UNIT III - MOBILE NETWORK LAYER

Mobile IP – DHCP – AdHoc– Proactive protocol-DSDV, Reactive Routing Protocols – DSR, AODV , Hybrid routing –ZRP, Multicast Routing- ODMRP, Vehicular Ad Hoc networks (VANET) –MANET Vs VANET – Security.

PART - A

1. What is the key mechanism in mobile IP? [Nov 2018]

- **Agent Discovery** - A Mobile Node discovers its Foreign and Home Agents during agent discovery.
- **Registration** - The Mobile Node registers its current location with the Foreign Agent and Home Agent during registration.
- **Tunnelling** - A reciprocal tunnel is set up by the Home Agent to the care-of address (current location of the Mobile Node on the foreign network) to route packets to the Mobile Node as it roams.

2. State the purpose of Home Location Register (HLR). [Nov 2018]

- The Home Location Register (HLR) is the main database of permanent subscriber information for a mobile network.
- The HLR is an integral component of CDMA (code division multiple access), TDMA (time division multiple access), and GSM (Global System for Mobile communications) networks.

3. What is the purpose of DHCP? [Apr 2018]

- DHCP's purpose is to enable individual computers on an IP network to extract their configurations from a server (the DHCP server) or servers, in particular, servers that have no exact information about the individual computers until they request the information.
- The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.

4. What is the purpose of agent solicitation message? [Apr 2018]

- In case a mobile node (MN) does not receive any COA, then the MN should send an agent solicitation message. But it is important to monitor that these agent solicitation messages do not flood the network.
- A mobile node can usually send up to three solicitation messages (one per second) as soon as it enters a new network. The basic purpose of the solicitation messages sent by a mobile node (MN) is to search for a foreign agent (FA).
- For a highly dynamic wireless network in which MNs move at great speed, even a time interval of the order of a second between these messages is too long.
- If an MN does not receive any address in response to its solicitation messages, then to avoid network flooding, the MN should exponentially reduce the rate of sending the solicitation messages.

5. To which layer do each of the following protocols belong to? What is their functionality? RARP, DNS [Nov 2017]

RARP (Reverse Address Resolution Protocol):
The RARP protocol is used by IP to find the IP address based on the physical (MAC address) address of a computer.
DNS: It stands for **D**omain **N**ame **S**ystem (or **S**ervice or **S**erver).
It is a software service available on the Internet that is responsible for translating domain names into IP addresses.

6. Differentiate the functionalities of a foreign agent and home agent. [Nov 2017]

Foreign Agent (FA):
The foreign agent is a router in a foreign network that functions as the point of attachment for a mobile node when it roams to the foreign network. The packets from the home agent are sent to the foreign node which delivers it to the mobile node.
Home Agent (HA):
It is located in home network and it provides several services for the MN. HA maintains a location registry. The location registry keeps track of the node locations using the current care-of-address of the MN.

7. What is Route Optimization? [May 2017]

- Route Optimization is the process of determining the most cost-efficient route.
- It's more complex than simply finding the shortest path between two points.
- It needs to include all relevant factors such as the number and location of all the required stops on the route.

8. List the modifications proposed in single-hop and multi-hop wireless network. [May 2017]

Single hop network:
In a single hop network , when a packet leaves the source it just takes a single hop (goes through another network or you can say it passes through another router from a different network) before reaching its destination address.
Multi-hop network:
In a multi-hop network a packet has to go through 2 or more networks in order to reach its destination address.
While taking a hop through a different network a packet may go through various devices like Routers, network bridges, switches, etc.

9. Define COA. [Nov 2016]

- Used in Internet routing, a care-of address (usually referred to as *CoA*) is a temporary IP address for a mobile device.
- This allows a home agent to forward messages to the mobile device.
- A separate address is required because the IP address of the device that is used as host identification is topologically incorrect - it does not match the network of attachment.

- The care-of address splits the dual nature of an IP address, that is, its use is to identify the host and the location within the global IP network.

10. Illustrate the use of BOOTP protocol? [Nov 2016]

The BOOTP protocol is used for booting (starting) computers from the network. These are popularly used in case of diskless computers. Whenever a client requests an IP address from the server machine, BOOTP searches a table which matches to its physical address.

11. What is DHCP? [May 2016]

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network.

12. What is encapsulation in mobile IP? [May 2016]

- Encapsulation describes the process of placing an IP datagram inside a network packet or frame.
- Encapsulation refers to how the network interface uses packet switching hardware

13. Define Tunnelling with its functions?

- The packet is forwarded by the home agent to the foreign agent. When the packet comes to the foreign agent (care-of-address), it delivers the packet to the mobile node. This process is called **tunnelling.**
- Tunnelling has two primary functions:
  1. Encapsulation of the data packet to reach the tunnel endpoint,
  2. Decapsulation when the packet is delivered at that endpoint.

14. Define Care-Of-Address (COA) with its types?

- **Care-of-Address (COA):** It is the address that is used to identify the present location of a foreign agent. The packets sent to the MN are delivered to COA.
- The COA can be any of the following two types:
  (a) Foreign agent COA: The COA is an IP address of foreign agent (FA).
  (b) Co-located COA: When the mobile node (MN) acquires a temporary IP address, that address acts as the COA.

15. Define Agent Discovery and its discovery methods?

- **Agent Discovery:** During call establishment it is necessary for a mobile node to determine its foreign agent. This task is referred to as **agent discovery.**
- The following two discovery methods are popularly used:
  (1) Agent advertisement and (2) Agent solicitation.

16. Describe some of the features of Mobile IP

- **Transparency:** The IP address is to be managed transparently and there should not be any effect of mobility on any ongoing communication.

