GSM (System Architecture, Localization and Calling, Handover, Security)

- GSM (Global System for Mobile Communications) is a widely-used mobile communication system that uses a combination of time division multiple access (TDMA) and frequency division multiple access (FDMA) techniques to provide voice and data services to mobile users.
- Primary goal of GSM was to provide a mobile phone system that allows users to roam around their continents.
- GSM has defined three different categories of services:
  1. **Bearer services**
     - interface to the physical medium
     - permit transparent and non-transparent, synchronous or asynchronous data transmission
     - only use function of the physical layer to transmit data
     - Non-transparent bearer services use protocols of layers two and three to implement error correction and flow control.
  2. **Telematic services**
     - service provided by the system to the end user
     - focuses on voice-oriented tele services
     - primary goal of GSM was the provision of high-quality digital voice transmission
     - same number can be used throughout this service is mandatory for all providers
     - useful for simple message transfer
     - transmission of messages of up to 160 characters
     - Enhanced message service(EMS) offers a large message size
     - Multimedia Message Service (MMS) offers the transmission of large picture, short video clips
  3. **Supplementary services**
     - associated with the tele service call forwarding, redirection
     - similar to ISDN network
     - these services offer various enhancement for the standard telephone service and may vary from provider to provider
- GSM standard operates on three different frequency:
  1. 900 MHz
  2. 1800 MHz
  3. 1900 MHz
- **System Architecture:** GSM architecture consists of several network elements, including mobile stations (MS), base transceiver stations (BTS), base station controllers (BSC), mobile switching centers (MSC), and the home location register (HLR) and visitor location register (VLR).

- **Localization and Calling:** GSM uses a combination of cell-based and location-based techniques to determine the location of a mobile device. This information is used to route calls and messages to the correct destination.
- **Handover:** Handover refers to the process of transferring a call or data session from one cell to another as a mobile device moves around. GSM uses a variety of handover techniques, including hard handover and soft handover, to ensure that calls and data sessions are maintained as a mobile device moves between cells. "hard handover" refers to a process where a call or data connection is transferred from one cell to another without any overlap between the two cells. This results in a temporary interruption of the call or connection during the handover. A "soft handover" refers to a process where a call or data connection is transferred from one cell to another with overlap between the two cells. This allows for a smooth transition between cells with no interruption in the call or connection.
- **Security:** GSM provides several security features to protect both voice and data communications. These include encryption of voice and data, authentication of the user and the network, and the use of secure SIM cards. Additionally, GSM includes a security feature called A5/1, A5/2 and A5/3 encryption algorithm to secure the signaling and voice traffic.
- It's worth noting that GSM has been phased out by most of the operators and replaced by newer technologies like 3G, 4G and 5G, However, GSM still used in some countries and areas.

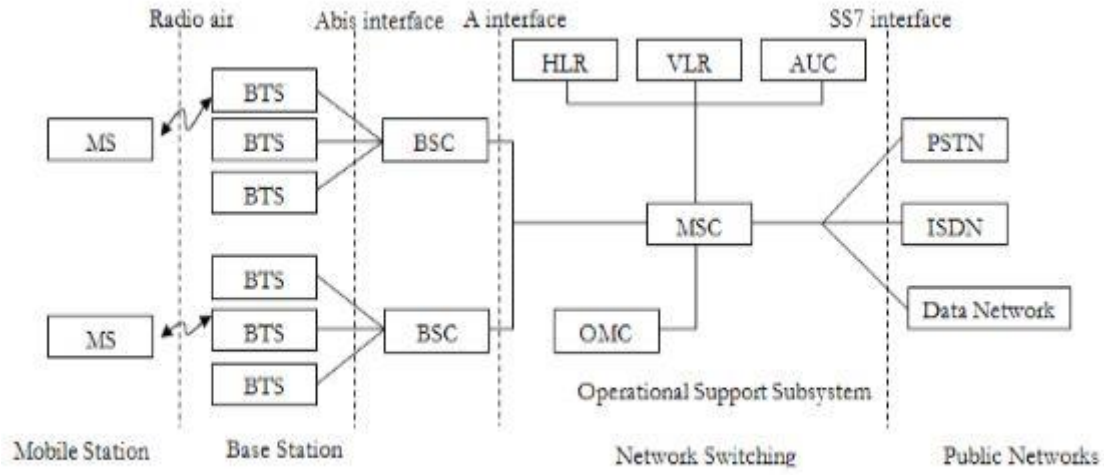


Fig: GSM Architecture

1. **MS (Mobile Station):** This is the physical device, such as a mobile phone, that the user carries and uses to communicate on the GSM network. MS need for communication with a GSM network. MS identify via the International mobile equipment identify (IMEI). Authentication are based on the SIM not on the device itself. Without SIM only emergency calls are possible.

