10M

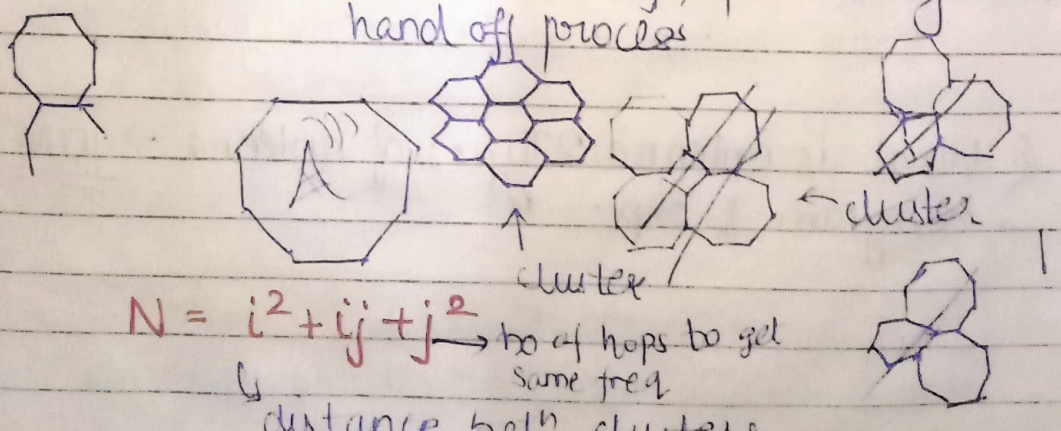
## * Applications of Mobile ~~Computing~~ Communication:

- The base stations for mobile com. are designed for a wider range (a few kilometers) whereas, Access point for wireless com covers a smaller range.
Thus, no disconnection of the ongoing comm.

- Hand off process - Switching from one B.S (Base Station) to another.
Authentication needs to be performed before the hand off process using ~~algo~~ security algos like $A_3$, $A_6$, $A_7$.

1) Vehicles
2) Wireless n/w replacement
3) Education
4) entertainment
5) location dependent services.
6) Emergencies

* **Cell** - The coverage area of a Base station.
Base station → Load balancing, providing comm, hand off process



- Advantages of mobile comm w.r.t wired n/w.

Applications:

5M
1) Emergencies
2) Business
3) Replacement of wired n/ws
4) Infotainment and more
5) Location dependent services

→ Follow-on service – automatic call forwarding, email reply
→ Location aware services – printer, fax
→ Privacy – privacy policies available
→ Information services – pull services, push services
→ Support services – cache, state information (Transaction time out, session expired, congratulations etc)

Q What is the range of visible light w.r.t. freq?

10M * Antennas

- Signal – physical representation of data
antenna – couples the electromagnetic energy

Q What is antenna? Types of antenna → 10M
→ diagram & expl.

- Omnidirectional → Single plane
- Marconi – mounted on moving elements (eg car)
↳ λ/4
- Dipole – λ/2

OTP sms
FB

- Directional antenna - 2 planes
→ Propagates only in a single direction
→ Thus, multiple antennas are required

- Sectorized antennas

- Diversity → combination of multiple ant

- Smart Antennas

* Signal propagation: 5M or + multipath 10M
Diagram imp.

- Transmission range
→ No errors expected
- Detection range
→ face atmospheric conditions
→ Authentications
- Interference range
→ gain / power is decided
→ Signal may not be detected after distortion is added

$$P = \frac{1}{d^2}$$

$$\text{Speed} = 4\pi d^2$$

* Attenuation: 10M

Q Attenuation at ~~their~~ its ~~types~~

* Multipath propagation. 5M

* Multiplexing. 10M

1) SDM → scalability problem
2) FDM } synchronisation
3) TDM }
4) TDM & FDM
5) CDMA

→ orthogonal code

Bipolar form

A = 1001 → (+1, -1, -1, +1) C

B = 1010 → (+1, -1, +1, -1) D

A * B (Bitwise multiplication)

A * B = (+1, +1, -1, -1)

Add (A * B)

= (+1, +1, -1, -1) = 0

- Guard space is maintained here as well

* Spread spectrum 10M

SS + DSS/FHSS 10M

separate - 5M

Q In DSSS list the operations occuring in ~~integrator~~ correlator (2 mks)

