Mobile Computing

UNIT IV:

GSM: Global System for mobile communications – GSM Architecture – GSM Entities – Call routing in GSM – PLMN Interfaces – GSM Addresses and Identifiers – Network Aspects in GSM –Mobility Management-GSM Frequency allocations – Authentications and Security.

TEXT BOOK

“Mobile Computing”, Asoke K Talukder ,Roopa R Yavagal, TMH, 2005.

Prepared By: Dr. D. DEVAKUMARI

Global System for Mobile Communications

- Originally GSM stood for Groupe Speciale Mobile
- GSM to meet the following business objectives

1. Support for international roaming
2. Good speech quality
3. Ability to support handheld terminals
4. Low terminal and service cost
5. Spectral efficiency
6. Support for a range of new services and facilities
7. ISDN compatibility

Use of TDMA and FDMA in GSM

- Uses a combination of FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access)
- Allocation of 50 MHz (890–915 MHz and 935–960 MHz) bandwidth in the 900 MHz frequency band and using FDMA further divided into 124 (125 channels, 1 not used) channels each with a carrier bandwidth of 200 KHz
- Using TDMA, each of the above mentioned channels is then further divided into 8 time slots
- So, with the combination of FDMA and TDMA, a maximum of992 channels for transmit and receive can be realized

