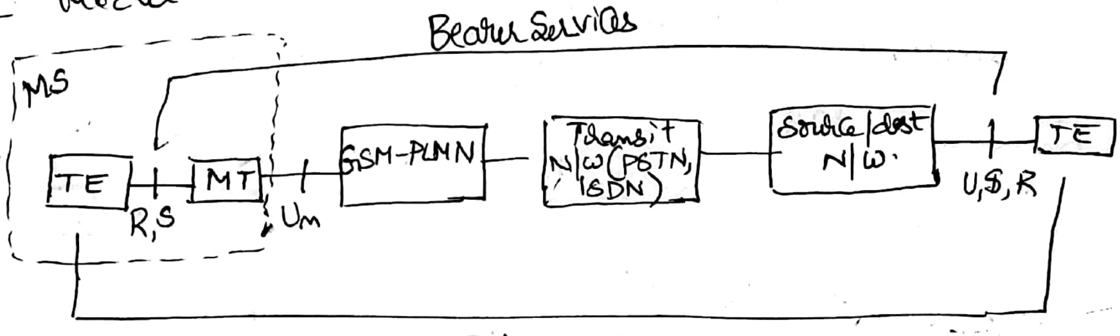
UNIT-II

- Global System for Mobile Communications.
- GSM is Second Generation System

GSM services :

- Mobile Services of GSM
1) Bearer Services
2) Tele services
3) Supplementary services.

Reference Model



- Mobile station is connected to GSM public land mobile Network (GSM-PLMN) via Um interface.
- GSM-PLMN is infrastructure needed for GSM N/W.
- This N/W is connected to transit N/W.
  Ex: integrated services digital N/W &
  Public switched Telephone N/W.
- Before Terminal TE, there can be another network, source/destination n/w.

- Mobile Termination (MT) performs all n/w functions tasks

Bearer Services

- GSM specifies different mechanisms for data transmission
- Bearer services permit
  transparent and non-transparent
  synchronous & asynchronous
  data transmission.
- Transparent bearer services use functions of physical layer to transmit data
- Data transmission has a constant delay and throughput if no transmission errors occur.
- The only mechanism to increase transmission quality is the use of forward error correction (FEC)
- Transparent bearer services do not try to recover lost data in case of shadowing & interruptions due to handover.
- Non transparent bearer services use protocols of layers 2 & 3 to implement error correction and flow control.

- The throughput and delay vary depending on transmission quality.

- Data transmission can be full-duplex, synchronous & full duplex asynchronous.

Teleservices

- GSM mainly focus on voice-oriented tele services
These comprise encrypted voice transmission
message services
basic data communication.

1) Main service is Telephony
- primary goal of GSM was the provision of high quality digital voice transmission
- special codes are used for voice transmission.

2) Emergency number -
- This no is used everywhere
- This service is mandatory for all providers & free of charge
- This connection has highest priority

3) Service for simple message transfer is Short Message Service (SMS).
offers transmission of msgs up to 160 chars

- SMS msg do not use standard data channels but exploit unused capacity in signaling channels.
- Sending & receiving SMS is possible during data & voice transmission.

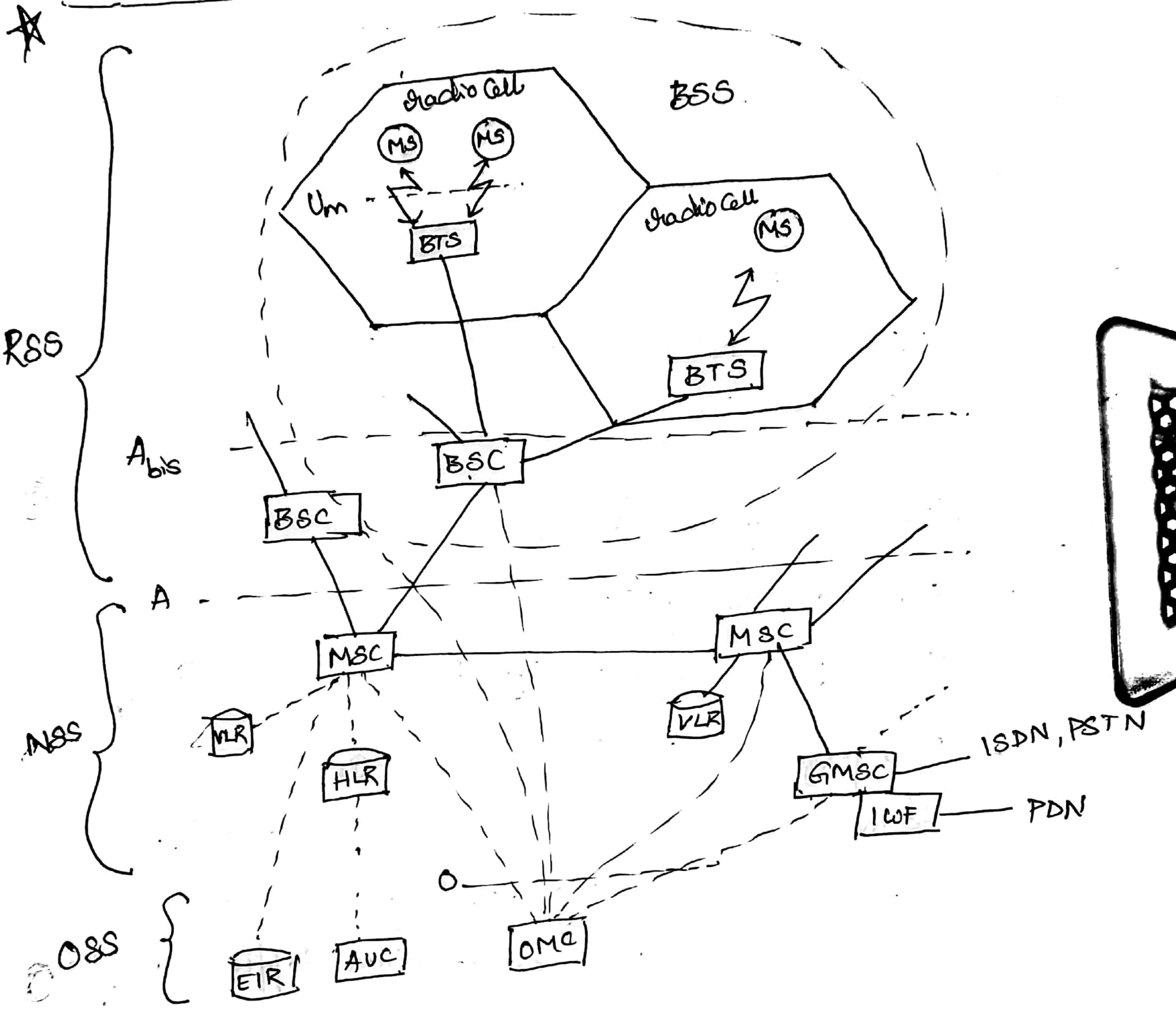
4) Success of SMS - Enhanced message service (EMS)
- offer larger msg size - 760 chars
- formatted text, animated pictures, small images, ringtones

5) MMS - Multimedia message service.
- offer transmission of larger pictures short videos & comes with mobile phones with small cameras.

6) non-voice tele service - group 3 fax.
- fax data transmitted as digital data over analog telephone n/w.

Supplementary services -
- vary from provider to provider
- user identification, call redirection or forwarding ongoing calls.
- closed user groups and multiparty communication.

GSM System Architecture



- Complex System architecture with many entities, interfaces, acronyms

- GSM consists of 3 subsystems
  1) Radio subsystem (RSS)
  2) Network and switching subsystem (NSS)
  3) Operation sub System (OSS)

1) Radio subsystem (RSS)

- Comprises all radio specific entities i.e
  - mobile stations (MS) and
  - Base station subsystem (BSS)

- Connection b/t
  RSS & NSS via A interface
  NSS & OSS via O interface.

Base station subsystem (BSS)

- GSM has many BSS's
- Each BSS controlled by Base station controller (BSC)
- BSS performs all functions necessary to maintain radio connections to MS.
  Coding/decoding of voice
  rate adaptation to/from wireless n/w.
- Besides BSC, BSS contain several BTS's.

