Subject Name: Mobile Computing and Wireless Communication
Subject Code: 3170710

Faculties: Ms. Alpa Rupala

CHAPTER NO -3: Multiple Access in Wireless System:

TOPIC 1. Multiple access scheme

DESCRIPTIVE QUESTIONS

1. Explain the following Multiple Access Techniques used to access the channel by mobile subscriber. **(June-2012)[L.J.I.E.T]** 7

- Frequency Division Multiple access.
- Space Division Multiple access.

ANS:

Multiple Access System:

→ In this kind of system multiple users can transmit by single channel.

→ The multiple access technique is used in the multiuser environment for applications such as satellite communication and wireless mobile communication.

→ Multiple access techniques are classified below:

1. Frequency Division Multiple Access (FDMA)
2. Time Division Multiple Access (TDMA)
3. Space Division Multiple Access (SDMA)
4. Code Division Multiple Access (CDMA)

➢ **Space Division Multiple access [SDMA]:**

→ It is used for allocating a separated space to users in wireless network.

→ It offers service to different users by using different spot beam antennas.

→ The antenna beam covers different areas that offers service at the same frequency.

→ The mobile phone may receive several base stations with different quality.

→ A MAC algorithm could now decide which basestation is best, taking into account which frequencies (FDM), time slots (TDM) or code (CDM) are still available (depending on the technology).

→ Typically, SDMA is never used in isolation but always in combination with one or more other schemes.

→ For SDMA, sectorized antenna are preferred to be used.

→ The basis for the SDMA algorithm is formed by cells and sectorized antennas which constitute the infrastructure implementing Space Division Multiplexing (SDM).

→ The spectral efficiency is increased in SDMA. The system capacity is expressed as:

$$C_{SDMA} = N_{SDMA} \; C$$

Where,

C_{SDMA} = Capacity of SDMA system

N_{SDMA} = Average number of simultaneous spatial channel per RF channel.

2. Explain the following Multiple Access Techniques used to access the channel by mobile subscriber. **(June-2012)[L.J.I.E.T]** 7

- Time Division Multiple access.
- Code Division Multiple access.

3. Explain FDMA with example of Frequency division duplex. **[L.J.I.E.T]** 4

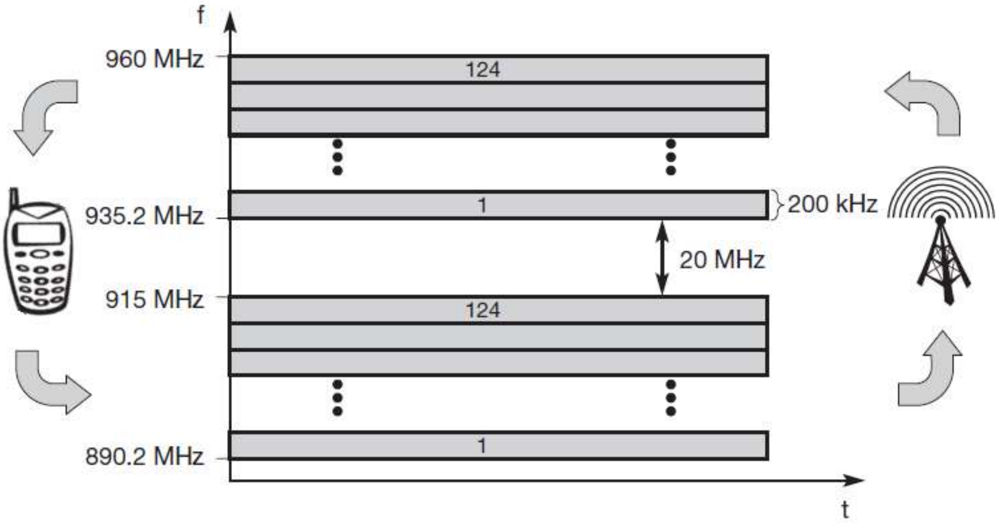
➢ **Frequency division multiple access (FDMA)**

→ In wireless communication, the individual users are allocated individual channels. The

channels or the frequency band is unique for each subscriber.
→ The entire allowed radio spectrum is divided into many slices of the frequency bands and each band or channel is allocated to users.

Features of FDMA:
→ It comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM).
→ Allocation can either be fixed (as for radio stations or the general planning and regulation of frequencies) or dynamic (i.e., demand driven).
→ Complexity of FDMA is less
→ It have narrow bandwidth as each channel supports only one circuit per carrier.
→ The symbol time is large in comparison to the delay spread
→ ISI (Inter symbol Interference) is low.
→ Cost of cell site is higher in comparison to the TDMA system.
→ It is a continuous transmission method. So few bits are required for overhead purpose.
→ FDM is often used for simultaneous access to the medium by base station and mobile station in cellular network.
→ Channels can be assigned to the same frequency at all times, i.e., pure FDMA, or change frequencies according to a certain pattern, i.e., FDMA combined with TDMA.
→ The latter example is the common practice for many wireless systems to circumvent narrowband interference at certain frequencies, known as frequency hopping.
→ Sender and receiver have to agree on a hopping pattern, otherwise the receiver could not tune to the right frequency.
→ Hopping patterns are typically fixed, at least for a longer period. The fact that it is not possible to arbitrarily jump in the frequency space (i.e., the receiver must be able to tune to the right frequency) is one of the main differences between FDM schemes and TDM schemes.
→ Furthermore, FDM is often used for simultaneous access to the medium by base station and mobile station in cellular networks.

FDD:
→ Here the two partners typically establish a duplex channel, i.e., a channel that allows for simultaneous transmission in both directions. The two directions, mobile station to base station and vice versa are now separated using different frequencies.
→ This scheme is then called frequency division duplex (FDD).
→ Again, both partners have to know the frequencies in advance; they cannot just listen into the medium. The two frequencies are also known as uplink, i.e., from mobile station to base station or from ground control to satellite, and as downlink, i.e., from base station to mobile station or from satellite to ground control.
→ As for example FDM and FDD, Figure shows the situation in a mobile phone network based on the GSM standard for 900 MHz.
→ The basic frequency allocation scheme for GSM is fixed and regulated by national authorities. (Certain variations exist regarding the frequencies mentioned in the examples.) All uplinks use the band between 890.2 and 915 MHz, all downlinks use 935.2 to 960 MHz. According to FDMA, the base station, shown on the right side, allocates a certain frequency for up- and downlink to establish a duplex channel with a mobile phone. Up- and downlink have a fixed relation.
→ If the uplink frequency is $f_u = 890$ MHz $+ n \cdot 0.2$ MHz, the downlink frequency is $f_d = f_u + 45$ MHz, i.e., $f_d = 935$ MHz $+ n \cdot 0.2$ MHz for a certain channel n. The base station selects the channel.
→ Each channel (uplink and downlink) has a bandwidth of 200 kHz.



→ This illustrates the use of FDM for multiple access (124 channels per direction are available at 900 MHz) and duplex according to a predetermined scheme.

→ Similar FDM schemes for FDD are implemented in AMPS, IS-54, IS-95, IS-136, PACS, and UMTS (FDD mode). Chapter 4 presents some more details regarding the combination of this scheme with TDM as implemented in GSM.

Advantages of FDMA:

1. All stations can operate continuously all 24 hours without having to wait for their turn to come.
2. No synchronization is necessary
3. The complexity of system is low.

Disadvantages of FDMA:

1. Intermodulation frequencies can cause adjacent channel interference.
2. As result of non linearities, intermodulation product are generated.
3. Cell site cost is high
4. Bandwidth is narrow.
5. Carrier only one circuit at a time.

4. Explain TDMA with example of Time division duplex. **[L.J.I.E.T]** 4

TDMA:

→ Compared to FDMA, time division multiple access (TDMA) offers a much more flexible scheme, which comprises all technologies that allocate certain time slots for communication, i.e., controlling TDM. Now tuning in to a certain frequency is not necessary, i.e., the receiver can stay at the same frequency the whole time.

→ Each user to allocate a time slot in which the user can access the channel.

→ In each slot only one user is allowed to transmit or receive.

→ Using only one frequency, and thus very simple receivers and transmitters, many different algorithms exist to control medium access. Listening to different frequencies at the same time is quite difficult, but listening to many channels separated in time at the same frequency is simple.

→ Almost all MAC schemes for wired networks work according to this principle, e.g., Ethernet, Token Ring, ATM etc. Now synchronization between sender and receiver has to be achieved in the time domain. Again this can be done by using a fixed pattern similar to FDMA techniques, i.e., allocating a certain time slot for a channel, or by using a dynamic allocation scheme.

→ Dynamic allocation schemes require an identification for each transmission as this is the case for typical wired MAC schemes (e.g., sender address) or the transmission has to be announced beforehand.

→ MAC addresses are quite often used as identification. This enables a receiver in a broadcast medium to recognize if it really is the intended receiver of a message.

→ Fixed schemes do not need identification, but are not as flexible considering varying bandwidth requirements.

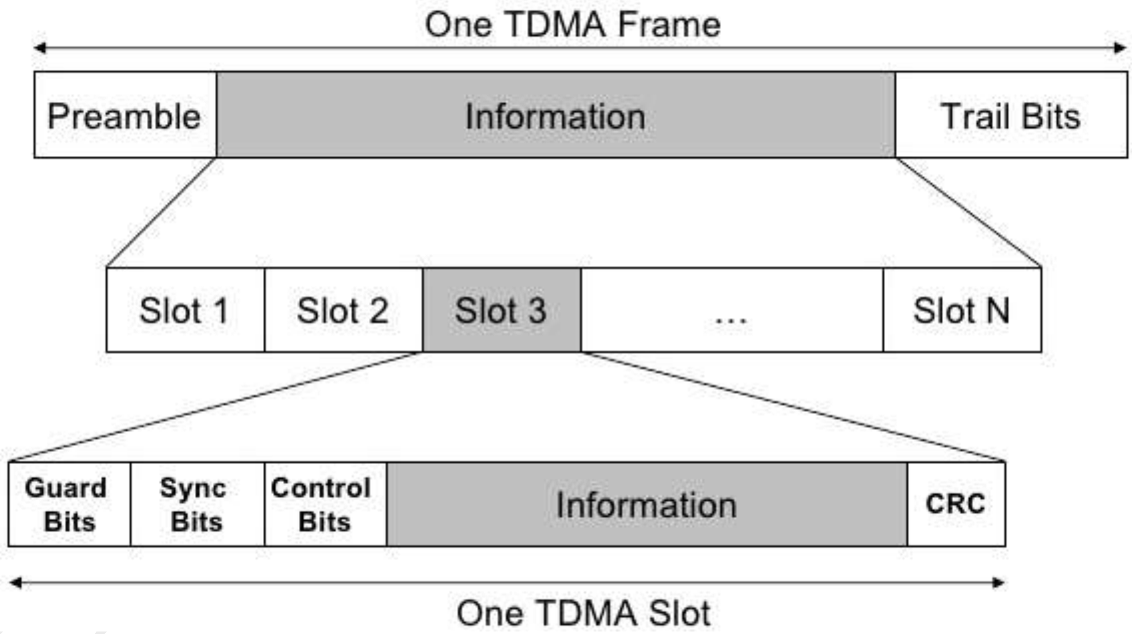
→ Typically, those schemes can be combined with FDMA to achieve even greater flexibility and transmission capacity. The simplest algorithm for using TDM is allocating time slots for channels in a fixed pattern.

→ This results in a fixed bandwidth and is the typical solution for wireless phone systems. MAC is quite simple, as the only crucial factor is accessing the reserved time slot at the right moment. If this synchronization is assured, each mobile station knows its turn and no interference will happen.

→ The fixed pattern can be assigned by the base station, where competition between different mobile stations that want to access the medium is solved.

→ Fixed access patterns (at least fixed for some period in time) fit perfectly well for connections with a fixed bandwidth.

→ Furthermore, these patterns guarantee a fixed delay – one can transmit, e.g., every 10 ms as this is the case for standard DECT systems. TDMA schemes with fixed access patterns are used for many digital mobile phone systems like IS-54, IS-136, GSM, DECT, PHS, and PACS.



→ The TDMA system transmit data in burst and buffer method. Means, the transmission from different users in interfaced into a repeating frame structure.

→ A frame consists of a number of slots. Each frame consists of preamble, an information message and trail bits.

→ Half of the time slots will be used for the forward link channel and the remaining half for reverse link channel.

→ The preamble field comprises the address and synchronization data that both the base stations and subscribers use to identify each other.

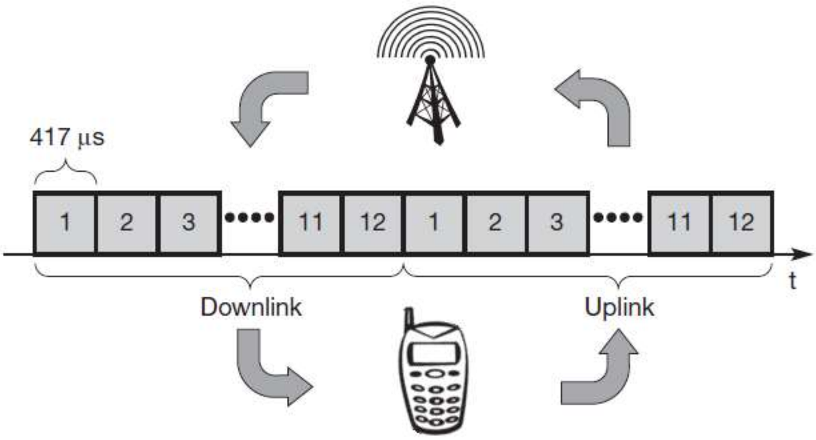
→ The guard bits are used to provide synchronization between different time slots and frames.

→ It is assumed that there are "N" number of slots for N users so that each user can access the

channel in their allowed time slot.
→ The TDMA/FDD system have identical frame structure that can be used for forward or reverse transmission, but the carrier frequencies will be different for both the links.

Features of TDMA:
→ TDMA uses different time slots for transmission and reception. So duplexer not required.
→ As the transmission rates are high adaptive equalization is necessary.
→ TDMA shares a single carrier frequency with several users where each user makes use of non-overlapping time slots.
→ The number of time slots depends on parameters like bandwidth, modulation method etc.
→ Bandwidth is supplied on demand to different users by assigned priority.
→ It can be turned off when not in use.
→ Guard time needs to be minimized.
→ Handoff process is simple.
→ Due to burst transmission high synchronization over head is needed in TDMA systems.

TDD:
→ Figure shows how these fixed TDM patterns are used to implement multiple access and a duplex channel between a base station and mobile station.
→ Assigning different slots for uplink and downlink using the same frequency is called time division duplex (TDD). As shown in the figure, the base station uses one out of 12 slots for the downlink, whereas the mobile station uses one out of 12 different slots for the uplink.
→ Uplink and downlink are separated in time. Up to 12 different mobile stations can use the same frequency without interference using this scheme. Each connection is allotted its own up- and downlink pair.