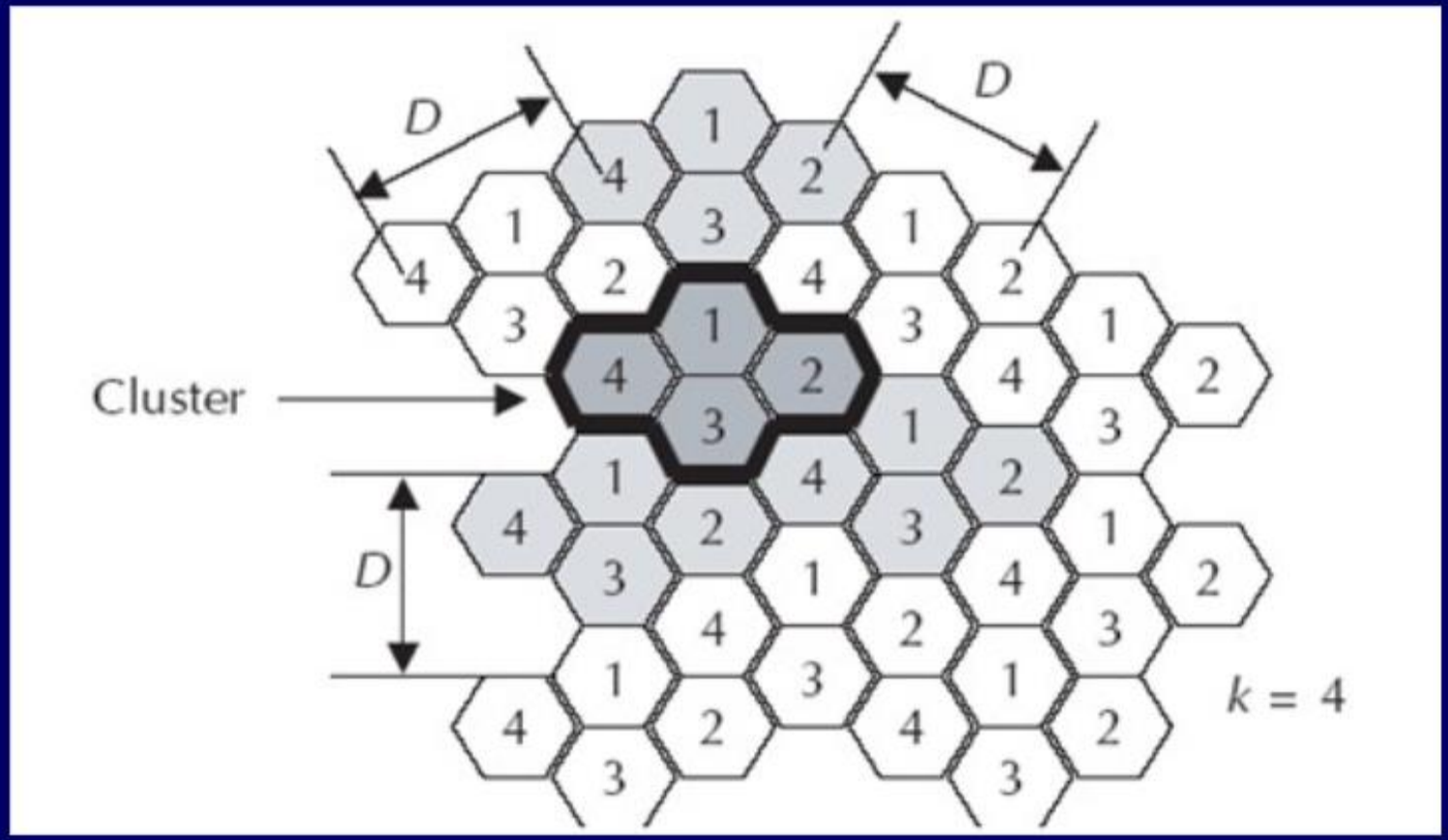
Frequency reuse in GSM

- To serve hundreds of thousands of users, the frequency must be reused and this is done through cells.
- The area to be covered is subdivided into radio zones or cells. Though in reality these cells could be of any shape, for convenient modeling purposes these are modeled as hexagons. Base stations are positioned at the center of these cells.
- Each cell *i* receives a subset of frequencies *fbi* from the total set assigned to the respective mobile network. To avoid any type of co-channel interference, two neighboring cells never use the same frequencies.

