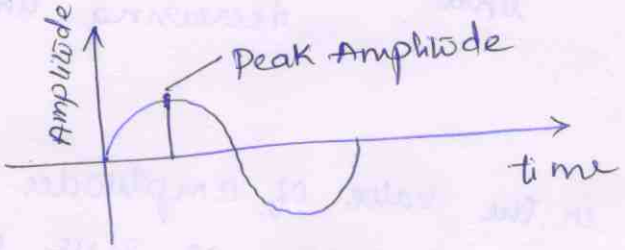
Signal: A signal is communicated by a variation of electrical voltage V or current i through a path between two points in a circuit. The values of V or i vary as a function of time t

Amplitude: The value of a signal at any specified value of the independent variable is called its amplitude. The sketch or plot of the amplitude of a signal as a function of independent variable is called its waveform.

A sine wave can be represented by three parameters.

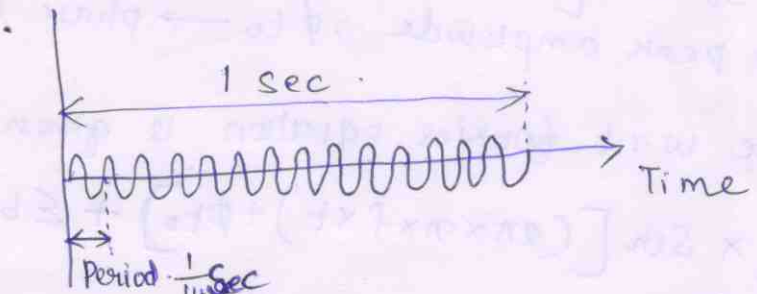
1) Peak amplitude 2) Frequency 3) Phase

- The peak amplitude of a signal is the absolute value of its highest intensity, proportional to the energy it carries & is measured in volts.



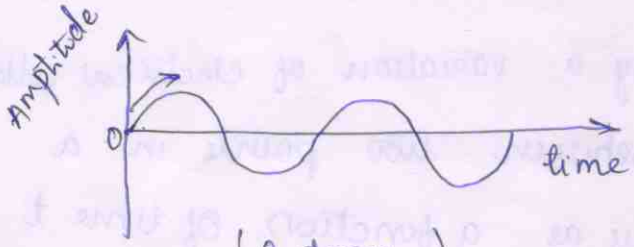
2) Frequency: It refers to number of periods in 1 second. Period is the inverse of frequency. Period is expressed in sec i.e, Time and frequency in Hertz (Hz).

$$\therefore f = \frac{1}{T} \Rightarrow T = \frac{1}{f}.$$



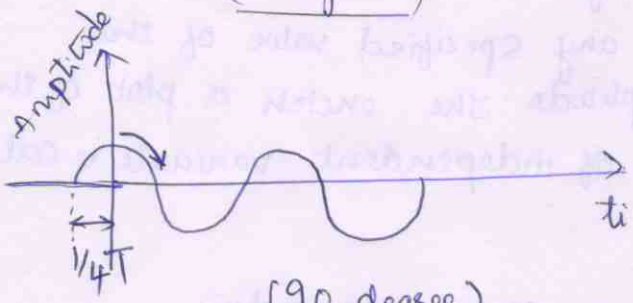
freq = 14 Hz because 14 periods occured in 1 second.

3) Phase : Phase describes the position of a wave form relative to time 0 and measured in degrees or radians.



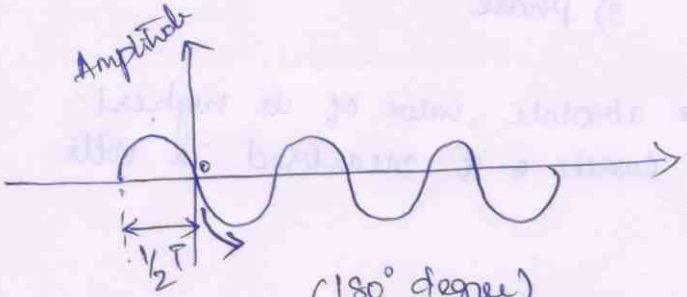
(0 degree)

Sine wave with phase 0° starts at time 0 ; zero amplitude → increasing amplitude.



(90 degree)

Sine wave with phase 90° starts at time 0 ; peak amplitude → decreasing amplitude.



(180° degree)

Sine wave with phase 180° starts at time 0 ; zero amplitude → decreasing amplitude.

* The instantaneous changes in the value of amplitudes of a signal are represented by s(t). The s(t) varies as sine of an angle varies between 0° and 360°.
* s(t) varies from 0 to maximum so, then to 0, then to minimum -so value, then to 0 during a cycle.
* Signal s(t), at an instant t, is given by a sinusoidal equation,

$$s(t) = s_o \sin\left[(2\pi \times f \times t) + \phi t_o\right] \quad \text{——} (1)$$

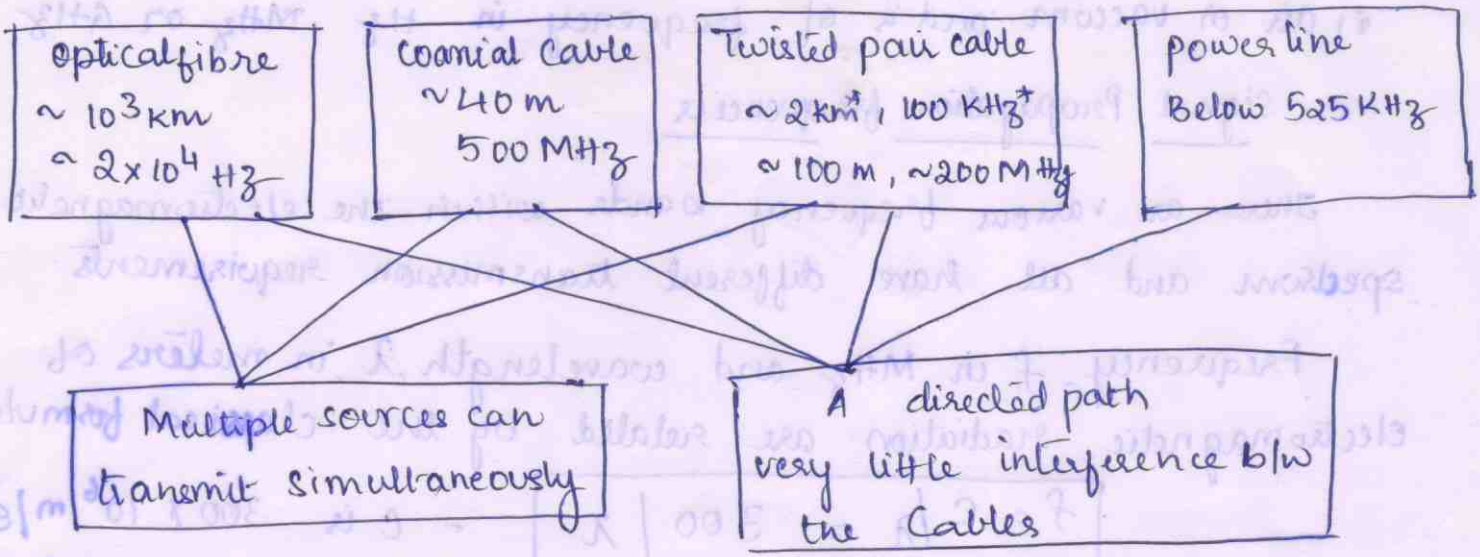
where, s_o → peak amplitude ; ϕt_o → phase angle.

* A periodic wave w.r.t fourier equation is given by;

$$s(t) = \sum a_n \times \sin\left[(2\pi \times n \times f \times t) + \phi t_o\right] + \sum b_n \times \cos\left[(2\pi \times n \times f \times t) + \phi t_o\right] + 0.5\, a_o \quad \text{——} (2)$$

Guided Transmission: It is also called wired Transmission.

- In a wired transmission, signals can be transmitted through fibre, wired or ~~wireless~~ medium like fibre, wire etc which are stated below



- Guided transmission of electrical signal takes place using four types of Cables.

(i) optical fibre for pulses of wavelength 1.35 - 1.5 μm

(ii) Coaxial cable for electrical signals of frequencies upto 500 MHz and upto a range of 40 m

(iii) Twisted wire pairs for Conventional (*with coding) electrical signals of upto 100 KHz and upto a range of 2 km, or for coded signals of frequencies upto 200 MHz and a range of about 100 m

(iv) Power lines friencies b/w 10 KHz and 525 KHz.

