Introduction to GSM :-

- GSM stands for Global System for Mobile.
- It is second generation digital cellular technology used for mobile voice & data services.
- It is developed by ETSI (European Technical Standards Institute).
- GSM uses narrowband (Time Division Multiple Access) TDMA for providing voice & text based services over mobile phone networks.
- It is the first cellular system to use digital modulation schemes & network level architectures.
- Presently GSM supports more than one billion mobile subscribers in more than 210 countries throughout the world.

Characteristics of GSM standards :-

1) Use of SIM :- GSM makes use of SIM (Subscriber Identity module) which is actually a storage device & it is available in the form of smart cards. It is removable & portable.

It stores following :-

(i) Subscriber identification number
(ii) Subscriber's home network and country information.
(iii) Private Keys.
(iv) User specific information etc.

2) Privacy of Data :- All the data streams are encrypted to provide necessary privacy & security to the data when it is transmitted on air. For this purpose specific cryptographic keys which are function of time are used which are known to the cellular device only.

3) GSM provides improved spectrum efficiency.

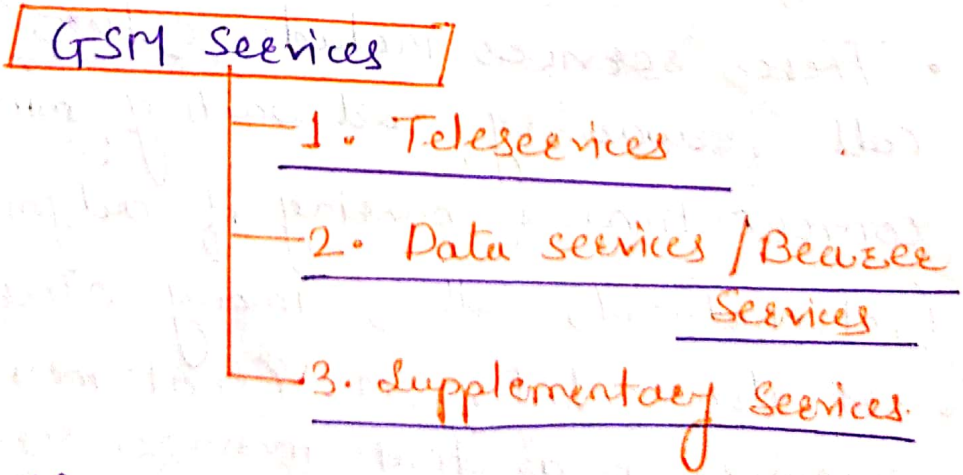
4) The facility of national & international roaming is provided.

5) GSM maintains good speech quality.

6) GSM is compatible with ISDN, PSTN & other telephone company services.

7) It can also be made compatible to newer services.

GSM Services :-



1. Teleservices :-

- These services allows subscriber to use terminal equipment functions for communication with other subscribers.
- It supports emergency calling, Fax services, videotex & Telex services.

2) Data Services / Bearer Services:-

- These services allow subscribers to transmit appropriate signals across user network interfaces.
- It supports packet switched protocols & data rates from 300bps to 9.6 Kbps.
- Data can be transmitted in two modes:-

(i) Transparent mode:- GSM provides standard Channel coding for user

(ii) Non-Transparent mode:- ↳ provides special coding methods based on particular data interface.