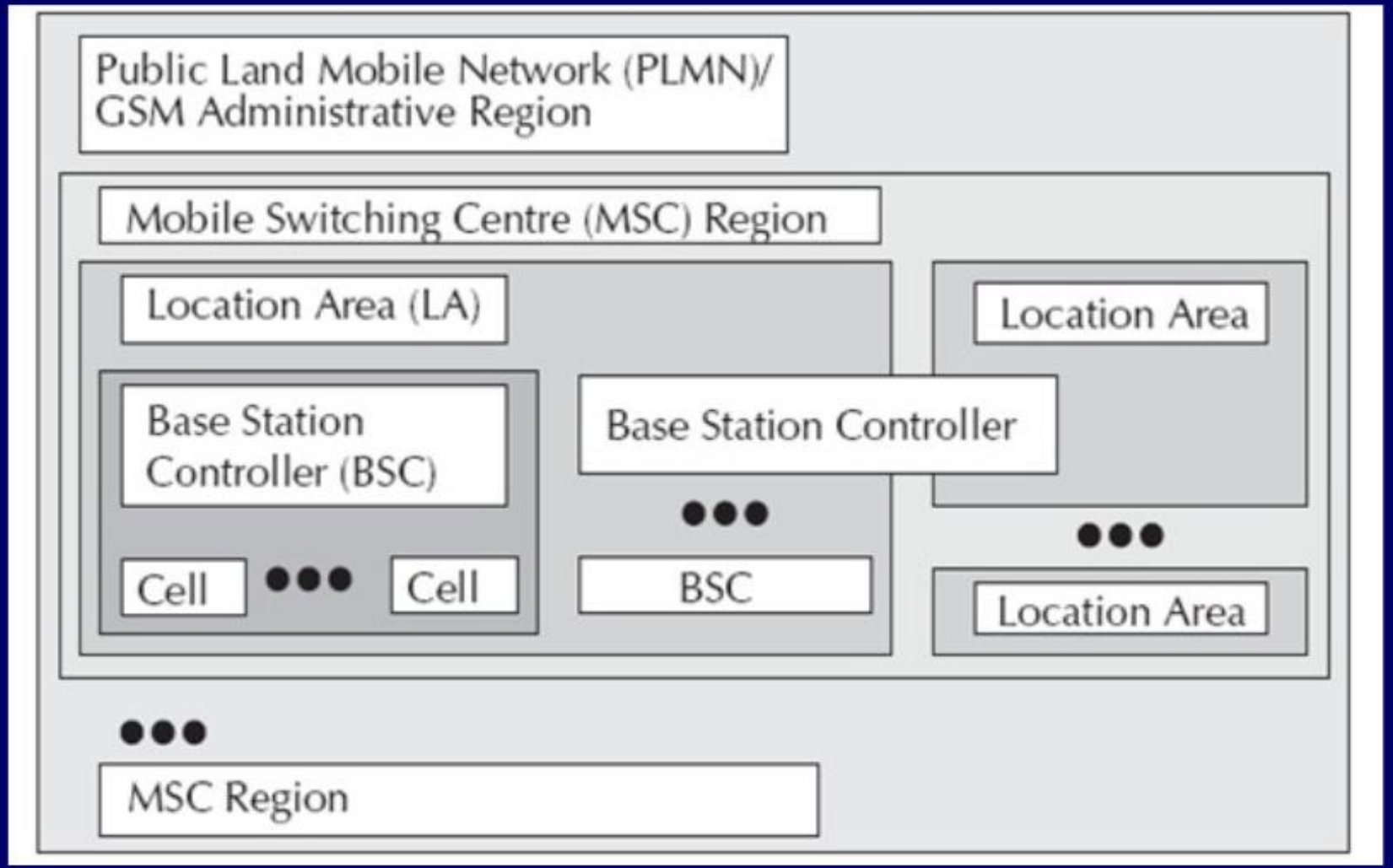
Frequency reuse in GSM

- Only at a distance of *D* (known as frequency reuse distance), the same frequency from the set *fbi* can be reused. Cells with distance *D* from cell *i*, can be assigned one or all the frequencies from the set *fbi* belonging to cell *i*.
- When moving from one cell to another during an ongoing conversation, an automatic channel change occurs. This phenomenon is called handover. Handover maintains an active speech and data connection over cell boundaries.
- The regular repetition of frequencies in cells result in a clustering of cells. The clusters generated in this way can consume the whole frequency band. The size of a cluster is defined by *k*, the number of cells in the cluster. This also defines the frequency reuse distance *D*.