- Sender Side

user data 0 1

chipping data 0110101 0110101

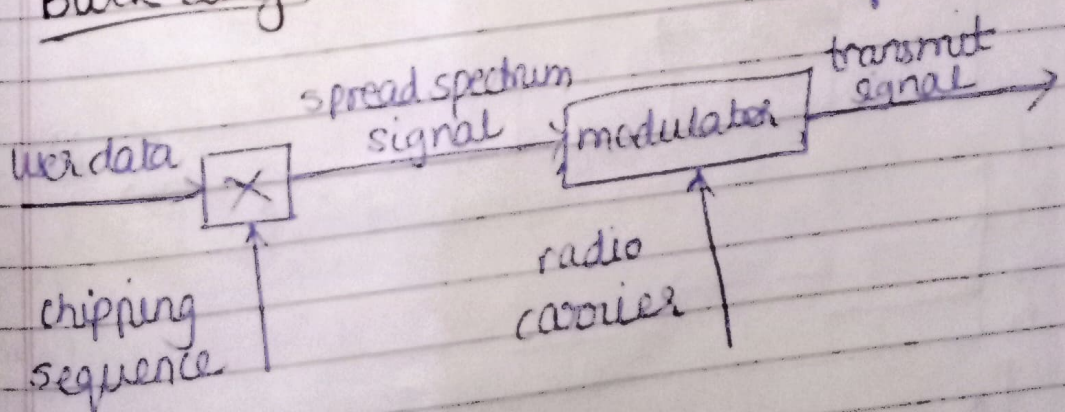
XOR → 0110101 1001010
resulting signal

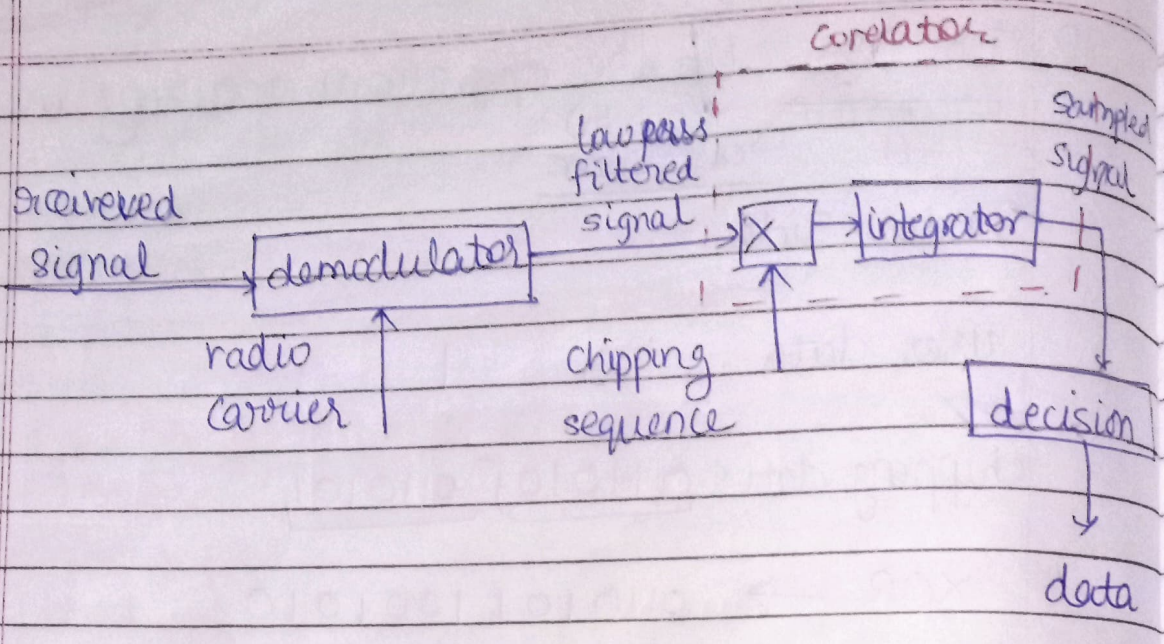
Receiver side
Resulting → 0110101 1001010

chipping → 0110101 0110101

XOR → 0000000 0000000

Block diagram





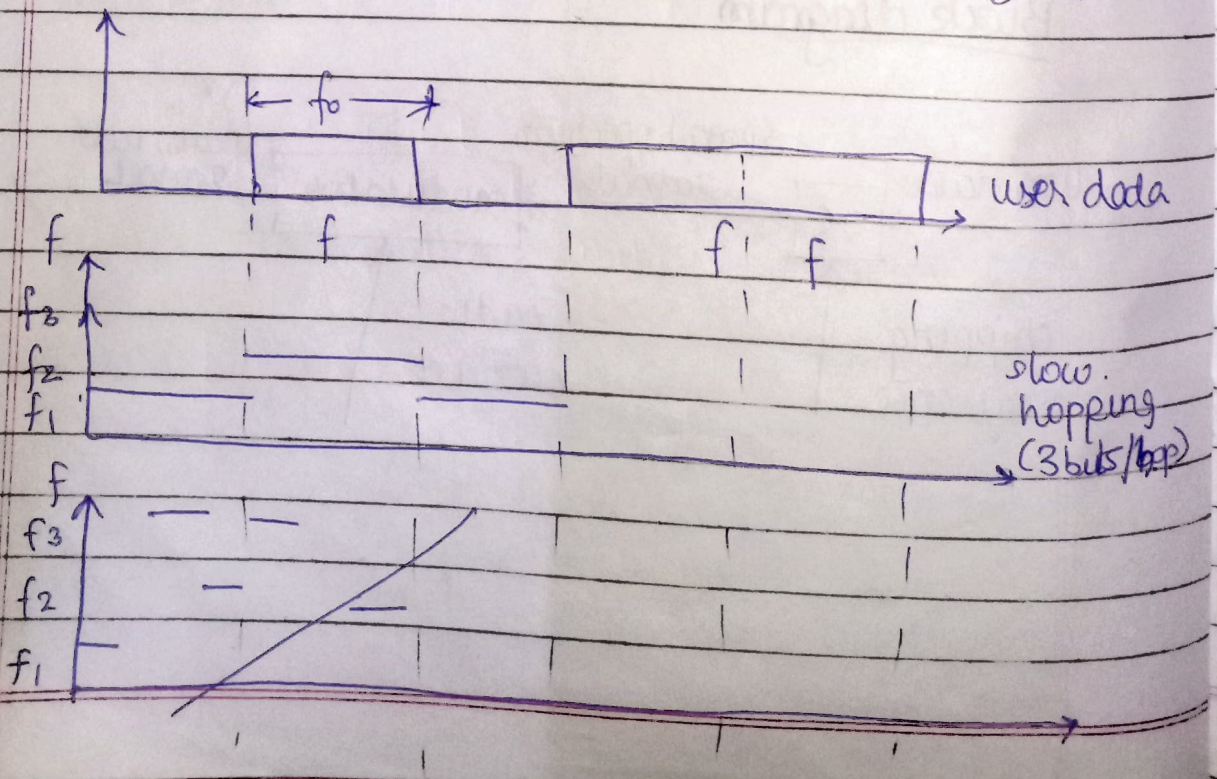

## – Frequency hopping Spread Spectrum (FHSS)

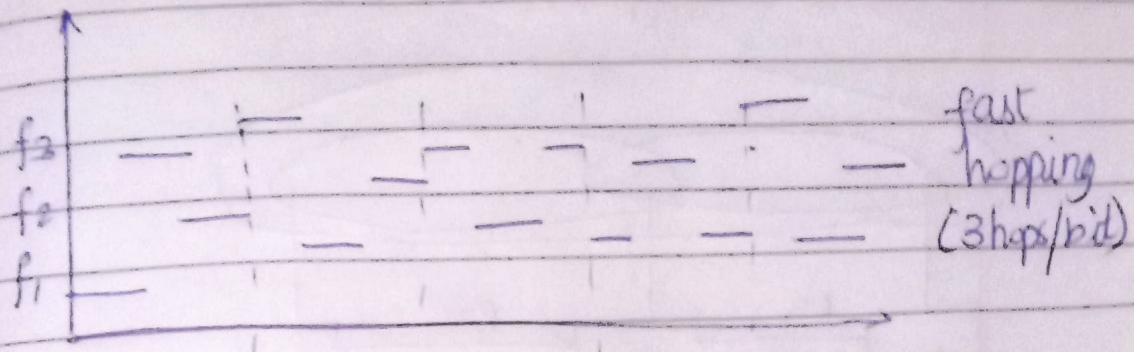
1) Slow hopping.