→ In the example below, which is the standard case for the DECT cordless phone system, the pattern is repeated every 10 ms, i.e., each slot has a duration of 417 µs. This repetition guarantees access to the medium every 10 ms, independent of any other connections.
→ While the fixed access patterns, as shown for DECT, are perfectly apt for connections with a constant data rate (e.g., classical voice transmission with 32 or 64 kbit/s duplex), they are very inefficient for bursty data or asymmetric connections.
→ If temporary bursts in data are sent from the base station to the mobile station often or vice versa (as in the case of web browsing, where no data transmission occurs while reading a page, whereas clicking on a hyperlink triggers a data transfer from the mobile station, often to the base station, often followed by huge amounts of data returned from the web server).
→ While DECT can at least allocate asymmetric bandwidth (see section 4.2), this general scheme still wastes a lot of bandwidth. It is too static, too inflexible for data communication.

5. What is CDMA? Explain the orthogonal codes for it. **[New] (Dec-2015)[L.J.I.E.T]** 7

CDMA:

→ Codes with certain characteristics can be applied to the transmission to enable the use of code division multiplexing (CDM).

→ Code division multiple access (CDMA) systems use exactly these codes to separate different users in code space and to enable access to a shared medium without interference.

→ The main problem is how to find "good" codes and how to separate the signal from noise generated by other signals and the environment.

→ The code directly controls the chipping sequence. But what is a good code for CDMA? A code for a certain user should have a good autocorre-lation2 and should be orthogonal to other codes. Orthogonal in code space has the same meaning as in standard space (i.e., the three dimensional space).

→ Think of a system of coordinates and vectors starting at the origin, i.e., in (0, 0, 0).3 Two vectors are called orthogonal if their inner product is 0, as is the case for the two vectors (2, 5, 0) and (0, 0, 17): (2, 5, 0)*(0, 0, 17) = 0 + 0 + 0 = 0.

→ But also vectors like (3, –2, 4) and (–2, 3, 3) are orthogonal: (3, –2, 4)*(–2, 3, 3) = –6 – 6 + 12 = 0.

→ By contrast, the vectors (1,2,3) and (4,2, –6) are not orthogonal (the inner product is –10), and (1, 2, 3) and (4, 2, –3) are "almost" orthogonal, with their inner product being –1 (which is "close" to zero).

→ This description is not precise in a mathematical sense. However, it is useful to remember these simplified definitions when looking at the following examples where the original code sequences may be distorted due to noise.

→ Orthogonality cannot be guaranteed for initially orthogonal codes.

→ Now let us translate this into code space and explain what we mean by a good autocorrelation. The Barker code (+1, –1, +1, +1, –1, +1, +1, +1, –1, –1, –1),

Features:

→ Soft handoff is done.

→ CDMA uses co channel cells

→ CDMA system users share the same frequency.

→ CDMA has a soft capacity limit.

→ Multipath fading can be reduced.

→ In CDMA more than one user is allowed to share a channel or sub channel with the help of DS-SS.

→ Each user is assigned a unique code.

→ At receiver the signal is recovered by using the same code sequence.

→ In CDMA the user access the channel in random manner. Hence overlap possible (near, far, hidden, exposed)

Encoding Rules for CDMA:

In CDMA each station is assigned a code which is simply a sequence of numbers called chips.

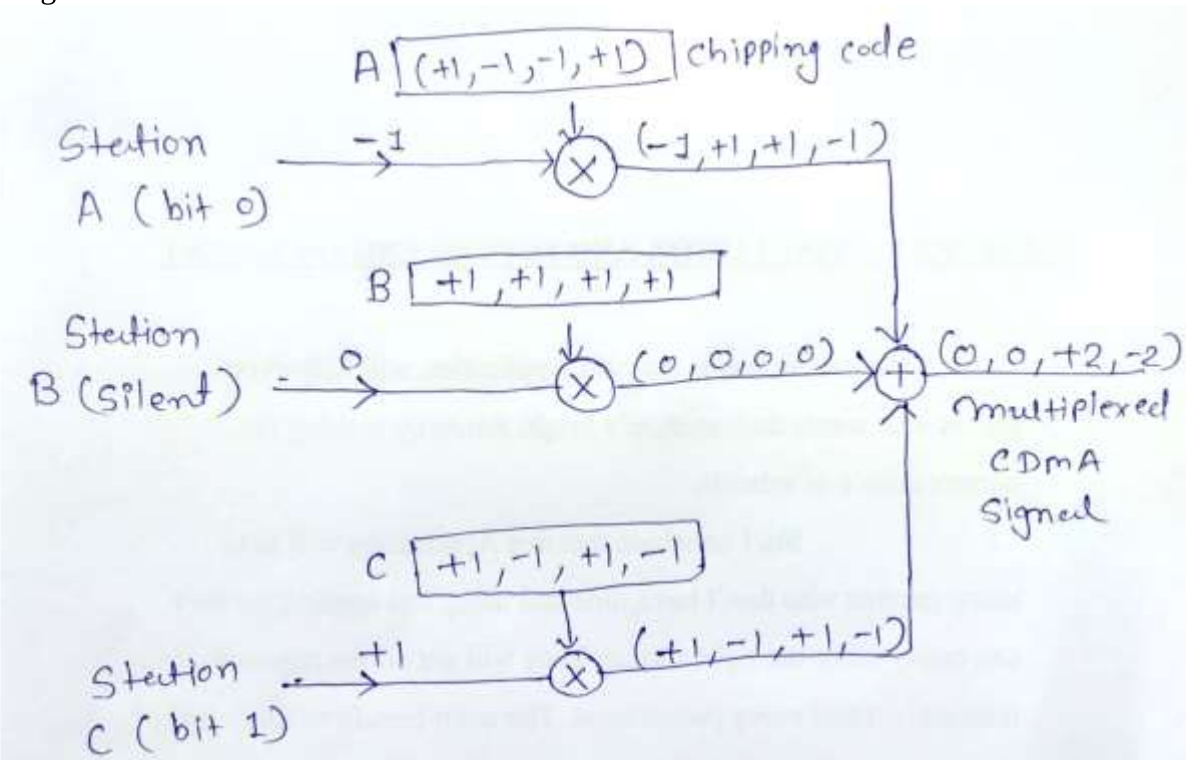
1. If station wants to send bit 0 then sends -1
2. If station want to send bit 1 then sends +1
3. If station does not want to transmit and want to remain idle, it is represented by 0.

CDMA Multiplexer:

→ Assume that we are having 3 stations with their chipping code say,

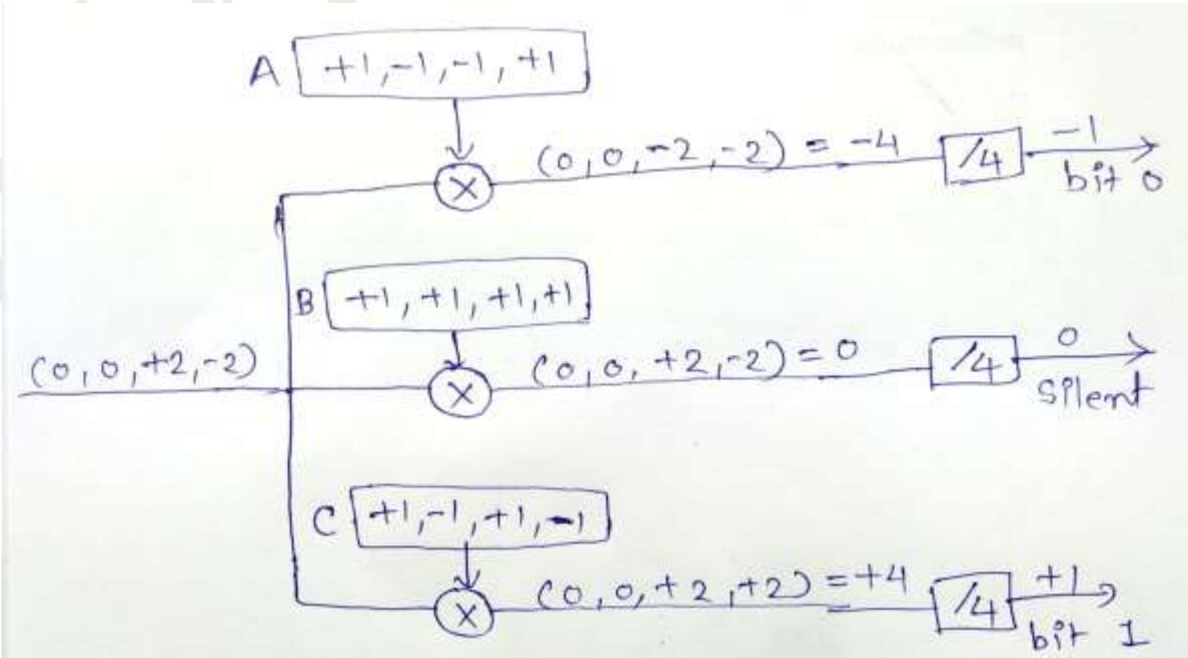
→ **A (+1, -1, -1, +1), B (+1, +1, +1, +1), C (+1, -1, +1, -1)**

→ Assume that A wants to transmit a bit 0, B wants to remain silent and C wants to transmit bit 1.
→ In this multiplexer receives one encoded no from each station (+1, -1, 0)
→ Each bit is multiplied with code no of corresponding station.
→ The output of multipliers are added to obtain the multiplexed CDMA signal.
→ Signal transmitted to link.



CDMA Demultiplexer:

→ CDMA signal is applied to all the multipliers.
→ It is multiplied with the code number assigned to each station A, B and C
→ The bits available at the output of each compiler are added together. This condition will always be either -4, 0, +4.
→ The result of addition at the output of each multiplier is divided by 4 to obtain the original transmitted bit.



Advantages of CDMA:

1. Biggest advantage over TDMA/FDMA provide secure communication.
2. In CDMA Multiplexer the frequency hopping phenomenon can be used.

Disadvantages of CDMA:

1. A problem of self-jamming can be occur.
2. Near and far problem occur in CDMA receiver if an unwanted user uses a high transmitted power.

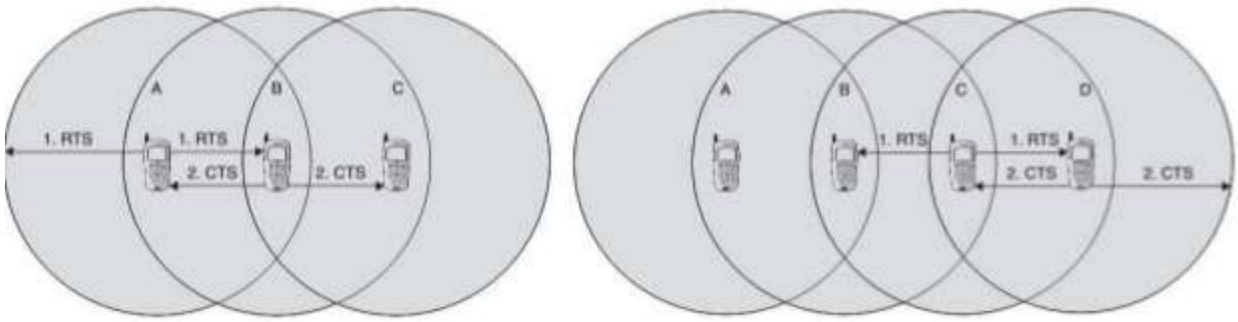
6. Why medium access control (MAC) is required in wireless networks? Explain with hidden and Exposed terminals & near and far terminals. **[L.J.I.E.T]** 7

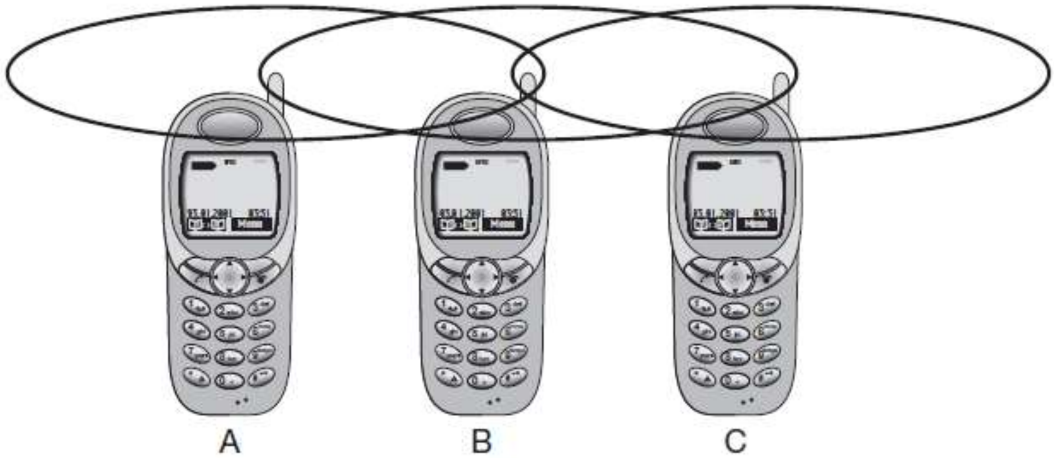
Hidden Terminal and Exposed Terminal:

→ The basic access mechanism, called Distributed Coordination Function in carrier sense Multiple Access with Collision Avoidance mechanism (CSMA/CA).

→ CSMA protocols are well known, the most popular being the Ethernet, which is CSMA/CD protocol.

→ In a Wired environment every station connected to the wire can sense the signal in the wire. In a wired LAN, if there is no activity or a collision of messages, every station connected to the LAN will be able to sense collection almost instantly. This is not true in the case of wireless media.





→ In the case of wireless LANs, a Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA) protocol is used, as it is not possible to detect a collision of data packets in mid-air.

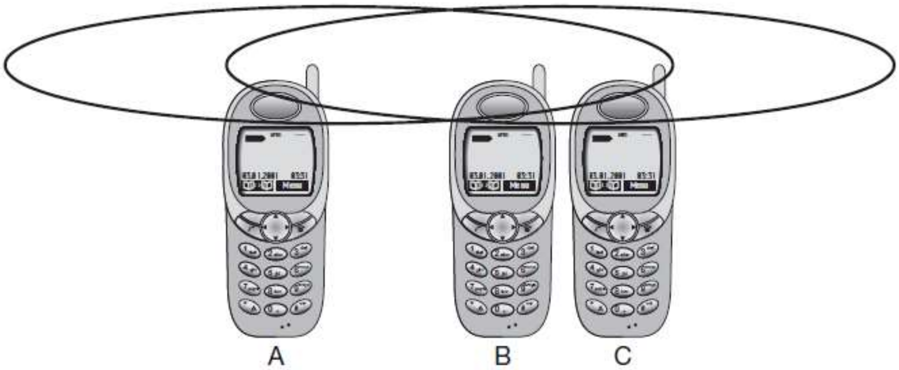
→ Consider the scenario with three mobile nodes shown in figure (a). The transmission of A reaches B, but not C. The transmission of C reaches B, but not A.

→ However, the radio signal of B reaches both A and C making both in the range of B. The net effect is A cannot detect C and vice versa.

