Mobile computing (unit II)

1. Enlist characteristics of SIM
*** 2. With the help of a neat sketch, describe GSM network architecture
3. Explain in detail the Frequency allocation in GSM.
*** 4. Write short notes on: UMTS
5. What you meant by security in GSM? Explain about that in detail.
*** 6. With the help of neat sketch, describe GPRS architecture.
7. Give the protocol architecture of signaling in GSM.
* 8. What is the relationship between the Base station & Mobile Switching Centre? Discuss the role of EIR entity of GSM network.
* 9. Network and switching sub-system of GSM architecture.
* 10. Authentication and privacy in GSM.

1. Characteristics of SIM -

1) Subscriber Identity - Stores the unique IMSI (International mobile Subscriber Identity) which helps identify the subscriber in the mobile network.

2) Authentication - Provides security by authenticating the user to the networks before allowing access to services.

3) Portability - SIM can be removed from one device & inserted into another, allowing the user to retain the same mobile number & services.

4) Data Storage - stores essential information such as SMS, Contacts, operators settings, and small application data.

5) Network Access - Enables connection to GSM / CDMA / LTE networks.

6) Roaming Support - Helps access services when moving b/w networks, even in different countries.

7) International Standardization - SIM cards follow global standards (ETSI, 3GPP) so they work universally across compatible devices.