For one bit, the signal jumps multiple frequencies

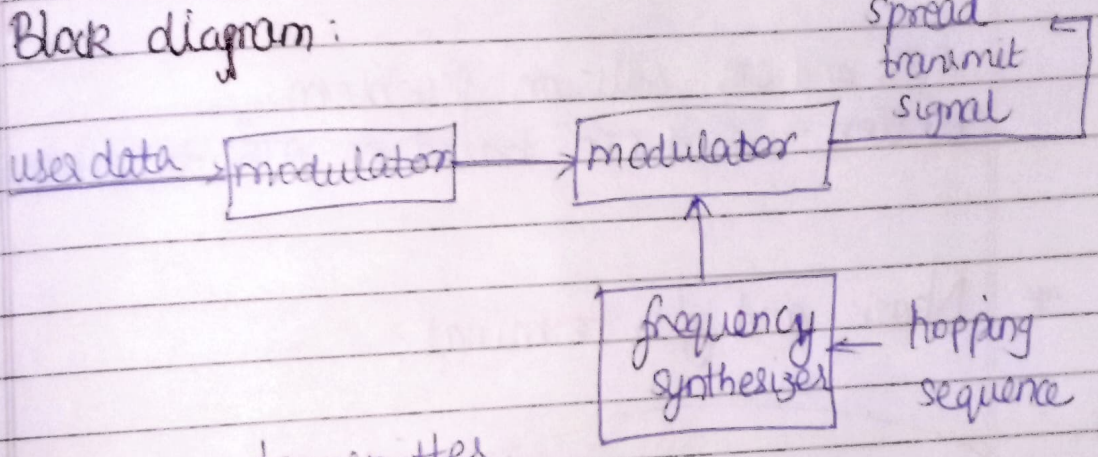
2) Fast hopping.

For one bit, the signal hops to multiple frequencies

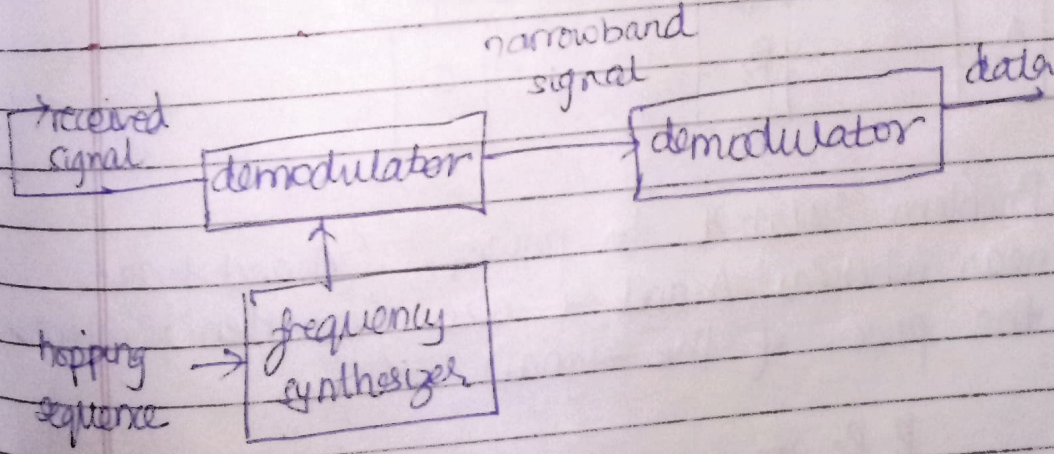




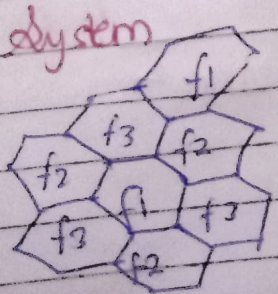

Block diagram:




transmitter

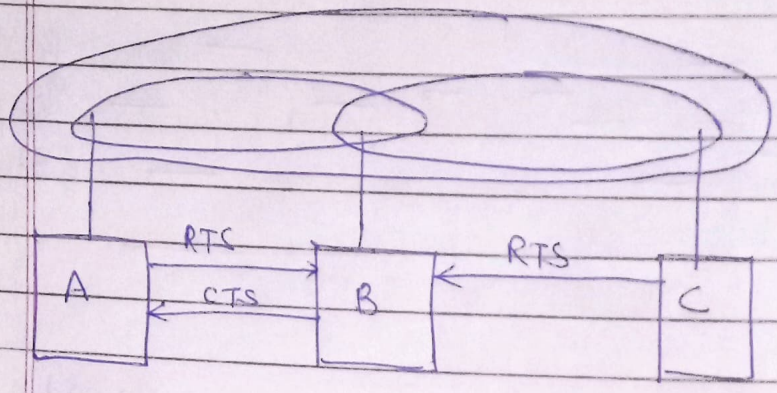



- cellular system



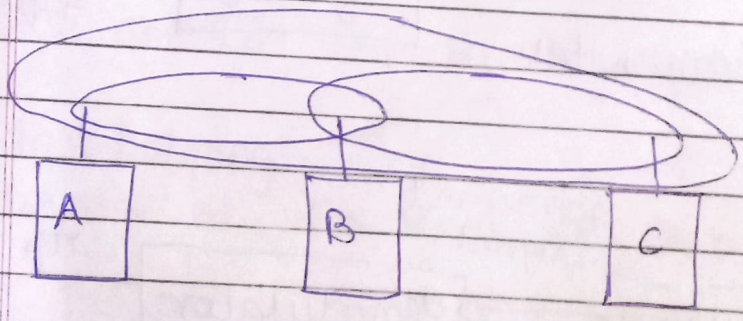
# Module 2

## * Hidden and Exposed Terminal:




RTS and CTS collision problem
Solution – send CTS based on RTS timestamp

## * Near and far terminal:

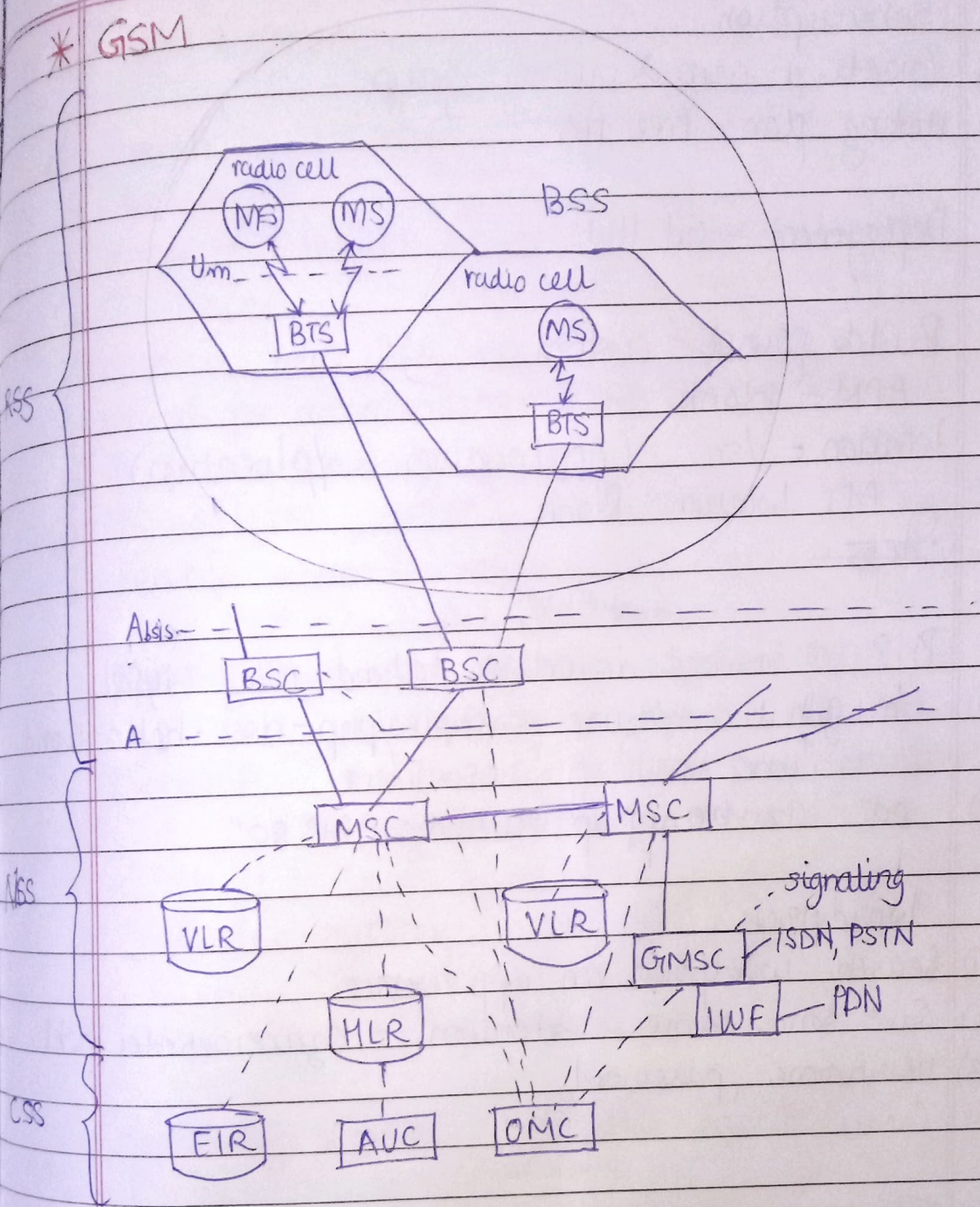



Problem related to power. (A and B are near whereas A and C are far. Hence calculate the power of the signal)

$$\text{Power} = \frac{1}{\text{distance}^2}$$

PAGE :
DATE : / /

# * GSM




⇒ * RSS [Radio Subsystem]
It consists of Base Station Subsystem (Bss) and Mobile Syste station wl

It also consists of BTS (Base Transreceiver Station) and BSC (Base ~~Controller~~ Station Controller)

PAGE :
DATE : / /

→ BSS :

performs
- functions necessary to maintain radio connection to MS.
- performs coding decoding of voice and data rate
* adaptation to and from wireless n/w.

→ BTS :
- It holds all equipments necessary for radio connection like antenna, amplifier and performs signal processing necessary for radio transmission.
- It is connected to MS using Um interface and connected to BSC using Abis interface.

→ Interfaces :

1) Um : It contains all the necessary mechanisms for wireless transmission like multiplexing and medium access mechanism.

2) Abis interface : It contains 16 or 64 Kbps data rate connections.

3) A interface : It manages multiplexing of radio channels.

→ MS (Mobile Station)
- It comprises all equipment and software needed for communication.
- It consists of : i) SIM (
It stores user specific data related to GSM
ii) IMEI (International Mobile Equipment Identity)
* used for identification of MS.

iii) PIN (Personal Identification No) used for protection to lock MS after specific attempts.

iv) PUK (Pin Unlock Key) - for unlocking SIM

v) TMSI & (Temporary Mobile Subscriber Identity) and LAI (Location area Identification).

⇒ NSS [N/w subsystem]
- known as heart of GSM.
- connects ~~to~~ wireless n/w with standard public n/w.
- performs handover.
- comprises functions for world wide localisation and supports charging, accounting and roaming.
- NSS ~~cons~~ consists of MSC, HLR, VLR.

→ MSC - It handles signaling for connection set up, call forwarding and number portability using SS7 (signaling System number 7)

→ HLR (Home Location Register)
- Stores user relevant data
- consists of IMSI, LAI and MSRN for dynamic information of MS.