- **Compatibility:** Mobile IP should be compatible with the existing Internet protocols.
- **Security:** Mobile IP should, as far as possible, provide users with secure communications over the Internet.
- **Efficiency and Scalability:** In the event of worldwide support, there can be a large number of mobile systems in the whole Internet. It should also be scalable to support billions of moving hosts worldwide.

17. What are the key mechanisms followed by Mobile IP?

- Mobile IP is associated with the following three basic mechanisms:
  1. Discovering the care-of-address
  2. Registering the care-of-address
  3. Tunnelling to the care-of-address

18. Mention the two main design issues of MANET? [Nov 2018]

- Network size and node density
- Connectivity
- Network topology
- User traffic
- Operational environment
- Energy constraint

19. What are the important steps in destination sequence distance vector routing? [Nov 2018]

- Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman–Ford algorithm.
- The main contribution of the algorithm was to solve the routing loop problem.
- Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present; else, an odd number is used.
- The number is generated by the destination, and the emitter needs to send out the next update with this number.
- Routing information is distributed between nodes by sending *full dumps* infrequently and smaller incremental updates more frequently.

20. Compare VANET and MANET? [Apr 2018]

- MANET is the short form of Mobile AdHoc Network. In ad-hoc networks all the nodes are mobile in nature and hence they can be interfaced dynamically in arbitrary fashion.
- While VANET is the short form of Vehicular Adhoc Network. It is sub-class of network of MANET type.

21. Differentiate cellular with adhoc networks? [Apr 2018]

Parameters	Cellular network	Ad Hoc network

Network routing	Centralized, all the traffic goes through the Base Station	Distributed, No centralized system such as Base station needed
Switching Type	Circuit Switching	Packet Switching
Number of Hops	single hop type	Multiple hops
Topology	Star	Mesh
Application	Designed and developed for voice traffic	Designed to meet best effort data traffic requirements
Cost and time for installation	Higher cost and takes more time for deployment	Lower cost and does not take more time for deployment
Call drops	Low call drops during mobility due to seamless connectivity across region	Higher breaks in the path during mobility
Network maintenance	requires periodic maintenance and hence it is costly.	nodes are self organising and hence it is less costly.
Frequency re-use	It utilizes same frequency channels in the nearby cells with proper RF planning and antenna placement. This is known as static frequency re-use.	Dynamic frequency re-use is employed using carrier sense mechanism.
Bandwidth (BW) mechanism	The allocation of BW is guaranteed and easy.	The allocation of BW is based on shared channel using complex MAC algorithms.
Technologies	IS-95, IS-136, GSM, Mobile WiMAX, CDMA, LTE	WLAN 802.11e

22. List the applications of MANET's. [May 2017]

- Communication among portable computers
- Environmental monitoring
- Military

- Emergency applications

23. Distinguish proactive and reactive protocols. [May 2017]

Proactive: A table -driven approach, follows a static route through out the lifetime.
Reactive: Dynamically changes the Routing decisions based on the present network conditions.

24. Compare AODV and DSR protocols. [Nov 2017]

- Adhoc on-demand routing protocol (AODV) and Dynamic Source Routing (DSR) under different performance metrics like throughput, packet drop rate and end-to-end delay.
- AODV protocol is better than DSR protocol as the nodes are increasing/adding to network. Packet drop rate and end-to-end delay of AODV protocol is less than DSR protocol as the nodes are increasing.

25. What are the contents of Link state Advertisement message?[Nov 17]

A link state advertisement message contains:

- The identity of the router originating the message.
- The identities of all its neighbours.
- The delays along various links to its neighbours.

26. Outline the concept of RTT? [Nov 2016]

- Round-trip time (RTT), also called round-trip delay, is the time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.
- In this context, the source is the computer initiating the signal and the destination is a remote computer or system that receives the signal and retransmits it.

27. Compare and contrast MANET Vs VANET [Nov 2016]
Compare MANET Vs VANET. [May 2016]

- These networks are used for communication between following: between vehicles and road-side infrastructure.
- MANET is the short form of Mobile AdHoc Network. In ad-hoc networks all the nodes are mobile in nature and hence they can be interfaced dynamically in arbitrary fashion.
- **VANET** is the short form of Vehicular Adhoc Network. It is subclass of network of MANET type. In VANET, the communication nodes are moving on pre-defined roads as finalized initially.

28. List the characteristics of MANETs. [May 2016]

- In MANET, each node act as both host and router. That is it is autonomous in behavior.
- Mobile nodes are characterized with less memory, power and light weight features.
- The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.

- All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
- High user density and large level of user mobility.
- Nodal connectivity is intermittent.

29. What is Adhoc Network?

Adhoc network is defined as a set of mobile devices can communicate with each other in the **absence of** any form of fixed networking infrastructures such as **hubs, routers, base stations**, etc.

30. What is Mobile Adhoc Network?

A MANET is a collection of mobile nodes that communicate with each other over bandwidth constrained wireless links without any infrastructure support.

31. What are the characteristics of MANET?

- Lack of fixed infrastructure
- Dynamic topologies
- Bandwidth constrained, variable capacity links
- Energy constrained operation
- Increased vulnerability

32. What are the types of traffic?

The common traffic types are the following:

- Bursty traffic
- Large packets sent periodically
- Combination of the above two types of traffic

33. What are the three important ways in which a MANET routing protocol differs from routing of packets in a traditional network?

1. In a MANET, each node acts as a router, whereas ordinary nodes in a traditional wired network do not participate in routing the packets.
2. In a MANET, the topology is dynamic because of the mobility of the nodes, but it is static in the case of traditional networks. Thus, the routing tables in a MANET quickly become obsolete, making the routing process complicated.
3. In the simple IP-based addressing scheme deployed in wired networks, the IP address encapsulated in the subnet structure does not work because of node mobility.