→ A start sending to B, C does not receive this transmission. C also wants to send to B and sense the medium. To C the medium appears to be free. Thus C starts sending causing collision at B. But now A cannot detect the collision and continues with its transmission. A is 'Hidden' for C and vice versa.
→ In another case as shown in figure (b). The radio transmission signal of A reaches C and B.
→ The radio signal of C reaches both A and D. A wants to communicate to B, A starts sending signal to B. C wants to communicate to D, C sense the carrier and finds that A is talking to B.
→ C has to wait till the time A finishes with B. However, D is outside the range of A, therefore waiting is not necessary.
→ In fact A, B and C, D can communicate to each other in parallel without any collision, but according to the protocol that is not possible.
→ A and C are 'Exposed' terminals.

Near and Far Terminal

→ Consider the situation as shown in Figure 2. A and B are both sending with the same transmission power. As the signal strength decreases proportionally to the square of the distance, B's signal drowns out A's signal. As a result, C cannot receive A's transmission.
→ Now think of C as being an arbiter for sending rights (e.g., C acts as a base station coordinating media access).



→ In this case, terminal B would already drown out terminal A on the physical layer. C in return would have no chance of applying a fair scheme as it would only hear B.
→ The near/far effect is a severe problem of wireless networks using CDM. All signals should arrive at the receiver with more or less the same strength.
→ Otherwise (referring again to the party example of chapter 2) a person standing closer to somebody could always speak louder than a person further away.
→ Even if the senders were separated by code, the closest one would simply drown out the others.
→ Precise power control is needed to receive all senders with the same strength at a receiver. For example, the UMTS system adapts power 1,500 times per second.

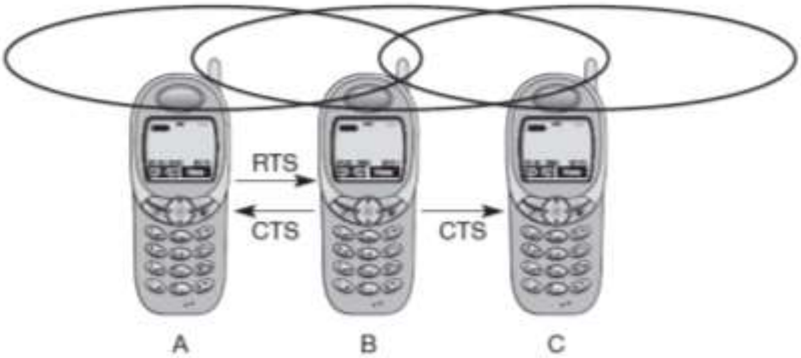
7.	What is hidden terminal problem? How it can be avoided? **(Nov-2017)[L.J.I.E.T]**	3
8.	Explain in brief Multiple access with collision avoidance (MACA). Justify how MACA can avoid hidden terminal problem. **[L.J.I.E.T]**	7
9.	Explain in brief Multiple access with collision avoidance (MACA). Justify how MACA can avoid exposed terminal problem. **[L.J.I.E.T]**	7
10	Why do MAC scheme in wired network fail in wireless networks. Explain how the multiple access with collision avoidance (MACA) scheme work does. **(Dec-2012)[L.J.I.E.T]**	7

Hidden terminal:

→ To all schemes with central base stations assigning TDM patterns, the problem of hidden terminals is unknown. If the terminal is hidden for the base station it cannot communicate anyway. But, more or less fixed access patterns are not as flexible as Aloha schemes.

→ What happens when no base station exists at all? This is the case in so-called ad-hoc networks.

→ Multiple access with collision avoidance (MACA) presents a simple scheme that solves the hidden terminal problem, does not need a base station, and is still a random access Aloha scheme – but with dynamic reservation.



→ Figure shows the hidden terminals. Remember, A and C both want to send to B. A has already started the transmission, but is hidden for C, C also starts with its transmission, thereby causing a collision at B. N mini-slots N * k data-slots e.g. N=6, k=2.

→ Other stations can use free data-slots based on a round-robin scheme Reservations for data-slots Figure 3.9 Reservation TDMA access scheme With MACA, A does not start its transmission at once, but sends a request to send (RTS) first. B receives the RTS that contains the name of sender and receiver, as well as the length of the future transmission.

→ This RTS is not heard by C, but triggers an acknowledgement from B, called clear to send (CTS). The CTS again contains the names of sender (A) and receiver (B) of the user data, and the length of the future transmission.

→ This CTS is now heard by C and the medium for future use by A is now reserved for the duration of the transmission. After receiving a CTS, C is not allowed to send anything for the duration indicated in the CTS toward B. A collision cannot occur at B during data transmission, and the hidden terminal problem is solved – provided that the transmission conditions remain the same. (Another station could move into the transmission range of B after the transmission of CTS.)

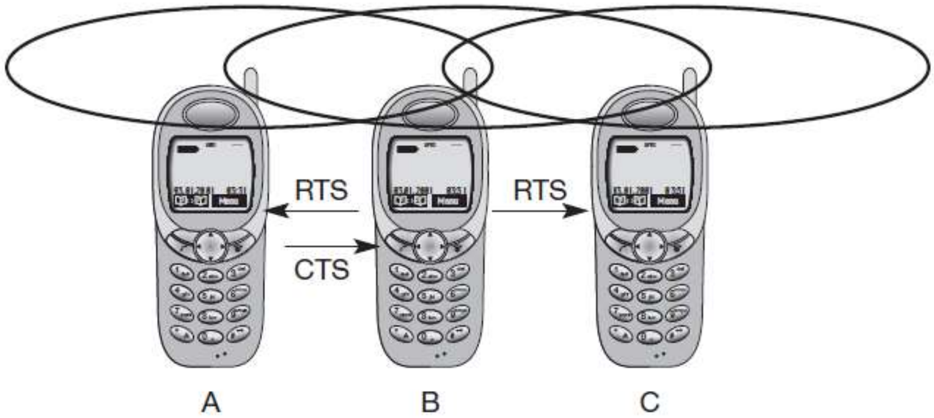
→ Still, collisions can occur during the sending of an RTS. Both A and C could send an RTS that collides at B. RTS is very small compared to the data transmission, so the probability of a collision is much lower.

→ B resolves this contention and acknowledges only one station in the CTS (if it was able to recover the RTS at all). No transmission is allowed without an appropriate CTS. This is one of the medium access schemes that is optionally used in the standard IEEE 802.11 Can MACA also help to solve the 'exposed terminal' problem?

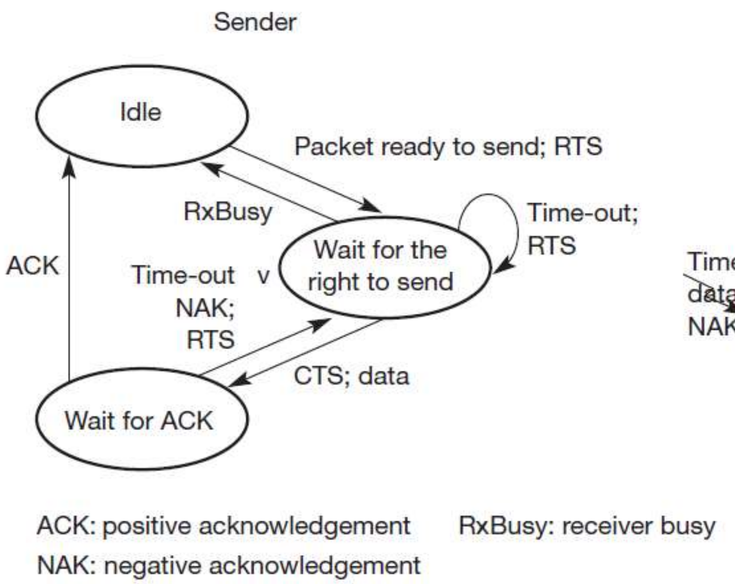
Exposed Terminal

→ B wants to send data to A, C to someone else. But C is polite enough to sense the medium before transmitting, sensing a busy medium caused by the transmission from B. C defers, although C could never cause a collision at A.

→ With MACA, B has to transmit an RTS first (as shown in Figure) containing the name of the receiver (A) and the sender (B). C does not react to this message as it is not the receiver, but A acknowledges using a CTS which identifies B as the sender and A as the receiver of the following data transmission. C does not receive this CTS and concludes that A is outside the detection range.



- → C can start its transmission assuming it will not cause a collision at A. The problem with exposed terminals is solved without fixed access patterns or a base station.
- → One problem of MACA is clearly the overheads associated with the RTS and CTS transmissions – for short and time-critical data packets, this is not negligible.
- → MACA also assumes symmetrical transmission and reception conditions. Otherwise, a strong sender, directed antennas etc. could counteract the above scheme.

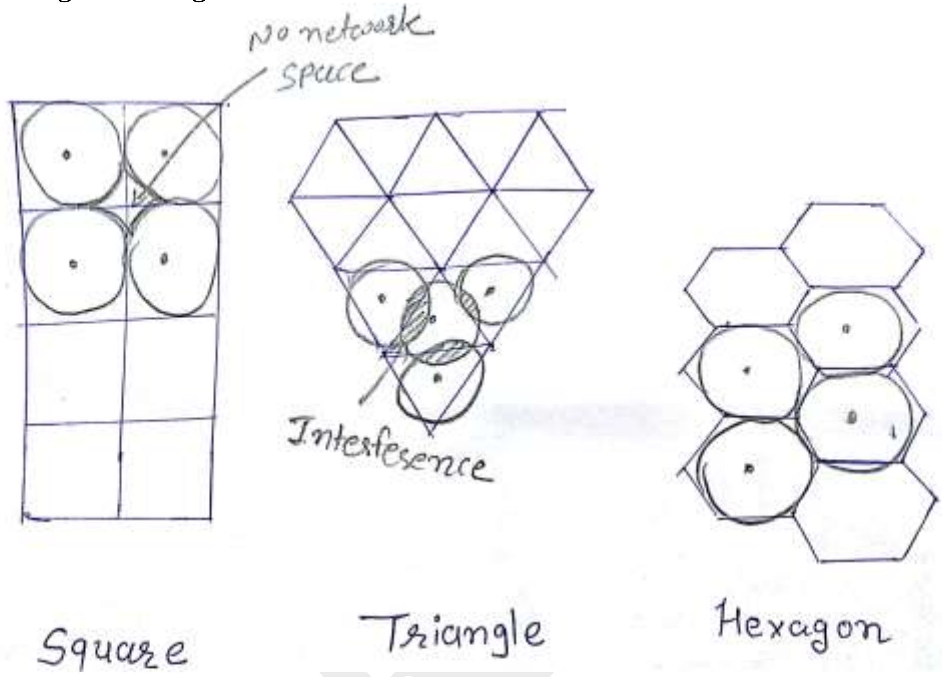


- → Figure shows simplified state machines for a sender and receiver. The sender is idle until a user requests the transmission of a data packet. The sender then issues an RTS and waits for the right to send. If the receiver gets an RTS and is in an idle state, it sends back a CTS and waits for data. The sender receives the CTS and sends the data. Otherwise, the sender would send an RTS again after a time-out (e.g., the RTS could be lost or collided).
- → After transmission of the data, the sender waits for a positive acknowledgement to return into an idle state. The receiver sends back a positive acknowledgement if the received data was correct. If not, or if the waiting time for data is too long, the receiver returns into idle state. If the sender does not receive any acknowledgement or a negative acknowledgement, it sends an RTS and again waits for the right to send.
- → Alternatively, a receiver could indicate that it is currently busy via a separate RxBusy. Real implementations have to add more states and transitions, e.g., to limit the number of retries.

	NUMERICALS	
1.	A cellular system uses FDMA with spectrum allocation of 12.5 MHz in each direction, a guard band at the edge of the allocated spectrum of 10 KHz, and a channel bandwidth of 30 KHz. Find out number of channels available. **(Nov-2017) [L.J.I.E.T]**	4
2.	Consider Global System for Mobile, which is TDMA/FDD system that uses 25 MHz for the forward link, which is broken in to radio channels of 200 KHz. If 8 speech channels are supported on a single radio channel and if no guard band is assumed, find the no of simultaneous users that can be accommodated in GSM. **(Nov-2017) [L.J.I.E.T]**	4
	TOPIC 2. Global system for mobile communication(GSM)	
	DESCRIPTIVE QUESTIONS	
1.	Explain the functioning of cellular network. How the given set of frequencies are used to increase the capacity of a network. **(June-2012)[L.J.I.E.T]** What is Cellular network? Explain frequency allocation in GSM network. **(Summer-2014) [L.J.I.E.T]** **Cellular Network:** In olden days, a single high powered transmitter with antenna mounted on a tall tower was used to cover a large service area. Spectral congestion and user capacity was a major problem. So, the radio telephone system was reconstructed to obtain high capacity with limited radio spectrum while at the same time covering large areas. **In cellular Network:** → The single high power transmitter is replaced with many low power transmitters each providing coverage to only a small part of service area. Each station is allocated a portion of the total number of channels and nearby base station are assigned different group of channels. → There vase station and their channel groups are systematically placed throughput a market then the available channels are distributed throughout the service area. They can be reused as many time as possible as many times as essential. Cellular system can be created with small cells. **Advantages of cellular system:** → **High Capacity:** Implementing SDM allows frequency reuse. If one transmitter is far away from another. i.e. Outside the interference range, it can reuse the same frequencies. → **Less Transmission power:** a Receiver is far away from a base station would need much more transmission power than the current few Watts. → **Local Interference:** Having long distance between sender and receiver result in even more interference problem with small cells, mobile stations and base station only have to deal with “Local Interference” → **Robustness:** Cellular systems are decentralized and so, more robust against the failures of single components. If one antenna fails, this only influences communication within small area. **Disadvantages of cellular system:** → **Infrastructure needed:** We need complex infrastructure to connect all base stations. → **Handover needed:** The MS has to perform a handover when changing from one cell to another. → **Frequency Planning:** To avoid interference between transmitters using the same frequencies, frequencies have to be distributed carefully.	7, 7

Hexagonal cell geometry cellular system: In, Cellular topology we need to consider qualitative means to characterize the interference. For, the cells of same shape to form a tessellation so that there is no ambiguous area that belongs to multiple cells or to no cell, the cell shape can be of only three types of regular polygons.