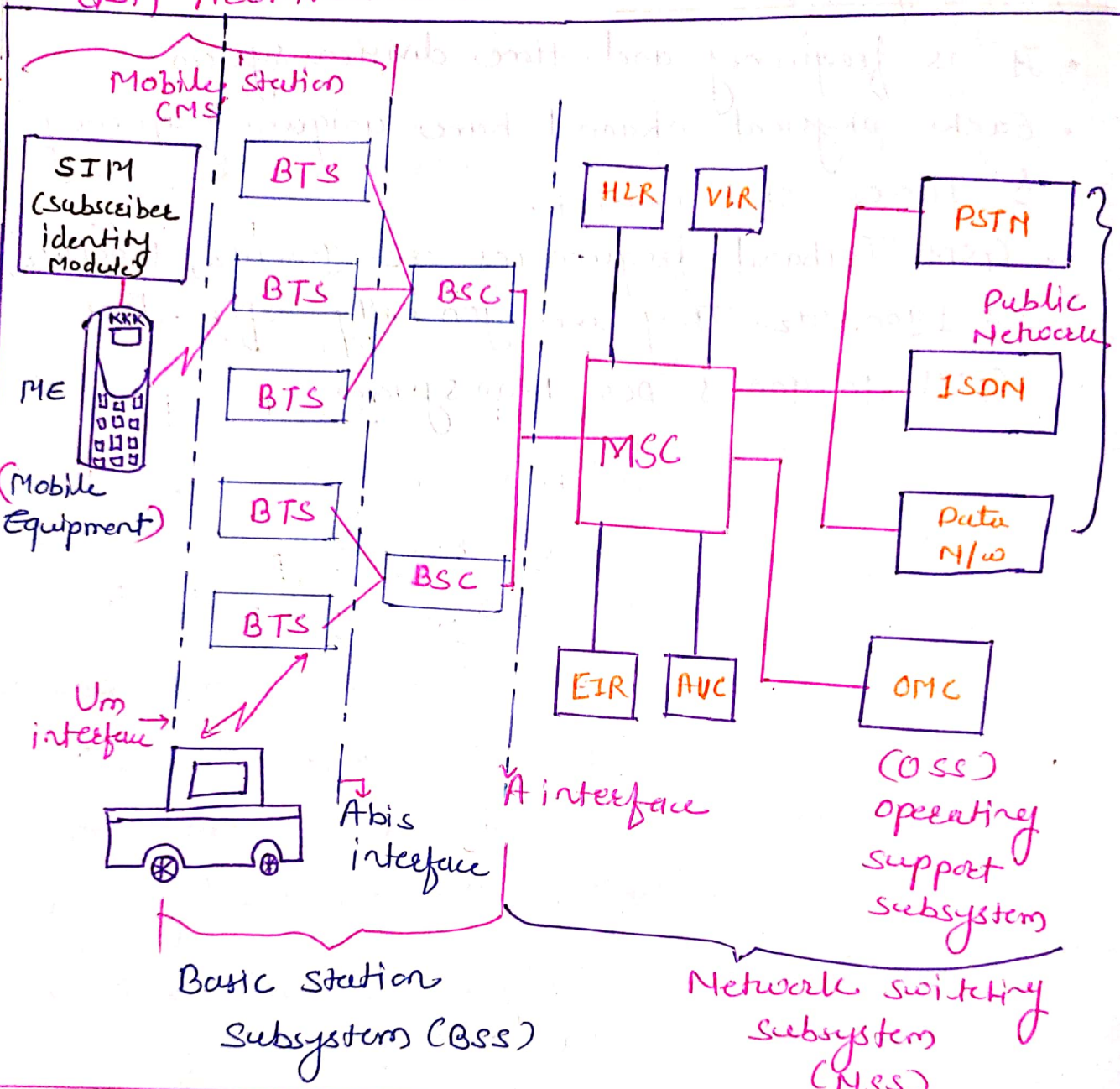
3) Supplementary services:-

- These services supplements the teleservices and are offered with basic teleservices.
- They are digital in nature.
- These services includes caller identification, call forwarding, call waiting, multiparty conversations & barring of outgoing (international) calls, among others.
- It also includes SMS (Short message service) Service is a text message service that allows sending & receiving text messages on your GSM mobile phone.
- Call conferencing, call waiting, call barring, call forwarding, Number identification, Advice of charge, closed user groups.

GSM Frequency Bands:-

- It is frequency and time division system.
- Each physical channel have unique frequency & time slot number.
- GSM Triband frequencies are 900MHz, 1800MHz, & 1900 MHz. They are generally referred as GSM 900 & DCS 1800 systems.

GSM Architecture :-



BTS :- Base Transceiver station
BSC :- Base station Controller
HLR :- Home location Register.
VLR :- Visitor location Register
MSC :- Mobile switching center
EIR :- Equipment Identity Register
AUC :- Authentication center
OMC :- operation Maintenance center

Fig :- GSM Architecture

- GSM architecture shows various functional entities and three main subsystems.
  1. BSS :- Base station subsystem
  2. NSS :- Network & switching subsystem
  3. OSS :- Operational subsystem

MS (Mobile station):-

- It consists of the physical mobile handset or equipment used by the subscriber to access the GSM network.
- It includes
  1. MT :- Mobile Termination.
  2. TE :- Terminal Equipment
  3. TA :- Terminal Adapter
- Types of MS are
  1. Vehicle mounted station.
  2. Portable station
  3. Handheld station

- Generally MS is available in five power classes as shown in table. It provides information about the maximum power level the mobile equipment can transmit.
- Class I & II for vehicular or portable units, classes III, IV & V refers to handheld units.

Class	Maximum RF power transmitted by MS in watts
I	20 (Not yet implemented)
II	8
III	5
IV	2
V	0.8

MS

1) Mobile Terminal 2) SIM

1. Mobile Terminal :- It is the combination of hardware & software. It manages all the radio & human interface functions. It is nothing but mobile handset.

2. SIM (Subscribed Identity Module) :-

It is plugged into mobile terminal. Without the SIM card MS cannot communicate with any user or network. It is provided by the mobile service providers.

It is microprocessor based entity implemented on smart card.

SIM

ID-1 SIM (Credit card size)

Plug in SIM (Normal SIM used in Commercial GSM phones).

SIM carries information like

1) IMSI 2) TMSI

3) Authentication key.

4) Cipher key.

5) Location area identity.

6) Access control class.

7) Administrative information.

Description of Subsystems:-

- GSM system architecture as shown in fig.
- It consists of four major subsystem blocks as under
  1. Mobile station (MS).
  2. Base station subsystem (BSS)
  3. Network and switching Subsystem (NSS)
  4. Operating Support Subsystem (OSS)

The functions of each subsystem block are discussed as under.

<1> Mobile station (MS):-

- The mobile station (MS) is also a subsystem, but it is usually considered to be a part of the Base station Subsystem (BSS) for architecture purpose.
- It communicates with the BSS over the radio air interface.
- It is used to support the connections of the external terminals such as PC or FAX.

<2> Base station Subsystem :- (BSS)

- It is also known as Radio station subsystem (RSS)
- It consists of number of base station controllers (BSCs) & Base Transreceiver Stations (BTSs).
- Each BSC is connected to a number of BTSs,
- It provides radio interface for device.
- The BSS gets connected to MS through a air interface & its connected to NSS.

(3) Network & Switching subsystems (NSS).

- The NSS consists of a number of (MSCs) Mobile switching centers (MSCs).
- Each MSC consists of the NSS interfaced to the number of BSCs & BTS.
- There are HLRs & VLRs & AUC present in NSS.
- The NSS uses the intelligent Network & the signaling is one of the main switching function of GSM.

(4) Operation Support Subsystem (OSS)

- OSS consists of the Authentication Center (AUC), Equipment Identity Register (EIR) & operation & maintenance center.
- The areas coming under OSS are as under.
  1. Network operation & maintenance
  2. Charging & billing.
  3. Management of mobile equipment.

BSS (Base station Subsystem)

- It manages all the signalling & traffic between MS & NSS.
- Functions performed by BSS are
  1) Coding of speech channels.
  2) Allocation of available radio channels to mobile on request.
  3) Transmission of paging signals.