Base TransCeiver Station (BTS)

- BTS comprises all radio equipment i.e antennas, signal processing, amplifiers necessary for radio transmission.
- BTS form radio cell using sectorized antennas.
- BTS connected to MS via U_m interface.
  " " BSC via A_{bis} interface.

Base station Controller (BSC)

- BSC manages BTS's
- It reserves radio frequencies, handles handover from one BTS to another within BSS.
- BSC multiplexes radio channels onto fixed n/w connections at A interface.

Tasks of BTS and BSC with in BSS.

Function	BTS	BSC
1. Management of radio channels		X
2. Frequency hopping	X	X
3. Management of terrestrial channels		X
4. Mapping of terrestrial onto radiochannels		X
5. channel coding and decoding	X	
6. Rate adaptation	X	
7. Encryption and decryption	X	X
8. Paging	X	X
9. Uplink signal measurement	X	
10. Traffic measurement		X
11. Authentication		X
12. Location registry, location update		X
13. handover management		X

Mobile Station (MS)

- Consists of all user equipment & Software needed for communication with GSM n/w.
- MS consists of user independent hard- and s/w & subscriber identity module (SIM)

  SIM stores all user specific data relevant to GSM
- MS identified via IMEI (International Mobile equipment identity)
- User specific mechanisms like charging and authentication are based on SIM

  Device specific mechanisms like theft protection use IMEI.
- without SIM only Emergency Calls are possible.
- SIM Cards Consists many identifiers & tables.

  Such as Card type
  Serial number
  list of subscribed services
  personal identity number (PIN)
  PIN unblocking key (PUK)
  authentication key (K_i)
  International mobile subscriber identity (IMSI)

- PIN used to unlock MS.
- If PIN is used wrongly for 3 times, SIM will be locked. Then PUK is used to unlock.
- MS stores dynamic information while logged to GSM
  eg. K_c - Cipher key
  location information
  L temporary Mobile subscriber identity (TMSI)
  location area identification (LAI)

- Apart of telephone interface, MS offer other types of interface to users with display, loudspeaker, microphone & programmable soft keys.

2) Network and switching subsystem (NSS)

- Heart of GSM
- NSS connects wireless n/w with public n/w.
  performs handovers b/t different BSS
  Comprises functions for
  - Worldwide localization of users
  - Support charging
  - accounting
  - roaming of users b/t providers.

Scanned by CamScanner

NSS Consists of following switches & databases:

1) Mobile services switching Center (MSC)

- MSC are high performance digital ISDN switches
- set up Connection to other MSCS and to BSC's via A interface.
- MSC are fixed backbone n/w of GSM
- Gateway MSC has Connections to other fixed n/w's such as PSTN & ISDN.
- using additional interworking functions IWF, MSC can connect to PDN.
- MSC handles signaling needed for
  - Connection setup
  - Connection release
  - handover of connection to other MSC's

2) Home location Register (HLR).

- important database in GSM
- Stores user relevant information.
- Contains static information like
  - mobile subscriber ISDN No. (MSISDN)
  - Subscribed Services (forwarding, roaming etc)
  - international mobile subscriber identity (IMSI)

Scanned by CamScanner

- Contains dynamic information like
  Current location area (LA) of MS
  Mobile subscriber roaming no (MSRN)
  Current VLR & MSC.

- when MS leaves current LA, information in HLR is updated.

c) Visitor location Register (VLR)

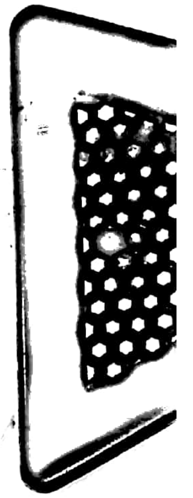
- VLR associated to each MSC is dynamic database which stores all important information needed for MS users currently in LA.
- If new MS comes in LA, VLR is responsible for it, it has to store/copy relevant info from HLR.

Operating Subsystem (OSS)

- Contains necessary functions for n/w operation & maintenance, OSS has following entities.

1) operation and maintenance center (OMC)

- Monitors and controlls all other n/w entities via o interface.



- OMC functions are

  traffic monitoring

  Status reports of n/w entities

  Subscriber and

  Security mgmt.

  accounting & billing.

2) Authentication Centre (AUC)

- AUC is defined to protect user identity and data transmission

- AUC consists of algorithms for authentication keys for encryption.

3) Equipment Identity Register (EIR)

- EIR is database for all IMEI's

- Stores all device identifications registered.

- If MS is stolen, any SIM can be use in MS. EIR has blacklist of stolen devices.

Localization and Calling

- feature of GSM is automatic, worldwise localization of users.
- System knows where a user currently is & same phone no is valid worldwide.
- To provide this service, GSM performs periodic location updates even if Mobile Station is not in use.
- HLR contains current location information. VLR responsible for MS information to HLR about location change.
- when MS ~~change~~ move to new VLR, HLR sends needed information to new VLR
- changing VLRs with uninterrupted availability of all services is called roaming.
- Roaming take place within n/w of one provider, b/t 2 providers in a country, (National roaming) b/w diff providers in diff countries (International roaming)

- To locate MS and to address MS Several numbers are needed.

1) Mobile Station International ISDN Number (MSISDN)

This number Consists of Country Code, (CC)

National destination Code, (NDC)

↓

address of n/w provider

Subscriber number (SN)

2) International Mobile Subscriber Identity (IMSI)

- IMSI for internal unique identification of subscriber

- Consists of

Mobile Country Code (MCC)

Mobile N/W Code (MNC)

Mobile Subscriber Identification Number (MSIN)

3) Temporary mobile Subscriber identity (TMSI)

- 4 bytes of TMSI for local Subscriber identification

- TMSI is selected by Current VLR & Valid within location area of VLR.

- VLR change TMSI periodically.

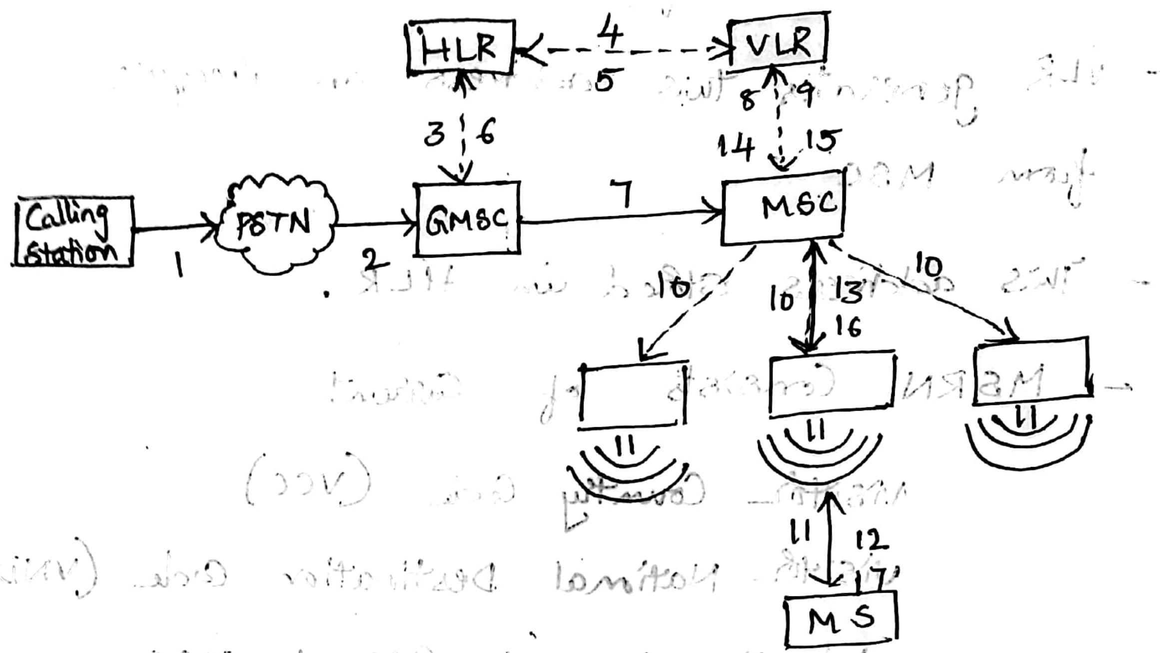
4) Mobile station Roaming Number (MSRN)

- Temporary address that hides identity and location of subscriber.
- VLR generates this address on request from MSC
- This address stored in HLR.
- MSRN consists of current
  - visitor Country Code (VCC)
  - visitor National Destination Code (VNDC)
  - identification of current MSC
  - subscriber No.
- MSRN helps HLR to find subscriber for an incoming call.