Cell clusters in GSM



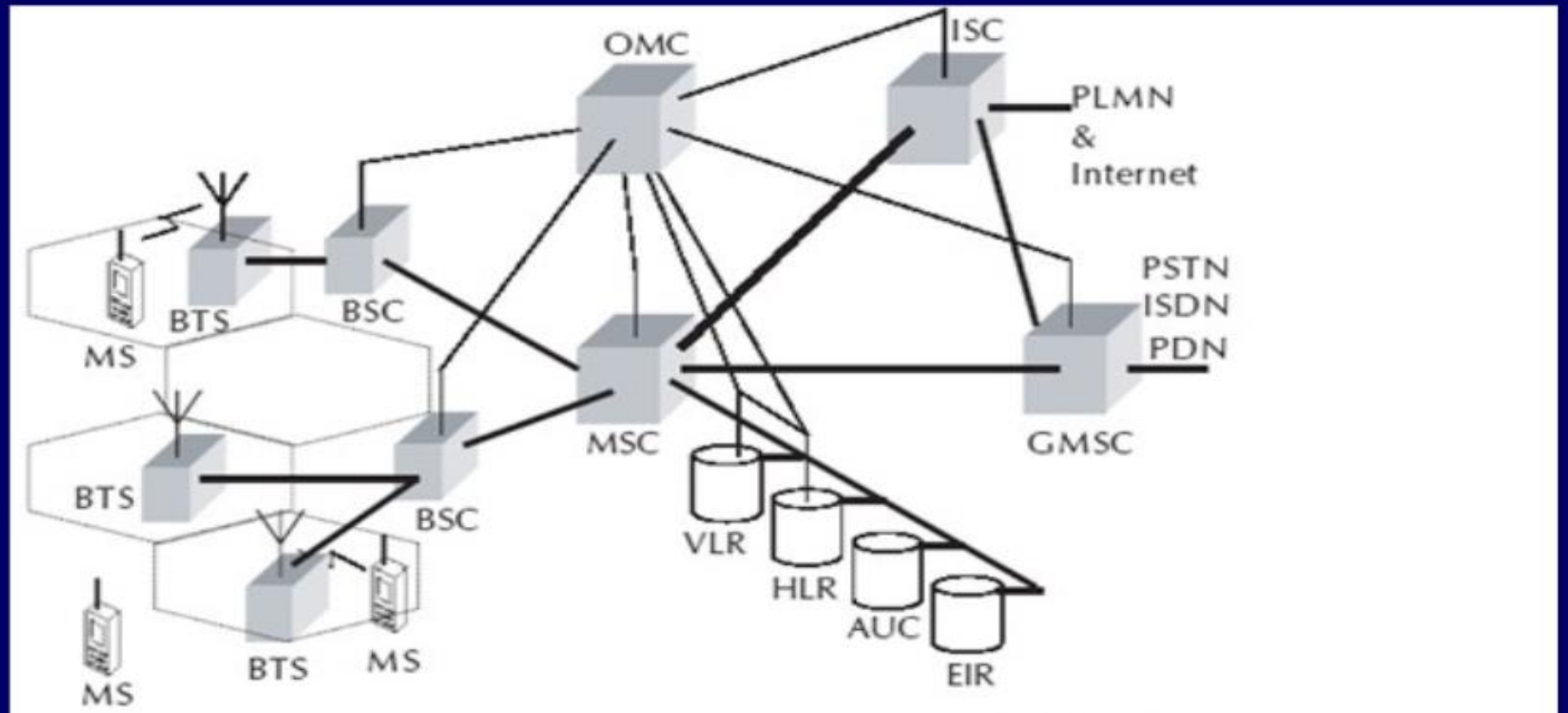
GSM System Hierarchy



GSM Architecture

- Consists at the minimum one administrative region assigned to one MSC (Mobile Switching Centre)
- Administrative region is commonly known as PLMN (Public Land Mobile Network)
- Each administrative region is subdivided into one or many Location Area (LA)
- One LA consists of many cell groups and each cell group is assigned to one BSC (Base Station Controller)
- For each LA, there will be at least one BSC while cells in one BSC can belong to different LAs

GSM Architecture



BTS	Base Transceiver Station
BSC	Base Station Controller
MSC	Mobile Switching Center
GMSC	Gateway MSC
ISC	International Switching Center

MS	Mobile Station
HLR	Home Location Register
VLR	Visitor Location Register
AUC	Authentication Center
EIR	Equipment Identity Register
OMC	Operation and Maintenance Center

GSM Architecture

- Cells are formed by the radio areas covered by a BTS (Base Transceiver Station)
- Several BTSs are controlled by one BSC
- Traffic from the MS (Mobile Station) is routed through MSC
- Calls originating from or terminating in a fixed network or other mobile networks is handled by the GMSC (Gateway MSC)

Entities in GSM

- The Mobile Station (MS) - This includes the Mobile Equipment (ME) and the Subscriber Identity Module (SIM).
- The Base Station Subsystem (BSS) - This includes the Base Transceiver Station (BTS) and the Base Station Controller (BSC).
- The Network and Switching Subsystem (NSS) - This includes Mobile Switching Center (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), and the Authentication Center (AUC).
- The Operation and Support Subsystem (OSS) - This includes the Operation and Maintenance Center (OMC).

Mobile Station

- Mobile Station (MS) consists of two main elements: mobile equipment or mobile device (that is the phone without the SIM card) and Subscriber Identity Module (SIM)
- Terminals distinguished principally by their power and application
- SIM is installed in every GSM phone and identifies the terminal
- SIM cards used in GSM phones are smart processor cards with a processor and a small memory
- SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other security

Base Station Subsystem

- Base Station Subsystem (BSS) connects the Mobile Station and the Network and Switching Subsystem (NSS)
- In charge of the transmission and reception for the last mile
- BSS can be divided into two parts: Base Transceiver Station (BTS) or Base Station and Base Station Controller (BSC)
- Base Transceiver Station corresponds to the transceivers and antennas used in each cell of the network
- BTS is usually placed in the center of a cell and its transmitting power defines the size of a cell

Base Station Subsystem

- BTS houses the radio transmitter and the receivers that define a cell and handles the radio-link protocols with the Mobile Station while handling between one and sixteen transceivers depending on the density of users in the cell
- Base Station Controller is the connection between the BTS and the Mobile service Switching Center (MSC) and manages the radio resources for one or more BTSs
- BSC handles handovers, radio-channel setup, control of radio frequency power levels of the BTSs, exchange function, and the frequency hopping

Network and Switching Subsystem

- Central component of the Network Subsystem is the Mobile Switching Center (MSC)
- Signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7)
- MSC together with Home Location Register (HLR) and Visitor Location Register (VLR) databases, provide the call-routing and roaming capabilities of GSM
- HLR contains all the administrative information of each subscriber registered in the corresponding GSM network
- Location of the mobile is typically in the form of the signaling address of the VLR associated with the mobile station
- HLR is always fixed and stored in the home network, whereas the VLR logically moves with the subscriber
- VLR is similar to a cache, whereas HLR is the persistent