- Using multiplexing and coding, a large numbes of signal sources can be simultaneously transmitted along an optical fibre, a coaxial cable, or a twisted pair cable.

- But the disadvantage in a guided transmission is, the
  * Signal transmitter & reciever, both are fixed.
  * No mobility.
  * Limited Nodes.

Unguided Transmission:

Unguided or wireless transmission is carried out through radiated electromagnetic energy. This electromagnetic energy flows in free space i) air or vaccum and is of frequency in Hz, MHz or GHz.

Signal Propagation frequencies.

There are various frequency bands within the electromagnetic spectrum and all have different transmission requirements.

Frequency, f, in MHz and wavelength, λ, in meters of electromagnetic radiation are related by the classical formula

$$f = c/\lambda = 300/\lambda$$

- c is 300×10^6 m/s Velocity of Signal Propagation

- The frequencies, & wavelengths of transmitters for various ranges are.

1. Long wavelength radio, very low frequency (LW):
   30 KHz to 1 MHz (10,000 to 300 m)
2. Medium wavelength radio, medium frequency (MW):
   0.5 to 2 MHz (600 to 150 m)
3. short - wavelength radio, high frequency (SW):
   6 to 30 MHz (50 to 10m)
4. FM radio band frequency : 87.5 to 108 MHz (3.4 to 2.8 m), maximum range 50 km.
5. Very High Frequency (VHF) :

   50 to 250 MHz 6 to 1.2 m

   (DAB) Digital Audio Broadcasting band III VHF 174 to 240 MHz, 226±4 MHz, maximum range 50 km.

   TV VHF channels 174 to 230 MHz maximum range 50 km.

6. Ultra High frequency (UHF):

   200 to ~2000 MHz 1.5 to 0.15 m

   DAB 1.452 to 1.492 GHz.

   TV UHF 470 to 790 MHz maximum range 10 km.

DVB
Digital Vedio Broadcasting
TV UHF Band IV/V — 470 - 830 MHz

Mobile TV band IV, — 554 MHz

Mobile Communication frequences — GSM 900, GSM 1800
GPRS, HSCSD, DECT,
3G, CDMA
Bwetooth 2.4 GHz.
maximum range ~5 km.

(7) Super high micro wave frequency (SHF):
2 ~~to~~ .40 GHz (~15 to 0.75 cm)

(8) Extreme High frequency (EHF):
Above 40 GHz to 10^{14} Hz (0.75 cm to 3 MM)

(9) Far infrared:
Optical wavelengths between 1.0 MM and 2.0 MM
and $(1.5 \text{ to } 3) \times 10^{14}$ Hz

(10) Infrared: 0.90 to 0.85 MM in wavelength
and ~$(3.3 \text{ to } 3.5) \times 10^{14}$ Hz

(11) Visible light: 0.70 MM to 0.40 MM in wavelength and
~$(4.3 \text{ to } 7.5) \times 10^{14}$ Hz

(12) ultraviolet: < 0.40 MM in wavelength (> 750 THz)

Properties of very high and Ulta High frequencies:

⇒ VHF and UHF frequencies of wireless transmission and their properties are discussed below.

VHF 50 - 250 MHz Range: ~ 50 km
TV VHF 174 - 230 MHz

Advantages:
- Frequency modulation and multiple frequency band transmission possible.
- Transmitting antennae length 3m to 60 cm.

Disadvantages:

- Mobility not practical as transmitting and recieving antennae length needed is 3m to 60 cm and a dish antenna is required at the recieving end.

Properties of UHF (ultra High frequency):

UHF 200 - 2000 MHz

GSM 1800 and 900 1710 - 1880 MHz ; 890 - 960 MHz

DECT and 3G ~1880 - 2190 MHz

DAB 1452 - 1472 MHz 223 - 230 MHz

Advantages:

+ Multiple frequency bands, modulation methods, multiplexing and coding are feasible due to availability of greater bandwidth

- Mobility is very practical,

Disadvantages:

- Signal quality degradation due to losses within buildings and reflections from large buildings.
- A large number of base stations required at seperations of about 1-5 km each

Mobile Computing

GSM - Global system for Mobile Communications.

GSM is one of the worlds most popular mobile communication standards in 2G communication. It uses cellular networks.

Frequency range of GSM:

GSM standard operates in three different frequency ranges.

1) 900 MHz 2) 1800MHz 3) 1900 MHz.

These three bands together are called triband. A cellular phone which operates in tri-band enables international roaming very easily in the countries which have adopted GSM.

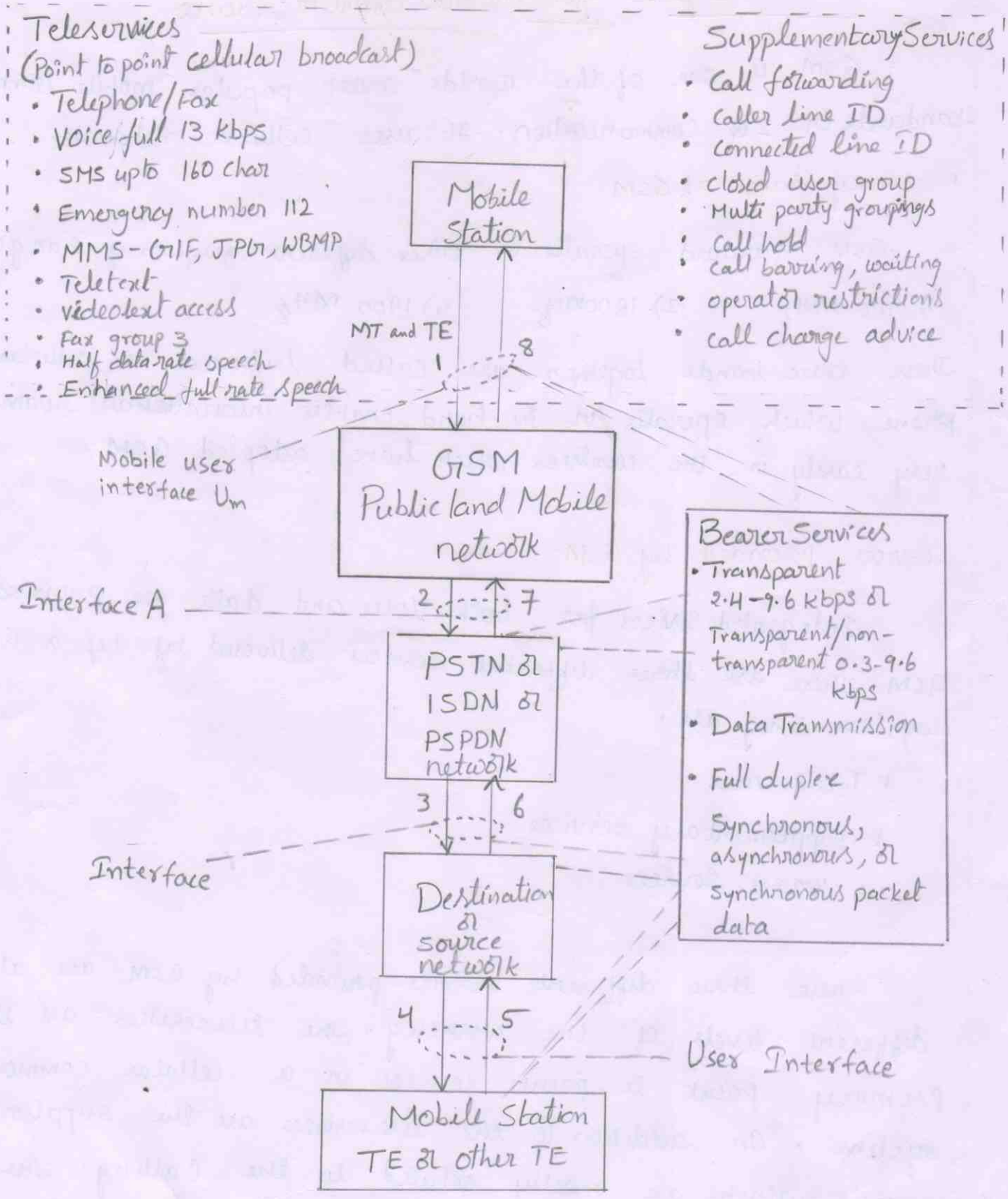
Services provided by GSM:

Integrated services for both Voice and data are provided by GSM. There are three different services delivered by by a GSM system. They are;

* Teleservices
* supplementary services
* Bearer Services.