Mobile terminated Call (MTC)

- Situation in which station calls a mobile station.
  (Calling station can be outside GSM or another station).

Finally steps to connect Calling station with mobile user.

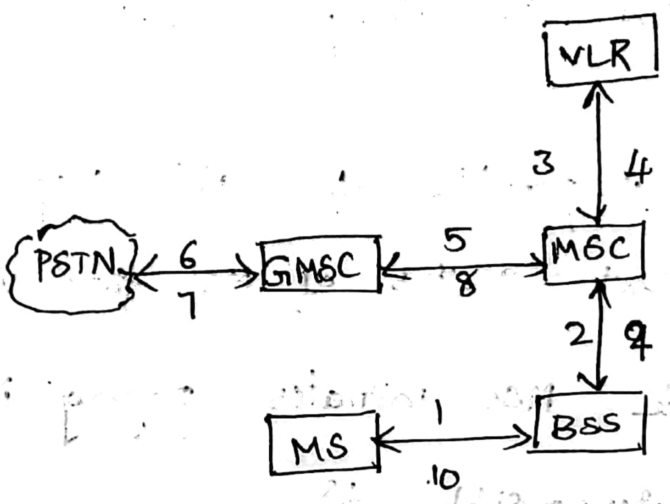


- 1) User dials phone number of GSM subscriber
- 2) Fixed n/w PSTN notices that no. belongs to user in GSM n/w & forward to Gateway MSC.
- 3) GMSC identifies HLR for subscriber and signals HLR
- 4) HLR checks whether i) the no exists & ii) subscribed to requested services & requests MSRN from current VLR.
- After receiving MSRN (5)
  6) HLR determine the MSC responsible for MS & forwards this information to GMSC

- 7) GMSC now forward Call Setup request
  to MSC
- from now MSC is responsible for all steps.
  8) requests Current Status of MS from VLR
- 10) If MS is available MSC initiates paging in
  all Cells it is responsible for.
- 11) BTSs of all BSSs transmit this paging
  signal to MS.
- 12) & 13) If MS answers, VLR has to perform security
  checks.
- 15-17 VLR then signals to MSC to setup
  Connection to MS.

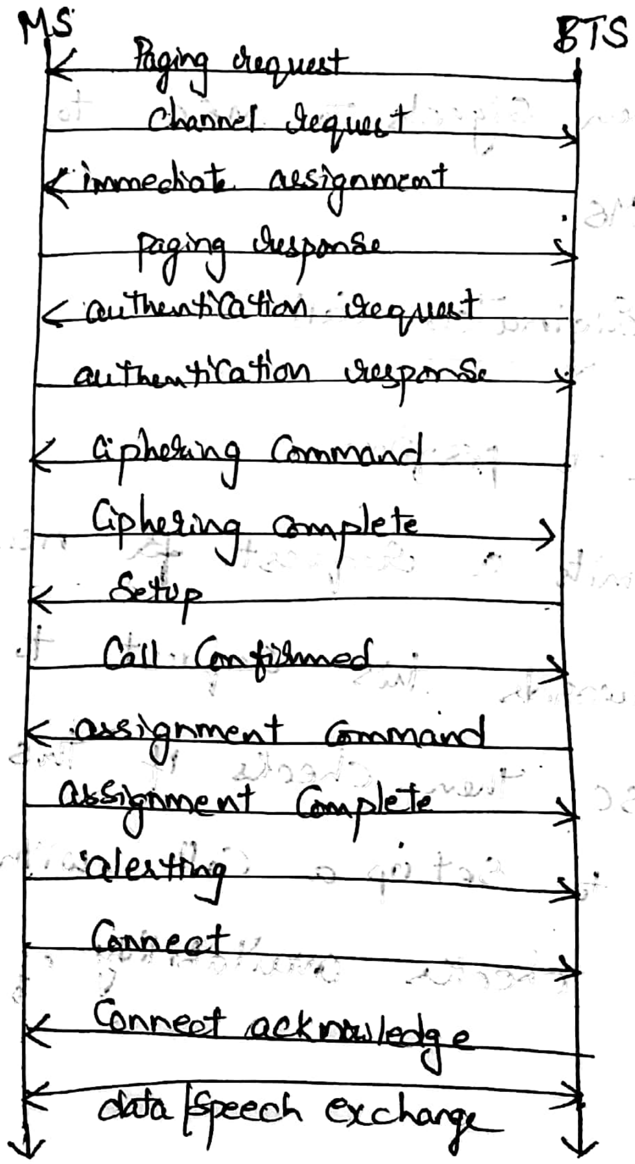
(MOC) Mobile Originated Call

- Much simple to perform.
  1) MS transmits a request for new Connection
  2) BSS forwards this request to MSC
  3) & 4) MSC then checks if this user is
  allowed to set up a Call with requested
  service & checks availability of resources.

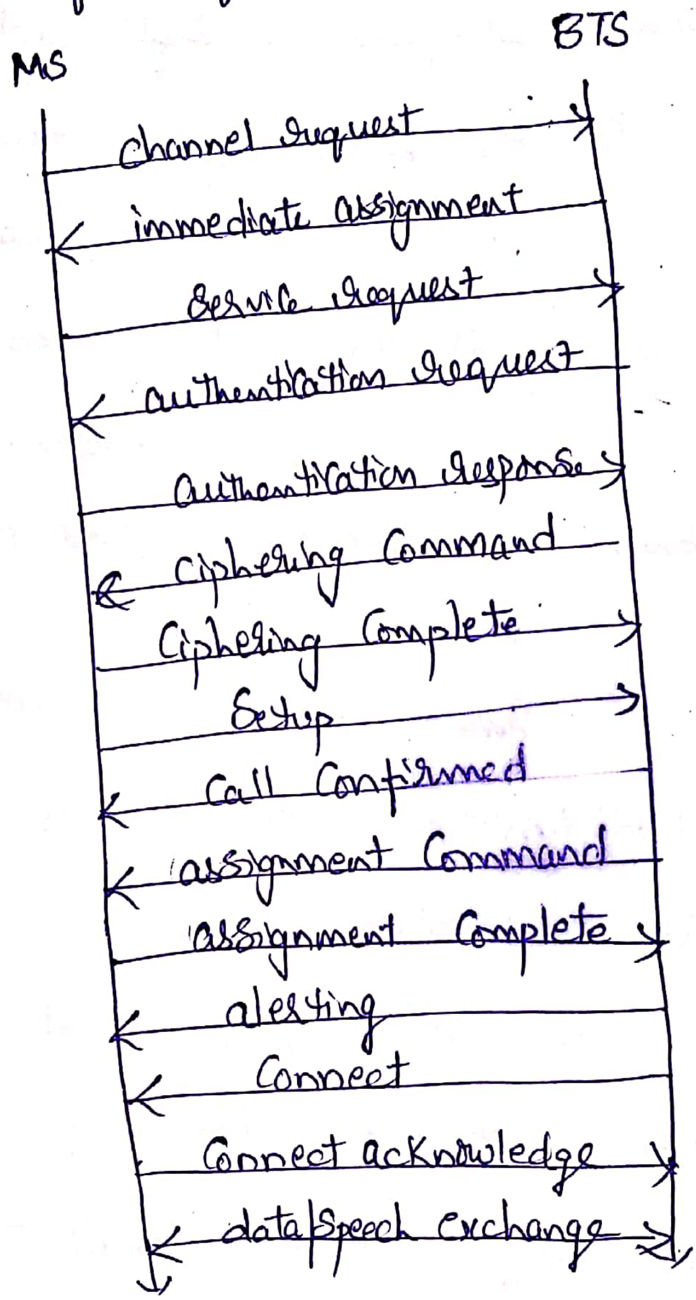


- If all resources are available MSC sets up a connection b/t MS & fixed N/w.

Message flow for MTC



Message flow for MOC



Handover

- Cellular systems require handover procedures because single cells do not cover the whole service area.
- Handover should not cause a cut off also called call drop.
- GSM aims at maximum handover duration of 60ms.