2. GSM

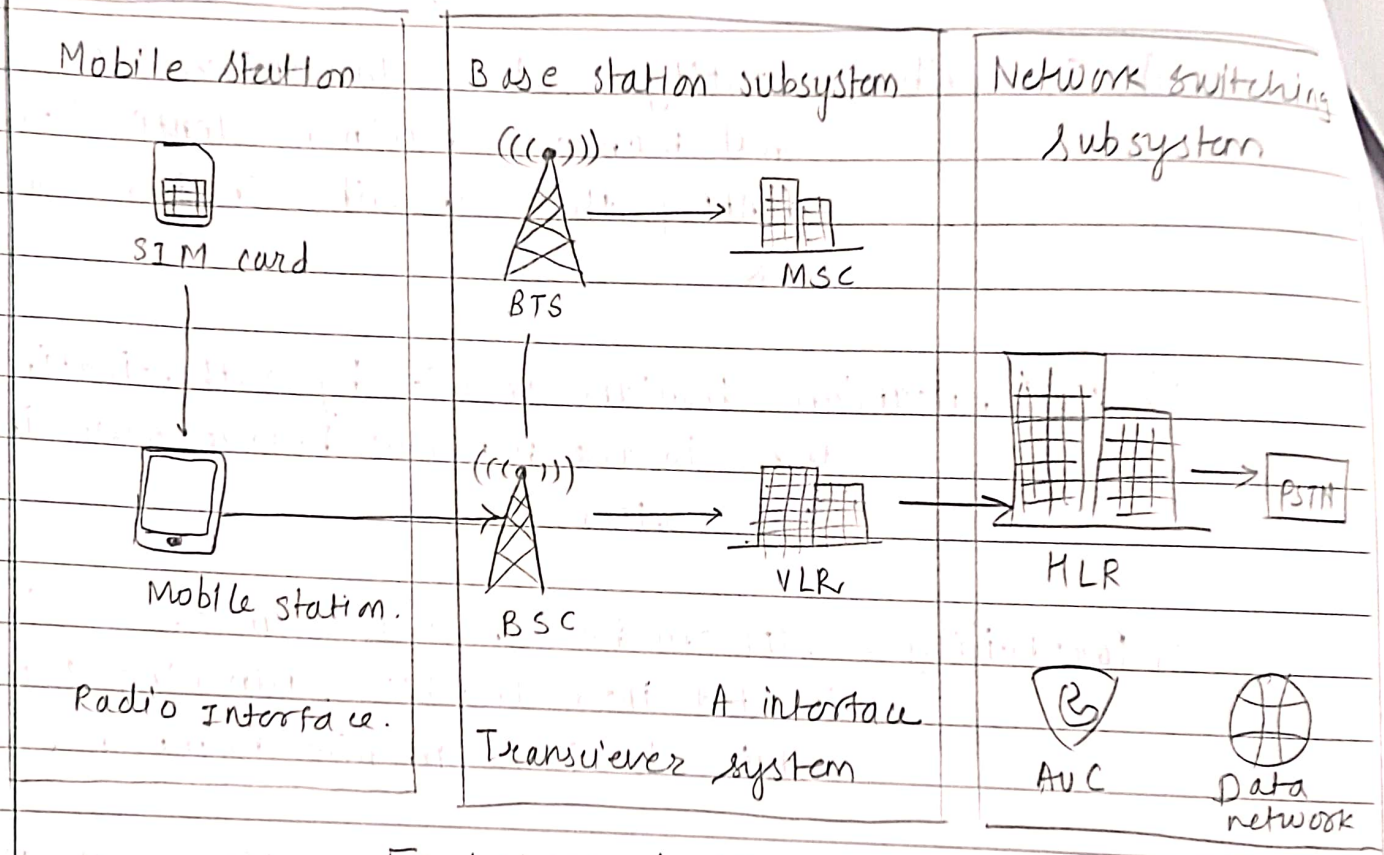


Fig: GSM Architecture.

GSM (Global system for Mobile Communication) is the second-generation (2G) digital mobile communication standard developed to replace analog cellular networks.

GSM system is divided into three main components.

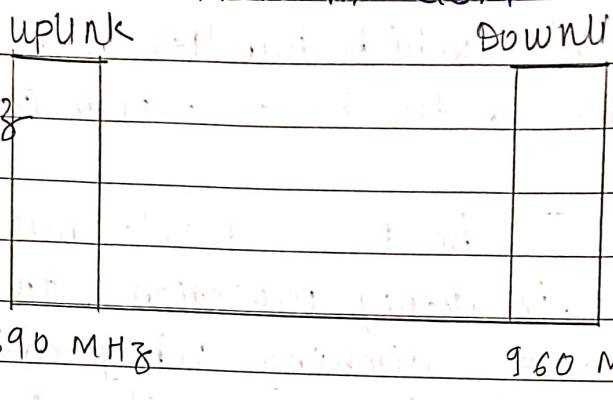
1) Mobile Station (MS)
   - The Mobile Station consists of the mobile equipment and the SIM card, which stores subscriber Identity and authentication keys.

- 2) Base station subsystem (BSS)
  - The BSS includes the Base Transciever Station (BTS), which handles radio communication with mobiles, & the base station controller (BSC).
  - The BSC controls multiple BTSs & manages call handover, frequency allocation, and power control.
- 3) NSS (Network switching subsystem) -
  - The NSS forms the core of GSM & contains
1) MSC (Mobile Switching Center) - Call routing & mobility management.
2) HLR (Home Location Register) - for permanent subscriber data
3) VLR (Visitor Location Register) - for temporary roaming data
4) AUC (Authentication Center) - For security and encryption.

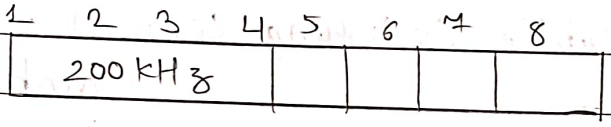
Working -

When a user makes call, the MS connects to the nearest (BTS). the BTS forwards the signal to BSC, which manages handovers & controls multiple BTSs. From there, call is sent to MSC which checks subscriber info. into HLR / VLR & verifies security using AUC. Finally, the MSC routes the call to another user or external N/w like PSTN/ ISDN.

3. Frequency allocation in GSM.



Channel structure



AU Time slots.