2. **BTS (Base Transceiver Station):** The BTS is the main component of the GSM network that communicates directly with the MS. It is responsible for transmitting and receiving signals between the mobile phone and the network.
3. **BSC (Base Station Controller):** The BSC is the component of the GSM network that controls and manages the BTS. It is responsible for allocating radio resources, managing handovers, and controlling the power levels of the BTS.
4. **MSC (Mobile Switching Center):** The MSC is the heart of the GSM network. It is responsible for managing the call processing and signaling between the mobile phone and the network, as well as routing calls to the appropriate destination. MSC manages several BSC in a geographical region.
5. **OMC (Operation and Maintenance Center):** The OMC is responsible for managing and maintaining the GSM network. It is responsible for monitoring the network, troubleshooting problems, and performing software upgrades. OMS monitor and control's all other network entities via the O interface.
6. **HLR (Home Location Register):** The HLR is a database that stores all the subscriber information for the GSM network. It is responsible for managing the subscriber's profile and location information. HLR is the most important database in a GSM. As soon as an MS leaves its current location area the information in the HLR is updated.
7. **VLR (Visitor Location Register):** The VLR is a database that stores the subscriber information for the GSM network. It is responsible for managing the subscriber's profile and location information. Stores all important information needed for the MS currently in the location area that is associated to the MSC
8. **AUC (Authentication Center):** The AUC is responsible for authenticating the subscriber's SIM card and providing a unique encryption key to the mobile phone. A separate AUC has been defined to protect user identity and data transmission. Contain the algorithm for authentication
9. **EIR (Equipment Identity Register):** EIR is a database for all IMEI it stores all device identification registered for this network. EIR has a blacklist of stolen devices. The EIR also contains a list of valid IMEI.
10. **PSTN (Public Switched Telephone Network):** The PSTN is the traditional telephone network that connects the GSM network to the rest of the world.
11. **ISDN (Integrated Services Digital Network):** ISDN is a digital communications network that provides high-speed data transfer and other advanced services. It is often used to connect the GSM network to other networks and services.

GSM Advantage

- Provide word wide roaming for its clients to roam throughout the world.
- Extremely secured
- Expensive coverage in all over the world
- Clear voice calls
- Compatible with wide range of handsets and accessories
- Compatible with ISDN and other telephone company services

GSM Disadvantage

- Multiple users share the same bandwidth cause limitation occur
- May caused electronic interference therefore sensitive locations like hospital and airplane require cell phone to be turned off

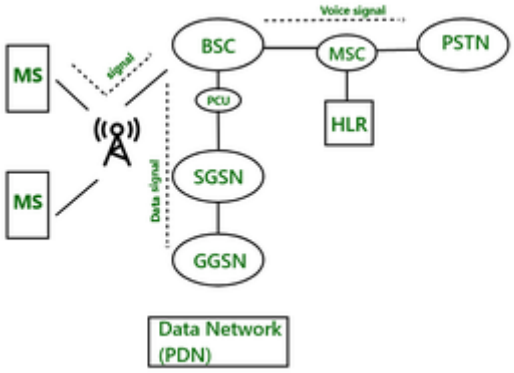
GPRS Architecture

- GSM network can be broadly divided into
  1. Radio Subsystem (RSS) : comprises MS and BSS
  2. Network Switching Subsystem (NSS)
  3. Operation Support Subsystem (OSS)
- Heart of the GSM system is formed by the network and switching subsystem(NSS).
- NSS connects the wireless network with standard public network performs handover's between BSS
- OSS(Operation subsystem) is the third part of a GSM system contain the necessary function for network operation and maintenance
- GPRS (General Packet Radio Service) is a 2G mobile communication technology that allows data to be transmitted over a cellular network. It is considered a 2.5G technology as it provides faster data transfer rates compared to traditional circuit-switched 2G networks (such as GSM). The GPRS architecture consists of several key components:

1. **Mobile Station (MS):** The mobile device, such as a phone or tablet, that is used by the end-user to access the network.
2. **Serving GPRS Support Node (SGSN):** The SGSN is responsible for managing the connection between the mobile station and the network. It keeps track of the location of the mobile station and authenticates the user.
3. **Gateway GPRS Support Node (GGSN):** The GGSN acts as a gateway between the GPRS network and other networks, such as the Internet. It is responsible for routing data packets between the mobile station and the appropriate external network.
4. **Base Station Subsystem (BSS):** The BSS is the part of the network that connects the mobile station to the SGSN. It includes the base transceiver stations (BTS) and the base station controller (BSC). BSS contains several BTS
5. **Packet Data Network (PDN):** The PDN is the data network that is used to transmit packets of data between the mobile station and other networks. It can be a public or private network and can be connected to the Internet or other data networks.
   In summary, GPRS architecture is designed to enable faster data transfer over 2G networks, connecting mobile stations to the Internet and other data networks through the SGSN, GGSN and BSS.

GPRS architecture in wireless communication

- General Packet Radio Service (GPRS) is a enhancement or the modified version of GSM architecture service.
- data is transmitted in packets
- GSM architecture we can only transport the voice signal.
- But if signal consists of the data then only GSM architecture cannot use
- For that there are two more software components are used SGSN(Service GPRS supporting Node) and GGSN(Gateway GPRS supporting Node)
- architecture consists of the following components:
    1. **Mobile Station (MS):** Required new MS such as smartphone or tablet because existing GSM phones are not capable of handling the enhanced air interface or the packet data.
    2. **Base Station Subsystem (BSS):** Each BSC requires the installation of Packet Control Units(PUC). The BSS consists of two components: Base Transceiver Station (BTS) and Base Station Controller (BSC).
    3. **Serving GPRS Support Node (SGSN):** It's responsible for authentication of GPRS mobiles, registration of mobile in the network. It also handles location management, security, and authentication.
    4. **Gateway GPRS Support Node (GGSN):** responsible for connecting the GPRS network to external packet-switched networks, such as the internet
    5. **Home Location Register (HLR):** database that stores user information, such as phone numbers, authentication keys, and service subscription information.
    6. **Authentication Center (AUC):** responsible for authenticating users on the network by verifying their SIM card information and generating authentication keys.
    7. **Equipment Identity Register (EIR):** database that stores information about mobile devices, such as their unique identifiers (IMEI)



Localization and calling

- Fundamental features of the GSM system is the automatic worldwide localization of user's.
- Always knows where a user currently
- Same phone number is valid worldwide
- Perform periodic location updates even if a user does not use the mobile station

- HLR always contains information about the current location.
- VLR currently responsible for the MS informs the HLR about location change's
- As soon as an MS moves into the range of a new VLR the HLR sends all user's data needed to the new VLR.

Roaming

- Changing VLR with continuing without a break availability of all services is also called roaming.
- Roaming can take place within the network of one provider between two providers in one country but also between different providers in different countries

Handover

- Single cells do not cover the whole service area
- Smaller the cell size and the faster the movement of a mobile station through the cells the more handovers of ongoing calls are required
- Handover refers to the process of transferring an ongoing call or data session from one cell to another without interrupting the communication.
- The purpose of handover is to ensure that the user continues to receive a high-quality service while moving within the coverage area.
- Two basic reasons for a handovers
    1. MS moves out of the range of a BTS or a certain antenna of a BTS respectively. The received signals levels decreases continuously until it falls below the minimal requirements for communication
    2. Wired infrastructure (MSC, BSC) may decide that the traffic in one cell is too high and shift some MS to other cells with a lower load(if possible). Handover may due to load balancing.
- **Handover scenario**
    1. **Intra-cell handover**: Within a cell
    2. **Inter-cell, intra-BSC handover**: mobile station moves from one cell to another, but stays within the control of the same BSC. Assign a new radio channel in the new cell and release the old one
    3. **Inter-BSC, intra-MSC handover:** BSC only controls a limited number of cells. GSM also has to perform handovers between cells controlled by different BSC. This handover then has to be controlled by the MSC
    4. **Inter MSC handover:** required between two cells belonging to different MSC. Both MSC perform the handover together