- 2 Reasons for handover

1) Mobile station moves out of range of BTS or certain antenna of BTS.
   - The received signal level decreases until it falls below minimal requirements
   - Error rate may grow due to interference
   - Distance of BTS may be too high.
   - All these effects diminish quality of radio link & make radio transmission impossible.

2) Wired infrastructure may decide that traffic in one cell is too high and shift some MS to other cells with lower load. Handover may be due to load balancing

4 handover Scenarios in GSM

1) Intra cell hand over

- within a cell, narrow band interference could make transmission at certain frequency impossible.

  The BSC could then decide to change the carrier frequency.

2) Inter-Cell, Intra BSC handover

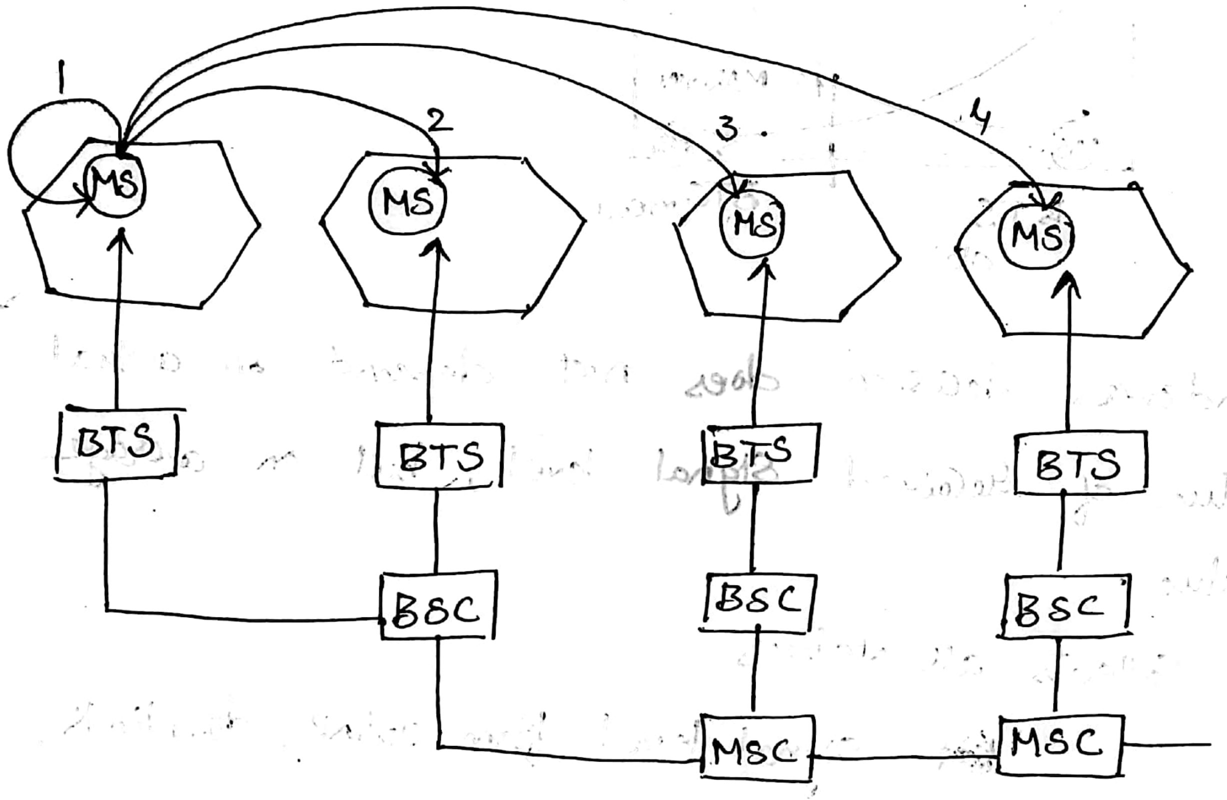
- The mobile station moves from one cell to another, but stays with in the control of same BSC.
- The BSC then performs a handover, assigns a new radio channel in new cell & releases old one.

3) Inter BSC, intra-MSC handover

- As BSC only controls limited no. of cells, GSM also has to perform handovers b/t cells controlled by different BSCs.
- The handover then has to be controlled by MSC.

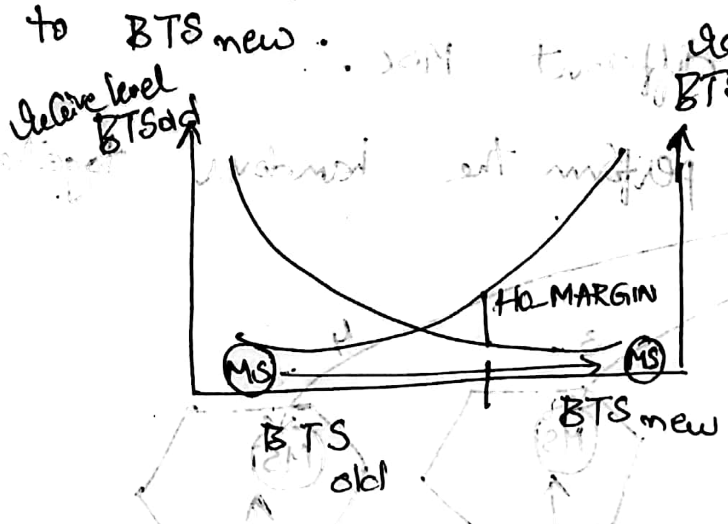
4) Inter MSC handover

- The handover could be required b/t 2 cells belonging to different MSC.
- Both MSC's perform the handover together.



- To provide necessary information for a handover due to weak link, MS & BTS both performs periodic measurements of downlink & uplink quality
- Measurement reports are sent by MS about every half second and contains quality of current link.

- Figure shows the behavior of received signal level, which MS moves away from BTS old to BTS new.



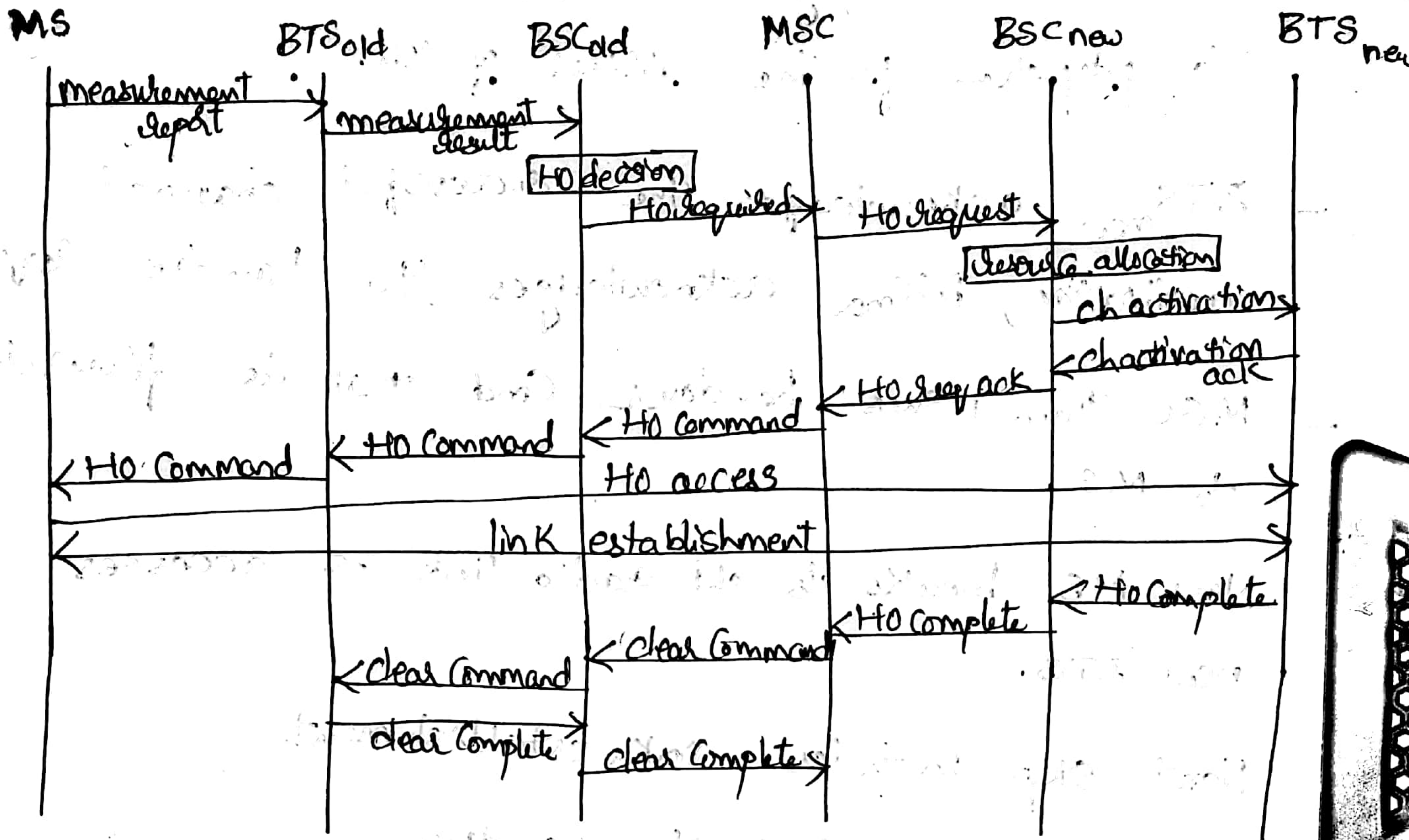
- Handover decision does not depend on actual value of received signal level, but on average value.