34. What are the types of communications?

- *Unicast:* In this, a message is sent to a single destination node.
- *Multicast:* In this type of transmission, a message is sent to a selected subset of the network nodes.
- *Broadcast:* In this type of transmission, a message is sent to all the nodes in the network.

35. What are the types of popular MANET routing protocols?

1. Destination-Sequenced Distance-Vector Routing Protocol
2. Dynamic Source Routing (DSR) Protocol
3. Ad Hoc On-demand Distance Vector (AODV)
4. Zone Routing Protocol(ZRP)
5. Multicast Routing Protocols for MANET

36. What is tree based protocol?

Tree-based schemes establish a single path between any two nodes in the multicast group. These schemes require minimum number of copies per packet to be sent along the branches of the tree. Hence, they are bandwidth efficient.

37. What is mesh based protocol?

Mesh-based schemes establish a mesh of paths that connect the sources and destinations. They are more resilient to link failures as well as to mobility.

The major disadvantage of this scheme is that multiple copies of the same packet are disseminated through the mesh, resulting in reduced packet delivery and increased control overhead under highly mobile conditions.

38. Define VANET.

- Vehicular Adhoc Network.
- A Vehicular Ad Hoc Network (VANET) is a special type of MANET in which moving automobiles form the nodes of the network.
- A vehicle communicates with other vehicles that are within a range of about 100 to 300 metres. Multi-hop communication often results in rather large networks.
- In a city or a busy highway, the diameter of the network can be several tens of kilometres.
- Any vehicle that goes out of the signal range of all other vehicles in the network is excluded from the network.
- A vehicle that was outside the communication range of all other vehicles of a VANET can come in the range of a vehicle that is already in the network and as a result can join the network.

39. What are the characteristics of secure Adhoc Network?

A secure ad hoc network should have the following characteristics:

Availability: It should be able to survive denial-of-service (DoS) attacks.

Confidentiality: It should protect confidentiality of information by preventing its access by
unauthorized users.

Integrity: It should guarantee that no transferred message has been tampered with.

Authentication: It should help a node to obtain guarantee about the true identity of a peer node.

Non-repudiation: It should ensure that a node having sent a message, cannot deny it.

40. What are the two phases of DSR?

1. Route discovery
2. Route maintenance

Route discovery

- Route discovery allows any host to dynamically discover the route to any destination in the ad hoc network.
- When a node has a data packet to send, it first checks its own routing cache.
- If it finds a valid route in its own routing cache, it sends out the packet using this route.
- Otherwise, it initiates a route discovery process by broadcasting a route request packet to all its neighbours.

Route maintenance

- Route maintenance is the process of monitoring the correct operation of a route in use and taking any corrective action when needed.
- When a host (source) while using a route, finds that it is inoperative, it carries out route maintenance.
- Whenever a node wanting to send a message finds that the route is broken, it would help if it already knows of some alternative routes.

41. What is the use of VANET?

A VANET can help drivers to get advance information and warnings from a nearby environment via message exchanges.

42. What is network topology?

The topology of a network denotes the connectivity among the various nodes of the network.

43. What are the classification of Unicast MANET Routing Protocols?

- Unicast routing protocols in MANETs are classified into **proactive** (table-driven), **reactive** (ondemand) and **hybrid protocols**.
- This classification is based on how a protocol manages to determine the route correctly in the presence of topology changes.

44. Draw a schematic model of a Mobile Adhoc Network.

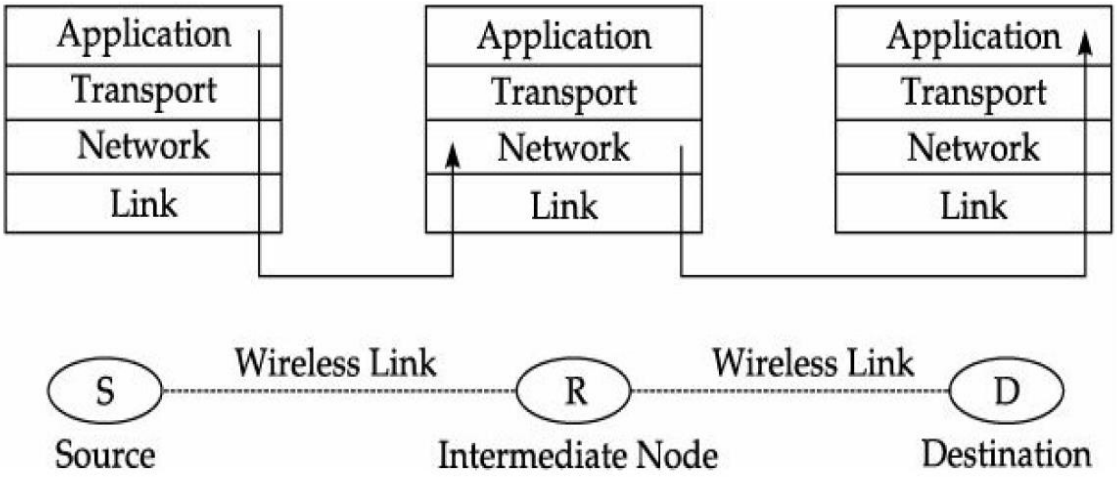


Figure 7.1 *A schematic model of a mobile ad hoc network.*

45. What is proactive protocol?

- A proactive routing protocol is also known as a *table-driven* routing protocol.
- In this protocol, each node in a routing table maintains information about routes to every other node in the network.
- These tables are periodically updated in the face of random network topology changes. An example of a proactive (table-driven) protocol is the Destination Sequenced Distance Vector (DSDV) protocol.