DECT – System Architecture

- Local communication structure that is connected to the outside world through a global network and the services.
- Public Switched Telephone Network (PSTN), Public Land Mobile Network (PLMN), Integrated Services Digital Network (ISDN) etc are the global networks.
- Local network of DECT can provide local telecommunication services such as simple switching to any call forwarding.
- Containing databases such as home database(HDB) and visitor database (VDB).
- Database operation here are similar to that of GSM system.
- Fixed Radio Terminal (FT) and Portable Radio Terminal (PT) which are responsible for multiplexing of the signals to take place whenever necessary.
- Fixed radio terminal is placed at the fixed network side while the portable radio terminal exists at the mobile network side of the network.
- DECT (Digital Enhanced Cordless Telecommunications) is a digital wireless telephone standard that is primarily used in Europe and other parts of the world. The DECT system architecture includes several components:
    1. **Base station:** This is the primary component of the DECT system and serves as the connection point between the cordless phones and the telephone network.
    2. **Cordless handset:** This is the portable device that allows users to make and receive calls wirelessly.
    3. **DECT Access Point:** This is the interface between the DECT system and the telephone network.
    4. **DECT Controller:** This is the device that controls the communication between the base station and the cordless handset.
    5. **DECT Radio Unit:** This is the radio transceiver that enables the wireless communication between the base station and the cordless handset.

In summary, DECT is a digital wireless standard for cordless telephone communications that uses a base station, cordless handset, DECT access point, DECT controller and DECT radio unit to provide wireless communication between the telephone network and the cordless handset.

- The protocol architecture in DECT is divided into three main layers
    1. **Physical Layer :** responsible for the transmission and reception of radio signals over the air interface. comprises all functions for modulation/demodulation, sender/receiver synchronization and collection of status information for the management plane.
    2. **Medium Access Control :** responsible for controlling access to the wireless medium and managing the data link between the DECT devices. Establish, maintain and releases channels for higher layers by activating and deactivating physical channels.
    3. **Data Link Control :** creates and maintains reliable connections between the mobile terminal and the base station

Network Layer : similar to those in ISDN and GSM and only exists for the C-Plane. Mobility management(MM) responsible for identity management, authentication and the management of the location data bases.

Advantage of DECT

- Secure way of communication
- Less prone to disturbances
- Handover process is easy
- Multiple mobile stations can be connected within a network

Disadvantage of DECT

- Multi-Cell System: one of the negative aspects
- Less Coverage: short-range features it covers less area
- Eye on battery: user has to keep an eye on batteries

UMTS – System Architecture, Handover

- UMTS network architecture is divided into three main components:
  1. **User Equipment :** UE was a major element of the overall 3G UMTS network architecture. UE refers to the mobile device that connects to the UMTS network. It can be a smartphone, tablet, or any other device that supports UMTS.

     Type of UE:
     - **UE RF circuitry:** handle all element of the single, both for the receiver and for the transmitter. Major challenges was to reduce the power consumption
     - **Baseband processing:** considerably more complicated than that used in phones for previous generations
     - **Battery:** While current consumption has been minimized as far as possible within the circuitry of the phone.
     - **Universal Subscriber Identity Module, USIM:** also contained a SIM card, although in the case of UMTS it was termed a USIM (Universal Subscriber Identity Module)
  2. **Radio Network Subsystem :** also known as UMTS Radio Access Network includes the Node B base stations, which communicate with the UE over the air interface. The Node Bs are connected to the RNC (Radio Network Controller), which controls the radio resources and manages the handovers between Node Bs. handled the wireless communications elements of the network. collectively all the Radio Network Subsystem was known as the UTRAN or UMTS Radio Access Network.