- BSC collects all values
  signal level from uplink, downlink, bit error rate
  from BTS & MS & calculates average values.

- These values are then compared to thresholds i.e handover margin HO_MARGIN

- A value which is too high could cause cut-off
  A value which is too low could cause too many handovers.

- Figure shows signal flow during inter-BSC, intra-MSC handover



- MS sends its periodic measurements reports, the BTS old forwards these reports to BSC old together with its own measurements.
- Based on these values, BSC old decide to perform handover & sends the message HO_required to MSC.
- The task of MSC then comprises the request of the resources need for the handover from new BSC, BSCnew.

- BSC checks if enough resources are available and activates physical channel at BTS_{new} to prepare for the arrival of MS.

- BTS_{new} acknowledges the successful channel activation, BSC_{new} acknowledges the handover request

- MSC then issues handover Cmd that is forwarded to MS.

- Now MS breaks its old radio link & accesses new BTS.

- Next step includes link establishment

- MS has then finished the handover & release the resources at old BSC and BTS & to signal the successful handover using handover & clear complete messages.

Scanned by CamScanner

Security

- GSM offers security services using confidential information stored in AuC and SIM.

Security services offered by GSM are

1) Access control and authentication.
   - First step: authentication of a valid user for the SIM
     The user needs a secret PIN to access SIM.
   - Next step: subscriber authentication.

2) Confidentiality
   - All user related data is encrypted
   - After authentication, BTS & MS apply encryption to voice, data & signaling
   - Confidentiality exists only b/t MS and BTS, but does not exist end-to-end or within GSM.

3) Anonymity
   - To provide user anonymity, all data is encrypted before transmission and user identifiers are not used over the air.

- Instead GSM transmits a temporary identifier (TMSI) which is newly assigned by VLR after each location update.
- VLR can change TMSI at any time.

- 3 algorithms are specified to provide security services in GSM
  - Algorithm A3 for authentication
  - A5 for encryption
  - A8 for generation of Cipher Key.

- Algorithms A3 and A8 are located on SIM and in AuC and can be proprietary
- only A5 is implemented in devices has to be identical for all providers.

Authentication

- Before subscriber use service from GSM n/w, he or she must be authenticated.
- Authentication is based on SIM. SIM stores
  - individual authentication key Ki
  - user identification, IMSI
  - Algorithm used for authentication A3.

- Authentication uses challenge response method.
  Access Control AC generates random number RAND as challenge, SIM within MS answers with SRES as response.

- AuC performs generation of

  Random values RAND

  Signed responses SRES and

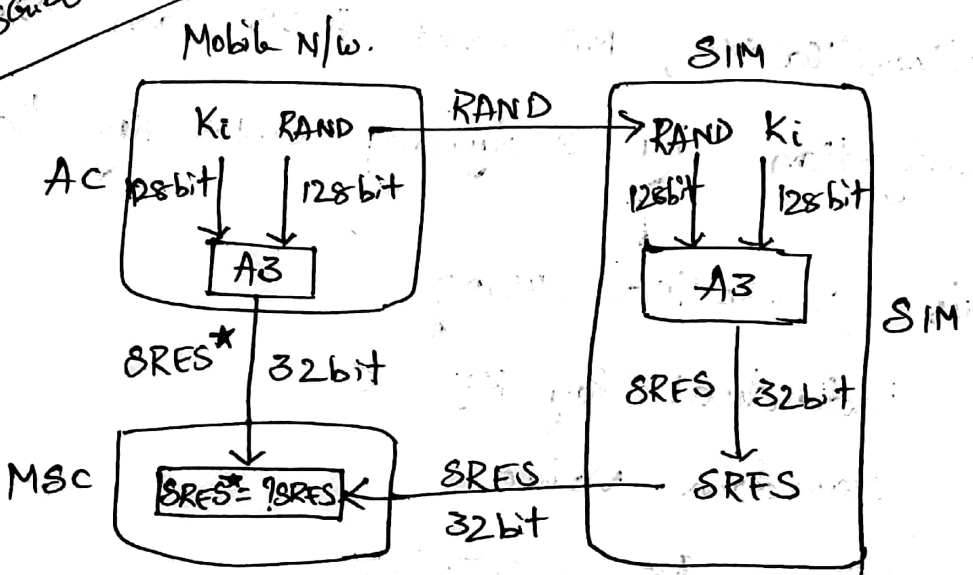
  Cipher keys Kc

  for each IMSI.

  and the forwards information to HLR.

- The current VLR requests the appropriate values for RAND, SRES and Kc from HLR.

Subscriber Authentication

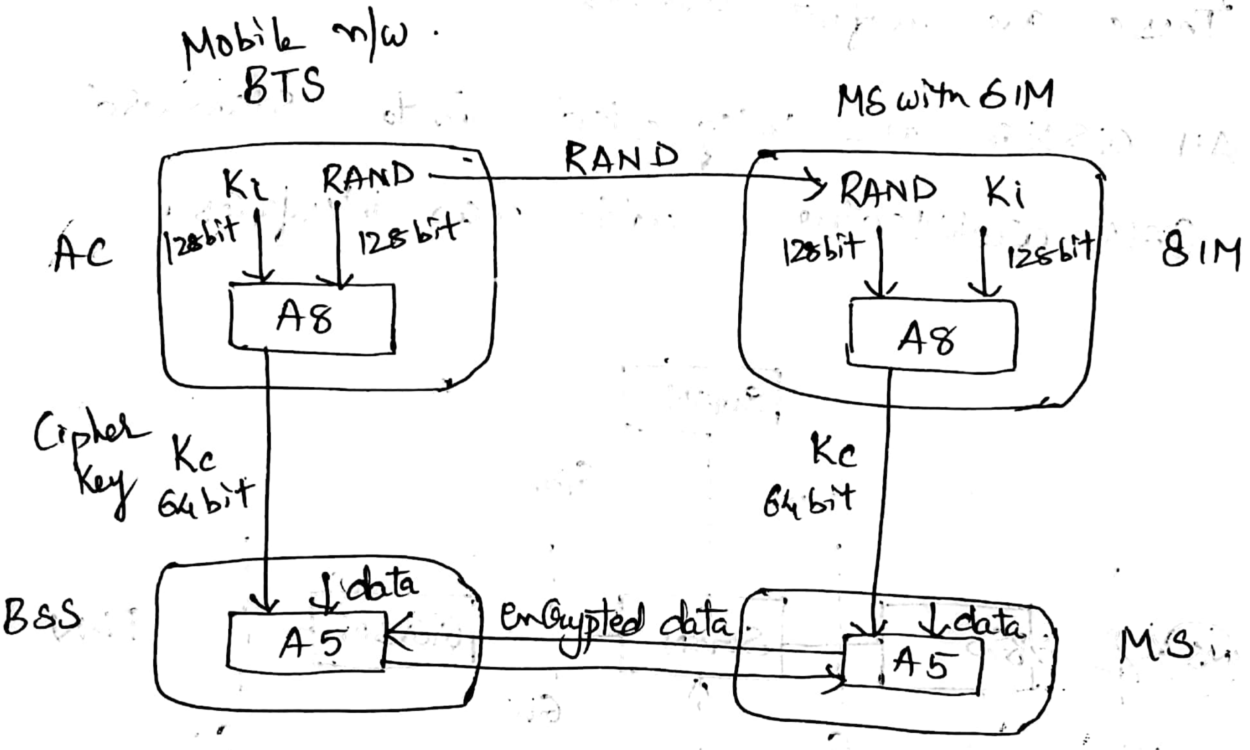


- For authentication, VLR sends the random value RAND to SIM.
- Both sides, n/w and subscriber module, perform same operation (A3) with RAND & Ki
- MS sends back SRES generated by SIM
- VLR compare both values.
- If they are same, VLR accepts the subscriber otherwise rejected.