→ Equilateral Triangle
→ Equilateral Square
→ Equilateral regular hexagon



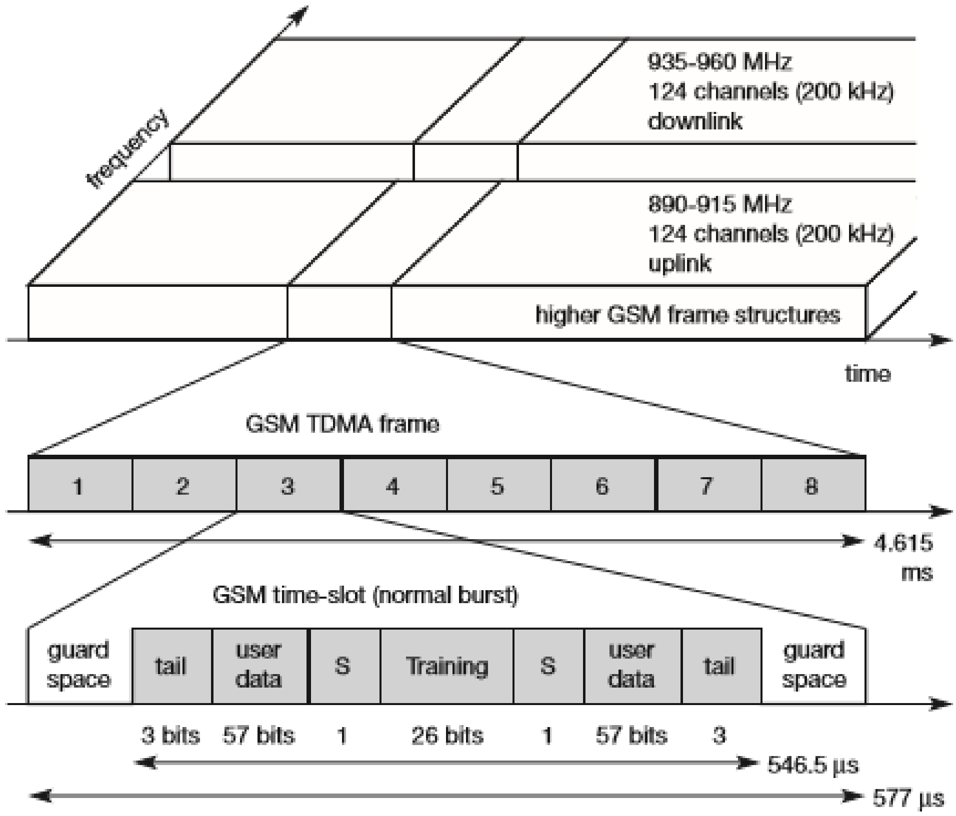
Advantage of Using Hexagonal:

→ It allows easy and manageable analysis
→ In circular, adjacent circles can have gaps in between or can create overlapping but hexagonal closely approximates the circular radiation pattern in an omni-direction base station antenna.
→ In hexagon, Geometry less number of cells can cover the entire market.

Frequency allocation: GSM implements SDMA using cells with BTS and assigns an MS to a BTS. Furthermore, FDD is used to separate downlink and uplink as shown in Figures.

→ Media access combines TDMA and FDMA.
→ In GSM 900, 124 channels, each 200 kHz wide, are used for FDMA, whereas GSM 1800 uses, 374 channels. Due to technical reasons, channels 1 and 124 are not used for transmission in GSM 900.
→ Typically, 32 channels are reserved for organizational data; the remaining 90 are used for customers. Each BTS then manages a single channel for organizational data and, e.g., up to 10 channels for user data.
→ The following example is based on the GSM 900 system, but GSM works in a similar way at 1800 and 1900 MHz. Figure shows the TDM used. Each of the 248 channels is additionally separated in time via a GSM TDMA frame, i.e., each 200 kHz carrier is subdivided into frames that are repeated continuously.
→ The basic frequency allocation scheme for GSM is fixed and regulated by national authorities. (Certain variations exist regarding the frequencies mentioned in the examples.) All uplinks use the band between 890.2 and 915 MHz, all downlinks use 935.2 to 960 MHz. According to FDMA, the base station, shown on the right side, allocates a certain frequency for up- and downlink to establish a duplex channel with a mobile phone. Up- and downlink have a fixed relation.

→ If the uplink frequency is fu = 890 MHz + n·0.2 MHz, the downlink frequency is fd = fu + 45 MHz, i.e., fd = 935 MHz + n·0.2 MHz for a certain channel n. The base station selects the channel.
→ The duration of a frame is 4.615 ms. A frame is again subdivided into 8 GSM time slots, where each slot represents a physical TDM channel and lasts for 577 µs. Each TDM channel occupies the 200 kHz carrier for 577 µs every 4.615 ms. Data is transmitted in small portions, called bursts.



→ Figure shows a so called normal burst as used for data transmission inside a time slot (user and signaling data). In the diagram, the burst is only 546.5 µs long and contains 148 bits.
→ The remaining 30.5 µs are used as guard space to avoid overlapping with other bursts due to different path delays and to give the transmitter time to turn on and off.
→ Filling the whole slot with data allows for the transmission of 156.25 bit within 577 µs. Each physical TDM channel has a raw data rate of about 33.8 kbit/s, each radio carrier transmits approximately 270 kbit/s over the Um interface.
→ The first and last three bits of a normal burst (tail) are all set to 0 and can be used to enhance the receiver performance.
→ The training sequence in the middle of a slot is used to adapt the parameters of the receiver to the current path propagation characteristics and to select the strongest signal in case of multi-path propagation.
→ A flag S indicates whether the data field contains user or network control data.
→ Apart from the normal burst, ETSI (1993a) defines four more bursts for data transmission:
→ A frequency correction burst allows the MS to correct the local oscillator to avoid interference with neighbouring channels.
→ A synchronization burst with an extended training sequence synchronizes the MS with the BTS in time
→ An access burst is used for the initial connection setup between MS and BTS
→ A dummy burst is used if no data is available for a slot.

2. Explain following : **[New] (Dec-2014)[L.J.I.E.T]** 7

i. Draw: Cellular Structure. [Marks : 1]
ii. Justify: Cell shape is Hexagon. [Marks : 2]
iii. How to reuse the limited frequency band in cellular architecture [Marks : 4]
[Explain Diagrammatically. Make following assumption: Frequency Band :100-170 Cluster Size : 7]

ANS:
1] Frequency : 100-170 so each cell contains 10 MHz frequency range

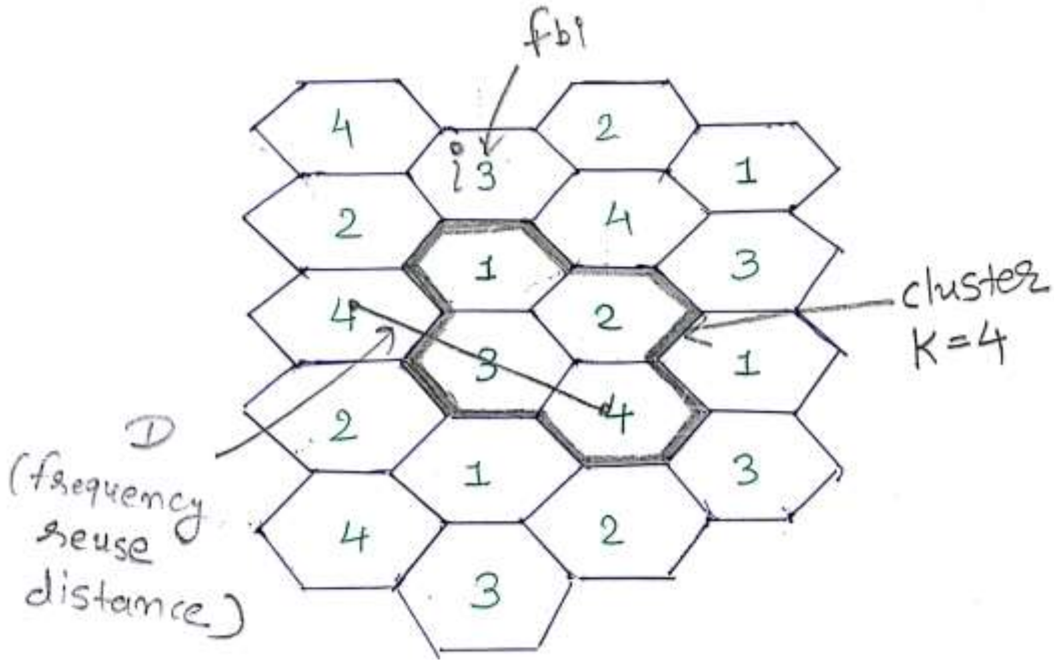
2] **Advantage of Using Hexagonal:**

1. It allows easy and manageable analysis
2. In circular, adjacent circles can have gaps in between or can create overlapping but hexagonal closely approximates the circular radiation pattern in an omni-direction base station antenna.
3. In hexagon, Geometry less number of cells can cover the entire market.

3] 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 modelling purposes these are modelled as hexagons. Base stations are positioned at the center of these cells.

→ Each cell i receive 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.

→ 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 results 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.	
3.	Explain the essential characteristics of frequency reuse concept. Draw and explain cell cluster in GSM for k=4.**[New] (May-2017) [L.J.I.E.T]**	7
4.	What is the principle of frequency reuse in context of cellular networks? List the ways of increasing the capacity of a cellular system? **(May-2017)[L.J.I.E.T]** What is Frequency Reuse? Explain with proper diagram. **(Nov-2017)[L.J.I.E.T]** What is Frequency Reuse? Explain Frequency Allocation in GSM. **[New](May-2016) [New](May-2018) [L.J.I.E.T]**	7, 3, 7, 7
5.	Explain different types of power control techniques in cellular networks. **(Nov-2017)[L.J.I.E.T]** **ANS:** ➢ Transmission power represents a key degree of freedom in the design of wireless networks. ➢ In both cellular and ad hoc networks, power control helps with several functionalities like interference management due to broadcast nature of wireless communication ,signal interfere with each other, energy management due to limited battery power in mobile terminals or any handheld devices and connectivity management. ➢ Different power control schemes has been discussed as below: a) **Fixed Power Allocation Scheme**: It keep power control target values constant regardless traffic load. → In this scheme, all the signals from the MSs within the coverage area are power controlled such that the receiver at BS maintain equal received bit-energy for every mobile no matter what transmission rate it uses. → Equal bit energy strategy implies the received SIR is the same for all types of media at one time instant. → This scheme doesn't balance well the natural dissimilarity between voice and data traffic. → In our multi-media system high-rate data traffic with lower BER requirements and lower-rate voice traffic with higher BER requirements are transmitted through the same channel. → Hence the performance of the more vulnerable traffic may degrade drastically when the user number is increased. **b) Adaptive Power Allocation Schemes** The difference between adaptive power control and fixed power allocation lies in the dynamic power allocation during a dynamic traffic situation. → With fixed power allocation the allocated power level is fixed for each type of media, no matter what kind of traffic profile it is. While with adaptive power allocation, the target power level is changed as traffic load changes. → However the decision of power allocation is done on the basis of traffic pay load i.e. either strength based optimal power allocation scheme, with this strategy, strength-based power control is used for individual traffic. → The objective is to always guarantee to meet the minimum required voice quality and	4

reserve the highest possible system capacity to data users.

→ In other words, the system adjusts the relationship between data users and voice users according to the system traffic load in order to make the BER of voice users equal to the required value.

→ This scheme outperforms equal bit-energy strategy in both nonfading and fading channel.

→ Besides, this scheme can take advantage of graceful degradation characteristics, so that the system can accommodate more users with just a little bit performance degradation.

c) **Canonical Power Control Scheme** A more general framework on convergence analysis is given that builds on the standard interference function in [10]. The authors define a broader class of synchronous and totally asynchronous power control algorithms known as the canonical algorithms.

d) **Stochastic Power Control Scheme** There are two types of stochastic dynamics often modeled in wireless cellular networks

→ One is channel variations and the other is user mobility.

→ Robustness against these dynamics has been analyzed and algorithms leveraging them have been designed.

→ In this a stochastic approximation based, on-line algorithm for controlling transmitter powers, using a fixed step size that provides weak convergence and faster response to time-varying channel conditions has been proposed.

e) **Binary Power Control Scheme** Binary power control is a power control scheme with only two allowable power values, usually Pmin (0) or Pmax (1).

→ Hence a link can either transmit at a full power or be switched off completely.

→ Binary power control (BPC) has the advantage of leading towards simpler or even distributed power control algorithms.

→ For N > 2 we propose a strategy based on checking the corners of the domain resulting from the power constraints to perform BPC.

→ We identify scenarios in which binary power allocation can be proven optimal also for arbitrary N [11, 12] as

$$P_{min} \le P \le P_{max}$$

6. What is Cellular network? Explain GSM architecture in detail. **(Winter-2015)[L.J.I.E.T]** 7

7. Explain functional architecture of GSM system. And also give different tele-services provided by GSM.**(Nov-2011) (May-2017) [L.J.I.E.T]** 7, 7

Functional Architecture of GSM: Follow GSM architecture thoery

GSM permits the integration of different voice and data services and the interworking with existing network.

There are three types of services:

1. **Bearer services:** It permits transparent and non-transparent, synchronous and asynchronous data transmission.
   Transparent service: only use the functions of the physical layer to transmit data. Data transmission has constant delay and throughput if no transmission error occurs.The only mechanism to increase transmission quality is the use of Forward Error Correction (FEC), which codes redundancy into the data stream and help to reconstruct the original data in

case of error.

Non Transparent bearer services: It uses layer 2 and 3 to implement error correction and flow control. This uses transparent services, adding a radio link protocol (RLP). Ex, PSTN, ISDN, packet switched PDN (x.25). Data transmission can be synchronous and asynchronous full duplex.

2. **Tele services:**
    1. **Telephony:** high quality digital voice transmission, offering at least the typical bandwidth of 3.1 KHz of analog.
    Special coder/decoder are used for voice transmission, while other codes are used for the transmission of analog data for communication with traditional computer modems. Example, fax machines.
    2. **Emergency number:** this service is mandatory for all providers and free of charge.
    It should be highest priority connection, possibly pre-empting other connection, and will automatically be set up with the closest emergency center.
    3. **SMS (Short message service):** which offers transmission of messages of up to 160 characters. The SMS do not use the standard GSM but exploit unused capacity in signaling channel. Sending and receiving of message is possible during data or voice transmission. Example, email headers or stock quotes. It can transfer, logos, ringtones, and horoscopes. SMS is used for updating mobile phone software or for implementing so called push services.
    4. **Enhanced message services (EMS):** It offers a large message size (760 characters), formatted text, and transmission of animated pictures, small images and ring tones.
    5. **Multimedia message services (MMS):** It offers transmission of larger pictures (GIF, JPG, and WBMP), short video clips and comes with mobile phones that integrate small cameras.
    6. **Group 3 fax:** fax is transmitted a digital data over the analog telephone network according to the ITU-T standard. T.4 and T.30 using modems. A transparent fax services is used 1) fax data and 2) fax signaling

3. **Supplementary services:** This services offers various enhancement for the standard telephony services and may vary from provider to provider. Typical supplementary services are user identification, call radiation or forwarding of outgoing calls.

8. Draw and explain GSM architecture. **(Winter-2013)[L.J.I.E.T]** 7,
Explain GSM architecture and role of its components**.(Summer-2014) [New] (Nov-2016) (Nov-2017) [L.J.I.E.T]** 7,
List out GSM Specification and explain functional architecture of GSM.**[New](Winter-2012) [L.J.I.E.T]** 7,
Explain functional architecture of GSM**. [New] (Dec-2014)[L.J.I.E.T]** 7,
Draw and explain System architecture of GSM **[New] (May-2015) [L.J.I.E.T]** 7,
(I) What is the frequency range of uplink and downlink in GSM network? **(Dec-2012)[L.J.I.E.T]** 7,
7

Ans:

- In the early 1980s, Europe had numerous coexisting analog mobile phone systems, which were often based on similar standards (e.g., NMT 450), but ran on slightly different carrier frequencies. To avoid this situation for a second generation fully digital system, the group special mobile (GSM) was founded in 1982.
- This system was soon named the global system for mobile communications (GSM).