3. **Core Network :** backbone of the UMTS network, and it provides various services such as call control, mobility management, and authentication. The CN consists of several components such as MSC (Mobile Switching Centre), SGSN (Serving GPRS Support Node), and GGSN (Gateway GPRS Support Node). Different ways in which data could be carried, the UMTS core network was split into two different areas:
    - **Circuit switched elements:** Elements were primarily based on the GSM network entities and carry data in a circuit switched manner. included the following network entities:
        - **Mobile switching center (MSC):** essentially the same as that within GSM, and it managed the circuit switched calls under way
        - **Gateway MSC (GMSC):** effectively the interface to the external networks
    - **Packet switched elements:** network entities were designed to carry packet data. This enabled much higher network usage as the capacity could be shared and data was carried as packets which were routed according to their destination.
        - **Serving GPRS Support Node (SGSN):** SGSN provided a number of functions within the UMTS network architecture.
            - Mobility management
            - Session management: managed the data sessions providing the required quality of service
            - Interaction with other areas of the network: able to manage its elements within the network only by communicating with other areas of the network
            - Billing: monitoring the flow of user data across the GPRS network.
        - **Gateway GPRS Support Node (GGSN):** central element within the UMTS packet switched network. handled inter-working between the UMTS packet switched network and external packet switched networks, and could be considered as a very sophisticated router. received data addressed to a specific user, it checked if the user was active and then forwarded the data to the SGSN serving the particular UE

- UMTS (Universal Mobile Telecommunications System) is a third-generation (3G) mobile communication technology that provides high-speed data and voice services.
- Designed to provide high-speed data and voice services to mobile devices
- The UMTS architecture consists of three main components: the User Equipment (UE), the UMTS Terrestrial Radio Access Network (UTRAN), and the Core Network (CN).
- The UE is the device used by the end user, such as a mobile phone or a computer with a wireless modem.
- The UTRAN is the network that provides radio access to the UE, and is made up of the Node B (base station) and the Radio Network Controller (RNC).

- The CN is the network that connects the UTRAN to the rest of the world, and includes the Mobile Switching Center (MSC) and the Gateway GPRS Support Node (GGSN).
- Handover in mobile computing refers to the process of transferring a call or data connection from one cell to another as the mobile device moves around.
- In UMTS, handover is managed by the RNC, which monitors the signal strength and quality of the connection between the UE and the Node B. When the signal strength or quality drops below a certain threshold, the RNC initiates a handover to a new Node B with a stronger signal. This process is transparent to the end user and is designed to ensure a seamless and uninterrupted connection.

Shared elements

- **Home location register (HLR):** database contained all the administrative information about each subscriber along with their last known location. able to route calls to the relevant RNC / Node B. Even when the UE was not active (but switched on) it re-registered periodically to ensure that the network (HLR) was aware of its latest position with their current or last known location on the network
- **Equipment identity register (EIR):** decided whether a given UE equipment could be allowed onto the network. Each UE equipment had a number known as the International Mobile Equipment Identity
- **Authentication centre (AuC) :** protected database that contained the secret key also contained in the user's USIM card

UTRAN - System Architecture

- UTRAN (UMTS Terrestrial Radio Access Network) is the radio access network used in the 3G (third generation) UMTS (Universal Mobile Telecommunications System) mobile communication system.
- It is responsible for connecting mobile devices to the core network and providing radio coverage over a certain geographic area.
- The UTRAN system architecture consists of three main components: the Node B (base station), the Radio Network Controller (RNC), and the Mobile Switching Center (MSC).
- The Node B is the physical connection point between the mobile device and the UTRAN network. It is responsible for performing radio transmission and reception, and for providing the mobile device with access to the UTRAN network.
- The RNC is the network element that controls the Node Bs in a certain geographic area. It is responsible for managing the radio resources, such as frequency and power, and for performing radio link control and mobility management.
- The MSC is the network element that connects the UTRAN to the core network. It is responsible for managing the connection between the mobile device and the rest of the network, and for providing the mobile device with access to services such as voice and data.

  In summary, UTRAN is a 3G mobile communication system's radio access network, it connects mobile devices to the core network and provides radio coverage over a

certain geographic area. It is composed of Node B, RNC and MSC which are responsible for performing radio transmission and reception, managing radio resources, managing connection between mobile device and rest of the network and providing the mobile device access to services.