46. What is reactive protocol?

- A reactive routing protocol is also known as an on-demand routing protocol, since in this protocol nodes do not maintain up-to-date routes to different destinations, and new routes are discovered only when required.
- When a node does not have knowledge about any route to a specific destination, it uses a flooding technique to determine the route.

Two examples of on-demand routing protocols are:
(i) Dynamic source routing (DSR)
(ii) Ad hoc on-demand distance vector routing (AODV)

PART-B

1. What is mobile IP? Explain various entities and terminologies used in Mobile Systems. (Or) Explain the services of Mobile IP and describe the tunneling process?

Explain mobile IP requirement and terminologies. (8) [Nov 2018]
Illustrate packet delivery mechanism in mobile IP network with a neat diagram. (16) [Nov 2017]
With a neat diagram explain how packet delivery to and from a mobile node is transferred in mobile IP. (16) [May 2017]

Mobile Internet Protocol

Key Points

- Correspondent node (CN)
- Mobile Node (MN)
- Home agent (HA)
- Foreign Agent (FA)
- Home Network (HN)
- Foreign Network (FN)
- Care-of-Address (COA)
- Agent discovery
  - Agent advertisement, and
  - Agent solicitation.
- Tunnelling and encapsulation
- Packet Delivery

- The Internet is built on top of a collection of protocols, called the TCP/IP protocol suite. Transmission Control Protocol (TCP) and Internet Protocol (IP) are the core protocols in this suite.
- IP is responsible for routing a packet to any host, connected to the Internet, uniquely identified by an assigned IP address.

- The nodes in the LAN are assigned an address based on the LAN address.
- Mobile Internet Protocol (Mobile IP) was proposed by the Internet Engineering Task Force (IETF).
- Mobile IP is a standard protocol that extends the Internet Protocol by making mobility transparent to applications and to higher level protocols like TCP.

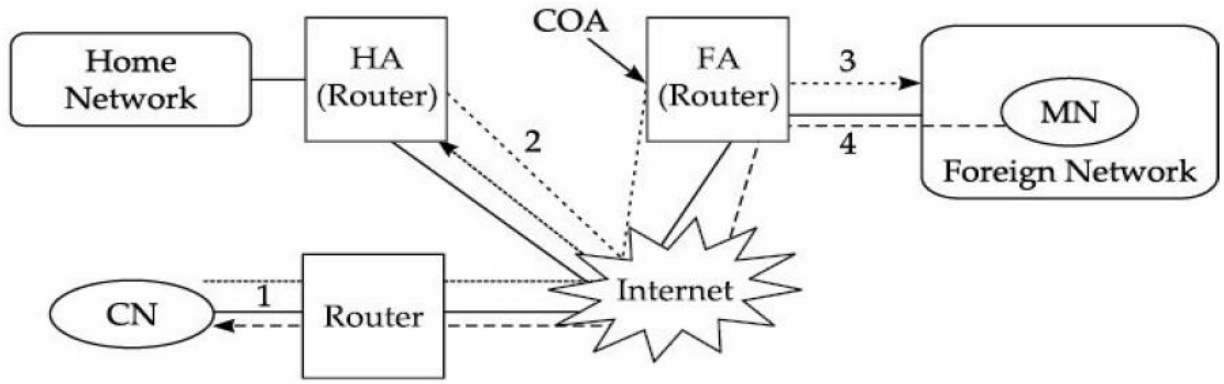


Figure 2.1 Packet deliveries to and from a mobile node.

- Correspondent node (CN) is connected via a router to the Internet, and the home network and the foreign network are also connected via a router, i.e. the home agent (HA) and foreign agent (FA), respectively, to the Internet.
- Home agent (HA) is implemented on the router connecting the home network with the Internet, a foreign agent (FA) is also implemented on the router connecting the foreign network with the Internet.
- The tunnel for the packets towards the mobile node starts at the home agent and ends at the foreign agent, again here the foreign agent has the care-of-address (COA).

Terminologies—Mobile IP

Mobile Node (MN):

A mobile node is hand held equipment with roaming capabilities. It can be a cell phone, personal digital assistant, laptop, etc.

Home Network:

The home network of a mobile device is the network within which the device receives its identifying IP address (home address). In other words, a home network is a subnet to which a mobile node belongs to as per its assigned IP address. Within the home network, there is no need of mobile IP.

Home Address (HA):

The home address of a mobile device is the IP address assigned to the device within its home network. The IP address on the current network is known as home address.

Foreign Agent (FA):

The foreign agent is a router in a foreign network that functions as the point of attachment for a mobile node when it roams to the foreign network. The packets from the home agent are sent to the foreign node which delivers it to the mobile node.

Foreign Network (FN):

The foreign network is the current subnet to which the mobile node is visiting. It is different from home network. In other words, a foreign network is the

network in which a mobile node is operating when away from its home network.

Correspondent Node (CN):

The home agent is a router on the home network serving as the anchor point for communication with the mobile node. It tunnells packets from a device on the Internet, called a correspondent node (CN), to the roaming mobile node.

Tunnelling Process
The packet is forwarded by the home agent to the foreign agent. When the packet comes to the foreign agent (care-of-address), it delivers the packet to the mobile node. This process is called **tunnelling.** Tunnelling has two primary functions: encapsulation of the data packet to reach the tunnel endpoint, and decapsulation when the packet is delivered at that endpoint.

Care-of-Address (COA):

It is the address that is used to identify the present location of a foreign agent. The packets sent to the MN are delivered to COA.

The COA can be any of the following two types:

(a) Foreign agent COA: The COA is an IP address of foreign agent (FA).

(b) Co-located COA: When the mobile node (MN) acquires a temporary IP address, that address acts as the COA.