GSM Specification

→ 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.

GSM Architecture

→ In System, It 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.

- **Radio subsystem (RSS):** As the name implies, the radio subsystem (RSS) comprises all radio specific entities, i.e., the mobile stations (MS) and the base station subsystem (BSS). Figure shows the connection between the RSS and the NSS via the A interface (solid lines) and the connection to the OSS via the O interface (dashed lines).
  - **Base station subsystem (BSS):** A GSM network comprises many BSSs, each controlled by a base station controller (BSC). The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS contains several BTSs.
    - **Base transceiver station (BTS):** A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission. A BTS can form a radio cell or, using sectorized antennas, several cells, and is connected to and to the BSC.
    - **Base station controller (BSC):** The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS. The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.
  - **Mobile station (MS):** The MS comprises all user equipment and software needed for communication with a GSM network. An MS consists of user independent hard- and software and of the subscriber identity module (SIM), which stores all user-specific data that is relevant to GSM. While an MS can be identified via the international mobile equipment identity (IMEI), a user can personalize any MS using his or her SIM, i.e., user-specific mechanisms like charging and authentication are based on the SIM, not on the device itself. Device-specific mechanisms, e.g., theft protection, use the device specific IMEI. Without the SIM, only emergency calls are possible. The SIM card contains many identifiers and tables, such as card-type, serial number, a list of subscribed services, a personal identity number (PIN), a PIN unblocking key (PUK), an authentication key Ki, and the international mobile subscriber identity (IMSI).

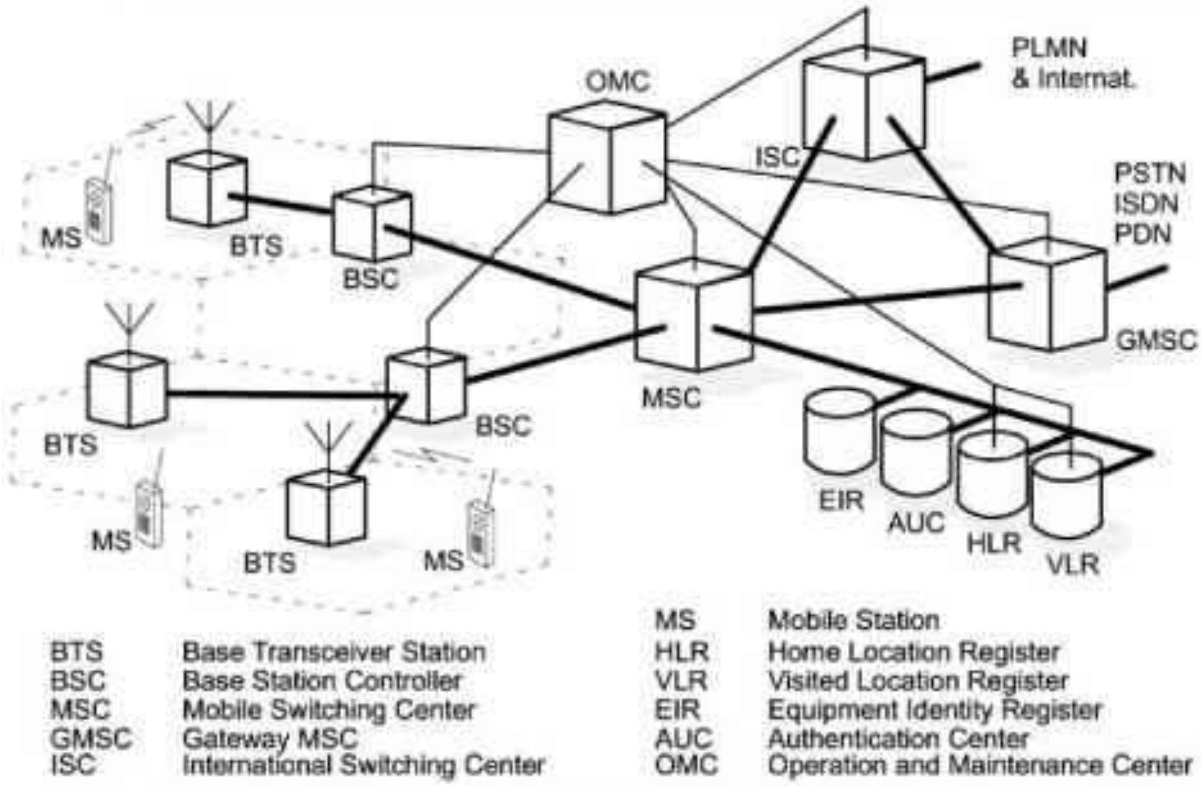


Figure: GSM Architecture

- **Network and switching subsystem (NSS):** The "heart" of the GSM system is formed by the network and switching subsystem (NSS). The NSS connects the wireless network with standard public networks, performs handovers between different BSSs, comprises functions for worldwide localization of users and supports charging, accounting, and roaming of users between different providers in different countries. The NSS consists of the following switches and databases:
  - **Mobile services switching center (MSC):** MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to the BSCs and form the fixed backbone network of a GSM system. Typically, an MSC manages several BSCs in a geographical region. A gateway MSC (GMSC) has additional connections to other fixed networks, such as PSTN and ISDN. Using additional interworking functions (IWF), an MSC can also connect to public data networks (PDN) such as X.25. An MSC handles all signalling needed for connection setup, connection release and handover of connections to other MSCs. The standard signalling system No. 7 (SS7) is used for this purpose. SS7 covers all aspects of control signalling for digital networks (reliable routing and delivery of control messages, establishing and monitoring of calls). Features of SS7 are number portability, free phone/toll/collect/credit calls, call forwarding, three-way calling etc. An MSC also performs all functions needed for supplementary services such as call forwarding, multi-party calls, reverse charging etc.
  - **Home location register (HLR):** The HLR is the most important database in a GSM system as it stores all user-relevant information. This comprises static information, such as the mobile subscriber ISDN number (MSISDN), subscribed services (e.g., call forwarding, roaming restrictions, GPRS), and the international mobile subscriber identity (IMSI). Dynamic information is also needed, e.g., the current location area (LA) of the MS, the mobile subscriber roaming number (MSRN), the current VLR and MSC. As soon as an MS leaves its current LA, the information in the HLR is updated. This information is necessary to localize a user in the worldwide GSM network. All these user-specific

information elements only exist once for each user in a single HLR, which also supports charging and accounting. HLRs can manage data for several million customers and contain highly specialized data bases which must fulfill certain real-time requirements to answer requests within certain time-bounds.

- **Visitor location register (VLR):** The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC (e.g., IMSI, MSISDN, HLR address). If a new MS comes into an LA the VLR is responsible for, it copies all relevant information for this user from the HLR. This hierarchy of VLR and HLR avoids frequent HLR updates and long-distance signalling of user information.

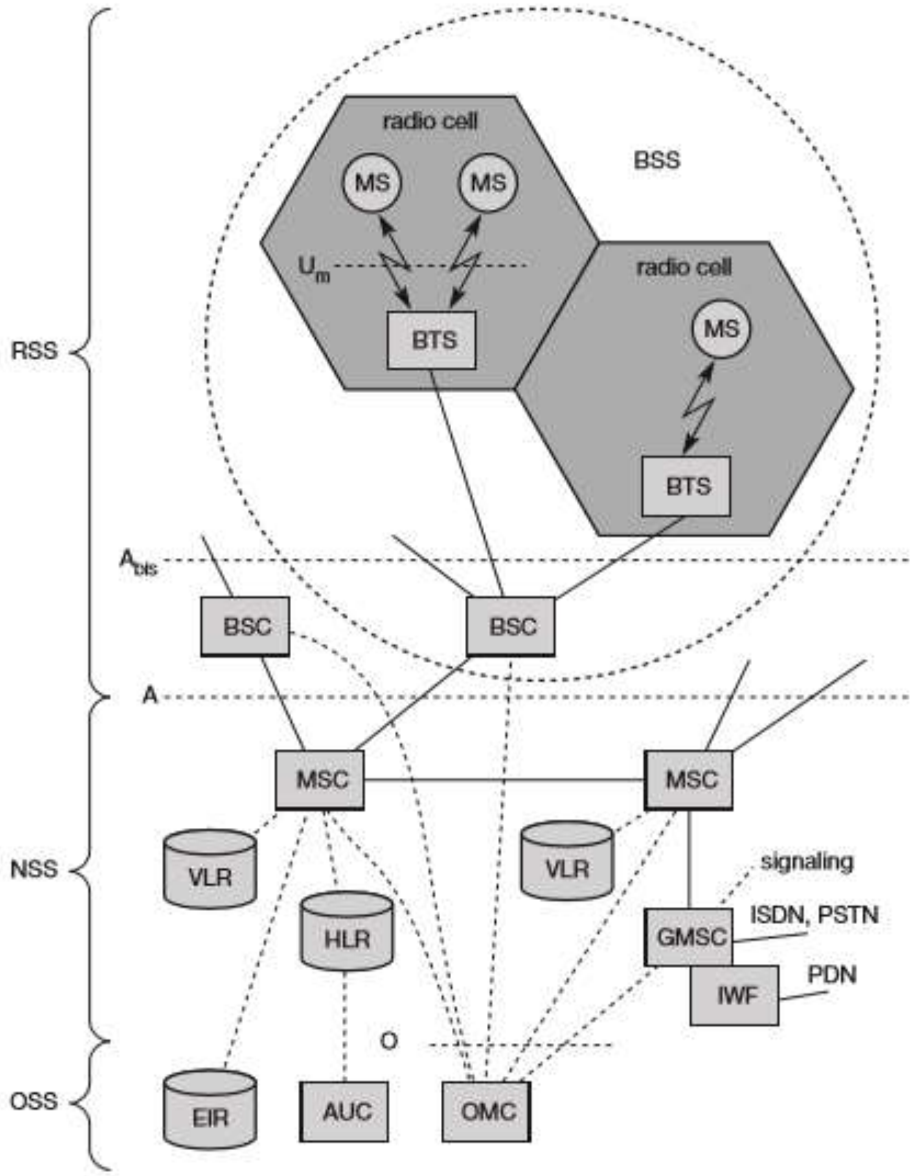


Figure : Function Architecture of GSM

- **Operation subsystem (OSS):** The third part of a GSM system, the operation subsystem (OSS), contains the necessary functions for network operation and maintenance. The OSS possesses network entities of its own and accesses other entities via SS7 signaling. The following entities have been defined:

- **Operation and maintenance center (OMC):** The OMC monitors and controls all other network entities via the O interface (SS7 with X.25). Typical OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing. OMCs use the concept of telecommunication management network (TMN) as standardized by the ITU-T.
- **Authentication center (AuC):** As the radio interface and mobile stations are particularly vulnerable, a separate AuC has been defined to protect user identity and data transmission. The AuC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR. The AuC may, in fact, be situated in a special protected part of the HLR.
- **Equipment identity register (EIR):** The EIR is a database for all IMEIs, i.e., it stores all device identifications registered for this network. As MSs are mobile, they can be easily stolen. With a valid SIM, anyone could use the stolen MS. The EIR has a blacklist of stolen (or locked) devices. In theory an MS is useless as soon as the owner has reported a theft. Unfortunately, the blacklists of different providers are not usually synchronized and the illegal use of a device in another operator's network is possible (the reader may speculate as to why this is the case). The EIR also contains a list of valid IMEIs (white list), and a list of malfunctioning devices (gray list).

Uplink: from mobile station to base station or from ground control to satellite
Range: 890 to 915 MHz
Downlink: from base station to mobile station or from satellite to ground control.
Range: 935 to 960 MHz

9. In GSM network, explain the role of Network and Switching subsystem. **(Summer-2013) [L.J.I.E.T]** 7

10. Explain term : BSS. **[New] (June-2014)[L.J.I.E.T]** 3

11. List and explain GSM entities**. (Winter-2013)[L.J.I.E.T]** 7

12. Explain the importance of following identifiers with that GSM is deals with: **[New] (May-2013) [L.J.I.E.T]** 8, 7, 7, 7, 7
• IMEI
• IMSI
• MSISDN
Define IMSI, TMSI, IMEI and MS-ISDN and write their use. **[New] (Dec-2013) [L.J.I.E.T]**
Describe different GSM addresses and identifiers **[New] (May-2015) [L.J.I.E.T]**
Define IMSI, IMEI and MS-ISDN and write their use**(Nov-2017)[L.J.I.E.T]**
List and explain various addresses and identifiers used in GSM. **[New](May-2017) [L.J.I.E.T]**

ANS:

Various addresses and identifiers used in GSM:
International Mobile Subscriber Identity (IMSI): Each registered user is uniquely identified by its international mobile subscriber identity (IMSI).

→ It is stored in the subscriber identity module (SIM). A mobile station can only be operated if a SIM with valid IMSI is inserted into equipment with a valid IMEI.

→ The following are the parts of IMSI:-
  - Mobile Country Code (MCC):- 3 decimal places, internationally standardized.
  - Mobile Network Code (MNC):- 2 decimal places, for unique identification of mobile network within the country.
  - Mobile Subscriber Identification Number (MSIN):- Maximum 10 decimal places, identification number of the subscriber in the home mobile network.

International Mobile Station Equipment Identity (IMEI): It uniquely identifies a mobile station internationally. It is a kind of serial number.

→ The IMEI is allocated by the equipment manufacturer and registered by the network operator, who stores it in the EIR.

→ By means of IMEI one can recognize obsolete, stolen or non-functional equipment. The following are the parts of an IMEI:
  - Type Approval Code (TAC):- 6 decimal places, centrally assigned.
  - Final Assembly Code (FAC):- 6 decimal places, assigned by the manufacturer.
  - Serial Number (SNR):- 6 decimal places, assigned by the manufacturer.
  - Spare (SP):- 1 decimal place.

Mobile Station International Subscriber Directory Number (MSISDN) (Mobile Station Integrated Services Digital Number): A number used for the international identification of mobile phone numbers.

→ Structure of the MSISDN:
Country Code (CC): of the visited network.
National Destination Code (NDC): of the visited network.
Subscriber Number (SN): in the current mobile network

Mobile station roaming number (MSRN): when a subscriber roaming in another network a temporary ISDN number is assigned to the subscriber that is called as MSRN Number.

→ The MSRN has the same structure as the MSISDN.
Country Code (CC): of the visited network.
National Destination Code (NDC): of the visited network.
Subscriber Number (SN): in the current mobile network.

Location Area Identity Within a PLMN, a Location Area identifies its own authentic Location Area Identity (LAI).

- The LAI hierarchy is based on international standard and structured in a unique format as mentioned below:
  - Country Code (CC): 3 decimal places.
  - Mobile Network Code (MNC): 2 decimal places.
  - Location Area Code (LAC): maximum 5 decimal places or maximum twice 8 bits coded in hexadecimal (LAC < FFFF).

Temporary Mobile Subscriber Identity (TMSI) can be assigned by the VLR, which is responsible for the current location of a subscriber. The TMSI needs to have only local significance in the area handled by the VLR. This is stored on the network side only in the VLR and is not passed to the Home Location Register (HLR). Together with the current location area, the TMSI identifies a subscriber uniquely. It can contain up to 4×8 bits.