→ VLR (Visitor Location Register)
- Stores information of MS using LAI.
- Copies all relevant information about MS from HLR and uses in authentication.

PAGE :
DATE : / /

⇒ OSS

- performs n/w operation and maintainance
- Consists of OMC, AUC and EIR.

→ OMC

- functions are:
  traffic monitoring, status reports, subscriber security management, accounting and billing.

→ AUC

- protects user's identity and data transmission.
- generates values for A3, A5, A8 algorithms for authentication and encryption of data.

→ EIR [Equipment Identity Register]

- Database of all IMEI consists of 3 lists.

i) Black list - stolen devices
ii) White list - valid IMEI
iii) Gray list - blocked / malfunctioning IMEI.

PAGE :
DATE : / /

* Services: 2M

Bearer Service

Transparent
Transport Service
- physical layer
- FEC
- Xack
- Xpacked loss

Non transparent transport service
- n/w layer
- data layer
- ~~lost~~ packets rate
- ack
- error correction

↑↓

Sync
- full duplex
- higher
- ~~data~~

Asynch
- data rate

Tele Service

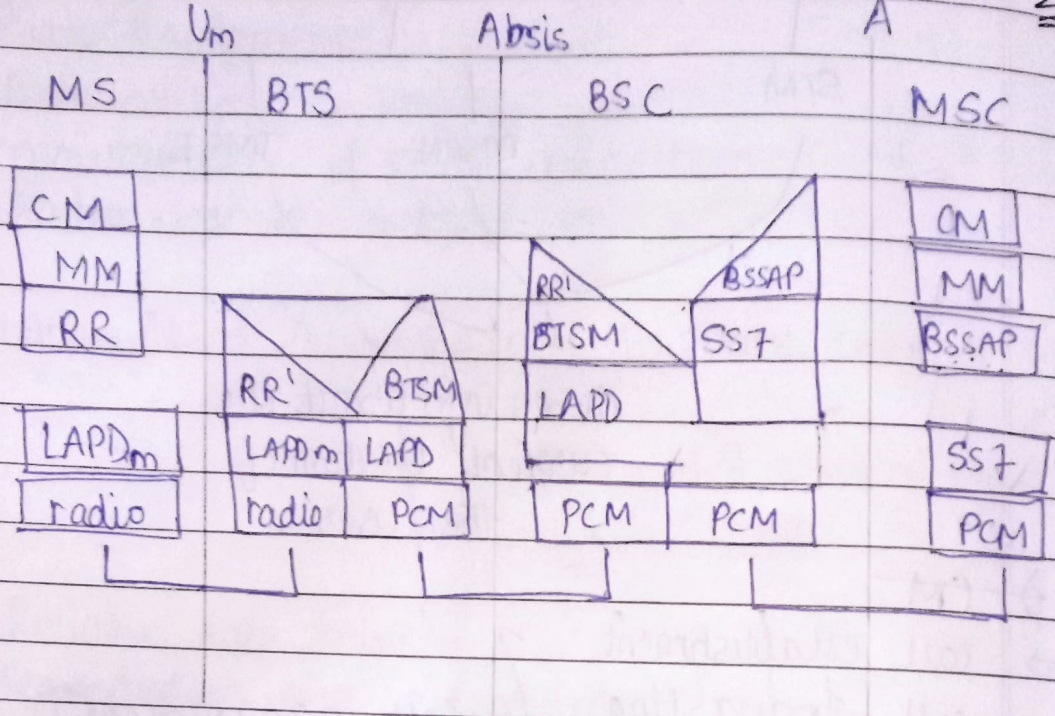
Voice

data
eg) SMS, MMS

Supplementary
eg) ~~call~~ services
eg) call forwarding, recording

PAGE :
DATE : / /

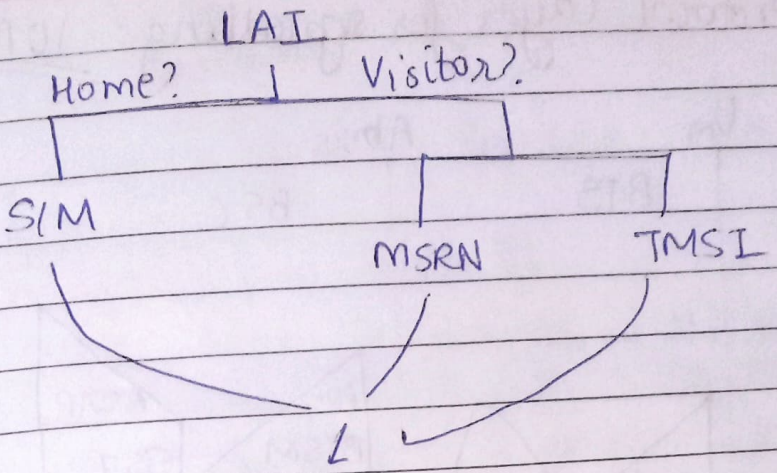
* GSM protocol layer for signalling: 10M specific comp: 2M




CM - Connection management / call management
MM - Mobility management
RR - Radio Resource
LAPD - Link Access Protocol for Data channels
PCM - Pulse Code modulation
BSS - Base Station Subsystem Application Part
~~BSC - Base~~
SS7 - Signaling System level 7
AP - Application part

PAGE :
DATE : / /

⇒ MM :




Gives info about the current location of the user.