GSM Interfaces and GSM protocol Architecture

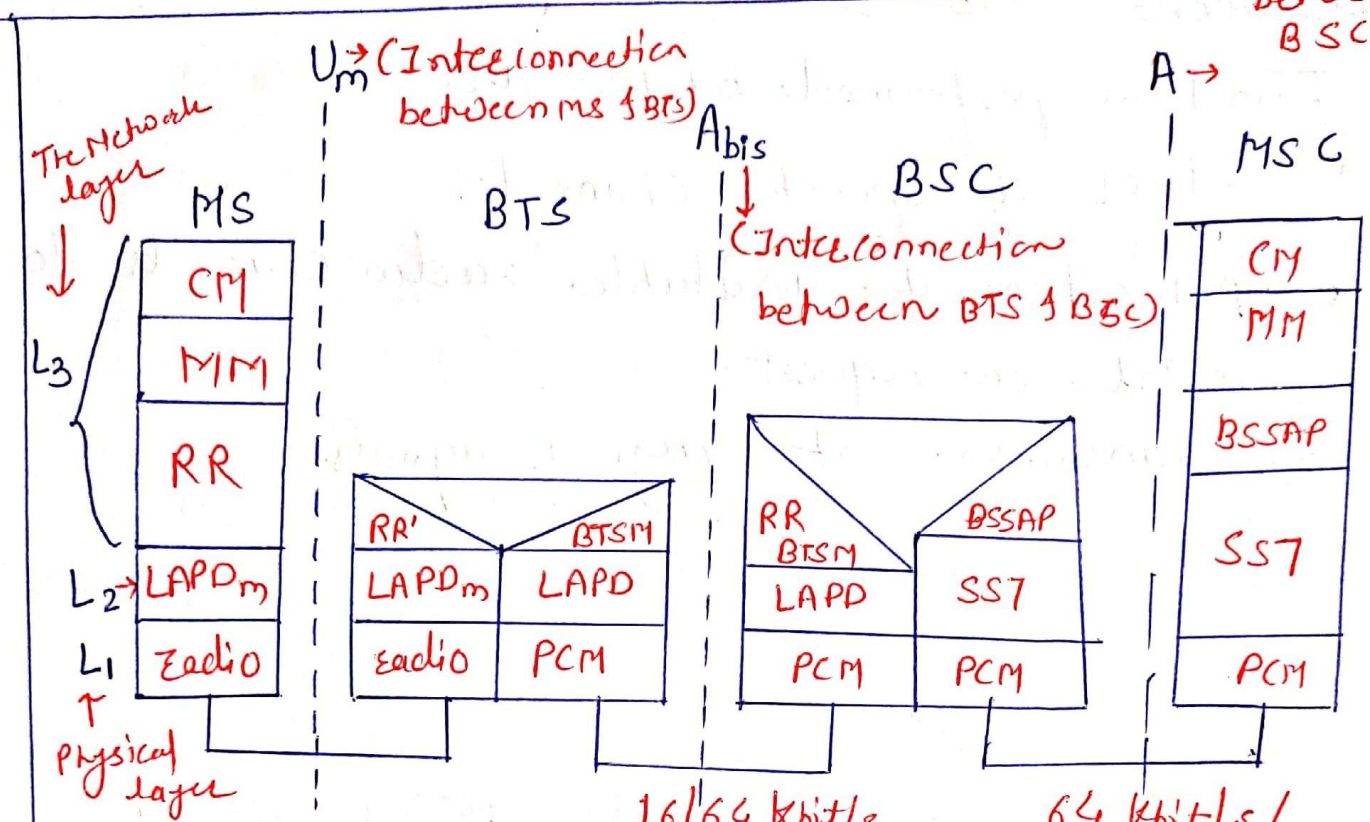


Fig :- Protocol Architecture for GSM signalling showing various radio interfaces.

L_1 - Physical layer
L_2 - Link access protocol ($LAPD_m$) on D channel modified

- There are 3 different interfaces present in GSM system they are.
  1. Um :- Interconnection between MS & BTS
  2. Abis :- Interconnection between BTS & BSC
  3. A :- Interconnection between BSC to MSC

Um Interface

- The radio interface between MS & Base transceiver station. is known as Um radio interface.
- The GSM radio interface depends on TDMA & FDD

- TDMA :- frequency is shared among different users by dividing the time in slots.
- FDD : it allows the use of two different frequencies for uplink i.e. from MS to BTS and downlink BTS to MS.

Three layers :-

1) L_1 :- Physical layer
2) L_2 (LAPDm) :- Link access protocal on D channel modified
3) L_3 :- The Network layer

Layer 1 :- The Physical layer :-

- Formation of bursts in 5 different formats.
- Formation of TDMA frame by multiplexing of bursts
- Synchronisation with BTS with timing advance technique.
- Monitoring the quality of channel on the downlink path.
- Identification of idle channels.
- Interfacing to the data link layer & radio resource management sublayer for traffic management
- Encryption & decryption of data between MS & BSS using FEC.

Layer 2:- LAPDm layer - This is based on ISDN LAPD Protocal.

- Reliable data transfer between GSM network and MS.
- Arrangement of sequencing of data frames.
- Flow control.
- Segmentation & reassembly of the data.

Layer 3:- The network layer

It consist of three sublayers.

1. RR: Radio Resource Management sublayer.
2. MM: Mobility Management sublayer.
3. CM:- Call Management sublayer.

1. RR :- It is used for setup, maintenance & disconnection of radio channels. It can directly access the physical layer & provides reliable communication path for upper layer.

2. MM :- It supports the functions of location updating, authentication & encryption, allocation of TMSI. It also supports reliable connection to upper layer.

3. CM :- It consists of three functional entities
   (1) call control (call control)
   (2) SMS (Short message service)
   (3) SS - (Supplementary service)

Abis Interface:-

It provides the interface between BTS & MSC.