These three different services provided by GSM are at different levels of the working. The teleservices are the primary, point to point service in a cellular communication system. In addition to the teleservices are the supplementary services which are mostly related to the Calling. The Bearer services focus on data transmission between the two networks.

Let us consider the GSM system and understand where exactly the various services are exhibited.



Integration of teleservices, bearer services, and supplementary services in a GSM system

A mobile station MS has a mobile Terminal, MT, which is a subunit and encodes voice and data signals from the terminal for transmission and also decodes the recieved signals back into voice or data to the terminal of user.

So, → An MT, mobile terminal acts as an interface between a communication network and a terminal, TE.

→ TE is used by a caller to connect and talk ie) either the source or destination of service.

→ Interface means a radio interface, consisting of a communication hardware and software which is capable of sending and detecting signals with the help of an antenna.

Connection:

→ A connection is established between the two terminals, TE's ie) source and destination. Here the destination may or may not belong to a GSM network.

It can be,

* GSM network
* PSTN - Public Switched Telephone network
* ISDN - Integrated services Digital Network
* PSPDN - Public Switched Public Data Network

→ When a user calling from a terminal TE, he uses

* interface 1 to transmit to a GSM public land mobile network.
* interface 2 to a PSTN network / PSPDN / ISDN network.
* interface 3 to a source - destination network
* interface 4 to a mobile station terminal.

→ Now the connected terminal TE, communicate back by using the interfaces 5, 6, 7 and 8. There are four sets of interfaces (1,8), (2,7), (3,6) & (4,5) each having a transceiver. A transceiver is a transmitter com receiver, which work is a full duplex mode here is GSM.

The GSM connection Establishment:

* The GSM mobile phone connects to the PSTN phone. In this case, a mobile station at the Caller end interface the GSM landline mobile network through user interface Um.
* A GSM mobile phone connects to another GSM phone. Here a mobile station TE at the caller end interfaces to a GSM public landline or mobile network. The destination for the call is another mobile station TE which interfaces the source - destination networks.
* A landline phone connects to a GSM phone. The source TE at the caller end interfaces to the PSTN networks. The destination for the call is a mobile station TE which interfaces to a GSM public land network.

Teleservices: These are offered to a caller(TE).

*) Telephone / fax
*) Telephonic voice at full data rate - 13.4 kbps
*) SMS upto 160 characters
*) Emergency number 112
*) MMS - in GIF, JPG, WBMP formats
*) Teletext and videotext access
*) Fax group 3
*) Half data rate speech
*) Enhanced full rate speech

Supplementary services:

Additional supplementary services are provided to the caller and destination TEs.

*) call forwarding
*) Caller line ID
*) Connected line ID
*) closed user group
*) Multiparty groupings
*) Call hold
*) Call barring, waiting
*) Operator restrictions
*) call charge advice.

Barrier services:

They are responsible for data transmission using the intermediate interfaces in a mobile network. Bearer means a set of data which is transmitted from or recieved by a TE, terminal is either by

*) transparent and uses data rates of 2.4 Kbps, 4.8 Kbps or 9.6 Kbps
*) non-transparent and uses lower data rates (300 bps to 9.6 Kbps)
*) Data transfer either as - synchronus data transfer
- Asynchronus data transfer
- synchronus data packet transfer

Transparent data transfer is transfer of data using physical layer and using only physical layer protocols. The physical layers transmits or recieves data after formatting or multiplexing or insertion of forward error correction bits using wired or wireless medium.

Non transparent data transfer

Non transperent means the service interface uses physical layer, data link layer and flow control protocols In the data link layer framing is done to the data from the physical layer.

When aditional bits are appended or the encryption of data is done or the error control bits are inserted and there is handshaking between the reciever and transmitter then data transfer is non transperent.

In GSM bearer service, a error correction facility called RLP - Radio Link Protocol is used which helps in robust transmission of data with very small bit error rate - BER.

Synchronus data transfer in GSM system:

Voice and SMS data transfers are synchronous. Voice is converted into bits after coding in a GSM system and then bits are transfered at data rates of 13 Kbps as synchronus data. Here there is no waiting time during the transmission of bits.

* An SMS is transmitted through a GSM channel as syn. data - There are no in-between acknowledgements and any transmission errors are corrected using FEC (Forward Error Correction)

Asynchronus data transfer in GSM system:

Asynchronus in the sense, data is transmitted by the transceiver at different or variable data rates. Usually Handshaking or Acknowledgement of messages such as 'reciever ready', 'receiver not ready', 'recievers acceptance of data unnumbered', 'receiver rejection', 'set asynchronus balance mode', or 'disconnect'.

Synchronous packet transmission in GSM :

Here each packet flow is transmitted as synchronous data. so there is no handshaking /Ack of data during the flow of packets The packets may flow through different interfaces, routes, channels or time slots to reach a common destination but the time taken for each packet remains constant after the route path is established.

data rate $= n/T$	$n \rightarrow$ no of bits. $T \rightarrow$ Time interval to transmit n bits

Sub systems of GSM architecture

GSM network is divided into three subsystems namely.

(1) Radio subsystem (RSS)
(2) Network subsystem (NSS)
(3) Operation Subsystem (OSS)

(1) Radio sub system :

It comprises all radio specific entities, The basic function of RSS is to connect the mobile station to the network. RSS consists of a number of Mobile stations (MS's), Base Transceiver Stations (BTS) and Base station controller stations (BSC)

Mobile station (MS) is the mobile device or phone. MS connects to the GSM network. MS consists of a mobile Terminal (MT). which is the device itself. It has both the hardware and software to transmit and recieve GSM data.
MS also consists of a user terminal (TE). User recieves and sends data through the TE.

Each Mobile station has a SIM. SIM is a card which is inserted into the MS.

SIM contains the following information which is..

* IMSI - International Mobile Subscriber Identity (unique 15 digit)
* Serial number and type of SIM card.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

_ _ _

3-digit Mobile Country code
2-digit Mobile Network code
10 digit Mobile Subscriber Identity number (MSIN)

* PIN (personal identification number)
* PUK (PIN Unblocking Key) to unlock SIM if it accedentally locked due to something.
* TMSI (Temporary mobile Subscriber Identity) used for identifying MS during connection to protect UID from hackers
* LAI (location Area Identification)
* Temporary mobile dynamic cipher key for Encryption.
* Cipher key is a 128-bit authentication key provided by service provider. If MS is not authenticated, the service is blocked to that number.

Base transceiver station : (BTS)

A BTS interfaces to a number of Mobile stations. The connection between BTS and each MS is established through user interface Um. Um is an ISDN U interface for a mobile. BTS - BSC interface is A bis. An Abis transciever transmits and recieves data with four multiplexed channels of 16 Kbps each or with the help of a single 64 Kbps fixed line channel.