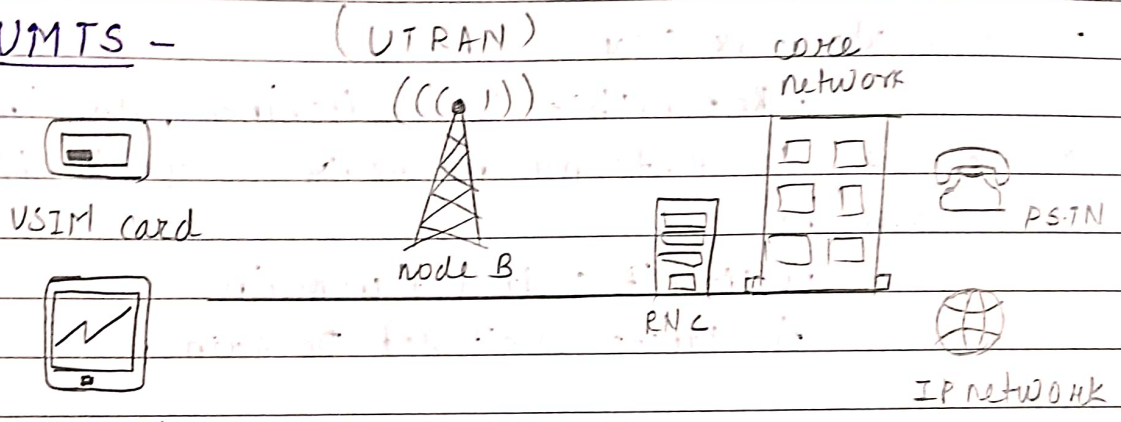
1) Frequency Bands - GSM uses two frequency bands :
   i) Uplink (MS → BTS) : 890 - 915 MHz
   ii) Downlink (BTS - MS) : 935 - 960 MHz.
   There's a 25 MHz gap b/w uplink & downlink for duplex communication.

2) Channel Allocation - The total band (25 MHz) is divided into 124 carrier frequencies, each of 200 kHz bandwidth.
   - Each carrier frequency acts as a separate channel.

3) Time Division - Each carrier frequency is further divided into 8 slots.
   - Thus, one frequency channel can support 8 simultaneous users.

4) Working Principle - When a call is made, the mobile is assigned a specific frequency channel + time slot.
- This ensures efficient spectrum usage & avoids interference.

4. UMTS -



UMTS (Universal Mobile Telecommunication system) is a 3G Technology using W-CDMA that provides faster data, better voice, and multimedia services. Its architecture has UE, UTRAN (Node B + RNC), and core Network, enabling video calls, internet, & global connectivity.

1. User Equipment (UE)
- This is the mobile handset + Universal SIM card.
- UE communicates with the network through radio signals.
- USIM stores subscriber identity, authentication keys, & provides security.

2. UTRAN (UMTS Terrestrial Radio Access Network)
   - It is the radio access part of UMTS.
   - Two main elements :
     1) Node B (Base station)
     2) RNC (Radio Network controller)

3. Core Network (CN)
   - Responsible for switching, routing, and connectivity to external networks. It is divided into two domains
     1) Circuit switched Domain
     2) Packet switched Domain.