Functions:-

1. Radio channel Management
2. Traffic channel Management
3. Terrestrial channel Management

It supports two different links

- 64 Kbps link (full rate or half rate carrying speech or user data)
- 16 Kbps link (Control information link between BSC - BTS & BTS-MSC)

- Three layers are present in this:-

1. The physical layer
2. LAPD layer.
3. Network layer - 'RR' is used, it is only part of radio resource management sublayer.
   All the functions of RR' are supported by BTSM

A Interface :-

- It provides the interconnection between BSS & MSC.
- SS7 is used for communication between MS & MSC
- The messaging required within the network to enable handover etc to be undertaken is carried over the interface.

Interfaces used within NSS

The mobile Application Part (MAP) is an SS7 protocol that provides an application layer for the various nodes in GSM & UMTS mobile core networks & GPRS core networks to communicate with each other in order to provide services to users.

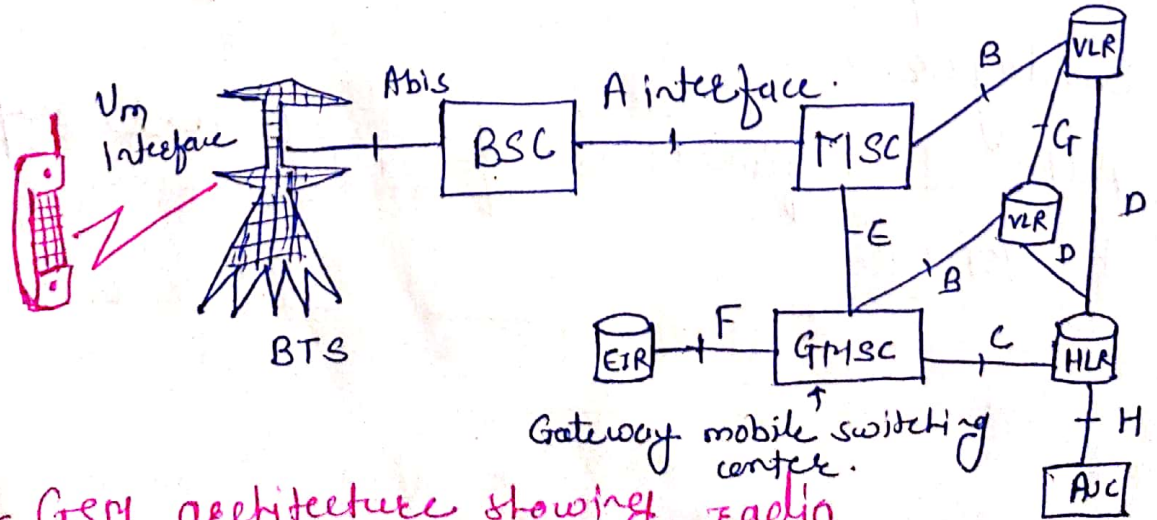


Fig:- GSM architecture showing radio interfaces between various functional entities

1. B interface :-

- It interconnects MSC & VLR. It is purely an internal interface.
- Protocol used : MAP / B
- It is used to access data regarding MS located in MSC area.

2. C interface :-

- It interconnects HLR & GMSC
- The Gateway Mobile switching center (GMSC) is a type of Mobile switching center (MSC) that is used to route calls outside the mobile network.
- Protocol used : MAP / C
- The MSC may optionally forward billing information to the HLR after the call is completed and cleared down.

3. D interface :-

- It interconnects HLR & VLR
- Protocol used : MAP / D
- It supports functions like exchange of the data related to the location of the ME & to the management of the subscriber.

4. E interface :-

- It interconnects two MSCs.
- Protocol used : MAP/E
- The E interface exchanges data related to handover between two MSCs.

---

5. F interface :-

- It interconnects MSC & EIR
- Protocol used : MAP/F
- Used to confirm the status of the IMEI of the ME gaining access to the network
  (International mobile Equipment Identity)

---

6. G interface :-

- It interconnects two VLRs of different MSCs
- Protocol used : MAP/G
- It is used to access subscriber information e.g. during a location update procedure.

7. H interface :-

- It interconnects MSC & SMSC (SMS centre)
- Protocol used MAP/H
- Used to support SMS services.

8. I interface :-

- It interconnects MSC & ME
- exchanges of transparent messages.
-

Security in GSM:-

- In any of the digital cellular systems, security provision is relatively easy compared to analog systems.
- Methods like encryption, scrambling, FEC etc. can be employed to ensure security in the system
- GSM offers several security services based on the information stored in AUC & SIM The security services offered by GSM are.

Security Services

- 1) Access control and authentication.
- 2) Confidentiality.
- 3) Anonymity.

1. Access control & authentication:-

Access to the GSM Network is allowed only through user authentication process. For this first user needs to have valid PIN to access the SIM & then using challenge response scheme authentication is done in mobile originated & mobile terminated calls.

2. Confidentiality:-

Once the authentication is done all the user data, voice etc are encrypted to provide confidentiality. It exists only between MS & BTS.

3. Anonymity :- (The situation where a person's name is not known)

- User's real identity is never transmitted on air.
- Every user is allowed with TMSI which is unique for each call. & VLR can change TMSI at any time.
- These three services are achieved by three algorithms in GSM network.
  1. A3 algorithm for authentication.
  2. A5 algorithm for encryption,
  3. A8 algorithm for generation of a cipher key.

TMSI - Temporary Mobile Subscriber Identity.