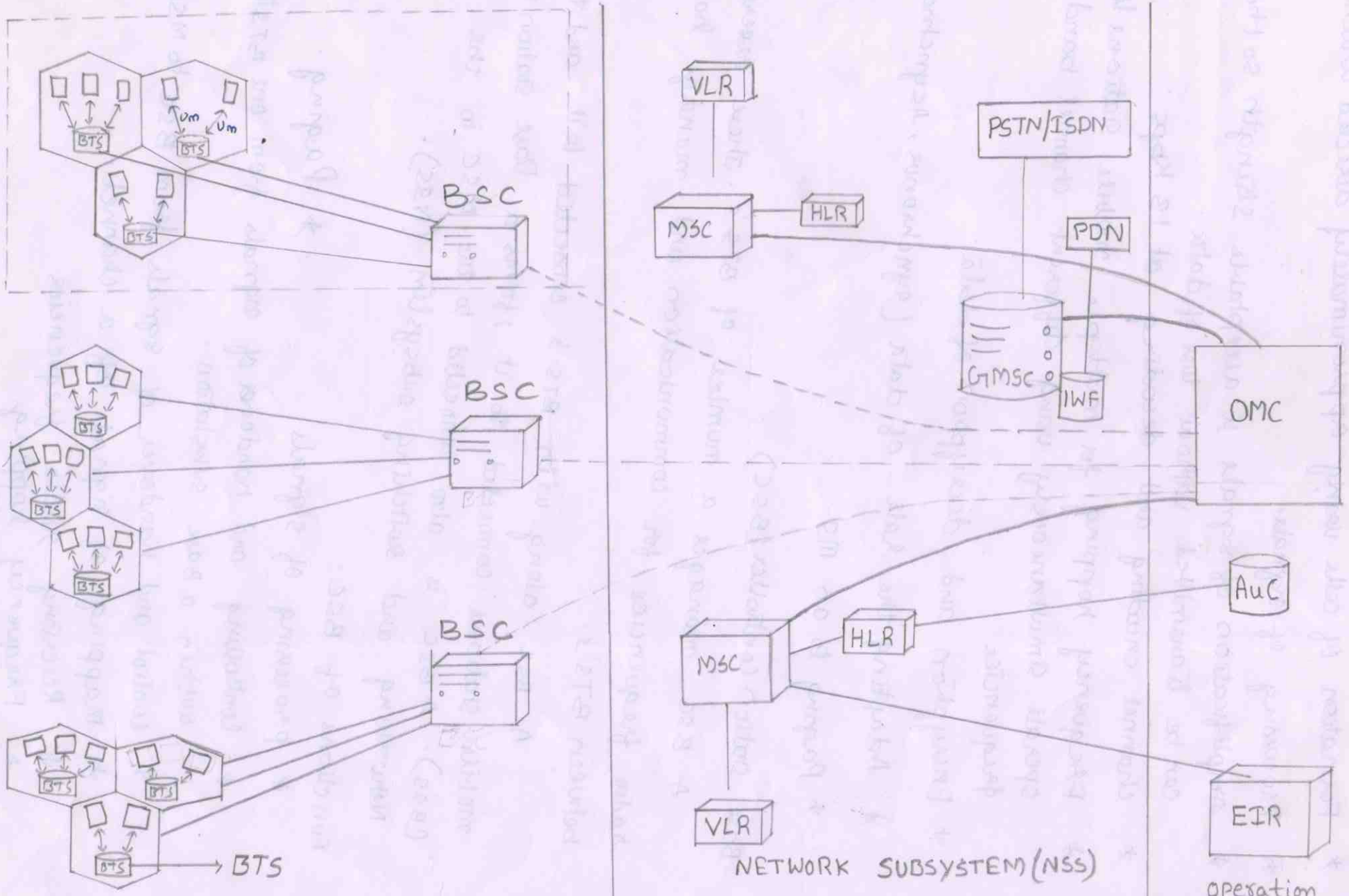


FIG- GSM NETWORK ARCHITECTURE

Functions of BTS:

* Formation of cells using approximately directed antennas.
* Processing of signals.
* Amplification of signals to acceptable strength so they can be transmitted without loss of data.
* channel encoding and decoding at 13 Kbps.
* Frequency hopping for multiple mobile stations to operate simultaneously using different channel band frequencies.
* Encryption and decryption of data.
* Adapting the rate of data (synchronus, Asynchronus)
* Paging to an MS.

Base station controller (BSC)

A BSC manages a number of BTS's. These reserve radio frequencies for communication and manage handovers between BTS's.

A BSC along with BTS's connected to it and the mobile stations connected to it, forms a Base station system (BSS). A BSC is also connected to the MSC in the Networking and switching subsystem (NSS).

Functions of BSC:

* processing of signals
* Paging.
* Controlling and handover of signals from one BTS to another within a Base substation.
* control and handover of signals from BSC to MSC.
* Mapping of signals of a channel.
* Reserving radio frequencies
* Frequency hopping
* Traffic control
* Authentication, encryption and decryption of data.
* Updating location registers of MS's.

(2) Network subsystem of GSM system (NSS):

The NSS consists of a number of mobile services switching centres (MSCs). Each MSC interfaces to a number of BSCs in RSS. There are also home location registers (HLRs) and visitor location registers (VLRs).

The network subsystem acts as a interface between wireless and fixed networks. It mainly consists of switches and databases and manages many functions such as handovers between BSS's, world wide user localization, maintainance of user accounts, call charges and management of roaming.

Functions of MSC

MSCs manage BSCs in a geographical area. MSC connects BSC over 'A' interface. They have high performance digital ISDN switches.

* processing of signals
* Establishing and terminating the connection between mobile stations via BSC's.
* Establishing and terminating the connection between an MS and a fixed line phone via a GMSC or IWF
* monitoring of calls made to and from an MS
* Call charging, multiway calling, call forwarding and other supplymentary services.

Home Location Register (HLR):

The home location register has the databases of MSes in a GSM network. It stores

* ISDN number - MSISDN
* details of subscription permissions like call forwarding, roaming etc.

* subscribers IMSI
* user location area
* users current VLR and MSC status.

Each user has only one HLR record world wide which is updated constantly in real time. The HLR contacts AuC in the OSS for authentication. Each HLR is associated with an MSC so that when an MS registered at a certain HLR moves to another location area (LA), serviced by another MSC, the user's home MSC updates the user's current VLR. HLR's help in location updating of a mobile station.

Visitor Location register (VLR):

Each MSC has a VLR. VLR is dynamic real time database that stores both permanent and temporary subscriber data which is required for data communication between MS's in coverage area of MSC associated with that VLR.

Gateway Mobile services switching centre (GMSC):

It handles connections to other fixed nodes in networks. The other networks may be ISDN, PSTN, PSPDN or other PLMN networks. Special Inter working functions (IWF) is used by a GMSC to connect to public data networks such as X.25.

(3) Operation sub system (OSS):

This facilitates the operations of MSC's. The OSS administers the operation and maintainance of entire network.

Operation and maintenance centre (OMC):

An OMC monitors and controls all other network entities through the 'O' interface. The OMC's typical tasks include management of status reports, traffic monitoring, subscriber security management, and accounting and billing.

Authentication centre (AuC)

An authentication centre (AuC) is used by HLR to authenticate a user. The AuC may be a secured partitioned part of HLR itself. Since mobile networks are quite vulnerable to attacks, the GSM standard specifies that the algorithm for key generation should be seperated out as an OSS network entity. This entity is the AuC. The AuC database stores Subscriber authentication keys. The authentication parameters are taken care by AuC and conveys them to HLR.

Equipment Identity Register (EIR):

The equipment identity register stores international mobile equipment identity (IMEI) numbers for the entire network. The IMEI enables the MSC in identifying the type of terminal, mobile equipment manufacturer, and model and helps the network in locating the device in case it is stolen or misplaced.

The EIR contains 3 different types of lists:

1. A black list that includes mobile stations which have been reported stolen or are currently locked due to some reasons.
2. A white list which records all MSs that are valid and operating.
3. A grey list including all those MSs that may not be functioning properly.

Working of GSM Architecture:

→ RSS consists of a number of base station controllers (BSCs) and each BSC connects to a number of base transceiver stations (BTSs) which in turn provide radio interfaces for mobile devices (MTs).

→ The various BSCs in the RSS layer connect to MSCs in the NSS. A single MSC can connect to multiple BSCs. Each BSC in turn communicates with a number of BTSes and so on.

- A Base Substration (Bss) layer consists of a set of BTS's interfaced to a BSC.
- The Network subsystem (NSS) consists of l mobile services switching centres (MSCs), m and n home and visitor location registers, gateway MSCs (GMSC) and interworking functions (IWF) with the mobile switching centres.

→ When a mobile station 'A' communicates to another mobile station 'B', a MSC established a connection or channel between (i) A is interfaced to BTS then to BSC and then to MSC
(ii) B is interfaced to BTS, BSC & MSC

- The RSS and NSS provide a radio subsystem for the communication. MSCs must have location registries to enable the NSS to discover a path between MS. 'A' and 'B'.
- In the OSS, each AuC is associated with an HLR in the NSS and each EIR connects to an MSC. An OMC at OSS can connect to an MSC or a GMSC in the NSS and to a BSC at RSS.

Radio Interfaces Of GSM:

A radio interface is a transceiver of signals, Um. Two electrical signals from two sources cannot have same set of frequencies at the same time as two sets of the signals should not interfere. Interference means one signal modifying the other the signals of same frequency band cannot access the medium at the same time.

SDMA multiplexing is a method in which the same set of frequency components of the same range and at the same time slot can access the medium in different directions or cells.

TDMA multiplexing is a method in which frequency components of same range in same direction or cell can access the medium in different time slots for different Um radio interfaces.