Encryption

- To ensure privacy, all messages containing user-related information are encrypted in GSM over air interface.
- After authentication, MS and BSS can start using encryption by applying cipher key Kc.
- Kc is generated using
  individual key Ki &
  random value
  by applying A8 algorithm.

- SIM in MS & n/w both calculate same Kc based on random value RAND.
- MS & BTS can now encrypt and decrypt data using algorithm A5 and cipher key Kc.
- Kc should be 64 bit



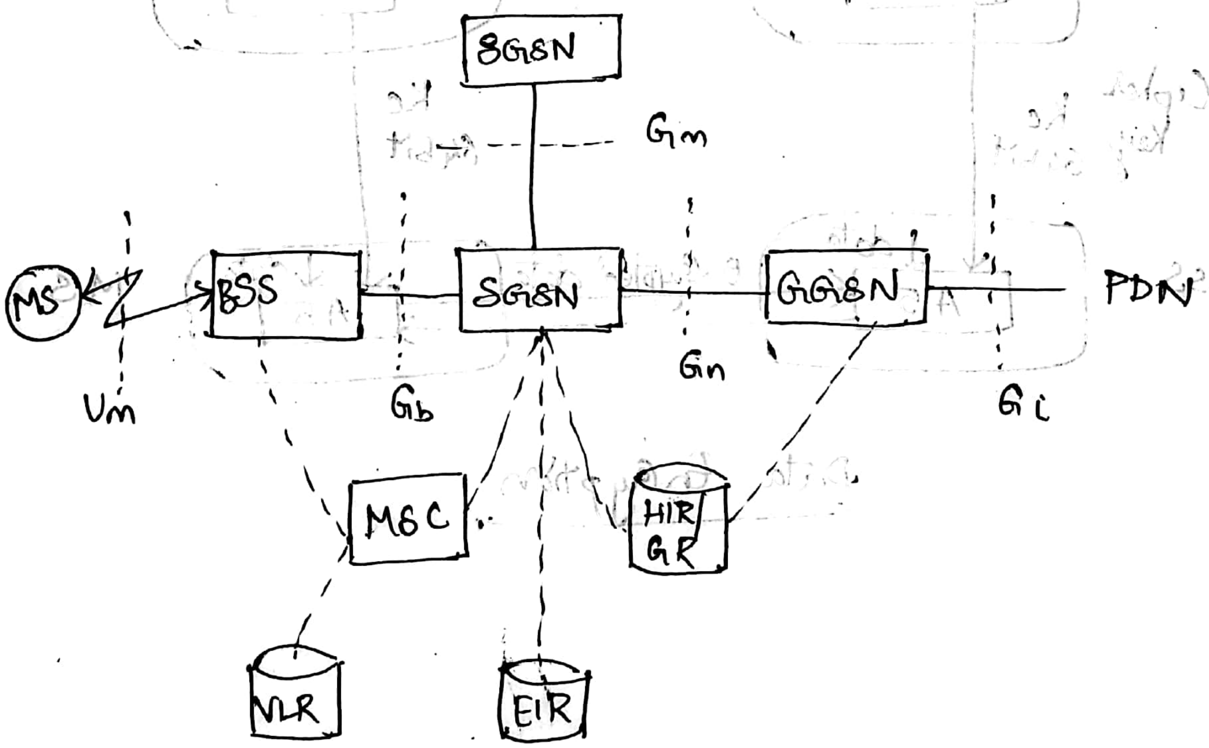
Data Encryption

GPRS

- General Packet Radio Service.
- provides packet mode transfer.

Architecture

- GPRS architecture has 2 new n/w elements called GPRS support nodes (GSN). These are in fact routers.
- All GSNs are integrated into standard GSM architecture with new interfaces.



- 1) Gateway GPRS support node (GGSN) is internetworking unit b/t GPRS n/w & packet data Networks (PDN)

- This node 1) contains routing information for GPRS users, 2) performs address conversion, 3) tunnels data to user via encapsulation.
- GGSN is connected to external n/w's via Gi interface, and transmits packets to SGSN via G_n (IP base GPRS backbone n/w)
- Other element 2). Serving GPRS support node (SGSN).

  It supports MS via G_b interface.
- This node 1) requests user addresses from GPRS register GR 2) keeps track of individual MS's location 3) responsible for collecting billing information 4) performs several security functions like access control.
- SGSN connected to BSC via frame relay
- GR is part of HLR which stores GPRS relevant data.
- Packet data is transmitted from PDN, via GGSN & SGSN directly to BSS & finally to MS.

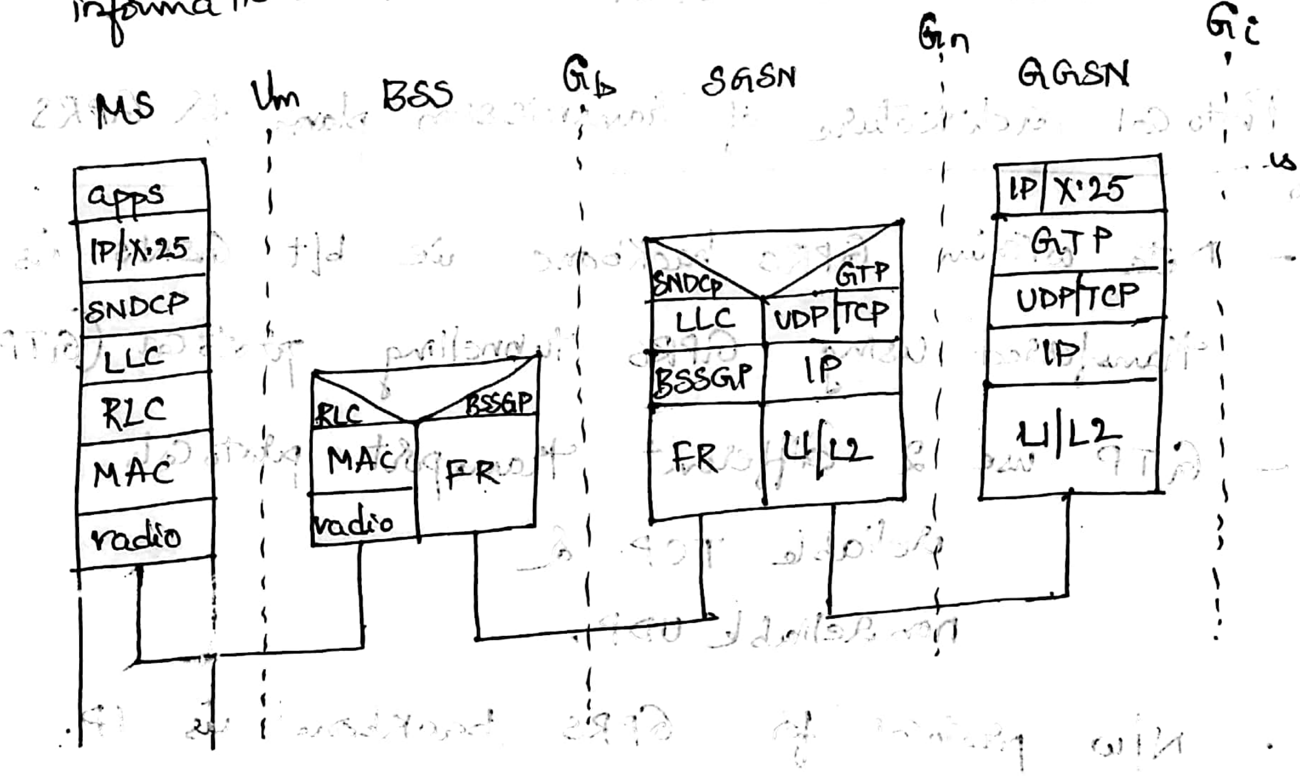
- MSC, which is responsible for data transport in GSM is used for signalling in GPRS.
- Before sending any data over GPRS n/w, an MS must attach to it, following procedures of Mobility Management.
- The attachment procedure includes assigning temporal identifier (Temporary logical link identity) – TLLI & Ciphering Key sequence number for encryption.
- For each MS, GPRS context is setup & stored in MS & corresponding SGSN.
- This context comprises
  - Status of MS (idle, ready, standby)
  - CKSN
  - a flag indicating if compression is used
  - routing data (TLLI)
    - Routing area RA
    - Cell identifier
    - packet data channel
    - PDCH
    - identifier