5. Security in GSM -

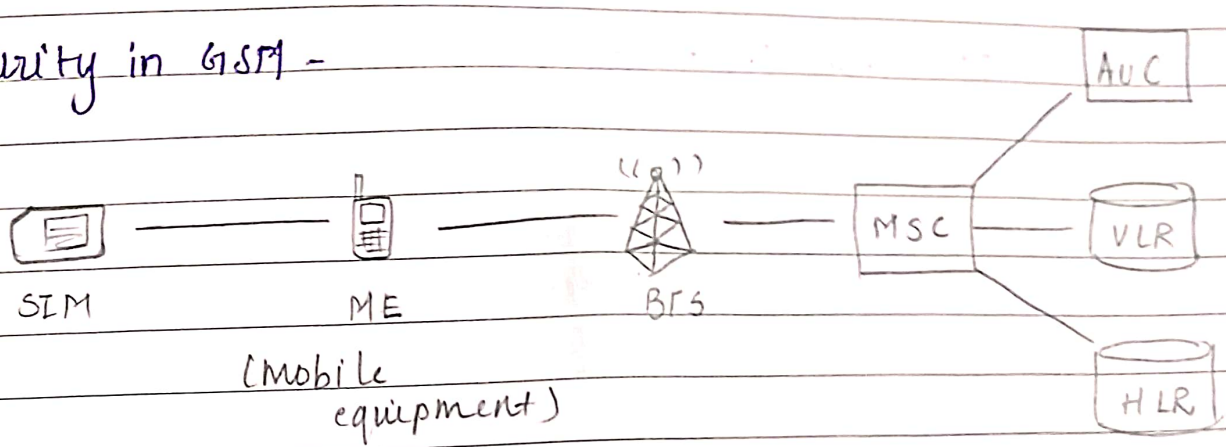


Fig: Security Framework in GSM.

Security in GSM refers to the set of techniques used to protect subscriber identity, authenticate users and ensure confidentiality of data during transmission. GSM ~~IF~~ provides three major security services.

1. Authentication - GSM verifies whether the user is genuine or not. The SIM card stores a secret key (K) & uses algorithm A3 to generate a response.

2. Confidentiality (Encryption) - To protect data and voice communication, GSM uses the A5 encryption algorithm.

3. Anonymity - Instead of sending the permanent IMSI (International Mobile Subscriber Identity) every time, GSM uses TMSI: This prevents tracking of users.

(General packet radio service)

6. GPRS Architecture

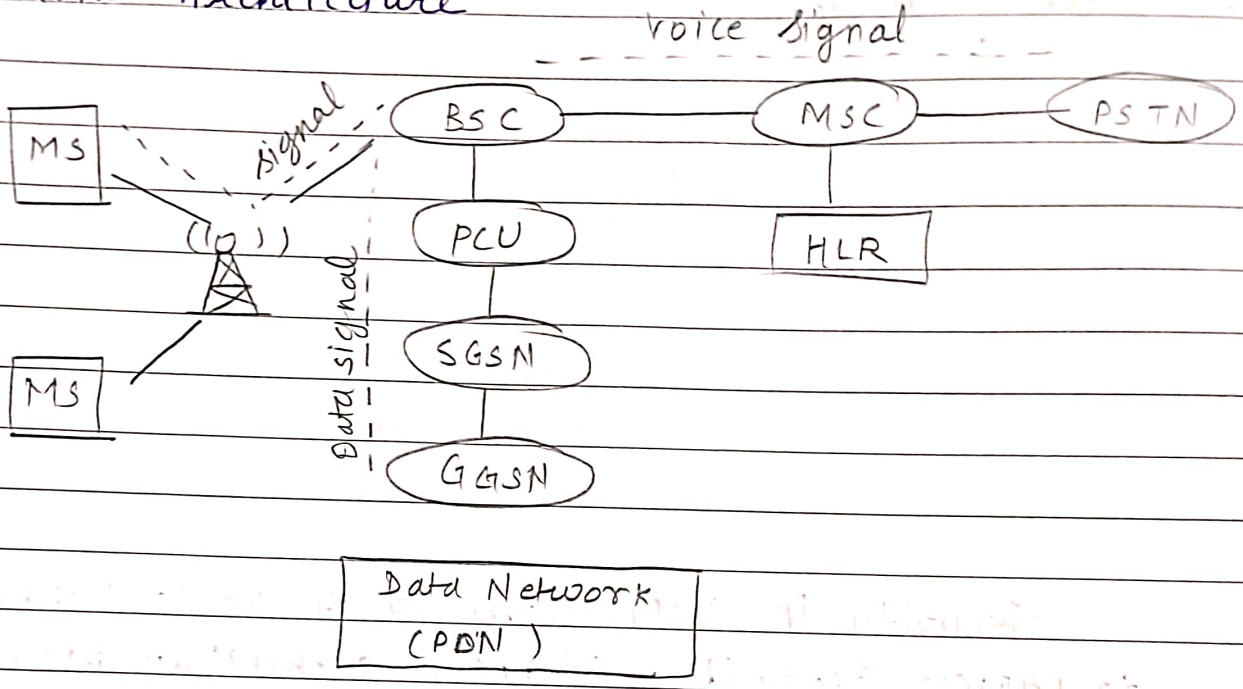


Fig: GPRS Architecture

GPRS is the modified version of GSM architecture. GPRS is a packet oriented mobile data mechanism, that can carry data packets as well.