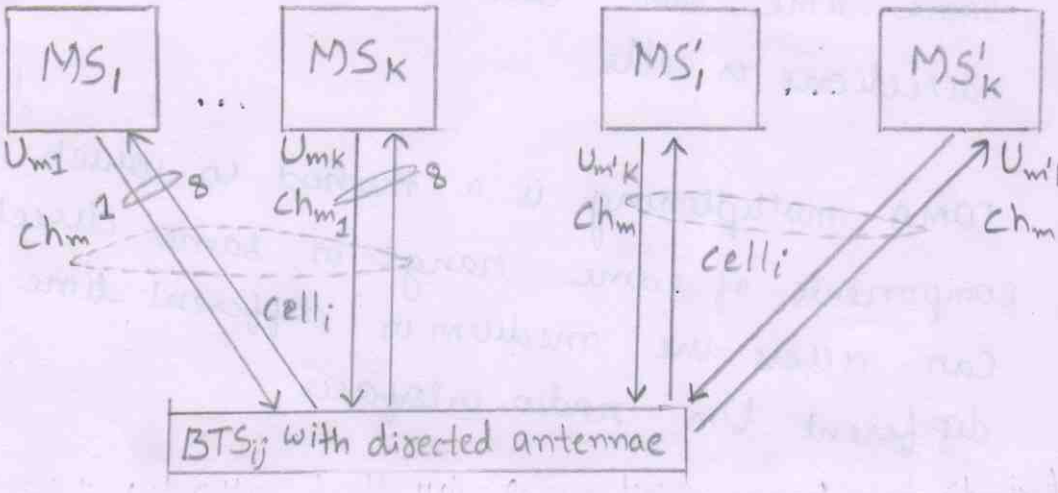
FDMA multiplexing is a method in which different set of frequency components of a frequency range are allotted to different Um radio interfaces and they can access the medium in same direction or cell and in same time slots.

The base transceiver and the mobile stations communicate across the Um interface for managing tasks such as call setup and voice and data traffic.

1) Space Division Multiple Access:

Assume a BTS_{pq} with n directed antennae covers mobile stations in n cells. Each cell defines a space. A given BTS covers the p^{th} cell and the cell is presently covering k mobile stations, $MS_1, MS_2 \ldots MS_K$. There is space division multiplexing of the signals from the MS's. Chm is the radio carrier channel. The MS's cell i and cell j uses the same Chm in the same time slot.

fig: SDMA for mobile stations



2) Time Division Multiple Access:

BTS has mobile stations in a cell. A set of a maximum of eight data bursts of MS's out of l MS's can be assigned a radio carrier channel by a BTS. The cell i covers eight mobile stations $MS_1, MS_2 \ldots MS_8$. There is time division multiplexing of the signals from each set of eight MS. An MS can use the same radio carrier channel Chm in one or more of the eight distinct time slots $SL_0, SL_1 \ldots SL_7$ each of 577 μs.

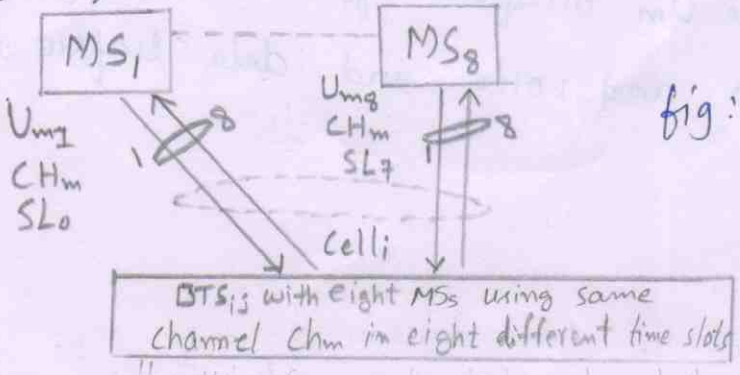


fig: TDMA by mobile stations

Data burst and Data frame in TDMA:

A set of data bits in an SL is known as a burst. A set of eight data bursts defines a data frame. A mobile can send multiple data bursts within a data frame.

Format of Data burst

H bits 3 bits	User or Control 57 bit	S bit	26 TR bits	S bit	User or control 57	T 3bit

H - Head bits

T - Tail bits

TR - Training bits

S - source bit < MS or NSS control data.

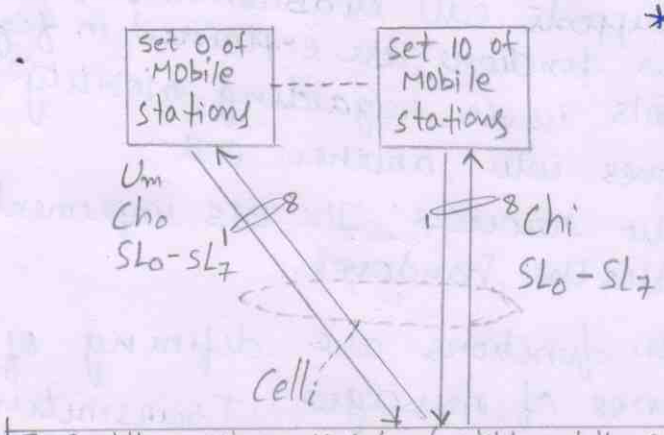
User or control < Subscriber data or NSS control data bits

3) Frequency Division Multiple Access:

FDMA divides the available spectrum bandwidth into different frequency channels for communication by multiple sources.

- A set of maximum of 124 radio - carrier channels each of 200 kHz band width can be used in GSM 900 downlink channel.
- A set of 124 in the uplink channel can be used.
- Each channel transmits frames of 4.615 ms (eight time slots each).
- The frequency slot of each channel is 200 kHz (= ±100 kHz).
- The figure shows FDMA by 124 sets of mobile station in cell i using different carrier channels between C_0 to C_{123} in available 124 different frequency bands.
- The frequency ranges are Ch_1: 890.1 MHz ± 100 kHz, Ch_2: 890.3 MHz ± 100 kHz ... Ch_{123}: 914.9 MHz ± 100 kHz. } uplink
- Ch_1: 935.1 MHz ± 100 kHz, Ch_2: 935.3 MHz ± 100 kHz ... Ch_{123}: 959.9 MHz ± 100 kHz. } downlink

* In 124, 90 channels are used by BTS & MS radio interfaces. 32 reserve channels are available for GSM 900.



FDMA by mobile stations in Cell i using different radio-carrier channels

Protocols of GSM:

Each layer of a communication network has different protocols for governing its communication with adjacent layers. The MS, BTS, BSC and MSC have 3 layers - physical, datalink and network. The transport and session layer functions are taken by network layer protocols. Presentation is taken care by other layers. The TE (uses) application at either end controls the application layer protocols.

1) Mobile Station - Base Transceiver Signalling Protocols:

The physical layer between MS and BTS is called radio, whose functions are shown in figure. The data link layer controls the flow of packets to and from network layer. Its protocol is LAPDm - Link Access protocol D-channel modified for Um interface. The functions of LAPDm is shown in the figure.

- The synchronization and error correction are handled by Um radio interface at the physical layer.
- LAPDm is 184 bit.
  - * Eight bit address field (optional)
  - * Eight bit control field (identifies frame type (command frame / response frame))
  - * Eight bit length field (of information)
  - * Information bits of variable length.
  - * Remaining filler bits as 1's.
- There are 16 filler bits to make 184-bit LAPD, when there is 144-bit info. With 24 bit address, control & length fields. If info is 160 bit then there are no filler bits.
- The CM sublayers supports call establishment, maintainance and termination and other functions are explained in fig.
- The MM layer controls issues regarding mobility management when an MS moves into another cell.
- RRM manages Radio resources. The BTS implements only RRM' as the BSC handles the handovers.
- The network layers functions are defining of protocols, defining addresses of messages, Transmiting the logical channels data and information bits as well as Receiving them.