Network and Switching Subsystem

- VLR contains selected administrative information borrowed from the HLR, necessary for call control and provisioning of the subscribed services
- When a subscriber enters the covering area of a new MSC, the VLR associated with this MSC can request information about the new subscriber from its corresponding HLR in the home network
- There is a component called Gateway MSC (GMSC) that is associated with the MSC
- GMSC is the interface between the mobile cellular network and the PSTN and also is in charge of routing calls from the fixed network towards a GSM user and vice versa
- GMSC is often implemented in the same node as the MSC
- GIWU (GSM Inter Working Unit) corresponds to an interface to various networks for data communications

Operation and Support Subsystem

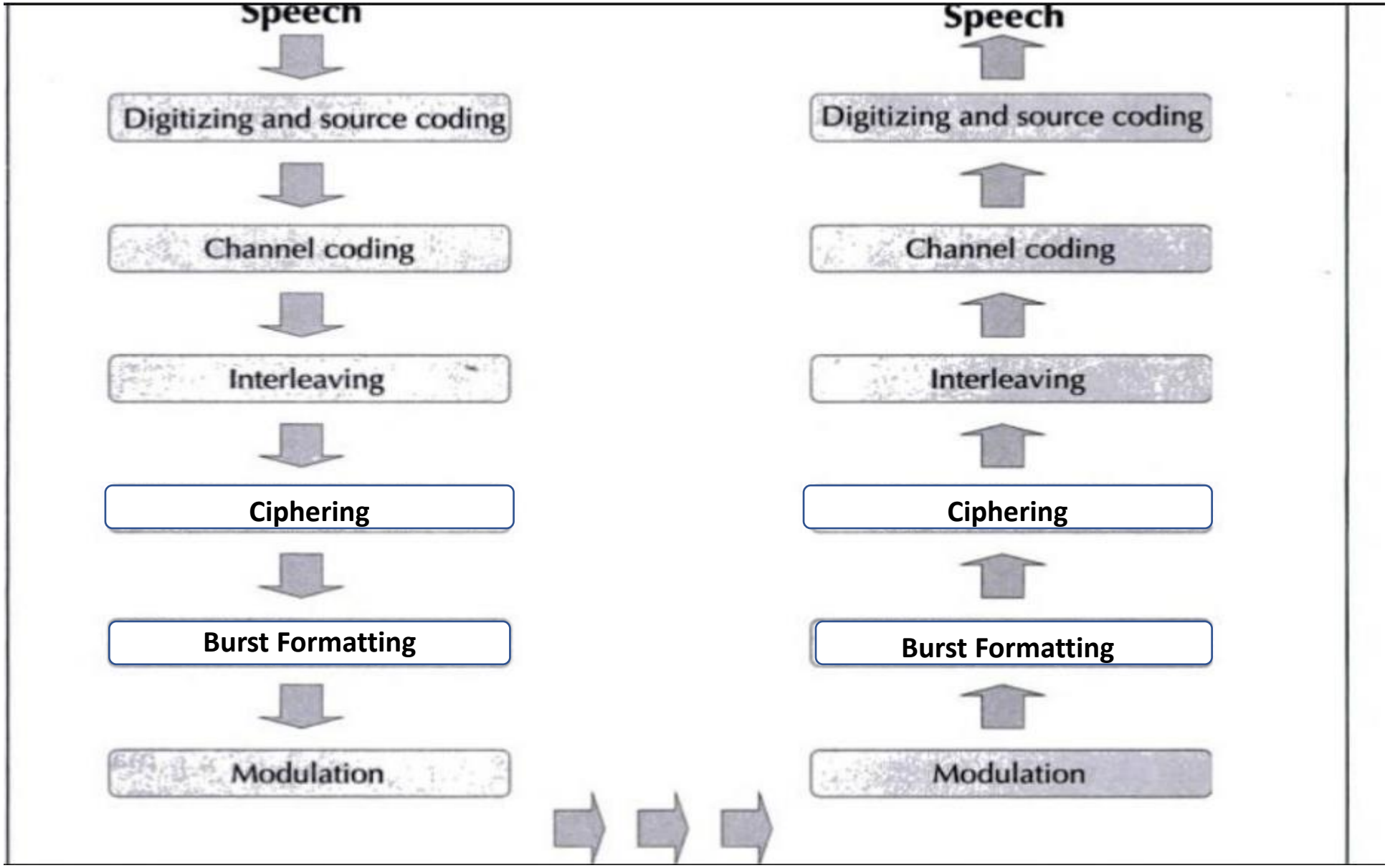
- Operations and Support Subsystem (OSS) controls and monitors the GSM system
- OSS is connected to the different components of the NSS and to the BSC and also in charge of controlling the traffic load of the BSS
- Equipment Identity Register (EIR) rests with OSS
- EIR is a database that contains a list of all valid mobile equipment within the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI)
- EIR contains a list of IMEIs of all valid terminals