Components of GPRS Architecture -

1. Mobile ~~Computing~~ station (MS) -
Special mobiles that can handle both GSM voice calls and GPRS data services.

2. Base station Controller (BSC) with PCU:
In GPRS, a Packet control Unit (PCU) is added to BSC. It detects data traffic

and forwards it to SGSN instead of GSM switching path.

3. GPRS support nodes -

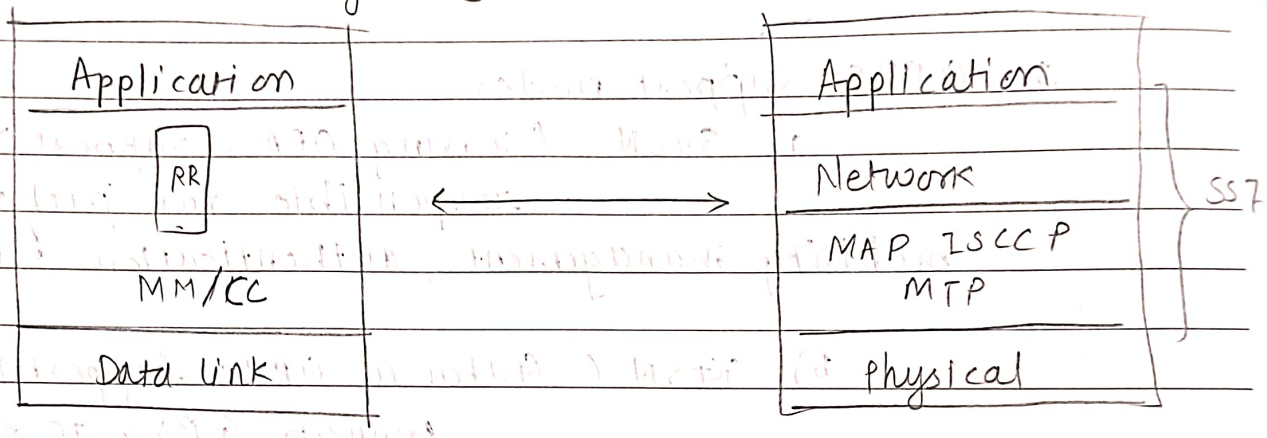
a) SGSN (serving GPRS Support Node) - responsible for packet delivery, mobility management, authentication & billing.

b) GGSN (Gateway GPRS Support Node) - connects GPRS to external packet data networks & stores user profile.

4.
The development enables mobile devices to manage both voice & data, allowing for a variety of apps and services that are essential to modern mobile communication.

7. Protocol architecture of signaling in GSM -

Air - interface signaling | Network side signaling



RR : Radio Resource
MM : Mobility management
CC : Call control

Air Interface signalling -

This is the radio part of signalling, happening over the Um interface (air)

- Physical layer - Responsible for transmitting raw bits over radio waves.

- Data link layer (LAPDm) : Ensures error-free transmission of signaling msg between MS and BTS.

- Signaling -

a) RR : Channel allocation, power control, handovers.

b) MM : Authentication, location update, roaming, TMSI assignment, security.

c) CC : Call setup, management, & release.

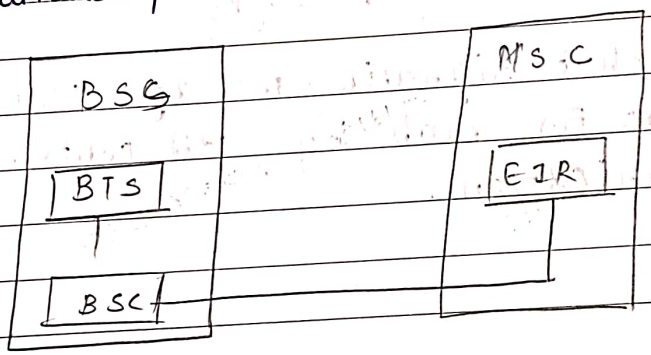
Network Side signaling (B/w BSC ⟷ MSC ⟷ Other networks)

- This is the core network signaling carried using SS7 protocols.
- This ensures that signaling messages flow properly in the network for mobility, call control, & inter network communication.