~~CM~~

⇒ call establishment
call forwarding
call continuation
call drop
} call management protocol

1) CM : (call management)

- call
- set up point-to-point communication
- hand off
- call clearing

2) MM (mobility management)

- authentication
- identification
- location update
- registration
- using TMSI, LAI, MSRN, IMSI

PAGE :
DATE : / /

3) RR (Radio Resource Management)

- Radio equipments
- Radio set up
- maintainance of radio connection
- radio channel release

4) LAPDm (Link Access Protocol for Data channel in ISDN)

Integrated services Digital N/w

- Reliable data transfer
- segmentation and assembling
- Resequencing
- Acknowledgement
- Request for retransmission

5) SS7 (Signalling System 7)

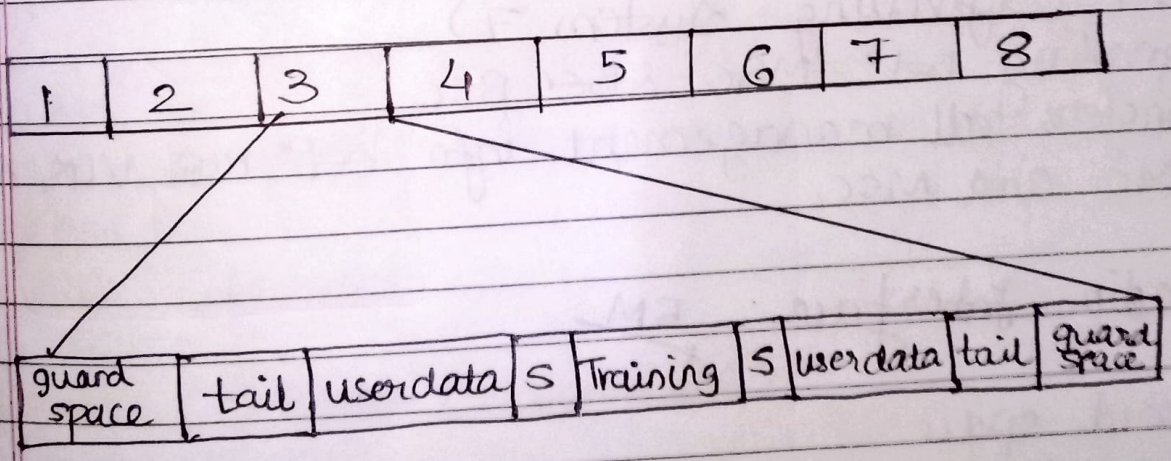
- Signalling bet^n MSC & BSC
- transfers all management info bet^n HLR, VLR, AUC, EIR, OMC and MSC

* Radio Interface 5M

- guard space
- tail bit → manipulations needed in the received signal eg 3 signals - Power↑ but noise↑, low pass, etc. Work one to choose and what make changes
- user data
- Synchronization burst - N/w data in user data? then sequencing if else N/w data : add dummy

info if no n/w or user data

- Training - which method of data encoding/decoding, multiplexing → checks; travel path (eg. vacuum, scattered, etc → checks. since the same process should be used for decoding




* Localisation & Roaming: 10M 5 to 6 (individually)

PAGE :
DATE : / /

5M * Mobile Originated Call (MOC) - outgoing call:

5M * Mobile terminated call:

5M * Handover:

1) Inter cell
2) Intra cell
3) Inter BSC
4) Inter MSC

1) Inter cell handover:
- It is also known as Intra BSC handover
- mobile moves from one cell to another but remains within the same BSC. Here, BSC handles ho process

2) Intra cell handover:
- It is performed to optimize the traffic load in the cell or to improve quality of a connection by changing carries frequency

3) Inter BSC handover.
- Intra MSC handover
- As BSC can control only a limited number of calls, a mobile is transferred from one BSC to another

PAGE :
DATE : / /

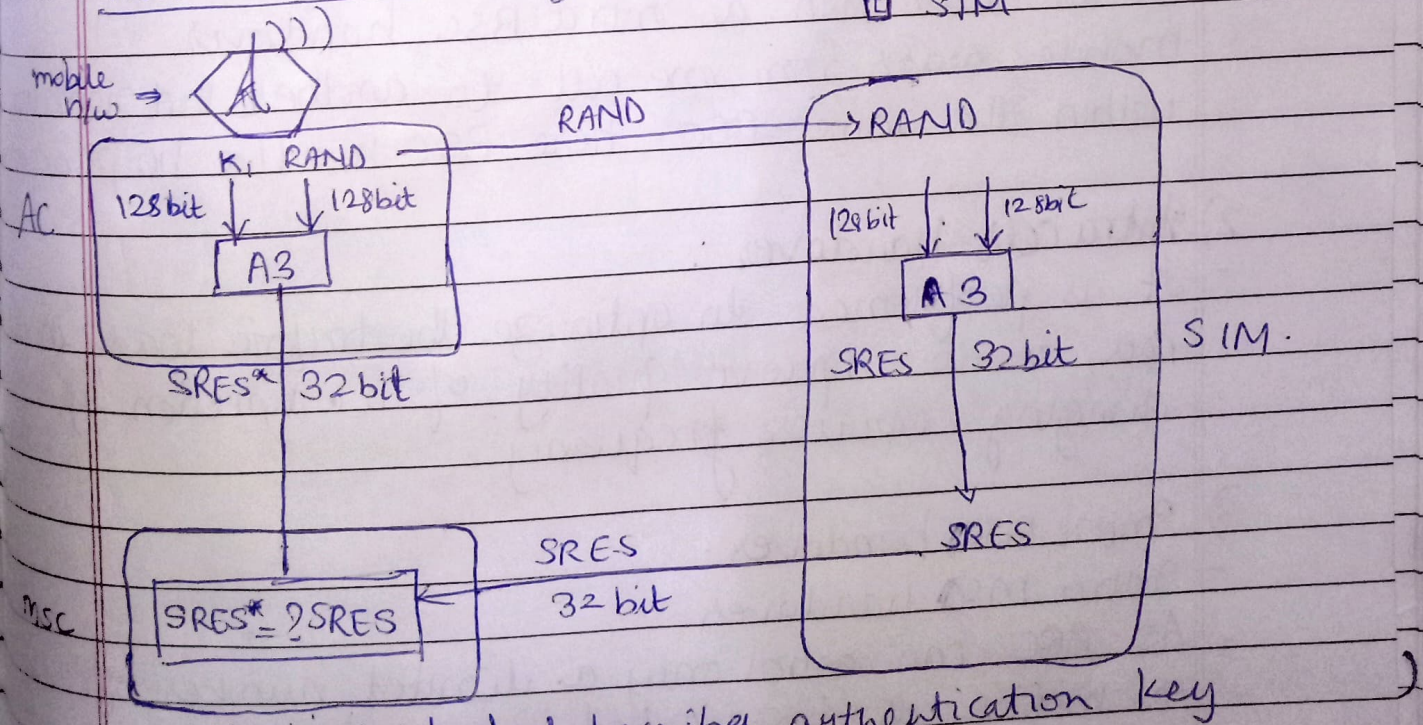
2) Inter MSC
- occurs when mobile moves from one