- Authentication Center (AUC) is responsible for the authentication of a subscriber
- AUC is a protected database and stores a copy of the secret key stored in each subscriber's SIM card

Call Routing in GSM

1. Digitizer and Source Coding – The user speech is digitized at 8 KHz sampling rate using Regular Pulse Excited – Linear Predictive Coder (RPE-LPC). In this technique, information from previous samples is used to predict the current sample
2. Channel Coding – This step introduces redundancy information into the data for error detection and possible error correction. The gross bit rate after channel coding is 22.8 kbps
3. Interleaving – This step rearranges a group of bits in a particular way. This is to improve the performance of the error correction mechanisms
4. Ciphering – Encrypts blocks of user data using a symmetric key shared by the mobile station and the BTS
5. Burst Formatting – Adds some binary information to the ciphered block. This additional information is used for synchronization and equalization of the received data
6. Modulation – Gaussian Minimum Shift Keying (GMSK) modulation technique is used. The binary data is converted back into analog signal to fit the frequency and time requirements for the multiple access rules. This signal is then radiated as radio wave over the air
7. Multipath and Equalization – Radio waves reflect from buildings, cars, hills etc. So the antenna receives the right signal as well as the reflected signals which corrupt the information. An Equalizer extracts the right signal from the received signal. For this the received signal is passed through the inverse filter
8. Synchronization – In FDMA, frequency synchronization is necessary so that the transmitter and receiver frequency match. In TDMA, time synchronization is necessary to identify the frame and bits

Call Routing in GSM contd.



PLMN Interfaces

- Basic configuration of a GSM network contains a central HLR and a central VLR where HLR contains all security, provisioning and subscriber related information and VLR stores the location information and other transient data.
- MSC needs subscriber parameter for successful call set-up.
- Any data related to user call (connection, teardown etc.) are processed with SS7 protocol for signaling using ISUP (ISDN User Part) stack between network nodes.
- For mobile specific signaling, a protocol stack called MAP (Mobile Application Part) is used over the SS7 network which does all database transactions and handover/roaming transactions between the MSC

GSM Addresses and Identifiers

- International Mobile Station Equipment Identity (IMEI): Every mobile equipment in this world has a unique identifier which is called IMEI. IMEI is allocated by the equipment manufacturer and registered by the network operator in the Equipment Identity Register (EIR).
- International Mobile Subscriber Identity (IMSI): When registered with a GSM operator, each subscriber is assigned a unique identifier called IMSI which is stored in the SIM card and secured by the operator. IMSI consists of several parts: 3 decimal digits of Mobile Country Code (MCC), 2 decimal digits of Mobile Network Code (MNC) and a maximum of 10 decimal digits of Mobile Subscriber Identification Number (MSIN) which is a unique number of the subscriber within the home network.

GSM Addresses and Identifiers

- Mobile Subscriber ISDN Number (MSISDN): The MSISDN number is the real telephone number as is known to the external world. MSISDN number is public information whereas IMSI is private to the operator. IMSI can be multiple such as when a subscriber opts for fax and data, he is assigned a total of three numbers: one for voice call, one for fax call and another for data call. MSISDN follows the international ISDN (Integrated Systems Data Network) numbering plan.
- ISDN has Country Code (CC) of 1 to 3 decimal digits, National Destination Code (NDC) of 2 to 3 decimal digits and Subscriber Number (SN) of maximum 10 decimal digits.

GSM Addresses and Identifiers

- Location Area Identity: Each LA in a PLMN has its own identifier called Location Area Identifier (LAI) which is structured hierarchically and unique. LAI consists of 3 digits of CC, 2 digits of Mobile Network Code and maximum of 5 digits of Location Area Code.

- Mobile Station Roaming Number (MSRN): When a subscriber is roaming in another network, a temporary ISDN number is assigned to the subscriber called MSRN. MSRN is assigned by the local VLR in charge of the mobile station and follows the structure of MSISDN.