8.

The Base station subsystem and Mobile Switching Center (MSC) are independent -

The BSS handles radio resources and passes both signaling and user traffic to the MSC, while the MSC performs call switching, mobility management, and connects the GSM network to external networks. Their relationship is essential for call setup, handover & roaming



IMEI - International Mobile Equipment Identity

The Equipment Identity Register (EIR) is a database that stores the IMEI numbers of mobile devices. It classifies devices into white (allowed), black (blocked) & grey (under observation) lists to allow, block or monitor them. By checking IMEIs, EIR prevents the uses of stolen or unauthorized mobile devices and adds a strong layer of security & fraud control to the GSM network.

9. Network & Switching Subsystem.

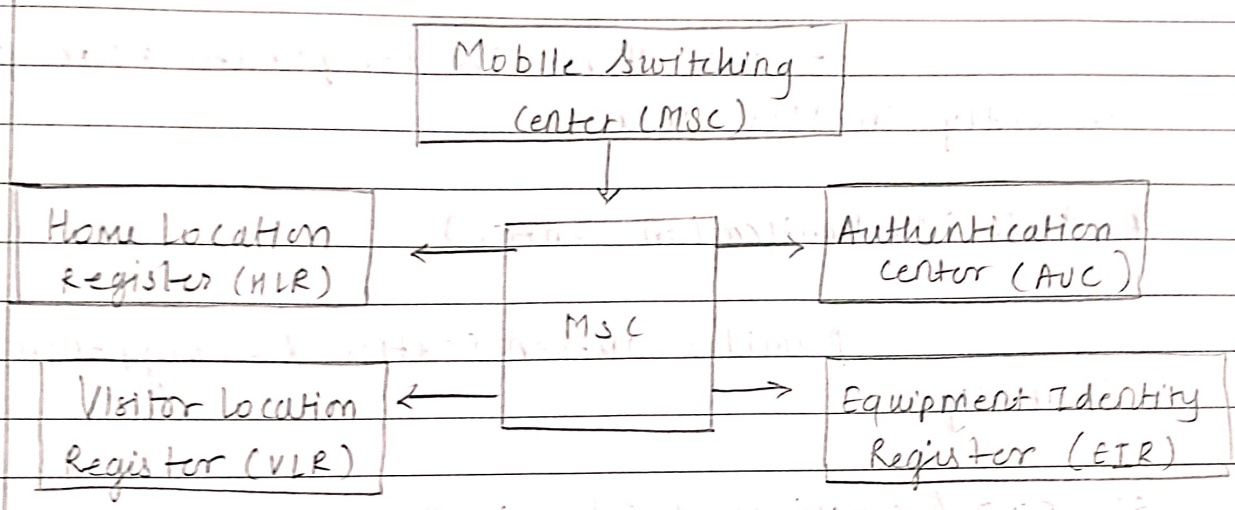


Fig: Network & Switching subsystem (NSS)

The Network and switching subsystem (NSS) manages call control, subscriber data, mobility, security, and connection to external networks.

Main components of NSS are -

1) MSC (Mobile switching center):

- MSC is the heart of MSC, which handles call setup, routing & handover.

2) HLR (Home Location Register):

- HLR stores the permanent subscriber info (IMSI, services, location)

3. VLR (Visitor Location Register)

- VLR stores the temporary data of us currently in MSC area.

4. AUC (Authentication Center)

- Provides authentication & encryption for security.

5. EIR (Equipment Identity Register)

- Stores IMEI lists (white, black, grey) to track valid stolen devices.

* Functions of NSS:

1) Call setup & routing
2) Mobility & roaming management
3) Authentication & security
4) Billing & interconnection with other networks.