- Besides attaching & detaching mobility management also comprises functions for
  - authentication
  - location management
  - Ciphering.
- In Idle mode, MS is not reachable & cell context is deleted
- In standby ~~mode~~ state, only movement across routing areas is updated to SGSN but not changes of the cell.
- In ready state, every movement of MS is indicated to SGSN.

Protocol architecture of transmission plane for GPRS

- Data within GPRS backbone ie b/t GSNs is transferred using GPRS tunnelling protocol (GTP)
- GTP use 2 different transport protocols
  - reliable TCP &
  - non reliable UDP,
- N/w protocol for GPRS backbone is IP.

- To adapt to different characteristics of networks, Subnetwork dependent Convergence protocol (SNDCP) is used b/t SGSN & MS.
- on top of SNDCP and GTP, user packet data is tunneled from MS to GGSN & viceversa.
- To achieve a high reliability of packet transfer b/t SGSN & MS, LL is used. LLC comprises ARQ & FEC mechanisms for PTP
- Base station Subsystem GPRS protocol (BSSGP) is used to convey routing & QoS related information b/t BSS & SGSN.



- BSSGP does not perform error correction and works on top of frame relay (FR) n/w.
- Radio link dependent protocols are needed to transfer data over Um interface.
- Radio link protocol (RLC) provides reliable link MAC controls access with signaling procedures for radio channel & mapping of LLC frames onto GSM phy channels.
- Radio interface at Um needed for GPRS does not require fundamental changes compared to standard GSM.
- New logical channels & their mapping onto physical resources are defined.
- MS can allocate 8 packet data traffic channels (PDTCHs)
- Capacity can be allocated on demand and shared b/t circuit switched channels & GPRS
- Allocation can be done dynamically with load supervision.

- very important factor for any application working end-to-end is that it does not notice any details from GSM/GPRS related infrastructure
- The application uses IP packets are tunneled to GGSN, which forwards them into PDN.
- All PDNs forward their packets for GPRS users to GGSN.
- GGSN asks the current SGSN for tunnel parameters and forwards packets via SGSN to MS.
- All MSs are assigned private IP addresses and then translated into global addressed at GGSN.
- The advantage of this approach is inherent protection of MS from attacks
- Disadv: if MS wants to offer a service using fixed, globally visible IP addres.

UMTS

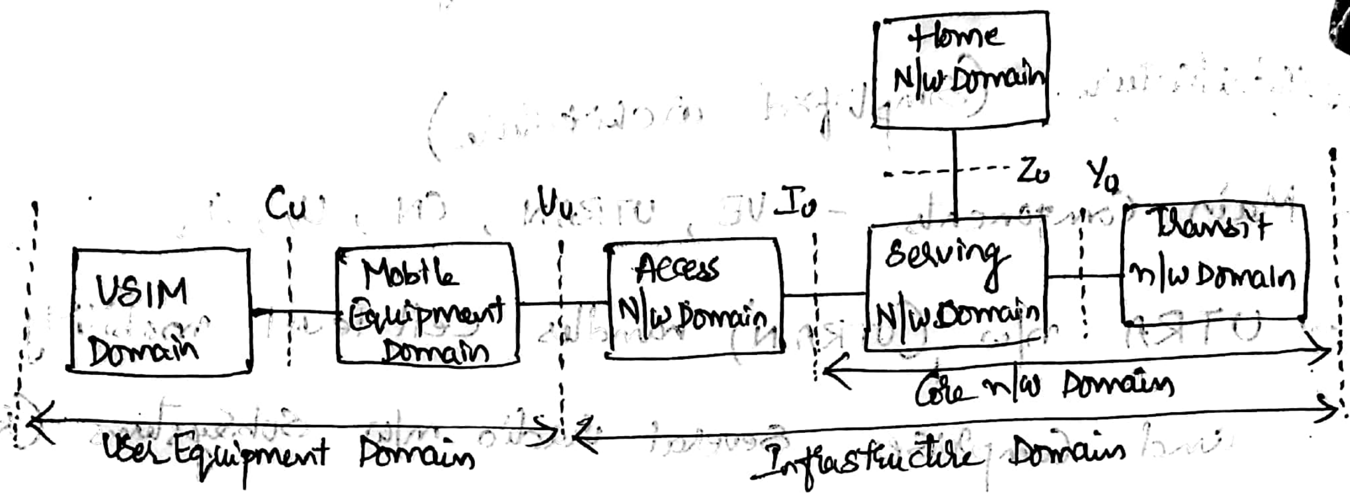
Universal Mobile Telecommunications System

* Architecture (Simplified architecture)

- Main Components - UE, UTRAN, CN, U_U, I_U
- UTRA n/w (UTRAN) handles cell level mobility and comprises several radio n/w subsystems (RNS)
- The functions of RNS
  - Radio channel ciphering
  - Radia channel deciphering
  - handover Control
  - radio resource management.
- UTRAN is connected to user equipment (UE) via radio interface U_U
- Via I_U interface, UTRAN commonicates with Core N/w (CN)

- CN contains functions for
  - inter-system handover
  - gateways to other n/ws
  - location management if No Connection b/t UE, UTRAN

- UMTS further subdivides simplified architecture into domains, interfaces.



- User equipment domain is assigned to single user and comprises all functions that are needed to access UMTS services.
- With in this domain 2 domains
  1) USIM domain
  2) Mobile Equipment Domain.
- USIM domain contains SIM for UMTS which performs functions for
  encryption & authentication
  stores all necessary user related data for UMTS
- USIM belongs to service providers and contains micro processor for enhanced program execution environment.

- End device itself is mobile equipment domain
  All functions for radio transmission as well as interfaces are located here.

- Infrastructure domain is shared among all users and offers UMTS services to accepted users.

- This domain consists of

  1) access n/w domain
     which contains radio access n/w's

  2) Core n/w domain
     which contains access n/w independent functions.

- The Core n/w domain separated into 3 domains

  1) Serving n/w domain
     functions currently used for accessing UMTS services.

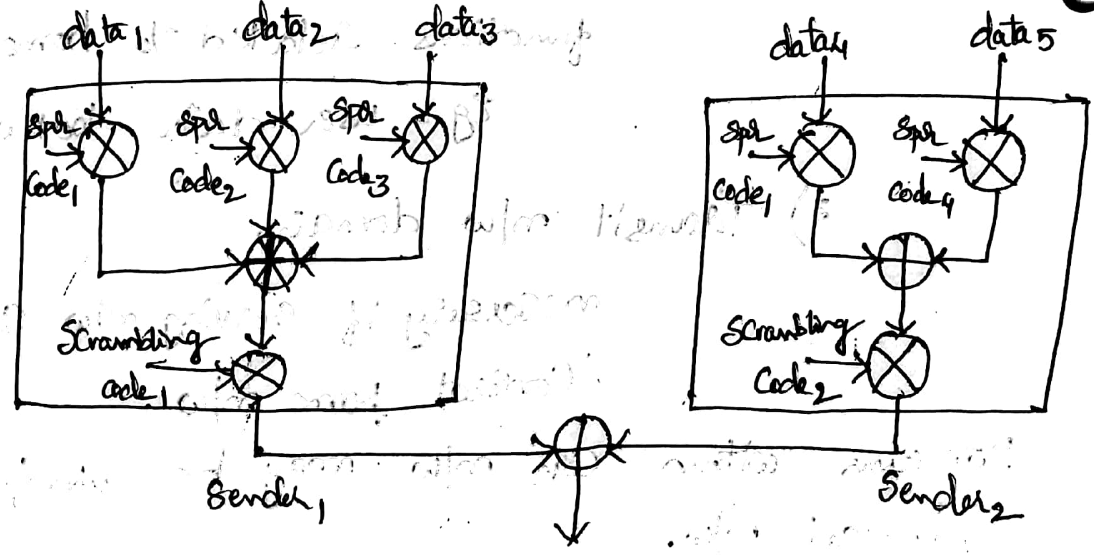
  2) Home n/w domain
     functions related to home n/w of user
     Eg :- user data look up

  3) Transit n/w domain
     necessary if serving n/w cannot directly contact home n/w.