Care-of-Address (COA):
In real life, if a person is not in his own house and living in a temporary location, that location is called his care-of-address (C/O) but, here, the care-of-address defines the current location of the mobile node from an IP point of view. All IP packets sent to mobile nodes are delivered to the care-of-address (COA), i.e. not directly to the IP address of the mobile node.

Note: The co-located address (temporary IP address) can be acquired using services like dynamic host configuration protocol (DHCP).

Home Agent (HA):

It is located in home network and it provides several services for the MN. HA maintains a location registry. The location registry keeps track of the node locations using the current care-of-address of the MN.

Explain the Agent Discovery Process in Mobile IP? (5) [Apr 2018]

Agent Discovery:

During call establishment it is necessary for a mobile node to determine its foreign agent. This task is referred to as **agent discovery.**

The following two discovery methods are popularly used:

(1) Agent advertisement, and

(2) Agent solicitation.

1. Agent advertisement:

- Generally the foreign and the home agents advertise their presence through periodic agent advertisement messages.
- An agent advertisement message, lists one or more care-of-addresses and a flag indicating whether it is a home agent or a foreign agent. Agent advertisement is a popularly used method in agent discovery.

2. Agent solicitation:

- In case a mobile node (MN) does not receive any COA, then the MN should send an agent solicitation message. But it is important to monitor that these agent solicitation messages do not flood the network.
- A mobile node can usually send up to three solicitation messages (one per second) as soon as it enters a new network. The basic purpose of the solicitation messages sent by a mobile node (MN) is to search for a foreign agent (FA).
- For a highly dynamic wireless network in which MNs move at great speed, even a time interval of the order of a second between these messages is too long. If an MN does not receive any address in response to its solicitation messages, then to avoid network flooding, the MN should exponentially reduce the rate of sending the solicitation messages.

Tunnelling and encapsulation

- Tunnelling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint.
- Tunnelling is the process of sending a packet via a tunnel and it is achieved by a mechanism called **encapsulation**. Encapsulation refers to arranging a packet header and data in the data part of the new packet.
- Disassembling the data part of an encapsulated packet is called **decapsulation**. Whenever a packet is sent from a higher protocol layer to a lower protocol layer, the operations of encapsulation and decapsulation usually take place.

Packet Delivery

- Let us consider the situation, where the corresponding node (CN) wants to send an IP packet to a mobile node. CN sends the packet to the IP address of the mobile node as shown in step 1 of Fig. 2.1.
- The IP address of the MN is the destination address, whereas the address of CN is the source address. The packet is passed to the Internet that does not have any information about the MN's current location. So the Internet routes the packet to the router of the MN's home network.
- The home agent examines the packet to determine whether the MN is present in its current home network or not. In case that MN is not present, then the packet is encapsulated by a new header that is placed in front of the existing IP header.
- The encapsulated packet is tunnelled to the COA, which act as the new destination address and the HA acts as the source address of the packet as shown in step 2 of Fig. 2.1
- The encapsulated packet is routed to the foreign agent which performs decapsulation to remove the additional header and forwards the decapsulated packet to the MN, which is the actual destination, as specified by the source node (CN), shown in step 3 of Fig. 2.1.

- The MN after receiving the packet from CN, forwards a reply packet to the CN by specifying its own IP address along with the address of the CN as shown in step 4 of
- The MN's IP address acts as the source address and the CN's IP address acts as the destination address. The packet is routed to the FA. After receiving the packet, FA forwards the packet to CN.

2. Answer the following with respect to missing and duplicate segments in TCP operation.

(a) What can cause segments to be missed at the receiver-end and also cause duplicate segments to arise? Explain your answer using a suitable scenario of operation.

(b) How exactly is a missing segment detected in TCP? Explain the specific actions that take place when a missing segment is detected.

Key Points

- Goal of mobile IP
- Scenario
- Advantages
- Disadvantages
- Desirable Features of Mobile IP

Overview of Mobile IP

The goal of mobile IP is to enable packet transmission efficiently without any packet loss and disruptions in the presence of host and/or destination mobility.

Scenario

- Suppose a person working as a business development executive for a company needs to take care of many regional offices in India and abroad.
- His home office is in Delhi where he spends about 40% of his time. The rest of the time he spends between the other offices, say, Kolkata, Mumbai, Chennai, Kathmandu and Singapore.
- A problem that arises in this context is: how does he make arrangements so that he would continue to receive postal mails regardless of his location? If we can answer this, we can easily understand how IP works in the context of a mobile device.
- There are two broad categories of solutions to this problem being faced by the business executive:
  (i) address changing,
  (ii)decoupling mail routing from his address.
- It would be difficult for the business development executive to inform about his changed address to all those who are likely to write letters to him each time he moves.
- Also, by the time, he would have informed everyone about his new address; it would have become time for the address to change again.
- And he certainly cannot decouple the routing of mail from his address, unless he has set up his own personal postal system.

- A practical solution to this problem is mail forwarding. Let us say that he leaves Delhi for Singapore for a couple of months.
- He will inform the Delhi post office that he will be in Singapore.
- The Delhi post office would intercept his mails headed for his normal Delhi address, reliable them, and forward them to Singapore.
- Depending on where he is staying, this mail might be redirected either straight to a new address in Singapore, or to a Singapore post office where he can pick it up.
- If he leaves Singapore to go to another city, say, Kathmandu, he would just call the Delhi post office and tell them about his new location.
- When he gets back to home office, he will cancel the forwarding arrangement and get his mail as usual.