Local Mobile Subscriber Identity (LMSI) Each mobile station can be assigned with a Local Mobile Subscriber Identity (LMSI), which is an original key, by the VLR. This key can be used as the auxiliary searching key for each mobile station within its region. It can also help accelerate the database access. An LMSI is assigned if the mobile station is registered with the VLR and sent to the HLR. LMSI comprises of four octets (4x8 bits).

Cell Identifier (CI) Using a Cell Identifier (CI) (maximum 2 × 8) bits, the individual cells that are within an LA can be recognized. When the Global Cell Identity (LAI + CI) calls are combined, then it is uniquely defined.

13 Explain the following in brief in context of GSM networks: **(Summer-2013)[L.J.I.E.T]** 7
(a) Mobile station (b) BSS (c) NSS (d) OSS
(e) IMSI (e) IMEI (f) MSRN

14 How is Mobility Management done in GSM? List the various handovers carried out in GSM and explain any one of them in detail. **(Dec-2012)[L.J.I.E.T]** 7, 8, 7, 7, 7, 7, 7, 7
Explain the handover procedure in GSM system. **[New] (May-2013) [New] (Dec-2013) [New] (June-2014) [New] (Dec-2014) [New] (Dec-2016) [New] (May-2018) [L.J.I.E.T]**
Explain Handoff in detail.**[New](Nov-2016) [L.J.I.E.T]**
What is handoff? Explain its various types. **(Nov-2017)[L.J.I.E.T]**
Ans:

→ The process of handover or handoff within any cellular system is of great importance.
→ It is a critical process and if performed incorrectly handover can result in the loss of the call.
→ Dropped calls are particularly annoying to users and if the number of dropped calls rises, customer dissatisfaction increases and they are likely to change to another network.

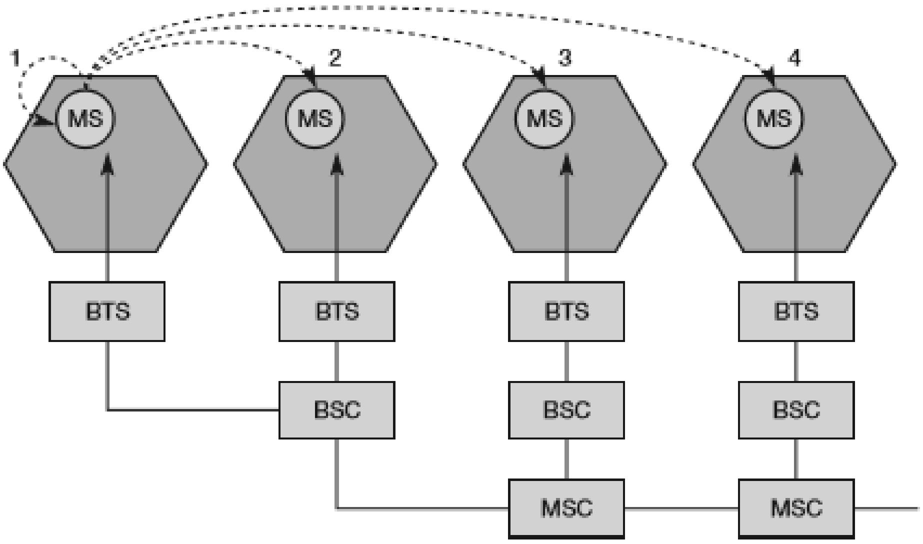
- There are two basic reasons for a handover (about 40 have been identified in the standard):
  - The mobile station moves out of the range of a BTS or a certain antenna of a BTS respectively. The received signal level decreases continuously until it falls below the minimal requirements for communication. The error rate may grow due to interference, the distance to the BTS may be too high (max. 35 km) etc. – all these effects may diminish the quality of the radio link and make radio transmission impossible in the near future.
  - The 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 be due to load balancing.

Types of GSM handover

→ Within the GSM system there are four types of handover that can be performed for GSM only systems:
  - **Intra-BTS handover:** This form of GSM handover occurs if it is required to change the frequency or slot being used by a mobile because of interference, or other reasons.
  - In this form of GSM handover, the mobile remains attached to the same base station transceiver, but change the channel or slot.
  - **Inter-BTS Intra BSC handover:** This GSM handover or GSM handoff occurs when the mobile is moved out of the coverage area of one BTS but into another controlled by the same BSC.
  - In this instance the BSC is able to perform the handover and it assigns a new channel and slot to the mobile, before releasing the old BTS from

communicating with the mobile.

- **Inter-BSC handover:** When the mobile is moved out of the range of cells controlled by one BSC, a more involved form of handover has to be performed, handing over not only from one BTS to another but one BSC to another.
- For this the handover is controlled by the MSC.
- **Inter-MSC handover:** This form of handover occurs when changing between networks. The two MSCs involved negotiate to control the handover.



Example: Figure shows the typical behavior of the received signal level while an MS moves away from one BTS (BTSold) closer to another one (BTSnew). In this case, the handover decision does not depend on the actual value of the received signal level, but on the average value. Therefore, the BSC collects all values (bit error rate and signal levels from uplink and downlink) from BTS and MS and calculates average values. These values are then compared to thresholds, i.e., the handover margin (HO_MARGIN)

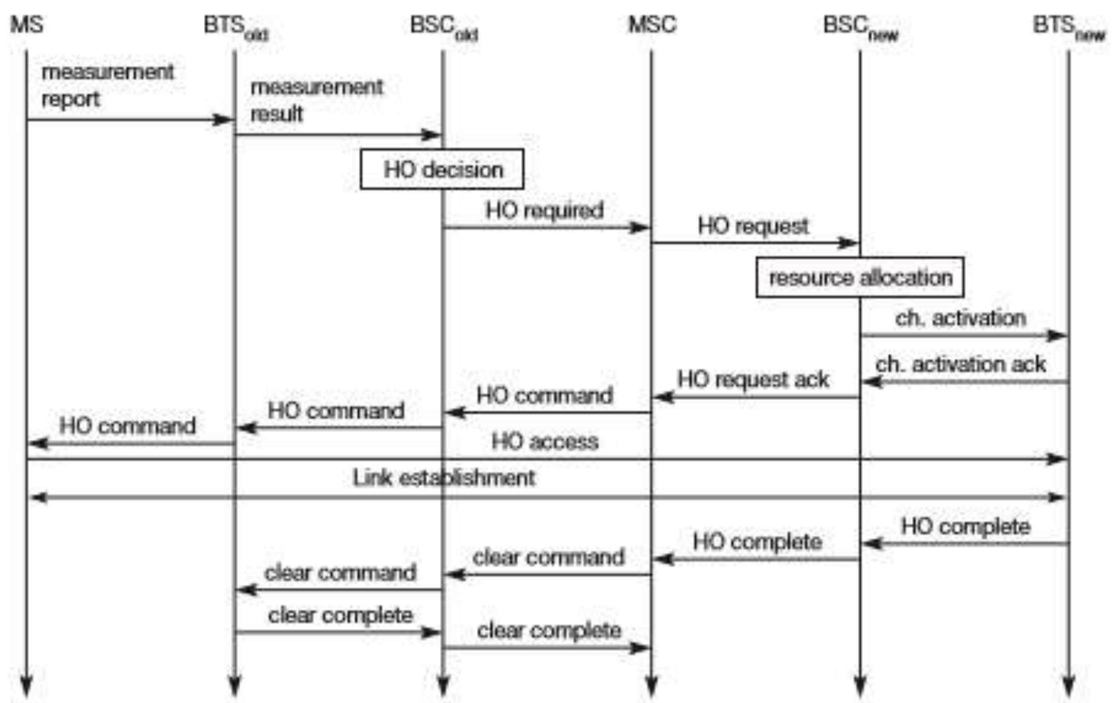


Figure shows the typical signal flow during an inter-BSC, intra-MSC handover.

- The MS sends its periodic measurements reports, the BTSold forwards these reports to the BSCold together with its own measurements. Based on these values and, e.g., on current traffic conditions, the BSCold may decide to perform a handover and sends the message HO_required to the MSC.
- The task of the MSC then comprises the request of the resources needed for the handover from the new BSC, BSCnew. This BSC checks if enough resources (typically frequencies or time slots) are available and activates a physical channel at the BTSnew to prepare for the arrival of the MS.
- The BTSnew acknowledges the successful channel activation, BSCnew acknowledges the handover request. The MSC then issues a handover command that is forwarded to the MS. The MS now breaks its old radio link and accesses the new BTS. The next steps include the establishment of the link (this includes layer two link establishment and handover complete messages from the MS).
- Basically, the MS has then finished the handover, but it is important to release the resources at the old BSC and BTS and to signal the successful handover using the handover and clear complete messages as shown. More sophisticated handover mechanisms are needed for seamless handovers between different systems.
- For example, future 3G networks will not cover whole countries but focus on cities and highways. Handover from, e.g., UMTS to GSM without service interruption must be possible. Even more challenging is the seamless handover between wireless LANs (see chapter 7) and 2G/3G networks. This can be done using multimode mobile stations and a more sophisticated roaming infrastructure. However, it is still not obvious how these

	systems may scale for a large number of users and many handovers, and what handover quality guarantees they can give.	
15	What are the possible handover scenarios in GSM? List out the numbers needed to locate a Mobile Station and to address the Mobile station **(Nov-2011)[L.J.I.E.T]**	7
16	What is handover/handoff? How handoff is different from roaming? **[New] (May-2015) [L.J.I.E.T]** What is handoff and Roaming? Explain the types of handoff in details? **(May-2017)[L.J.I.E.T]**	7, 7
17	What is Handover? Explain GSM Architecture with suitable diagram. **[New] (May-2016) [L.J.I.E.T]**	7
18	**Preprocessing of Call Routing.** **Ans:** **Note: Write "mobile originated call and mobile terminated call procedure" in call routing.** → Human interface is analog. However, the advancement in digital technology makes it very convenient to handle information in digital way. → **Digitizer and source coding:** The user speech is digitized at 8 KHz sampling rate using Regular Pulse Excited–Linear Predictive Coder (RPE–LPC) with a Long Term Predictor loop where information from previous samples is used to predict the current sample. Each sample is then represented in signed 13-bit linear PCM value. This digitized data is passed to the coder with frames of 160 samples where encoder compresses these 160 samples into 260-bits GSM frames resulting in one second of speech compressed into 1625 bytes and achieving a rate of 13 Kbits/sec. → **Channel coding:** This introduces redundancy into the data for error detection and possible error correction where the gross bit rate after channel coding is 22.8 kbps (or 456 bits every 20 ms). These 456 bits are divided into eight 57-bit blocks and the result is interleaved amongst eight successive time slot bursts for protection against burst transmission errors. → **Interleaving:** This step rearranges a group of bits in a particular way to improve the performance of the error-correction mechanisms. The interleaving decreases the possibility of losing whole bursts during the transmission by dispersing the errors. → **Ciphering:** This encrypts blocks of user data using a symmetric key shared by the mobile station and the BTS → **Burst formatting:** It adds some binary information to the ciphered block for use in synchronization and equalization of the received data. → **Modulation:** The modulation technique chosen for the GSM system is the Gaussian Minimum Shift Keying (GMSK) where 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. → **Multipath and equalization:** An equalizer is in charge of extracting the 'right' signal from the received signal while estimating the channel impulse response of the GSM system and then it constructs an inverse filter. The received signal is then passed through the inverse filter.	7, 7, 7, 7, 7, 7

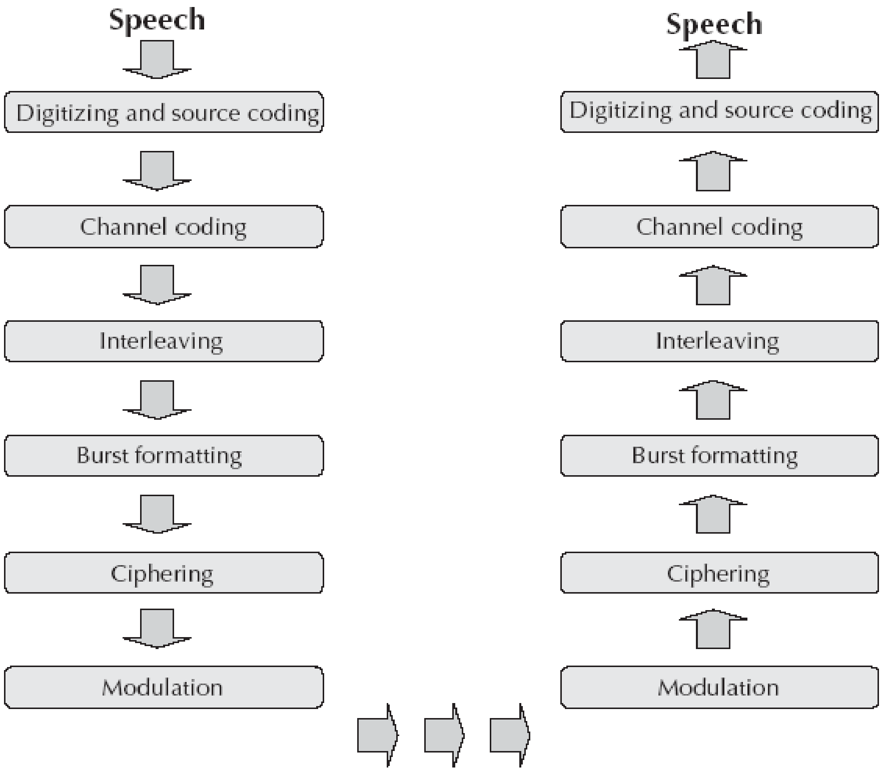


Figure 8: From speech to radio waves

→ **Synchronization:** For successful operation of a mobile radio system, time and frequency synchronization are needed. Frequency synchronization is necessary so that the transmitter and receiver frequency match (in FDMA) while Time synchronization is necessary to identify the frame boundary and the bits within the frame (in TDMA). To avoid collisions of burst transmitted by MS with the adjacent timeslot such collisions, the Timing Advance technique is used where frame is advanced in time so that this offsets the delay due to greater distance.

→ Using this technique and the triangulation of the intersection cell sites, the location of a mobile station can be determined from within the network.

Example

→ The MSISDN number of a subscriber in Bangalore associated with Airtel network is +919845XYYYYY which is a unique number and understood from anywhere in the world.

→ Here, + means prefix for international dialing, 91 is the country code for India and 45 is the network operator's code (Airtel in this case).

→ X is the level number managed by the network operator ranging from 0 to 9 while YYYYY is the subscriber code which, too, is managed by the operator.

→ The call first goes to the local PSTN exchange where PSTN exchange looks at the routing table and determines that it is a call to a mobile network.

→ PSTN forwards the call to the Gateway MSC (GMSC) of the mobile network.

→ MSC enquires the HLR to determine the status of the subscriber. It will decide whether the call is to be routed or not. If MSC finds that the call can be processed, it will find out the address of the VLR where the mobile is expected to be present.

→ If VLR is that of a different PLMN, it will forward the call to the foreign PLMN through the Gateway MSC. If the VLR is in the home network, it will determine the Location Area (LA).