LAPDm:
- Data flow Control
- Acknowledged / unacknowledged data transmission
- Address and sequence number checks
- Access Point for the multiple services
- Re-sequencing of data
- Segmentation
- Data re-assembly

Radio:
- Full or half duplex access
- SDMA, TDMA and FDMA
- Bursting and framing
- Synchronizing the MSs and path delays corrections
- Frequency correction
- Coding, FEC, CRC, data interleaving and encryption
- Error handling
- GMSK digital modulation and transmission
- Demodulation and reception
- Decryption and decoding

CM:
- Protocols for call setup maintenance, termination, and resetting on interruption at MM (uses CCCH)
- Protocols supplementary services using CCCH (uses SADCCH)
- Protocols for SMS (uses SADCCH)
- DTMF Signal Control

MM:
- Registration
- Location update
- Authentication and identification methods IMSI
- Use of TMSI allocated by VLR in place of IMSI at HLR
- Maintaining reliable communication with upper layers

RRM:
- Radio link quality management
- Frequency assignment
- Frequency hopping Sequence option
- Signal measurements and handover management
- Adaptation of the timing advance for synchronizing

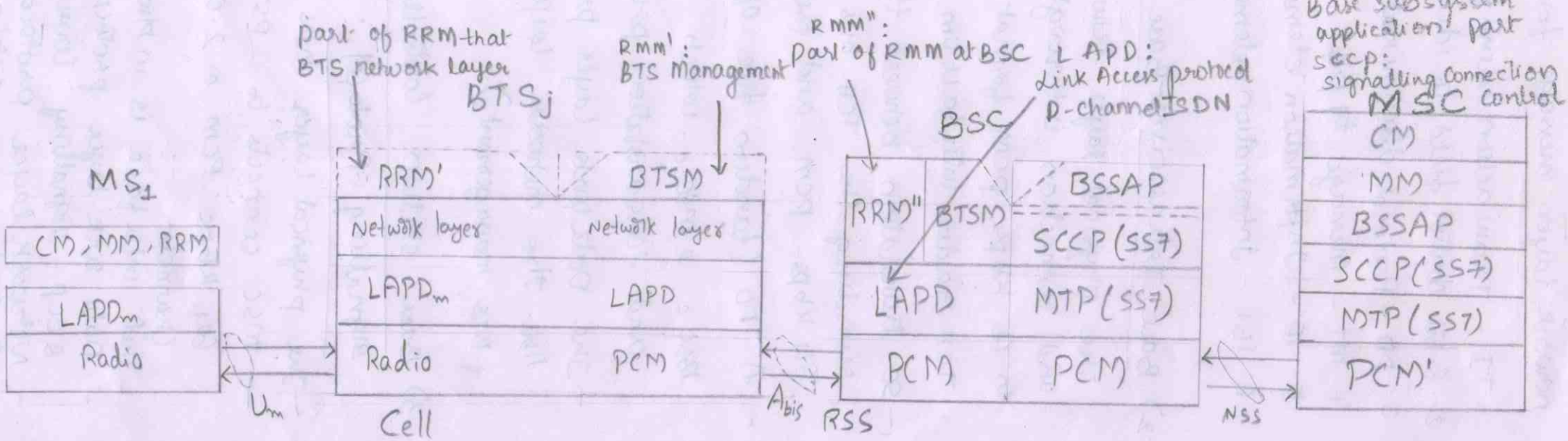


FIG: Protocols of GSM

network layer message format :

1. TI - Transaction Identifier
2. 8-bit control field to identify frame type
3. PD - Protocol discriminator
4. MT - message type
5. IE - Information element for optional information.
6. IEI - Information element identifier to identify IE field information.

2) Base Transceiver-Base station controller Signalling Protocols:

The physical layer between BTS and BSC is A_{bis} interface. and connection is through wired network. The voice is coded to 64 kbps PCM format in PSTN n/w at A_{bis}. whereas TCH radio interface Um uses 22.8 kbps b/w MS & BTS.

- So translation between these coding formats is performed by recording the TCH bits recieved from the caller MS to 64 kbps PCM and from PCM to TCH for the reciever MS.
- A TFO (tandem free operation) can be adopted at BTSs, BSCs & MSCs. which helps to avoid repeteted translation and retranslation process to maintain voice quality.
- The Data link layer protocol b/w BTS and BSC is LAPD for A_{bis}. The network layer protocol b/w BTS & BSC is BTSM (BTS management).

3) Base station Controller - Mobile services Switching Centre signalling Protocol :

- The physical layer has PCM' - Pulse code modulation multiplexed
- MSC connects to PSTN, ISDN, PSPDN n/w which employ 64 kbps PCM or 2.048 Mbps CCITT which carries 32 PCM channels.
- This interface is in b/w BSC & MSC which are wired.
- Data link layer protocols are MTP - message transfer Protocol, SCCP - signalling Connection control Protocol
- Network layer protocal at BSC is BSSAP - Base Substation Application part. The sublayers are depicted in figure.

Localization:

Localization is a process in which the mobile station is identified, authenticated and provided service by a MSC. MSC performs these functions through BSC and BT either at home location or visitor location.

- User wants instantaneous service but the mobile service provider will initially identify the mobile station of user and verify the services subscribed to by the user or the services presently allowed and then he will be serviced. Localization fulfils both the requirements.

NSS of GSM periodically updates the location of those MSs which are not switched off and are not struck off from the list of subscribers to the given mobile service. The SIM in MS stores LAI - Location Area Identification. which is updated by MSC which covers MS's current location. TMSI - Temporary Mobile Subscriber Identity is also stored with SIM which is assigned by VLR.

The VLR updating process is, each MSC is associated to a VLR and an HLR. An MSC_A has an HLR_A at which mobile station is originally registered on subscription to a mobile service. The HLR_A copies the HLR information of MS to VLR_B when the MS moves out to the area covered by MSC_B. The copy saves time as the MSC_B gets instantaneous information regarding MSi from VLR_B instead of having to fetch of information for relocated MSi from HLR_A is saved. The storing of LAI into the SIM from the VLR through MSC_B, BSC, BTS saves the time that otherwise would have been spent in identifying the BTS, BSC, MSC_B. These processes help the MS in getting service from MSC_B instantaneously.

Call Handling:

The various types of calls handled by a GSM networks are

(1) Mobile → PSTN Calls
(2) Mobile → Mobile calls
(3) PSTN → Mobile Calls
(4) Mobile → Base Transceiver for Message exchange.

(1) Mobile → PSTN Calls:

MS (Mobile station) tries to establish connection with a PSTN, the procen is as follows:

1. MS_i connects to BTS_i, then to BSC_i and then to MSC_i.
2. MSC_i verifies and authenticates MS_i using the VLR through k and l.
3. MSC_i switches to MSC_j, then to GMSC$_j$, then to TE_j.
4. TE_j transmits back to GMSC$_j$ and MSC_j
5. MSC_j switches to MSC_i, which transmits back to BSC_i, BTS_i, and MS_i.

(2) Mobile → Mobile Calls:

When a mobile terminal MS_i calls and communicates with another mobile phone MS_j, the communication between them is routed and procen is as follows:

1. MS_i connects to BTS_i, then to BSC_i and then to MSC_i.
2. MSC_i verifies and authenticates MS_i using the VLR through i and j. It also discovers through available paths to a mobile phone MS_j through MSC_j.
3. MSC_i switches to the MSC_j and verifies and authenticates MS_j using the VLR through k and l.
4. MSC_j connects to BSC_j, BTS_j and MS_j
5. MS_j transmits back to MSC_j.
6. MSC_j switches to MSC_i, which transmits back to BSC_i, BTS_i, and MS_i.

(3) PSTN → Mobile calls :

PSTN → mobile calls are calls originating from a PSTN phone and terminating in a mobile destination employ the GMSC. When making a call to a mobile terminal MSj, the PSTN terminal TEi connects to GSM C which, in turn, requests HLR, to discover MSCj. MSCj uses VLRj to verify and authenticate the MSj and then MSCj directs the call to MSj through BSCj and BTSj.

(4) Message exchange between Mobile Station → Base Transciever:

This is done through the following process

(1) The MS request the BTS to grant it a channel for communication and BTS responds immediately by assigning a channel to the MS.

(2) The MS sends a request to BTS for service and BTS replies with a request for authentication to MS.

(3) The BTS transmits its response for authenticating the MS along with a command for ciphering at MS.

(4) The MS runs an algorithm on ciphering number sent by the BTS and the cipher key stored in SIM.

(5) The call is set up using CM (Call Management) protocol by the MS and the BTS management protocols by BTS.

(6) Call setup is confirmed by the BTS to MS

(7) Assignment commands are sent by the BTS to the MS and assignment completion messages are sent by the MS to the BTS.

(8) An alert message is sent from the BTS to MS and ~~assignment~~ completion before the connection.

(9) A connection establishment message is sent from the BTS to the MS and connection ~~establishment~~ acknowledgement is sent from the MS to the BTS.

(10) Voice & data interchange starts.

Handover :

A mechanism to hand over the control of a mobile device to the neighbouring cell is called HANDOVER. It is transferring a call in progress from one channel to another.

The two main reasons of handover in a cellular network:

(a) If the mobile device moves out of the range of one cell and a different base station can provide it with a stronger signal.

(b) If all channels of one base station are busy, then a nearby base station can provide service to the device.