Advantages

- Simple mechanism to understand and implement.
- This scheme is transparent to everyone sending mails

Disadvantages

- To keep communicating with his home post office each time he moves.
- Every piece of mail has to be sent through the system twice—first to Delhi and then to wherever he moves, which is inefficient and delay in delivering and also loads the postal system.
- The mobile node is normally resident on its home network, which is the one indicated by the network ID in its IP address.
- Devices on the internetwork always route using this address, so the pieces of "mail" (datagrams) always arrive at a router at the device's "home".
- When the device "travels" to another network, the home router ("post office") intercepts these datagram's and forwards them to the device's current address.
- The mobile node's home router serves as the home agent and the router in Singapore as the foreign agent. The mobile has been assigned a temporary "care-of address" to use in Singapore
- As per mobile IP terminology, the home agent tunnells the packet to the COA.

The steps used in the operation of mobile IP are the following:

Step 1: The remote client sends a datagram to the MN using its home address. It reaches the home agent as usual.

Step 2: The home agent encapsulates that datagram in a new packet and sends it to the foreign agent.

Desirable Features of Mobile IP

Some of the features required of mobile IP are the followings.

Transparency: The IP address is to be managed transparently and there should not be any effect of mobility on any ongoing communication.

Compatibility: Mobile IP should be compatible with the existing Internet protocols.

Security: Mobile IP should, as far as possible, provide users with secure communications over the Internet.

Efficiency and Scalability: In the event of worldwide support, there can be a large number of mobile systems in the whole Internet. It should also be scalable to support billions of moving hosts worldwide.

3. Explain the operation of mobile IP with the help of a suitable schematic diagram and by using suitable examples.
Explain about the key mechanism in Mobile IP. (16) [Nov 2016]

Key Points
- Discovering the care-of-address
- Registering the care-of-address
- Tunnelling to the care-of-address

Key Mechanism in Mobile IP

Mobile IP is associated with the following three basic mechanisms:
- Discovering the care-of-address
- Registering the care-of-address
- Tunnelling to the care-of-address

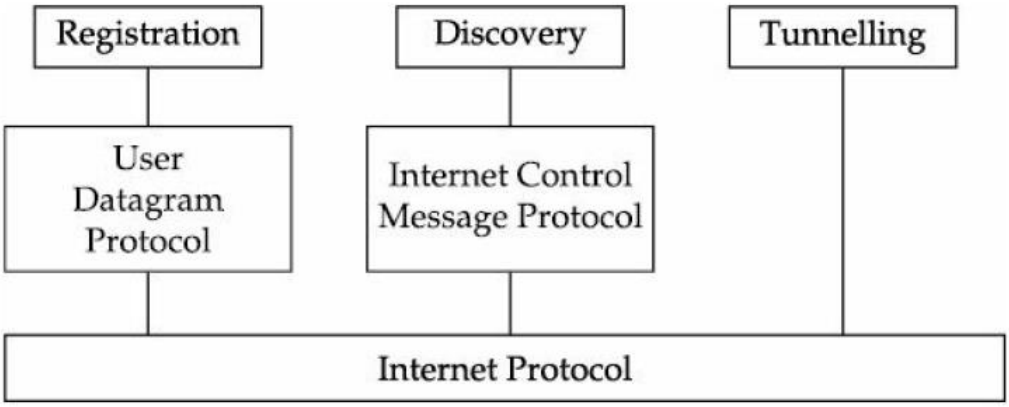


Figure 4.2 A schematic model of Mobile IP.

Discovering the care-of-address

Each mobile node uses a discovery protocol to identify the respective home and foreign agents.

The discovery of the care-of-address consists of four important steps.

1. Mobile agents advertise their presence by periodically broadcasting the **agent advertisement** messages.
2. The mobile node receiving the **agent advertisement** message observes whether the message is from its own home agent and determines whether it is on the home network or on a foreign network.
3. If a mobile node does not wish to wait for the periodic advertisement, it can send out **agent solicitation** messages that will be responded to by a mobility agent.
4. The process of agent advertisements, involves the following activities:
   - Foreign agents send messages to advertise the available care-of-addresses.
   - Home agents send advertisements to make themselves known.
   - Mobile hosts can issue agent solicitations to actively seek information.
   - If a mobile host has not heard from the foreign agent to which its current care-of-address belongs, it takes up another care-of-address.

Registering the care-of-address

- If a mobile node discovers that it is on the home network, it operates without requiring any mobility services.
- If a mobile node obtains a care-of-address from a foreign agent, then this address should be registered with the home agent.
- The mobile node sends a request for registration to its home agent along with the care-of-address information whenever the home agent receives the registration request information.
- The routing table is updated and it sends back the registration reply to the mobile node.
- The mobile node makes use of the registration procedure to intimate the care-of-address to a home agent.

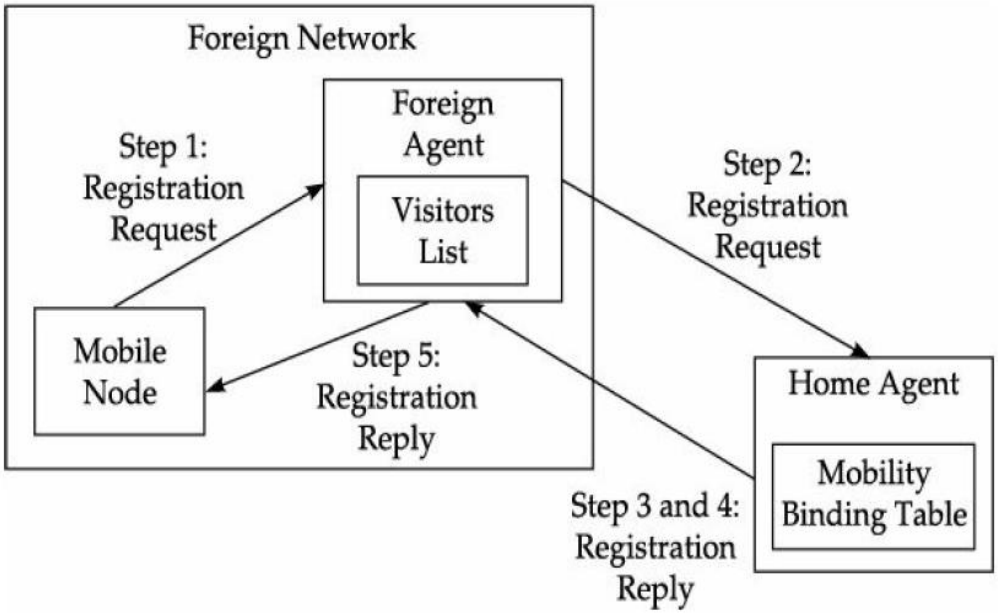


Figure 4.3 Registration process in Mobile IP.