GSM Addresses and Identifiers

- Temporary Mobile Subscriber Identity (TMSI): TMSI is a temporary identifier assigned by the serving VLR used in place of the IMSI for identification and addressing of the mobile station. Together with the current location area, a TMSI allows a subscriber to be identified uniquely.

- Local Mobile Subscriber Identity (LMSI): LMSI is assigned by the VLR and stored in the HLR and is used as a searching key for faster database access within the VLR.

- Cell Identifier: Within a LA, every cell has a unique Cell Identifier (CI) and together with a LAI, a cell can be identified uniquely through Global Cell Identity (LAI & CI).

Network aspects in GSM

- Layer 1 is the physical layer which uses the channel structures over the air interface.
- Layer 2 is the data link layer and across the Um interface, the data link layer is a modified version of the LAPD protocol used in ISDN or X.25, called LAPDm.
- Layer 3 of the GSM signaling protocol is itself divided into three sub-layers:

1. Radio Resources Management: It controls the set-up, maintenance and termination of radio and fixed channels, including handovers.
2. Mobility Management: It manages the location updating and registration procedures as well as security and authentication.
3. Connection Management: It handles general call control and manages Supplementary Services and the Short Message Service.

Mobility Management (MM)

- Using MM one can make outgoing calls and receive incoming calls while in motion
- Mobile originated outgoing calls are relatively easy to handle
- For mobile terminated incoming calls the following dour important aspects are necessary:

1) **Paging –** The MS is traced through the paging process within a location. A single paging message across the MSC to BSS interface contains information of the cells in which the page shall be broadcast
2) **Location Update –** To know the current location of a powered on MS so that the mobile terminated call routing can be completed. Through location update, the presence and location information is kept up to date within the VLR and HLR
3) **Handover –** As a user moves away from a tower the signal will become weak and break. So user needs to be moved to another cell where the signal strength is higher. This is called handover or handoff.

    i) Internal Handover – Channels in the same cell or cells under the control of same BSC

    ii) External Handover – Cells within same MSC or cells under different MSC
4) **Roaming –** Moving from one point of attachment to another point of attachment between two different networks, is called as roaming

GSM Frequency Allocation

- Normally, GSM uses 900 MHz band wherein 890-915 MHz is allocated for the uplink (mobile station to base station) and 935–960 MHz is allocated for the downlink (base station to mobile station). Each way the bandwidth for the GSM system is 25 MHz which provides 125 carriers uplink/downlink each having a bandwidth of 200 kHz.

- GSM uses a combination of Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) encoding.

- One or more carrier frequencies are assigned to each base station and each of these carrier frequencies is then divided in time using a TDMA scheme where fundamental unit is called a burst period lasting approximately 0.577 ms.

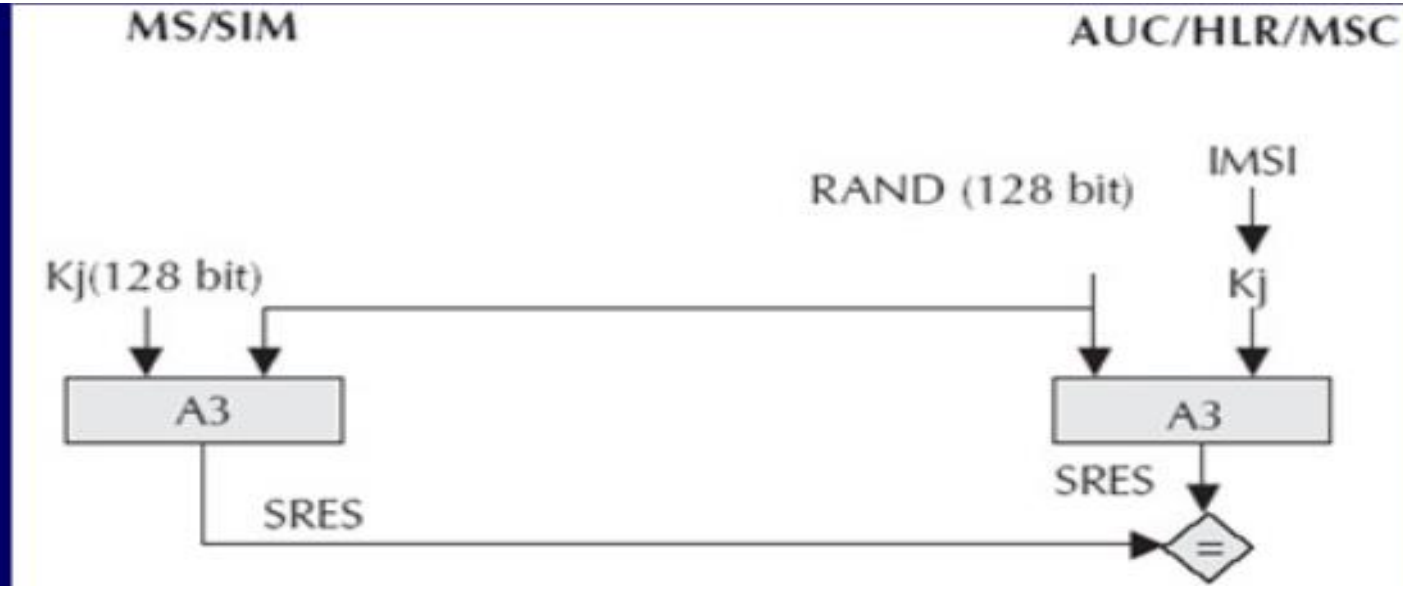
- Eight burst periods are grouped into a TDMA frame of approximately 4.615 ms which forms the basic unit for the definition of logical channels.