Authentication using A3 algorithm :-

- Authentication is done with the help of SIM. SIM stores authentication key & the user IMSI.
- Authentication is done by challenge response or request response method between MS & BTS
- RAND random number is generated by AC (access control) which acts as a challenge & SIM responds to it by SRES (signed response)
- AUC generates RAND, SRES & cipher key Kc (used to encrypt the data) for each IMSI received & then forwards this to HLR. VLR may ask for these values from HLR.
- This RAND is sent to SIM by VLR for authentication purpose.
- On network side as well as on SIM side algorithm A3 is carried out on the RAND & Ki.
- Then MS sends SRES generated by SIM on air & VLR compares this received value with the one generated in the network.
- If both the values matches, subscriber is allowed to access the network otherwise he is denied the access.

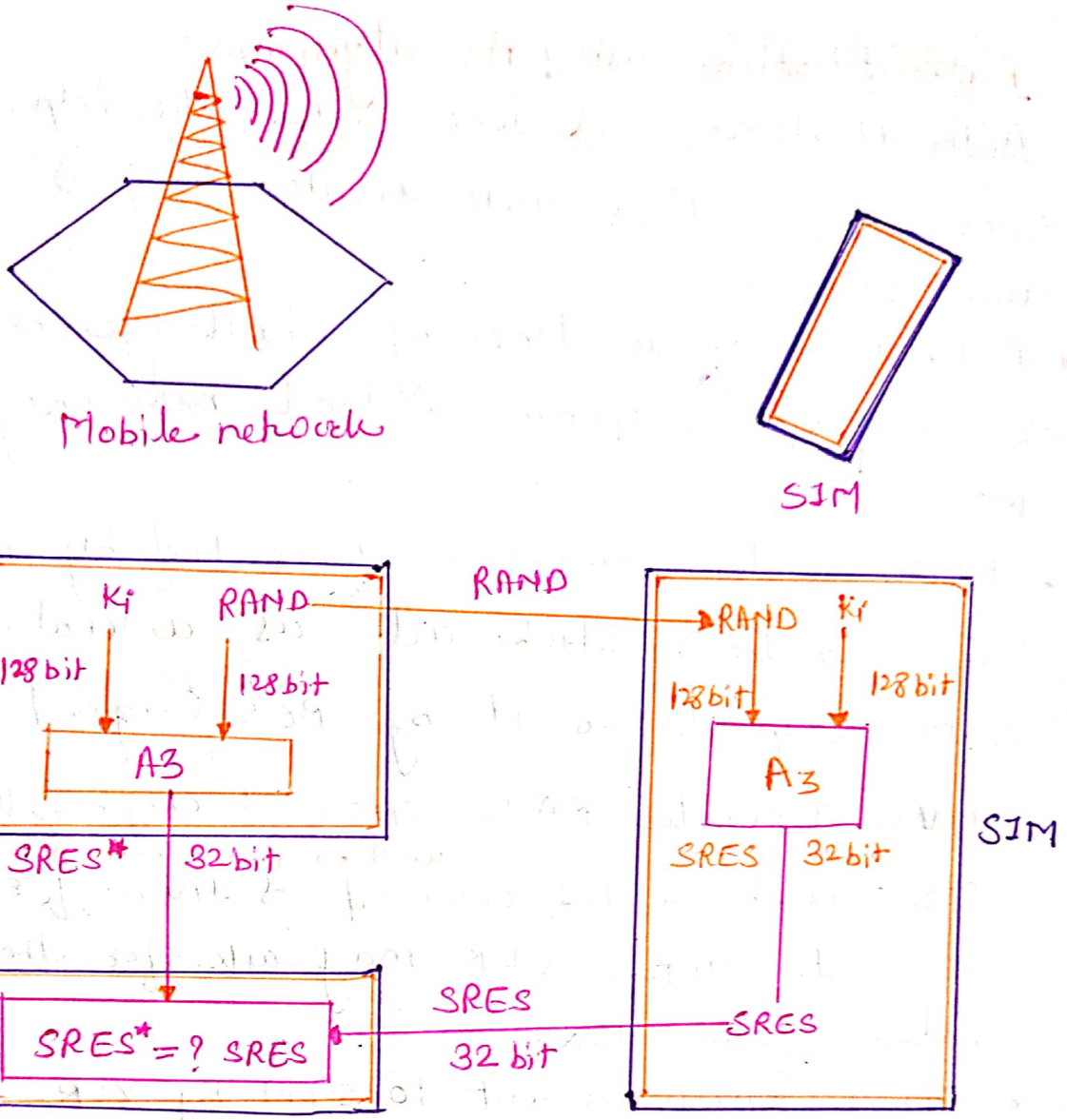


Fig:- Subscribee's authentication using A3 algorithm

Data Encryption using A5 and A8 Algorithm :-

- All the user information is always encrypted before it is sent on air.
- For encryption A5 algorithm is used which is an European standard. Only manufacturers of the cellular devices has access to this algorithm.
- Entire encryption is based on encryption key or cipher key K_c which is never sent on air to maintain secrecy
- 64 bit cipher key K_c is generated using the values already SIM has (received during authentication process) which are Ki and RAND. This is done by A8 algorithm.
- SIM & Network both calculates K_c based on these values.
- Now encryption & decryption is carried out using A5 algorithm & K_c.
- Based on K_c current TDMA frame number, A5 algorithm generates 114 bits.
- These 114 bits are then modulo 2 added to the information bits in the normal GSM burst & then it is transmitted.
- Same operation is carried at the network side on the received normal burst
- If the received data has no errors the modulo 2 addition of the received data

and the generated encrypted data gives out the original data sequence.

- This is decryption process.