The registration process consists of the following steps:

1. If the mobile node is on a new network, it registers with the foreign agent by sending a **registration request** message which includes the permanent IP address of the mobile host and the IP address of its home agent.
2. The foreign agent in turn performs the registration process on behalf of the mobile host by sending a Registration Request containing the permanent IP address of the mobile node and the IP address of the foreign agent to the home agent.
3. When the home agent receives the Registration Request, it updates the mobility binding by associating the care-of-address of the mobile node with its home address.
4. The home agent then sends an acknowledgement to the foreign agent.
5. The foreign agent in turn updates its visitors list by inserting the entry for the mobile node and relays the reply to the mobile node.

Box – Security in Mobile IP

Security is very important in Mobile IP as mobile nodes are often connected to the Internet via wireless links which are very vulnerable to security attacks.
For example, during the registration procedure the home agent should be convinced that it is getting the authentic registration request from a mobile node. Mobile IP solves this problem by specifying a security association between the home agent and the mobile node.

Tunnelling to the care-of-address

Tunnelling takes place to forward an IP datagram from the home agent to a care-of-address.
This involves carrying out the following steps:

- When a home agent receives a packet addressed to a mobile host, it forwards the packet to the care-of-address using IP-within-IP (encapsulation).
- Using IP-within-IP, the home agent inserts a new IP header in front of the IP header of any datagram.
- Destination address is set to the care-of-address.
- Source address is set to the home agent's address.
- After stripping out the first header, IP processes the packet again.

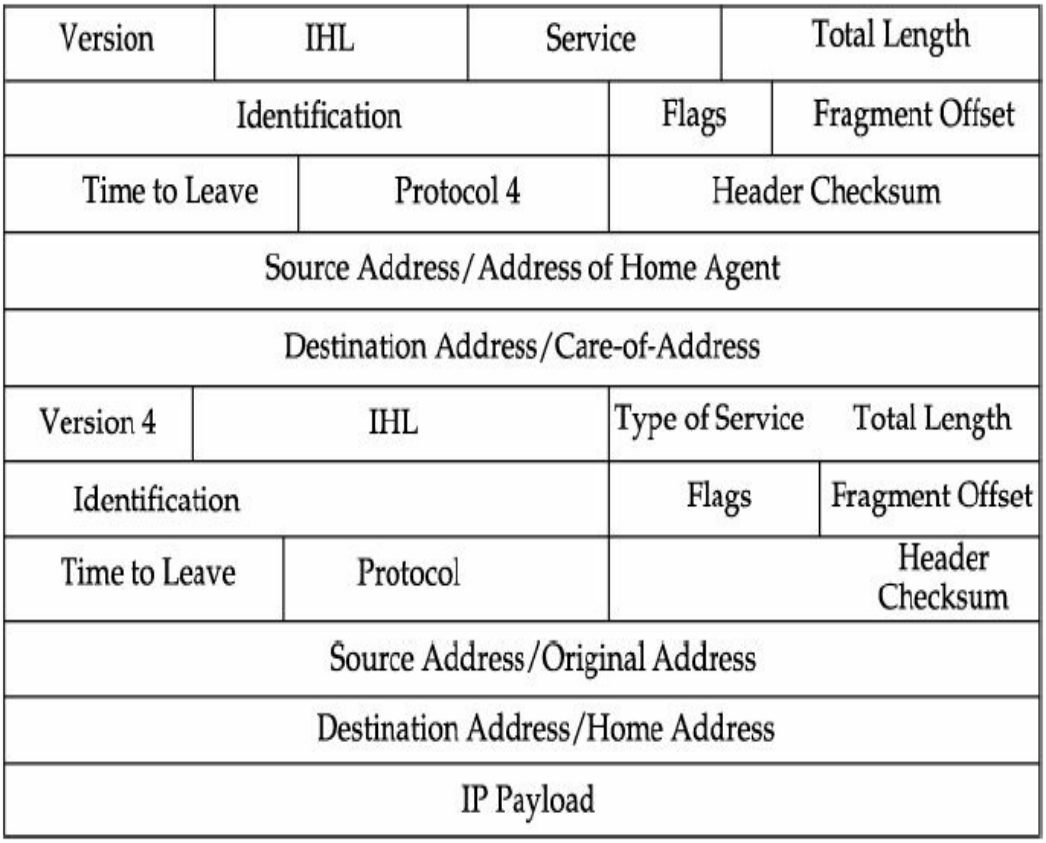


Figure 4.4 IP encapsulation in mobile IP.

4. Discuss how optimization in achieved in mobile IP?

Key Points
- Route Optimization
- Binding request
- Binding acknowledgement
- Binding update
- Binding warning

Route Optimization

In the mobile IP protocol, all the data packets to the mobile node go through the home agent. Because of this there will be heavy traffic between HA and CN in the network, causing latency to increase.