→ Within the LA, it will page and locate the phone and connect the call.

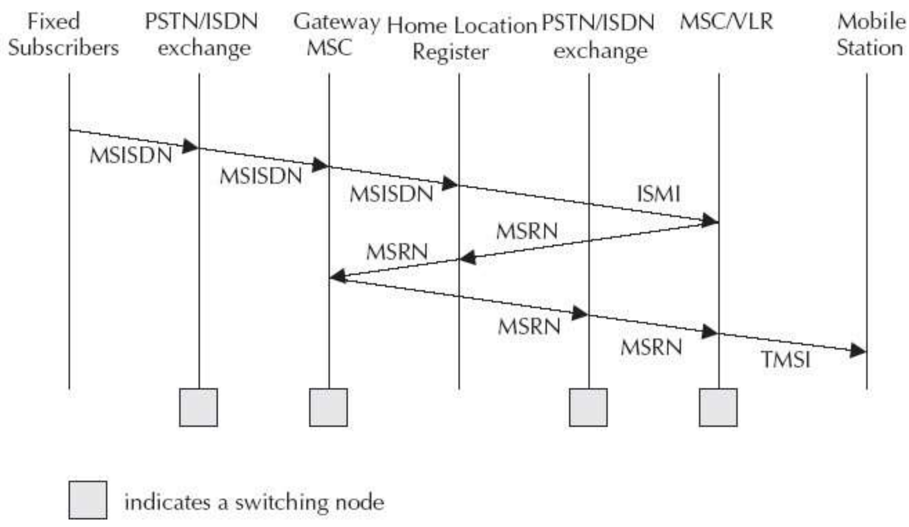


Figure 9: Call Routing for a mobile terminating call

19 Explain Call routing in GSM with block diagram. **[New] (June-2014)[L.J.I.E.T]** 7
Explain Call routing in GSM. **(Summer-2014) [New] (Dec-2016) [L.J.I.E.T]** ,
What is GSM? Explain how a call is routed in GSM with diagram**. [New] (Dec-2015)[L.J.I.E.T]**
Explain Call routing in GSM network. **(Winter-2015)[L.J.I.E.T]** 7
Explain routing in mobile network. **(Winter-2015) [L.J.I.E.T]** ,
Explain mobile originated call and mobile terminated call procedure. **[New] (Winter-2012) [L.J.I.E.T]** 7
Explain call routing for a mobile terminating call. **(Winter-2013)[L.J.I.E.T]**
Draw and Explain Call routing for a mobile terminating call in GSM.**(Winter-2014)[L.J.I.E.T]**

- All these numbers are needed to find a subscriber and to maintain the connection with a mobile station. The interesting case is the mobile terminated call (MTC), i.e., a situation in which a station calls a mobile station (the calling station could be outside the GSM network or another mobile station).
- Figure 4.8 shows the basic steps needed to connect the calling station with the mobile user.
- In step,
  1. a user dials the phone number of a GSM subscriber.
  2. The fixed network (PSTN) notices (looking at the destination code) that the number belongs to a user in the GSM network and forwards the call setup to the Gateway MSC
  3. The GMSC identifies the HLR for the subscriber (which is coded in the phone number) and signals the call setup to the HLR
  4. The HLR now checks whether the number exists and whether the user has subscribed to the requested services, and requests an MSRN from the current VLR
  5. After receiving the MSRN
  6. the HLR can determine the MSC responsible for the MS and forwards this information to the GMSC
  7. The GMSC can now forward the call setup request to the MSC indicated.
  8. From this point on, the MSC is responsible for all further steps. First, it requests the

current status of the MS from the VLR.
9. If the MS is available, the MSC initiates paging in all cells it is responsible for (i.e. the location area, LA.
10. as searching for the right cell would be too time consuming (but this approach puts some load on the signaling channels so optimizations exist). The BTSs of all BSSs transmit this paging signal to the MS
11. If the MS answers (12 and 13), the VLR has to perform security checks (set up encryption etc.). The VLR then signals to the MSC to set up a connection to the MS

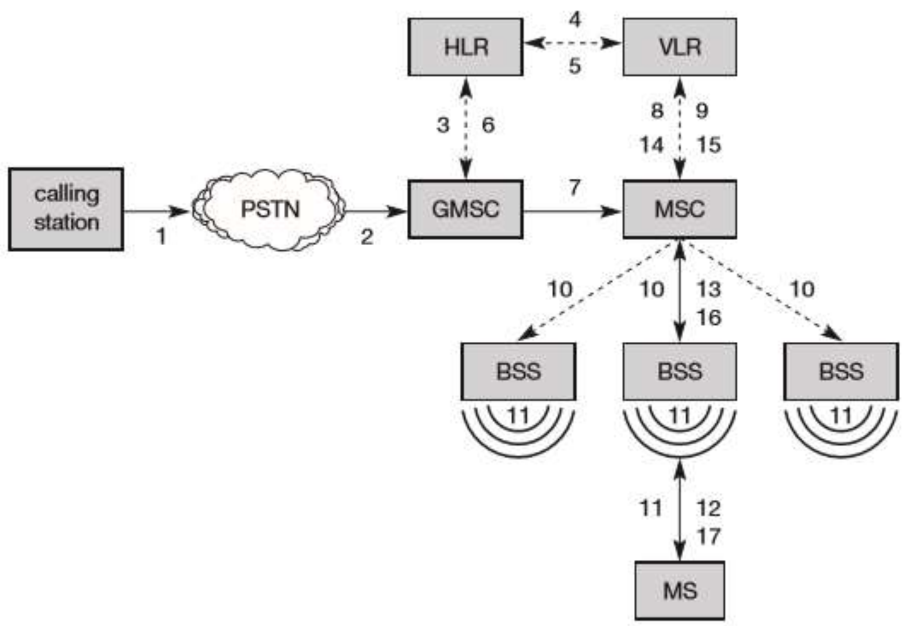


Figure 4.8 Mobile terminated call (MTC)

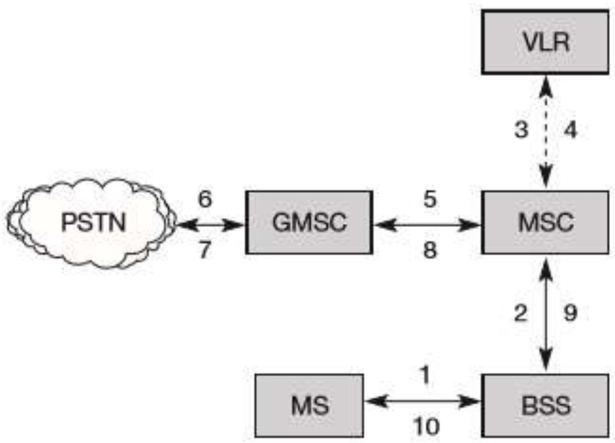


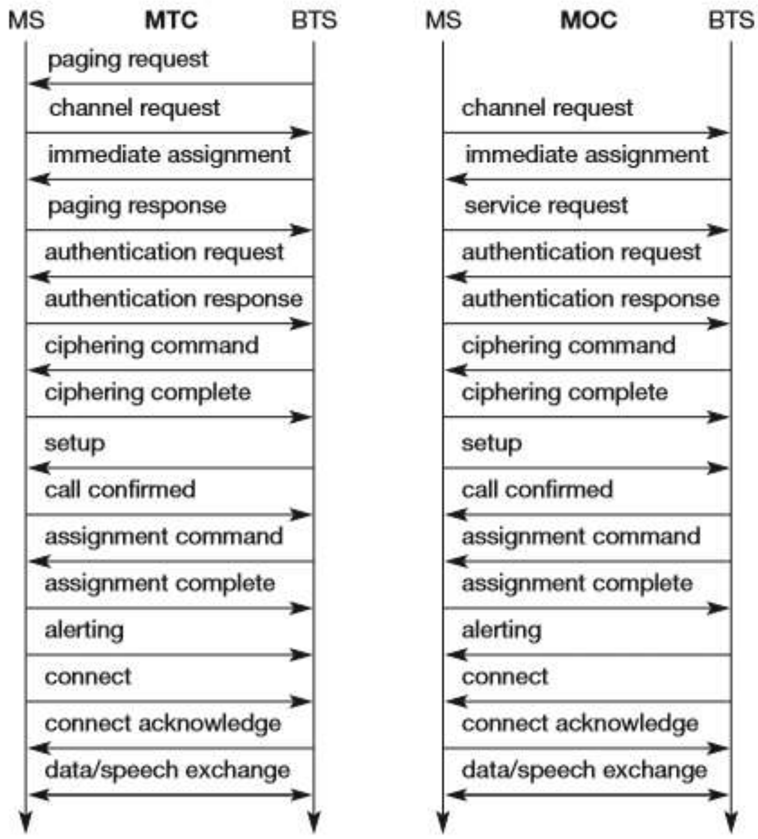
Figure 4.9 Mobile originated call (MOC)

mobile originated call (MOC):
- It is much simpler to perform a mobile originated call (MOC) compared to a MTC (see Figure 4.9).
  1. The MS transmits a request for a new connection.
  2. the BSS forwards this request to the MSC
  3. The MSC then checks if this user is allowed to set up a call with the requested service (3 and 4) and checks the availability of resources through the GSM network and into the PSTN.

4. If all resources are available, the MSC sets up a connection between the MS and the fixed network.

- In addition to the steps mentioned above, other messages are exchanged between an MS and BTS during connection setup (in either direction).
- These messages can be quite often heard in radios or badly shielded loudspeakers as crackling noise before the phone rings.
- Figure 4.10 shows the messages for an MTC and MOC. Paging is only necessary for an MTC, then similar message exchanges follow.
- The first step in this context is the channel access via the random access channel (RACH) with consecutive channel assignment; the channel assigned could be a traffic channel (TCH) or a slower signalling channel SDCCH.
- The next steps, which are needed for communication security, comprise the authentication of the MS and the switching to encrypted communication. The system now assigns a TCH (if this has not been done).
- This has the advantage of only having to use an SDCCH during the first setup steps. If the setup fails, no TCH has been blocked. However, using a TCH from the beginning has a speed advantage.
- The following steps depend on the use of MTC or MOC. If someone is calling the MS, it answers now with ‘alerting’ that the MS is ringing and with ‘connect’ that the user has pressed the connect button.
- The same actions happen the other way round if the MS has initiated the call. After connection acknowledgement, both parties can exchange data. Closing the connection comprises a user-initiated disconnect message (both sides can do this), followed by releasing the connection and the radio channel.

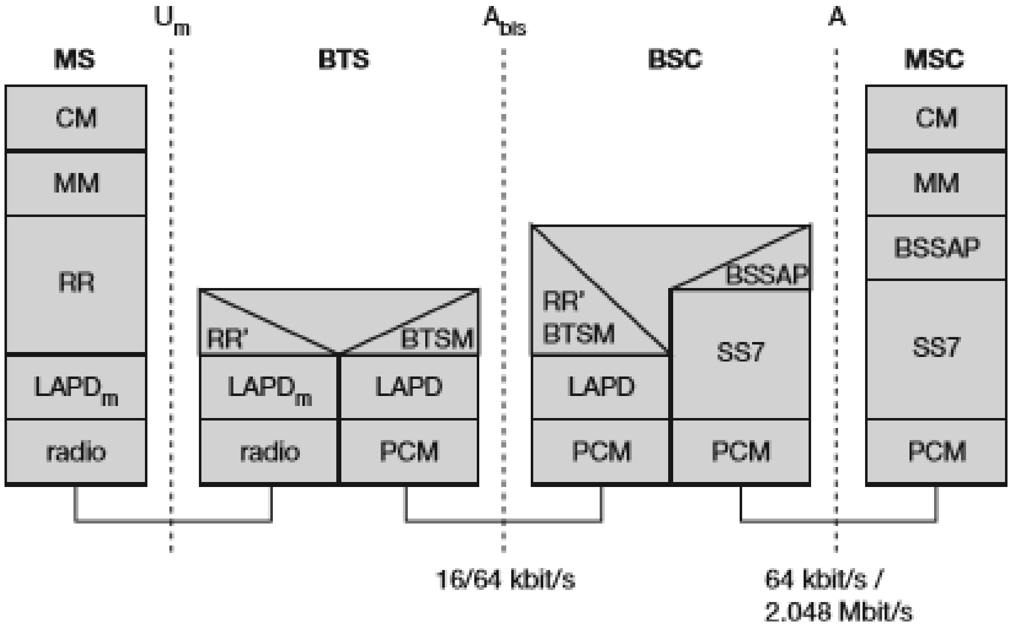
Figure 4.10
Message flow for MTC and MOC



2(	What are HLR and VLR? Describe its functions in call routing and roaming. **(June-2012) (May-2018) [L.J.I.E.T]**	7 ,

	Explain the functionality of HLR and VLR in call routing. **[New] (Dec-2015)[L.J.I.E.T]** **HLR:** It is a kind of distributed database, There is only one HLR per GSM network. The HLR contains only the administrative information of each subscriber registered in the GSM network. It includes information like 1. Authentication information like IMSL number. 2. Identification information like name, address, etc. of the subscriber. 3. Identification information like MSISDN 4. Billing information like prepaid or postpaid. 5. Operator selected denial of service to a subscriber. 6. Handling of supplementary service like for CFU (Call Forwarding Unconditional) CFB (Call Forwarding Busy) CFNR (Call Forwarding Not Reachable) CFNA (Call Forwarding Not Answered) 7. Storage of SMS service (SC) number in case the mobile is not connectable so that whenever the mobile is connectable, a paging signal is sent to the SC. 8. Provisioning information like whether long distance and international calls allowed or not. 9. Provisioning information like whether roaming is enables or not. 10. Information related to auxiliary services like voice mail, data, fax services etc. 11. Information related to supplementary services for call routing.	4, 7
21	Explain Different types of GSM Channels. **[New] (Winter-2012)[L.J.I.E.T]** The physical separation of the medium into 8*124 duplex channels, GSM specifies two basic groups of logical channels, i.e., traffic channels and control channels: • **Traffic channels (TCH):** o GSM uses a TCH to transmit user data (e.g., voice, fax). Two basic categories of TCHs have been defined, i.e., full-rate TCH (TCH/F) and half-rate TCH (TCH/H). o A TCH/F has a data rate of 22.8 kbit/s, whereas TCH/H only has 11.4 kbit/s. Improved codes allow for better voice coding and can use a TCH/H. Using these TCH/HSs doubles the capacity of the GSM system for voice transmission. However, speech quality decreases with the use of TCH/HS and many providers try to avoid using them. o The standard codecs for voice are called full rate (FR, 13 kbit/s) and half rate (HR, 5.6 kbit/s). A newer codec, enhanced full rate (EFR), provides better voice quality than FR as long as the transmission error rate is low. An additional increase in voice quality is provided by the so-called tandem free operation (TFO). This mode can be used if two MSs exchange voice data. o In this case, coding to and from PCM encoded voice (standard in ISDN) can be skipped and the GSM encoded voice data is directly exchanged. o Data transmission in GSM is possible at many different data rates, e.g., TCH/F4.8 for 4.8 kbit/s, TCH/F9.6 for 9.6 kbit/s, and, as a newer specification, TCH/F14.4 for 14.4 kbit/s. These logical channels differ in terms of their coding schemes and error correction capabilities. • **Control channels (CCH):** o Many different CCHs are used in a GSM system to control medium access, allocation of traffic channels or mobility management. o Three groups of control channels have been defined, each again with sub-channels ● **Broadcast control channel (BCCH):** A BTS uses this channel to signal	7