Handover in GSM :

(1) Inter Cell Handover :

SDMA by mutiple antennae usage at same BTS, forms multiple cells. The signal measurements are continously performed at the RRM sublayers in the MS, BTS and BSC. RRM is responsible for handover management. When the signal strength goes weak due to several reasons, there is handover from a cell to another. This process is called inter cell handover. There is a boundary region where the signal quality improves and error rates decrease on handover.

(2) Inter - MSC handover :

Handover also takes place for load balancing when the traffic from the cells and BSCs is high. An ongoing call, which is being handled by a cell, may be handed over to another MSC. Since the two MSCs are interfaced through PCM, the handover is performed over a wired line.

(3) Inter - BSC handover :

Handover that takes place for load balancing when the traffic from the cells and BTSs ~~as well as the BSCs is~~ is high. The ~~BTSs connected to a BSC and~~ BSCs connect to an MSC. A call going in a cell through a BTS, may be handed over to another BSC connected to the same MSC. Since the BSCs

connect to the MSC interfaces by PCM, the handover is over a wired line.

4) Inter-BSC, inter MSC handovers:

The BTSs connect to a BSC and BSCs connect to an MSC. A call, being handled by a cell through a BTS, may be handed over to another BSC connected to a different MSC.

5) Intra cell handover:

Due to interference at certain frequencies, the signal quality becomes poor. The BSC can handover the call to another frequency of the cell in such cases.

6) Inter-cell, intra-BSC handovers:

When an MS moves to a neighbouring cell and suffers poor signal quality, the BSC can handover the call to a different BTS channel of the same BSC. Since the BTSs connect to the BSC interfaced by PCM, the handover within the BTSs is over a wire but each BTS has different radio channels. The BSC, therefore, assigns a different radio channel.

7) Inter cell - Intra MSC handover:

The inter cell - intra MSC handover takes place by the following interchange of message:

* The RRM sublayer transmits a signal report from MS_i to BTS_i and from BTS_i to BSC_i. When a handover is necessary BSC_i signals the handover requirement to MSC_i

* MSC_i signals handover requirement to another BSC_j and BSC_j allocates radio resources and transmits the activated channel to another BTS_k.

* BTS_k sends acknowledgement of the channel to BSC_j and BSC_j acknowledges the handover request grant via a message to MSC_i.

* MSC_i transmits handover command to BSC_i, in turn, BSC_i to BTS_i, and BTS_i to MS_i's RRM layer. The RRM directs to operate at another channel.

Security

GSM is a radio based network system. It employs various security features to protect subscriber privacy, against misuse of resources by unregistered users. It provides Authentication centre, TMSI (temporary mobile subscriber identity and other Encryption algorithms to maintain security.

Authentication.

The Operation and maintenance subsystem of the GSM network has an AuC (authentication centre) for authenticating MS. The AuC first authenticates the subscriber MS and only then does the MSC Provide the switching service. Authentication alg uses a random number sent by the AuC during the connection setup and an authentication key which is already saved in the SIM. Authentication algorithms used can differ for different mobile services providers.

TMSI :

When an MS moves to a location area, the VLR (visitor location register) assigns a TMSI which is stored in the SIM of the MS. The identification of subscriber during communication is done using not the IMSI but the TMSI. This ensures anonymous call number identity transmission over the radio channels. This protects the MS against eavasdropping from external sources.

Encryption:

The BTS and the MS have to perform ciphering before call initation or before connecting for ~~the~~ receiving a call. The MS uses a Chipher for encryption. The cipher is a result of performing mathematical operations on

(a) the Cipher key saved in the SIM, and
(b) the ciphes number received from the BTS when the call setup is initialid.

- The randoms no. used in authentication and ciphering processes are also known as challenge to the mobile station to generate the results and if correct, BTS grants access to challenged MS.

GPRS - General Packet Radio Service

GPRS is speed enhanced data transmission service designed for GSM systems. This is done by packetizing of data and simultaneous transmission of packets over different channels. GPRS is defined by the European Telecommunication Standards Institute (ETSI)

There are different switching modes circuit and packet switching. In packet switching, packets of data at any given instant can take multiple time-slots, channels, paths or routes depending on the idle slots available at the instant and the reciever assembles the packets into original sequence in data.

GPRS is packet oriented service for mobile stations. It uses the unused slots and channels in TDMA mode of a GSM network for packetized transmission from a mobile station

GPRS Architecture :

There are four subsystems

(1) RSS - Radio sub system
(2) BSS - Base sub system
(3) NSS - Network sub system
(4) GSS - Gateway sub system

* The RSS consists of a number of MSs, BTSs, BSC_1, BSC_2 ... BSC_n
* An MS having GPRS capability stores CKSN - Cipher key sequence number, similar to that in SIM. It also stores TLLL - temporary logical link identity like TMSI in SIM
* The NSS consists of a number of serving GPRS support nodes (SGSNs) and mobiles services (MSCs).
* The GPRS system creates a GPRS Context which is stored in the MS as well as in SGSN - Serving GPRS support nodes. It stores status of MS, data compression flag, identifies for cell and channel for the packet data, and routing area information.