Authentication and Security

- Authentication involves two functional entities - the SIM card in the mobile phone and the Authentication Center (AUC).
- Following authentication by algorithm A3, a key is generated for encryption.
- An algorithm A8 is used to generate the key while a different algorithm called A5 is used for both ciphering and deciphering procedures for signaling, voice and data.

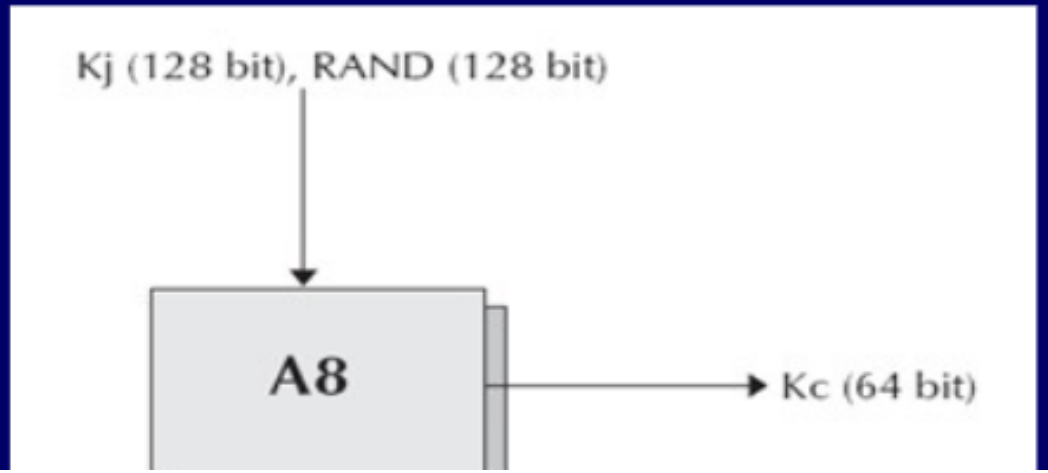
A3 Algorithm

- During authentication, MSC challenges the MS with a random number (RAND).
- SIM card uses this RAND received from the MSC and a secret key Kj stored within the SIM as input. Both the RAND and the Kj secret are 128 bits long. Using the A3 algorithm with RAND and Kj as input a 32-bit output called signature response (SRES) is generated in the MS and then sent back to MSC.
- Using the same set of algorithms, the AUC also generates a SRES. The SRES from MS and the SRES generated by the AUC are compared.
- If they are the same, the MS is authenticated.



A8 Algorithm

- A8 algorithm is the key generation algorithm.
- A8 generates a session key, Kc, from the random challenge RAND (received from the MSC) and from the secret key Kj.
- Keys are generated at both the MS and the network end. The session key, Kc, is used for ciphering till the MSC decides to authenticate the MS once again.



A5 Algorithm

- A5 is the stream cipher algorithm used to encrypt over-the-air transmissions. The stream cipher is initialized all over again for every frame sent with the session key, Kc, and the number of the frame being encrypted or decrypted.
- Same Kc is used throughout the call but the 22-bit frame number changes during the call, thus, generating a unique key stream for every frame.