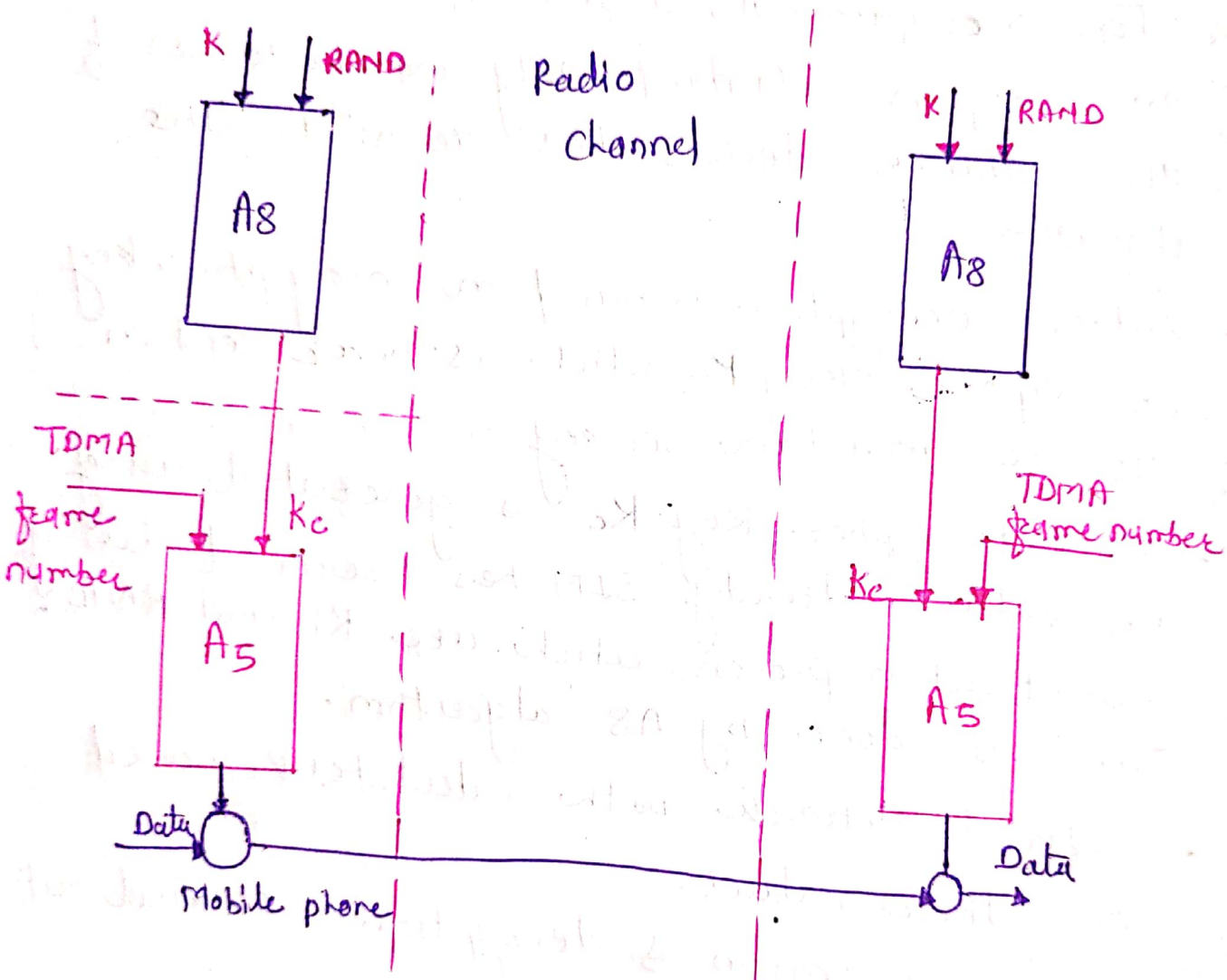


Fig:- Data encryption using A5 & A8 algorithm

GSM Services:-

1. Teleservices
2. Data services / Bearer services.
3. Supplimentary services.

---

1) Teleservices:- These services allows subscribers to use terminal equipment functions for communication with other subscribers.

- It supports emergency calling, FAX. services, videotex & Teletex services though they are not integral part of the GSM standard.

2) Data services / Bearer services:-

- These services allow subscriber to transmit appropriate signals across user network interfaces.
- It supports packet switched protocols & data rates from 300 bps to 9.6 Kbps.

(i) Transparent mode:- GSM network provides standard channel coding method for user data

(ii) Non-transparent mode:- GSM network provides special coding methods based on particular data interface.

---

3. Supplementary services:-

- These services supplements the teleservices & are offered with basic teleservices.
- They are digital in nature
- These services include called identification, call forwarding, call waiting, multiparty conversations, international calls.
- It also includes SMS.
- Supplementary services.

(i) call conferencing (ii) call waiting
(iii) call barring (iv) call forwarding
(v) Number identification.
(vi) Advice of charge.
(vii) closed user groups.

Signalling system No. 7

- The SS7 signaling protocol is used for common channel signaling between the interconnected networks.
- Common channel signaling is the technique by which simultaneous transmission of user data, signalling data and other related traffic through out a network is achieved.
- SS7 is used to interconnect maximum MSCs throughout USA. It enabled autonomous registration & automated roaming features in 1G cellular system.
- A comparision of SS7 protocol model with the standard OSI -7 layer is model
- The lowest three layers of the OSI model are equivalent to the network service part (NSP) of the SS7 protocol
- NSP [Network service part) is made up of
  - MTP [Message Transfer Part]
  - SCCP [signaling connection control part]

Need of 3G & 4G :-

1. Global mobility & service delivery without interruption.
2. Interconnection of the other wireline & wireless network.
3. Flexibility to accommodate changes for next generation evolution.

---

1. Global Mobility & service delivery without interruption :-

- Before 3G every country has adopted their own standard for wireless communication.
- IMT 2000 has standardised the spectrum & also the standards.
- This made worldwide roaming & service delivery of voice & non voice data seamlessly.
- It is need of global market to have international wireless connectivity.
- With 3G/4G technologies, global communication has become really very easy & simple.
- It also provides video calling & multimedia transfer which is not present in 2G.