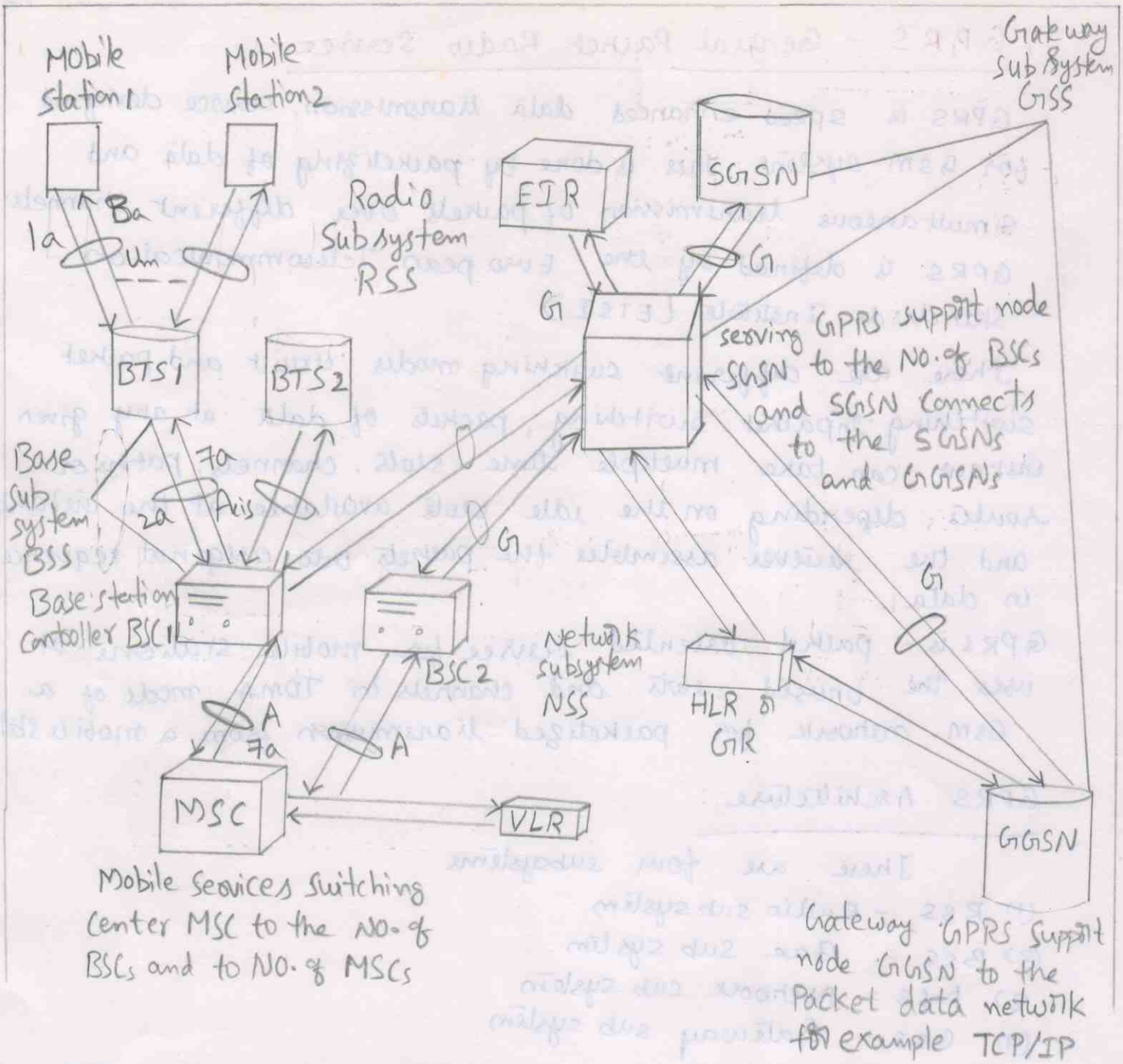


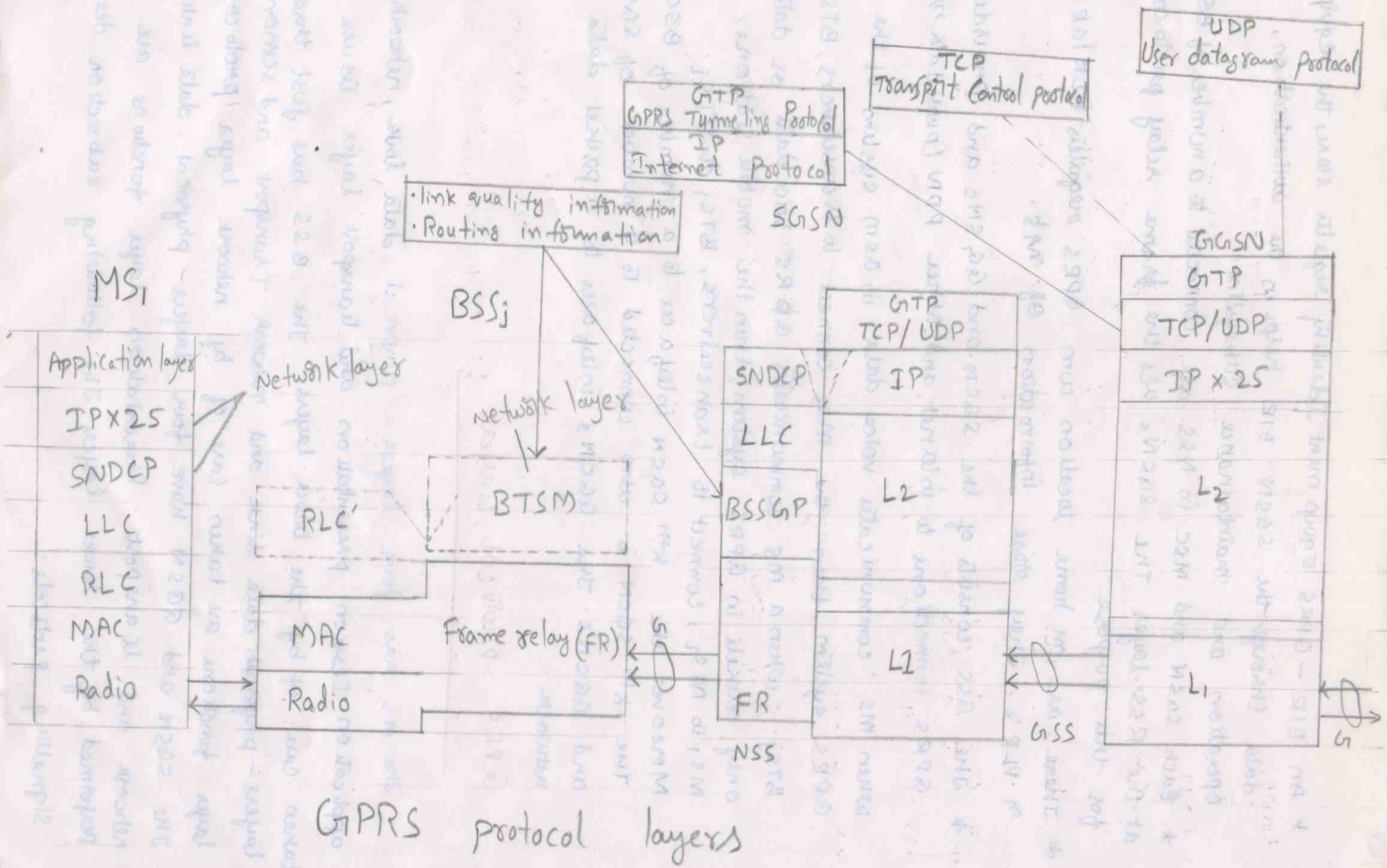
Fig: GPRS system architecture - RSS (radio subsystem) BSS (base subsystem), NSS (network subsystem) and GSS (gateway subsystem)

* An EIR – GPRS Equipment Identity register stores the equipment data through the SGSN. EIR helps in the authentication, Operation and maintainance subsystem.
* Each SGSN and MSC in NSS are connected to a number of BSCs at the RSS layer. The SGSNs ues the frame relay protocol for this purpose.
* There are m home location cum GPRS registers HLR/GRs and n VLR's. They store information of MS.
* The GSS consists of the SGSN and GGSNs and provides GPRS connections to internet and other PDN (public data n/w)

When MS communicates voice data in GSM system of the GPRS system, then the MSs connect to transcievers, BTS$_1$ to BTS$_j$. When a MS communicates GPRS voice data or data only packets in GPRS system, then the mobile stations, MS$_1$ to MS$_i$, connect to transceivers, BTS$_1$ to BTS$_i$. Moreover the k^{th} SGSN interfaces to a number of BSCs. The k^{th} SGSN is also connected to a number of SGSNs and GGSNs. The GGSNs interfaces to a packet data network.

GPRS protocol Layers :

The MS has four layers - physical, data link, network and application. Session presentation and transport layer issues are taken care of by the lower layers. The BSS has just three layers - physical, data link and network. Transport and session layer functions are taken care of by network layer protocols. The SGSN and GGSN have four layers - physical, data link, network and transport. Presentation layer functions are performed by the lower layers. The following subsection describe signalling protocols.



GPRS protocol layers

1) Mobile station and Base station subsystem signalling protocols:

The physical layer between MS and BTS is called the radio link layer in the GSM system. Data link layer protocols between MS and BSS link through the physical layer which has the interface Um, as in the case of GSM. Data link layer controls the flow of packets to and from the network layer and provides access to multiple services.

GPRS data link layer at the MS has three sublayers

1) MAC - medium access control
2) RLC - Radio link control
3) LLC - Logical link control

A special LLC provides the FEC and ARQ protocol.

→ Data link layer at BSS has two sublayers, MAC and RLC 2. The RLC manages radio link resources issues. The MS can transmit maximum eight PDTCHs. TCHs in GSM are formatted as packets and transmitted in PDTCHs. The BSS implements only RLC as the BSC and BSSGP handle the handover.

→ Network layer at the MS has two sublayers — IP / X.25 and SNDCP (sub network dependent convergence protocol). IP and X.25 are packet formatting protocols for the transmission and reception of packetized data. There are two services, voice-data and data only as in Internet.

→ The application layer at the MS provides end to end applications like voice and internet.

2) Base station subsystem and serving GPRS support system signalling protocols:

The protocol layers between the BSS and the SGSN. The physical layer for transmission and reception of data and network information between the BSS and SGSN is FR (frame relay). FR also implements several functions for the data logical link.

Datalink sublayers at the BSS and SGSN transmit and receive using BSS GP (base station subsystems GPRS protocol) A datalink sublayer at the SGSN is LLC. The network layer at the SGSN transmits and receives using SNDCP.

3) Serving GPRS support node and gateway GPRS support node signalling protocols:

Here physical layers between the SGSN and GGSN are layer 1 (L1) protocols of the Internet or other PDN.

Data link layer protocol layers between SGSN and GGSN are layer 2 (L2) protocols of the Internet or other PDN.

Network layer protocols layers at the SGSN are TCP and GTP (GPRS Tunnelling protocol). TCP is for X.25 protocol at layer 3 and UDP is for IP protocol at layer 3.
GTP uses TCP and IP or UDP and IP. The GTP facilitates flow of packets from multiple protocols. GTP information of TID (tunnel ID) helps in transmitting and assembling the packets for each sessions of the MS.

New Data Services:

GSM system provides data rates of TCH/13.4, TCH/HS 11.4, TCH/12.8, TCH/F14.4, TCH/F9.6 and TCH/F4.8. for voice data but are too low for high speed data transfer. So, speed enhancement is required for a GSM system to be able to provide data services such as transfer of large files and internet access.

- After this 2G data services, later 3G and present 4G data services are made available to the users.