	information to all MSs within a cell. Information transmitted in this channel is, e.g., the cell identifier, options available within this cell (frequency hopping), and frequencies available inside the cell and in neighbouring cells. The BTS sends information for frequency correction via the frequency correction channel (FCCH) and information about time synchronization via the synchronization channel (SCH), where both channels are sub channels of the BCCH. ● **Common control channel (CCCH):** All information regarding connection setup between MS and BS is exchanged via the CCCH. For calls toward an MS, the BTS uses the paging channel (PCH) for paging the appropriate MS. If an MS wants to set up a call, it uses the random access channel (RACH) to send data to the BTS. The RACH implements multiple access (all MSs within a cell may access this channel) using slotted Aloha. This is where a collision may occur with other MSs in a GSM system. The BTS uses the access grant channel (AGCH) to signal an MS that it can use a TCH or SDCCH for further connection setup. ● **Dedicated control channel (DCCH):** While the previous channels have all been unidirectional, the following channels are bidirectional. As long as an MS has not established a TCH with the BTS, it uses the stand-alone dedicated control channel (SDCCH) with a low data rate (782 bit/s) for signaling. This can comprise authentication, registration or other data needed for setting up a TCH. Each TCH and SDCCH has a slow associated dedicated control channel (SACCH) associated with it, which is used to exchange system information, such as the channel quality and signal power level. Finally, if more signaling information needs to be transmitted and a TCH already exists, GSM uses a fast associated dedicated control channel (FACCH). The FACCH uses the time slots which are otherwise used by the TCH. This is necessary in the case of handovers where BTS and MS have to exchange larger amounts of data in less time.	
22	Write Note on Signaling Protocol Structure in GSM**. [New] (Dec-2014)[L.J.I.E.T]** Figure shows the protocol architecture of GSM with signaling protocols, interfaces, as well as the entities already shown in Figure. The main interest lies in the Um interface, as the other interfaces occur between ntities in a fixed network. • **Layer 1, the physical layer**, handles all radio-specific functions. This includes the creation of bursts according to the five different formats, multiplexing of bursts into a TDMA frame, synchronization with the BTS, detection of idle channels, and measurement of the channel quality on the downlink.	7



- The physical layer at Um uses GMSK for digital modulation and performs encryption/decryption of data, i.e., encryption is not performed end-to-end, but only between MS and BSS over the air interface. Synchronization also includes the correction of the individual path delay between an MS and the BTS. All MSs within a cell use the same BTS and thus must be synchronized to this BTS. The BTS generates the time-structure of frames, slots etc. A problematic aspect in this context are the different round trip times (RTT). An MS close to the BTS has a very short RTT, whereas an MS 35 km away already exhibits an RTT of around 0.23 ms.
- The main tasks of the physical layer comprise channel coding and error detection/correction, which is directly combined with the coding mechanisms. Channel coding makes extensive use of different forward error correction (FEC) schemes. FEC adds redundancy to user data, allowing for the detection and correction of selected errors. The power of an FEC scheme depends on the amount of redundancy, coding algorithm and further interleaving of data to minimize the effects of burst errors. The FEC is also the reason why error detection and correction occurs in layer one and not in layer two as in the ISO/OSI reference model.
- The GSM physical layer tries to correct errors, but it does not deliver erroneous data to the higher layer. Different logical channels of GSM use different coding schemes with different correction capabilities. In GSM, the physical layer also contains special functions, such as voice activity detection (VAD), which transmits voice data only when there is a voice signal.
- **In GSM, Data link Layer:** Signaling between entities in a GSM network requires higher layers (see Figure). For this purpose, the LAPDm protocol has been defined at the Um interface for layer two.
- LAPDm, as the name already implies, has been derived from link access procedure for the D-channel (LAPD) in ISDN systems, which is a version of HDLC (Goodman, 1997), (Halsall, 1996). LAPDm is a lightweight LAPD because it does not need synchronization flags or checksumming for error detection. (The GSM physical layer already performs these tasks.) LAPDm offers reliable data transfer over connections, re-sequencing of data frames, and flow control. As there is no buffering between layer one and two, LAPDm has to obey the frame structures, recurrence patterns etc. defined for the Um interface. Further services provided by LAPDm include segmentation and reassembly of data and

acknowledged/unacknowledged data transfer.

- **The network layer** in GSM, layer three, comprises several sublayers as Figure shows. The lowest sublayer is the radio resource management (RR). Only a part of this layer, RR’, is implemented in the BTS, the remainder is situated in the BSC. The functions of RR’ are supported by the BSC via the BTS management (BTSM).
- The main tasks of RR are setup, maintenance, and release of radio channels. RR also directly accesses the physical layer for radio information and offers a reliable connection to the next higher layer.
- Mobility management (MM) contains functions for registration, authentication, identification, location updating, and the provision of a temporary mobile subscriber identity (TMSI) that replaces the international mobile subscriber identity (IMSI) and which hides the real identity of an MS user over the air interface. While the IMSI identifies a user, the TMSI is valid only in the current location area of a VLR. MM offers a reliable connection to the next higher layer.
- Call management (CM) layer contains three entities: call control (CC), short message service (SMS), and supplementary service (SS). SMS allows for message transfer using the control channels SDCCH and SACCH (if no signaling data is sent), CC provides a point-to-point connection between two terminals and is used by higher layers for call establishment, call clearing and change of call parameters.

23 Explain: Handover, Authentication and Security in GSM. **(Summer-2014) (Winter-2015) (May 2018) [L.J.I.E.T]** 7, 7, 4

Authentication and Security:

GSM offers several security services using confidential information stored in the AuC and in the individual SIM (which is plugged into an arbitrary MS). The SIM stores personal, secret data and is protected with a PIN against unauthorized use. (For example, the secret key Ki used for authentication and encryption procedures is stored in the SIM.) The security services offered by GSM are explained below:

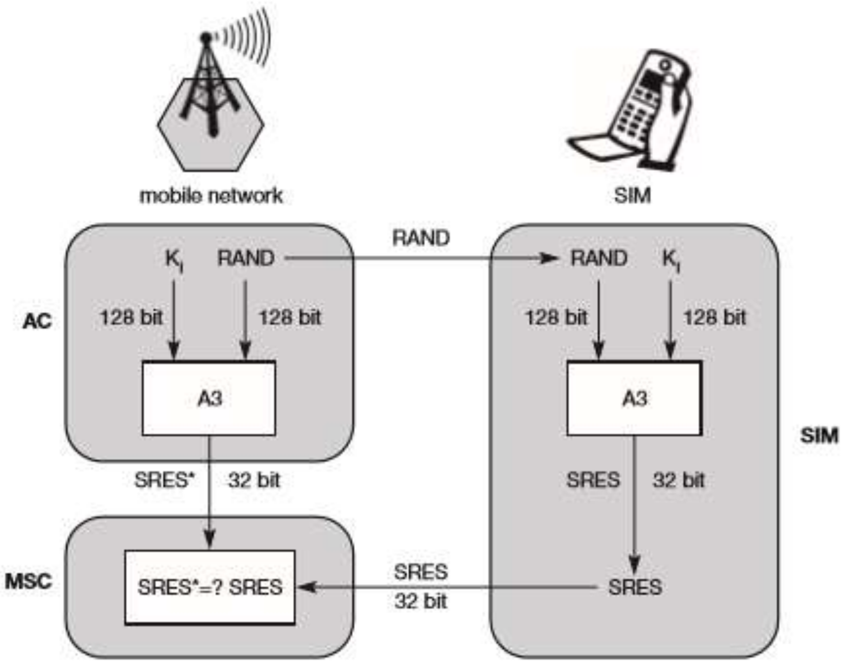
● **Access control and authentication:** The first step includes the authentication of a valid user for the SIM. The user needs a secret PIN to access the SIM. The next step is the subscriber authentication. This step is based on a challenge-response scheme.

● **Confidentiality:** All user-related data is encrypted. After authentication, BTS and MS apply encryption to voice, data, and signaling. This confidentiality exists only between MS and BTS, but it does not exist end-to-end or within the whole fixed GSM/telephone network.

● **Anonymity:** To provide user anonymity, all data is encrypted before transmission, and user identifiers (which would reveal an identity) are not used over the air. Instead, GSM transmits a temporary identifier (TMSI), which is newly assigned by the VLR after each location update. Additionally, the VLR can change the TMSI at any time.

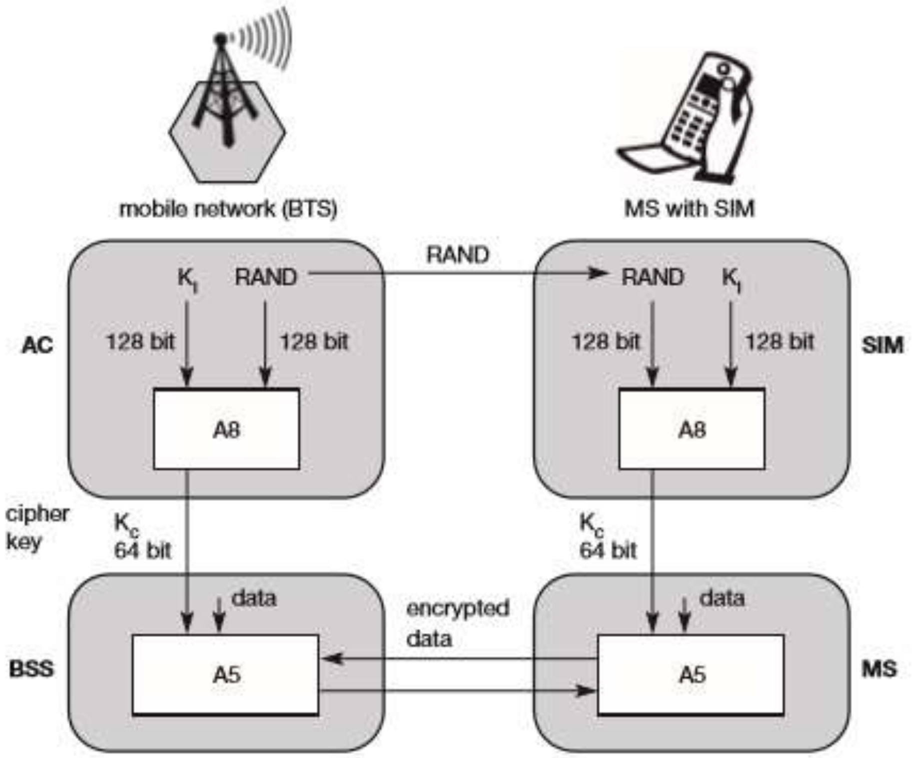
Three algorithms have been specified to provide security services in GSM.

- Algorithm A3 is used for authentication, A5 for encryption, and A8 for the generation of a cipher key.
- In the GSM standard only algorithm A5 was publicly available, whereas A3 and A8 were secret, but standardized with open interfaces. Algorithms A3 and A8 (or their replacements) are located on the SIM and in the AuC and can be proprietary. Only A5 which is implemented in the devices has to be identical for all providers.



- **Authentication [A3 Algorithm]:** Before a subscriber can use any service from the GSM network, he or she must be authenticated. Authentication is based on the SIM, which stores the individual authentication key Ki, the user identification IMSI, and the algorithm used for authentication A3.
- Authentication uses a challenge-response method: the access control AC generates a random number RAND as challenge, and the SIM within the MS answers with SRES (signed response) as response (see Figure). The AuC performs the basic generation of random values RAND, signed responses SRES, and cipher keys Kc for each IMSI, and then forwards this information to the HLR. The current VLR requests the appropriate values for RAND, SRES, and Kc from the HLR. For authentication, the VLR sends the random value RAND to the SIM. Both sides, network and subscriber module, perform the same operation with RAND and the key Ki, called A3. The MS sends back the SRES generated by the SIM; the VLR can now compare both values. If they are the same, the VLR accepts the subscriber, otherwise the subscriber is rejected.

- **Encryption [Algorithm A8- Cipher key generation and Algorithm A5- Encryption]:** To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface. After authentication, MS and BSS can start using encryption by applying the cipher key Kc (the precise location of security functions for encryption, BTS and/or BSC are vendor dependent). Kc is generated using the individual key Ki and a random value by applying the algorithm A8. Note that the SIM in the MS and the network both calculate the same Kc based on the random value RAND. The key Kc itself is not transmitted over the air interface.
- MS and BTS can now encrypt and decrypt data using the algorithm A5 and the cipher key Kc. As Figure shows, Kc should be a 64 bit key – which is not very strong, but is at least a good protection against simple eavesdropping. However, the publication of A3 and A8 on the internet showed that in certain implementations 10 of the 64 bits are always set to 0, so that the real length of the key is thus only 54 consequently, the encryption is much weaker.



24 Give six functions where CDMA is different from GSM. **(June-2012)[L.J.I.E.T]** 6,7,7,3,7,7,7,7
Differentiate CDMA technology and GSM technology. **[New] (Winter-2012)[L.J.I.E.T]**
Give six functional differences between CDMA and GSM. **(Summer-2013)[L.J.I.E.T]**
List and discuss at least seven functions where CDMA is different from GSM**. [New] (Dec- 2013) [L.J.I.E.T]**
Compare : CDMA and GSM**(Summer-2014) (Winter-2015) (May-2016) (Nov-2017) [L.J.I.E.T]**

Parameters	GSM	CDMA
Stands for	Global System for Mobile Communication	Code Division Multiple Access
Storage Type	SIM (subscriber identity module) Card	Internal Memory
Signal quality/coverage area	Good coverage indoors on 850/900 MHz. Repeaters possible. 35 km hard limit.	Unlimited cell size, low transmitter power permits large cells
Technology	Time-division multiple access (TDMA) and Frequency-division multiple access (FDMA).	CDMA
Voice and Data at the same time	Yes GPRS Class A	No
Security	GSM technology allows various people to access the same connection, hence it makes it less safer compared to CDMA.	Higher security is provided on this network as it is inbuilt with encryption. Each person has a unique code.
Data Transfer Rate	GSM has a maximum download speed of 384 kbps.	CDMA has a maximum download speed of 2 mbps.
Carrier (Channel) spacing	200 kHz	1.25 kHz

Time Slot in Full Rate Frames	8 TS	64 TS
Time Slot in Half Rate Frames	16 TS	128 TS
Uplink Frequency	890-915 MHz	824-849 MHz
Downlink Frequency	935-960 MHz	869-894 MHz
Carrier (Channel) total bit rate	270.833 kbps	1228.8 kbps
Modulation Technique	GMSK	QPSK / BPSK
Handoff	Hard	Soft
Economy	Expensive	Lower than GSM
System capacity	Fixed and limited	Flexible and Higher than GSM