2. Interconnection of the other wireline & wireless network :-

- 3G/4G has interconnectivity to other wireline networks like PSTN.
- It also supports backward compatibility for circuit switching networks. This allows use of previous technologies as well.

3. Flexibility to accomodate changes for next generation evolution :-

- As the common spectrum is used in 3G onwards standards, it has become very easy to adapt changes in the network.
- It also supports various additional features & improved spectrum efficiency & increased capacity.

IMT 2000 Global standards:-

- ITU (International telecommunications union) has specified IMT2000 specification.
- IMT 2000 means international mobile standards.
- It includes UMTS → CDMA-2000, TD-CDMA, TDS – CDMA etc. It also includes WIMAX.
- It provides the services like video calls, voice telephones, wireless data.
- The main advantage of IMT2000 standards is simultaneous transmission of speech & data services together.
- It provides high data rates at cell.

* Imp *

Vision of IMT 2000 OR specification, objectives, Advantages, Features :-

1. Common spectrum world wide (1.8 - 2.2 GHz)

- 3G & 4G common freq^{n} spectrum of 1.8 - 2.2 MHz worldwide
- It provides global connectivity.

2. Multiple radio environments :-

- 3G not only support cellular network it also support cordless, satellite, LAN, WLL environments.

3. Wide range of telecommunication services.

- It provides multiple services like. voice, high speed internet, video calling, multimedia file sharing.

4. Flexible radio bearers for increased spectrum efficiency :- WCDMA (wideband CDMA) technology is used.

- It helps in ~~accomo~~ accommodating increasing user demand.

5. Data rates upto 2 Mbps for Indoor environments :- It provides data rate upto 2 Mbps for Indoor environment applications.

6. Maximum use of IN capabilities (for service provision & transport)

- 3G standard makes use of IN intelligent node capabilities to the maximum extent.
- supports enhanced services.

7. Global seamless roaming :-

- Common frequency spectrum accepted in 3G, worldwide roaming is possible.
- Interconnectivity between countries is provided.
- International roaming is possible.

8. Enhanced security & performance :-

- IMT 2000 provides enhanced security & performance.
- Data security is better than 2G.

9. Integration of satellite & terrestrial systems.

- Provides interconnectivity of terrestrial & satellite communication.
- → Multimedia application services & terminals.
- → Improved spectrum efficiency.
- → Flexibility for evolution to the next generation of wireless systems.
- → High speed data

Compatibility of IMT 2000 or Backward Compatibility :-

- IMT 2000 provides backward compatibility with IS-95 & GSM.
- Provides interconnection bet^N terrestrial & satellite Networks.
- It is used with or incorporates the LAN, PSTN, ISDN, satellite N/W.
- Every 2G standard is evolved to some of the standard belonging to IMT 2000 family. For example GSM is evolving towards UMTS, IS95 to CDMA2000

IMT 2000 services :-

(a) Multimedia communication services

(b) Global services

(c) Seamless services.

(a) Multimedia communication services :-

- Voice communication, video calling, Data communication, (VHE) Virtual Home entertainment.
- Due to these services we can access Internet on laptop even outdoors
- Laptop access the data communication via mobile.
- Provides exact location information using mobile networks.
- (M-Commerce) mobile commerce.

(b) Global service :-

- It allows global roaming.
- Provides Global coverage
- High degree of security
- Provides Terminal mobility, User mobility & service mobility.

(c) Seamless service :-

- It allows user to use previous networks & internet with current quality of services irrespective of wireless environment, location & service provider.

UMTS (Universal Mobile Telecommunication Systems) OR W-CDMA

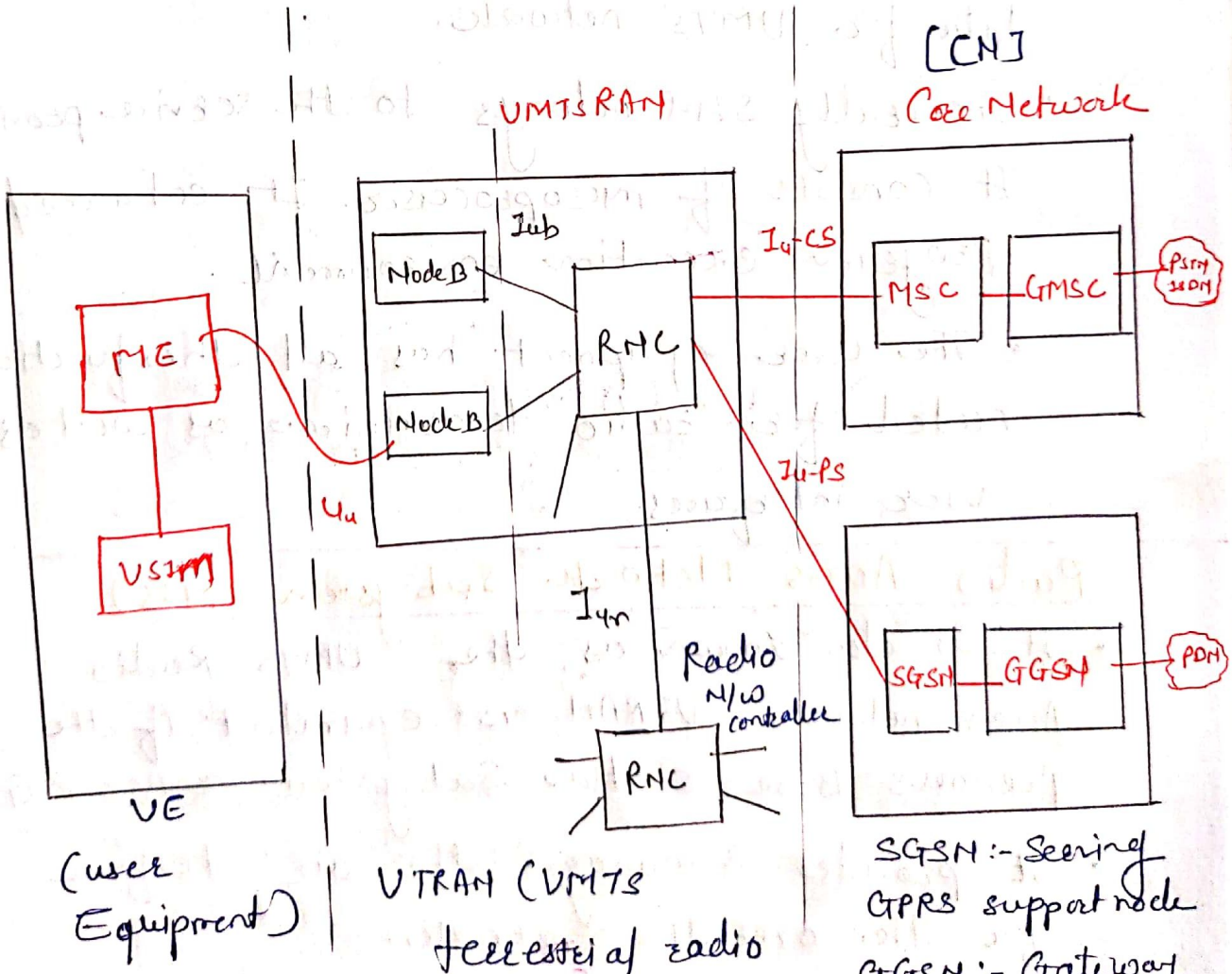
- UMTS used for variety of data & speech services.
- It is standared evolution of TDMA based GSM.
- It provides fixed & mobile access for public & private networks.
- It is 3G standard developed by ETSI in 1998.
- It is also called as Wireless CDMA.
- It was designed to provide a high capacity upgrade path for GSM.
- UMTS has backward compatibility with 2G GSM, IS-136 & PDC TDMA, 2.5 G TDMA.
- UMTS air interface designed for "always-on" packet based wireless service, so that computers, entertainment devices & telephones can all share the same wireless network & be connected to the internet, anytime & anywhere.
- supports data rates upto 2.048 Mbps per user.