## * GSM Security

- 3 aspects:

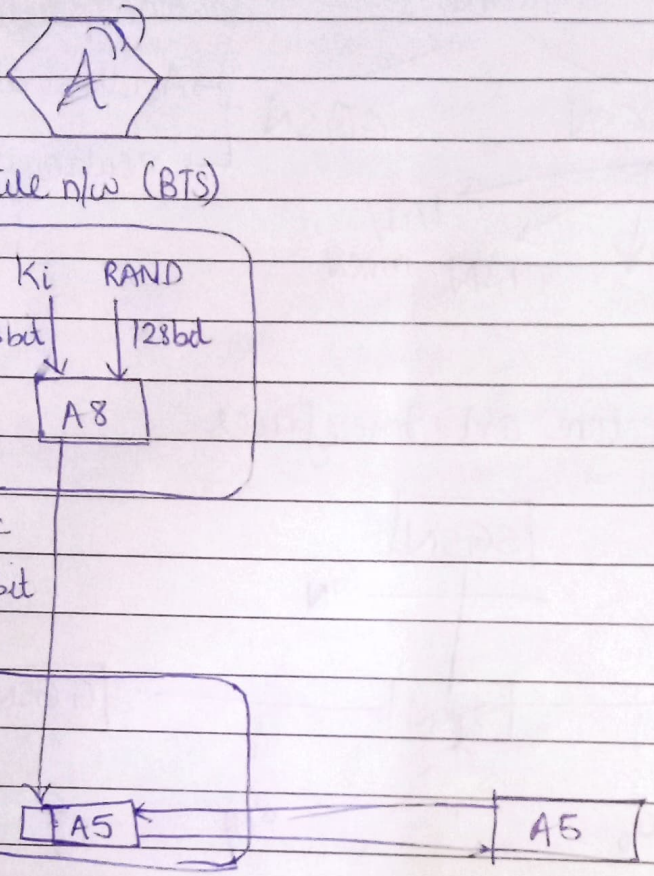
1) Authentication - $A_3$ algo
2) Confidentiality } $A_8$ & $A_5$ algo
3) Anonymity
1) Authentication:
Signed Response - SRES ⇒ $A_3$ algo
↳ 32 bits
When the user is validated, he will be added to whitelist.

Authentication diagram:




$K_i$ - individual subscriber authentication key
SRES - signed response

GSM- key generation and encryption




* GPRS: (General Packet Radio Service) → 2.5G

- packet switched
- volume
- on demand
- 'always on' uplink ↑ ↓ downlink

↳ ensure that one freq band is allocated to each cell

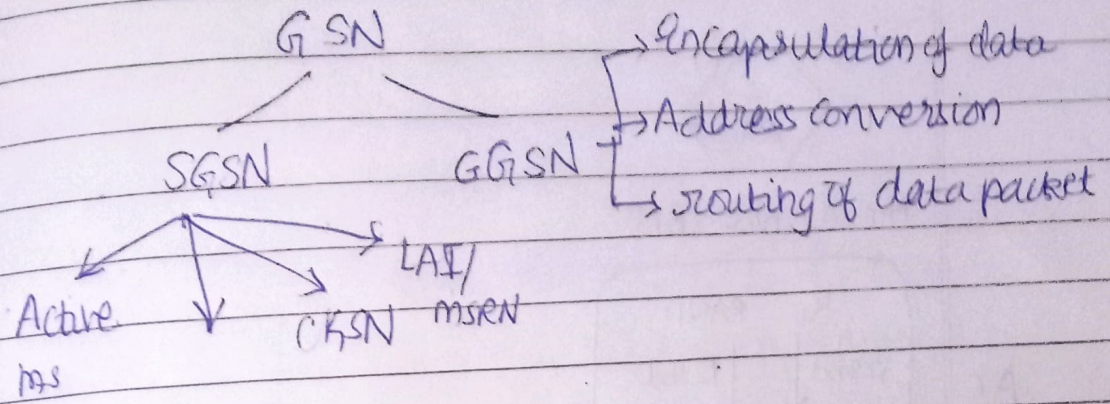
GSN

SGSN
Serving GPRS Support Node

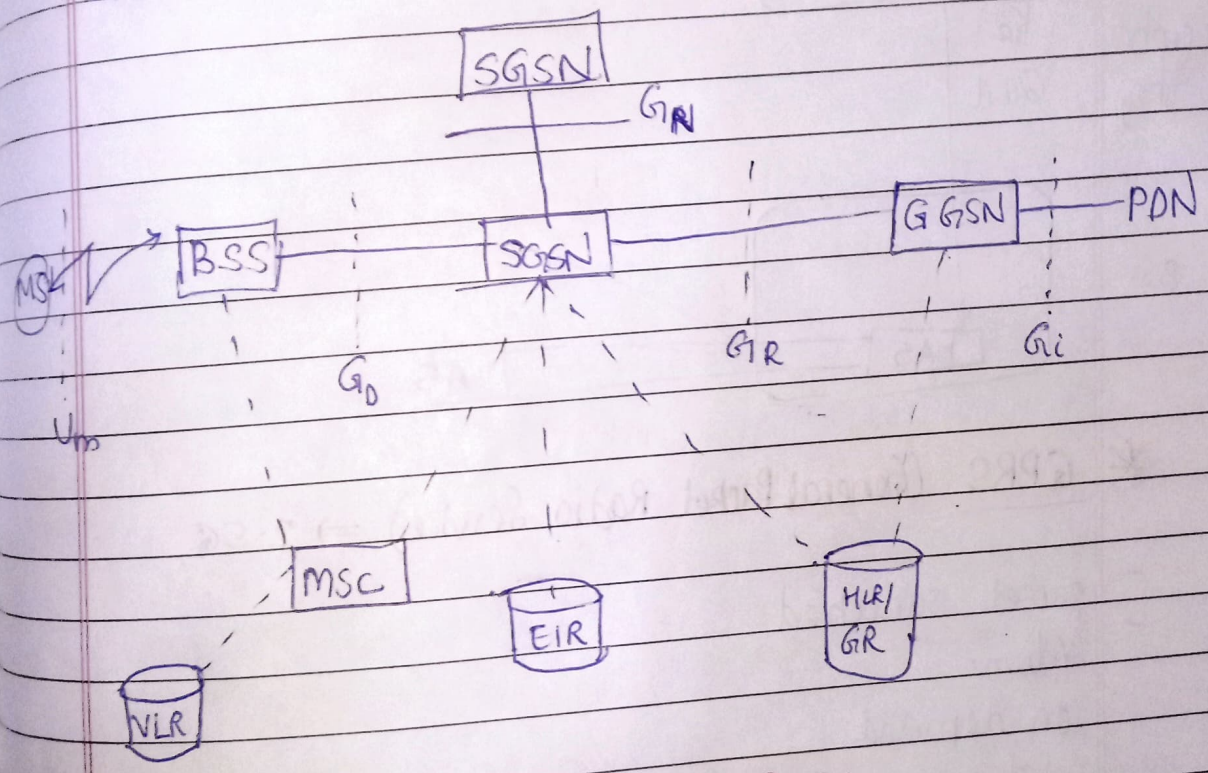
GGSN
Gateway GPRS Support Node

PAGE :
DATE : / /

- Here, instead of HLR → GR same functions.

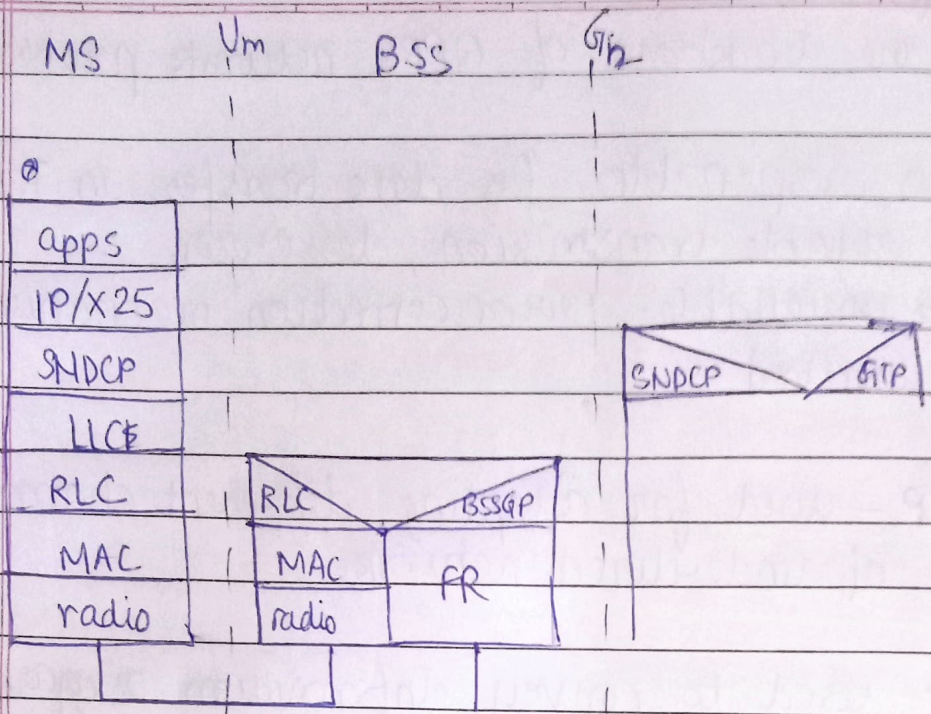



GPRS Architecture and Interfaces.




→ Difference between GSM and GPRS.

| GSM | GPRS |
| --- | --- |
| | |




MAC- Medium Access Control
RLC - Radio Link layer / connection
LLC - logical link control
SNDCP- ~~Subnetwork Data~~ Dependent Conversion protocol
Network conversions
APPs - Application
FR - Frame Relay
BSSGP- Base Station Subsystem GPRS protocol
IP < TCP / UDP } GTP - GPRS Tunneling Protocol

termed as

IP is the backbone of GPRS network protocol.

GTP is responsible for data transfer in TCP or UDP
TCP → reliable transmission, less errors
UDP → unreliable, error correction mechanisms involved.

SNDCP - used for adapting different characteristics of underlined network.

BSSGP - used to convey information regarding quality of service

RLC - Radio link protocol
- Used for transmission of data over Um interface with a reliable link.

MAC - signaling procedure for radio channels and multiplexing techniques.

* DECT (Digital Enabled Cordless Telephone) system architecture reference model:

PA - Personal Assistant (Simi
PT - Portable terminal
FT - fixed Terminal → auth, reg, call transfer, routing of packets, encr, decryp.
local n/w behaves like MSC, also functions like gateway
HDB - Home
VDB - Visitor

→ DECT protocol layers.

C plane - Control plane → n/w layer (data comes from)
U plane - user's plane
↳ data directly comes from DLL

physical layer - connections, mode, allocation of radio channel

MAC - multiplexing

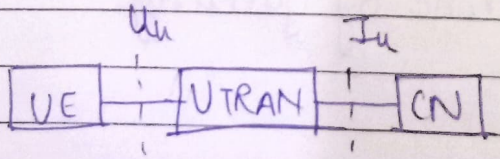
Data link control - fragments → sequence numbers

n/w layer - handover, signaling

→ DECT multiplex & Frame Structure

→ Unprotected → transmit the entire chunk of data
→ risk associated → may involve multiple retransmissions

* UMTS: Universal Mobile Telecommunication System




UE - User Equipment
UTRAN - Universal Terrestrial Radio Access N/w
CN - Core n/w → handover, acts like a gateway
Address translation, format translation & routing of packets

PAGE:
DATE: / /

UTRAN
|
RNS

RR
channel allocation/ deallocation

ciphering/ Deciphering

→ UMTS domains & interfaces:

UE → sim, equipment → send and receive radio signals

- UTRA FDD

uplink (FDD)
- Pilot
- TFCI - Transfer format Combination Indication
- FBI - feedback Indication
- TPC - Transmit Power control

- UTRA TDD

- Data
- midamble
- GP - guard period

conversions are done by gateway