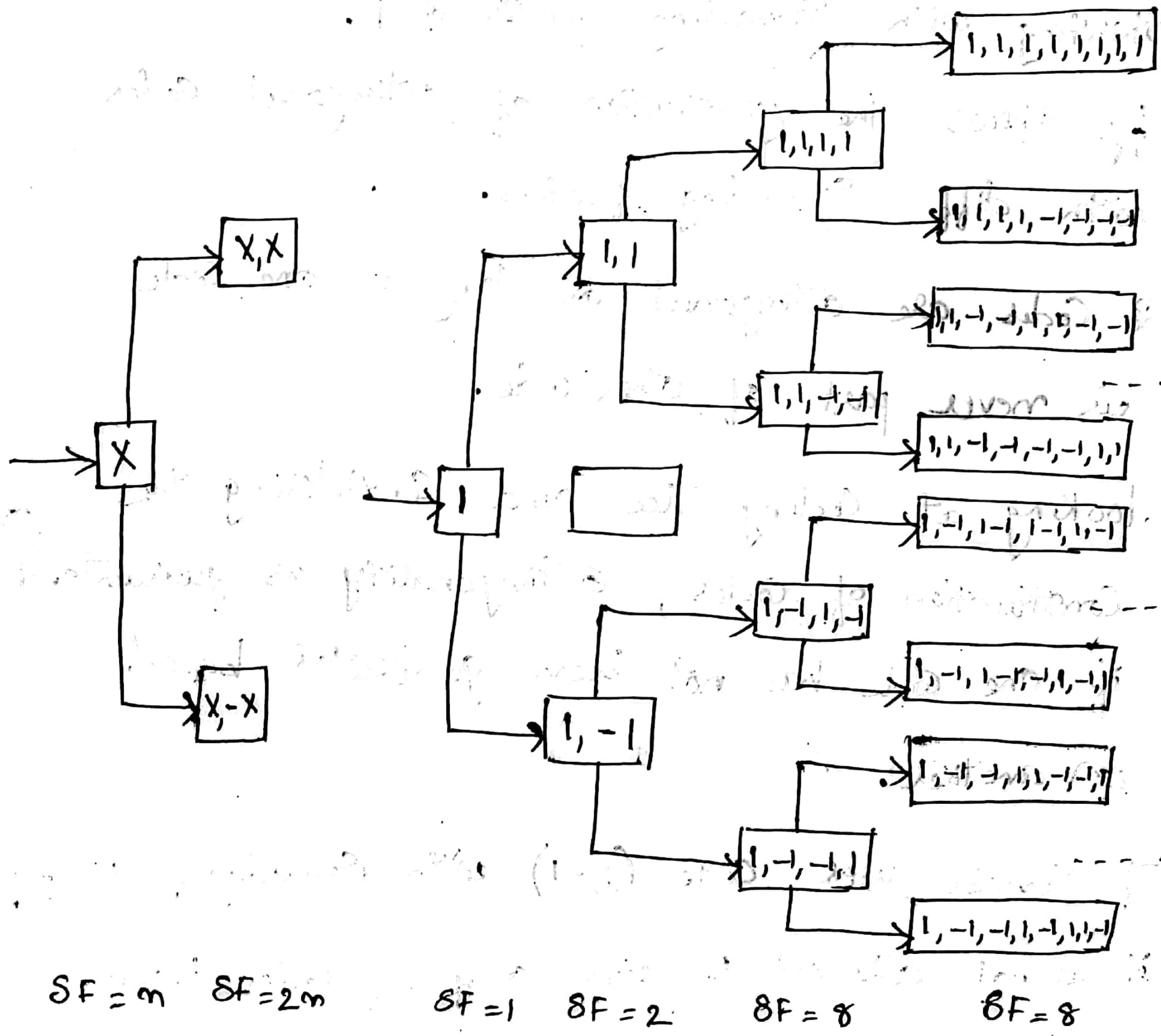
- Domains within Core n/w may be in fact same physical n/w.

UMTS radio interface

- Biggest difference b/t UMTS and GSM comes with new radio interface Uu.
- Direct sequence (DS) CDMA used in UMTS is new, not in US. This technologies multiplies stream of bits with chipping sequence
- This spreads the signal and if chipping sequence is unique, can separate diff users.
- To separate diff users, codes used for spreading should be orthogonal, i.e. their cross correlation should be 0.
- UMTS uses constant chipping rate.
- Figure shows basic ideas for spreading and separation of diff senders in UMTS.



- First step in sender is spreading of user data using orthogonal spreading codes.
- Using orthogonal codes separates the different data streams of a sender.
- UMTS uses orthogonal variable spreading factor (OVSF) codes.
- Basic idea of OVSF.



- Orthogonal Codes are generated by doubling a chipping sequence X with and without flipping the sign of chips.
- This results in X and −X.
- Doubling the chipping sequence also results in spreading bit twice as much as before.
- Spreading factor SF = n becomes 2n.
- Starting with spreading factor of 1.
- fig shows the generation of orthogonal codes with diff spreading factors.
- 2 Codes are orthogonal as long as one code is never part of other code.
- looking at coding tree and considering the construction of codes, orthogonality is guaranteed if one code has not been generated based on another.
- If sender uses code (1, −1) with spreading factor 2, it is not allowed to use any of codes located in subtrees generated out of (1, −1)

  Eg: (1, −1, 1, −1), (1, −1, −1, 1, −1, 1, 1, −1) & (1, −1, −1, 1, −1, 1, 1, −1, −1, 1, 1, −1, 1, −1, −1, 1) Cannot be used anymore.

- It is no problem to use codes with different spreading factors if one code has not been generated using other.

Thus (1,-1) block only the lower subtree, many other codes from upper part can still be used.

- An example for valid combination in OVSF is
  (1,-1), (1,1,-1,-1), (1,1,1,1,1,1,1,1),
  (1,1,1,1,-1,-1,-1,-1,1,1,1,1,-1,-1,-1,-1),
  (1,1,1,1,-1,-1,-1,-1,-1,-1,-1,-1,1,1,1,1)

- This combination occupies the whole code spaces and allows for transmission of data with different spreading factors (2,4,8, and 2*16)

- This example shows the tight coupling of available spreading factors and orthogonal codes.

- UMTS uses constant chipping rate (3.84 Mchip/s) using diff spreading factors this directly translates into the support of diff data rates.

- If chipping rate is constant, doubling the spreading factor means dividing the data rate by 2.

- Also, UMTS can only support a single data stream with SF=1 as then no other code may be used

- Using ex. combination above, a stream with half max. data rate, one with fourth, one with an eighth and 2 with 16th are supported at same time
- Each sender uses OVSF to spread its data stream
- The spreading codes chosen in senders can be the same.
- Using diff spreading codes in all senders within a cell would require a lot of mgmt and would increase complexity.
- After spreading, chip streams are added and scrambled.
- Scrambling does not spread the chip sequence any further but XORs chips based on code.
- In FDD mode, scrambling code is unique for each sender and separates all senders in a cell.
- In TDD, scrambling code is cell specific i.e all stations in cell use same code & cells are separated using diff codes.
- After scrambling, signals of diff senders are quasi orthogonal (stay quasi orthogonal even if they are not synchronized)