Features of UMTS :-

- Works with TDD & FDD duplexing schemes.
- Backward compatibility with GSM, IS-136
- Data rate - up to 2.048 Mbps.
- Minimum forward channel bandwidth - 5MHz
- Network structure & bit level packaging remains same as that of GSM.
- Always on packet based wireless network
- Maximum 350 voice calls are supported simultaneously,
- Better spectrum efficiency.

UMTS Architecture :-

- UMTS architectures partially based on 3G technologies while keeping few features of 2G Technology i.e. GSM.
- The main blocks in the architecture are
  1. UE (user Equipment)
  2. UTRAN (UMTS terrestrial radio access network) OR Radio Network Subsystem (RNS)
  3. Core Network



SGSN :- Serving GPRS support node

GGSN :- Gateway GPRS support node.

USER Equipment (UE)

- The User Equipment or UE is the name given to what was previous termed the mobile, or cell phone.
- It is assigned to the single user. It comprises of all the functions which are needed to access the UMTS network.
- The SIM present here, performs the functions like encryption & authentication of users. It stores all the user related data for UMTS network.
- Generally SIM belongs to the service provider. It consists of microprocessor. It enhanced program execution environment.
- The user equipment has all the functions needed for radio transmissions as well as user interfaces.

Radio Access Network Subsystem (RNS)

- It is also known as the UMTS Radio Access network, UTRAN is equivalent of the previous Base station Subsystem or BSS in GSM.
- It provides & manages the air interface for the overall network.

- It consists of Node B & RNC ie. Radio network controller.

- **Node B:-** Radio cell is controlled by Node B. It means it controls the antennas which are located in the cell sites.
- UE connected to one or more antennas.
- Node B also takes care of the handover required.

- **RNC (Radio network controller):-**
  - RNC is connected to the CN (core network) with the air interface Iu. It is connected to the node B via air interface Iub.
  - Two RNCs are interconnected with radio interface Iur.
  - Tasks performed by RNC
    <1> Call admission control
    <2> Congestion control
    <3> Encryption & decryption
    <4> Multiplexing of signals & protocol conversion.
    <5> Radio Resource management
    <6> Radio bearer setup & release.
    <7> Code allocation.
    <8> Power control
    <9> Handover control & RNS relocation
    <10> Management.

(CN) Core Network :-

- It consists of two ports:
  (1) CSD (Circuit switched Domain)
  (2) PSD (Packet switched Domain)
- The core network provides all the central processing & management for the system.
- It is equivalent of the GSM network switching subsystem or NSS.

CSD :- Circuit switched Domain

- It has same blocks like GSM i.e. MSC, HLR, VLR etc. & have same functions also.
- CSD is connected to RNS via Iu interface & it is known as IuCS.

PSD (Packet switched Domain)

- It consist of SGNS ie. Serving GPRS support node & GGSN ie gateway GPRS support node are present)
- GPRS (General packet Radio service)
- SGNS & GGSN are connected to RNS via Iu interface & it is known as IuPS.
- It performs same functions as MSC.
- These are capable of handling Packetized data.

The UMTS interfaces

(i) U_u :- It is the interface between the network & the user equipment.

(ii) IuCS :- It represents a circuit switched connection for carrying control signaling & voice traffic between the core network & UTRAN.

(iii) IuPS :- It represents a packet switched connection for carrying signaling & voice traffic between the core voice network & UTRAN.

(iv) Iub :- This interface is used for controlling many Node-B.

(v) Iur :- This interface is used for supporting mobility of MSCs. When subscriber moves Iur transfers subscriber data to new RNC as UE moves.