Therefore, the following route optimization needs to be carried out to overcome this problem.
- Enable direct notification of the corresponding host
- Direct tunnelling from the corresponding host to the mobile host
- Binding cache maintained at the corresponding host

The mobile IP scheme needs to support the four messages shown in Table 4.1.
The association of the home address with a care-of-address is called **binding.**

TABLE 4.1 Messages Transmitted in Optimized Mobile IP

Message type	Description
Binding request	If a node wants to know the current location of a mobile node (MN), it sends a request to home agent (HA).
Binding acknowledgement	On request, the node will return an acknowledgement message after getting the binding update message.
Binding update	This is a message sent by HA to CN mentioning the correct location of MN. The message contains the fixed IP address of the mobile node and the care-of-address. The binding update can request for an acknowledgement.
Binding warning	If a node decapsulates a packet for a mobile node (MN), but it is not the current foreign agent (FA), then this node sends a binding warning to the home agent (HA) of the mobile node (MN).

5. Explain IP in IP, minimal IP and GRE encapsulation methods. (8)
[May 2016]

What is Encapsulation? Explain in detail the various encapsulation techniques in mobile IP. (16) [May 2017]

Encapsulation:

- Encapsulation describes the process of placing an IP datagram inside a network packet or frame.
- Encapsulation refers to how the network interface uses packet switching hardware

IPIP

- IP-in-IP encapsulation is exactly what it sounds like: one IP packet encapsulated inside another. The protocol field of the outer header is set to 4 for IPv4 or 41 for IPv6.

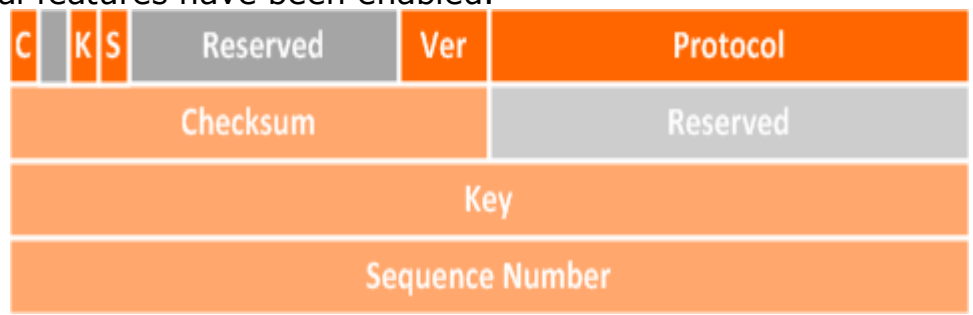
Minimal IP

- A minimal forwarding header is defined for datagrams which are not fragmented prior to encapsulation. Use of this encapsulating method is optional.
- Minimal encapsulation MUST NOT be used when an original datagram is already fragmented, since there is no room in the minimal forwarding header to store fragmentation information.
- To encapsulate an IP datagram using minimal encapsulation, the minimal forwarding header is inserted into the datagram.

GRE

- Generic Routing Encapsulation (GRE) and IP-in-IP (IPIP) are two rather similar tunneling mechanisms which are often confused.
- GRE (defined in RFC 2784 and updated by RFC 2890) goes a step further than IP-in-IP, adding an additional header of its own between the inside and outside IP headers.

- The GRE header is variable in length, from 4 to 16 bytes, depending on which optional features have been enabled.



- C, K, and S: Bit flags which are set to one if the checksum, key, and sequence number fields are present, respectively
- Ver: GRE version number (zero)
- Protocol: Ethertype of the encapsulated protocol
- Checksum: Packet checksum (optional)
- Key: Tunnel key (optional)
- Sequence Number: GRE sequence number (optional)

Here's a sample capture of GRE in action. Note that GRE can theoretically encapsulate any layer three protocol with a valid Ether type, unlike IPIP, which can only encapsulate IP.
GRE can be encapsulated by either IPv4 or IPv6 on IOS. (The multipoint option is used for Dynamic Multipoint VPN (DMVPN).)

```
Router(config)# interface tun0
Router(config-if)# tunnel mode gre ?
  ip          over IP
  ipv6        over IPv6
  multipoint  over IP (multipoint)
```

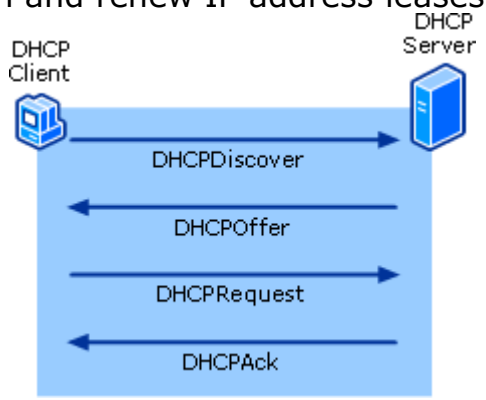
To summarize, GRE can:

- Encapsulate any layer three protocol (versus just IP)
- Add an additional checksum (which isn't useful for TCP/IPv4)
- Specify a tunnel key
- Enforce packet sequencing

6. With a diagram explain DHCP & its protocol architecture. (8) [Nov 2016]

DHCP Architecture

- The DHCP architecture consists of DHCP clients, DHCP servers, and DHCP relay agents on a network. The clients interact with servers using DHCP messages in a DHCP conversation to obtain and renew IP address leases.



Interactions between client and server

- DHCP servers and DHCP clients communicate through a series of DHCP messages. To obtain a lease, the DHCP client initiates a conversation with a DHCP server using a series of these DHCP messages.

DHCP messages

- The following list includes the eight types of messages that can be sent between DHCP clients and servers.

DHCPDiscover

- Broadcast by a DHCP client when it first attempts to connect to the network. The DHCPDiscover message requests IP address information from a DHCP server.

DHCPOffer

- Broadcast by each DHCP server that receives the client DHCPDiscover message and has an IP address configuration to offer to the client.
- The DHCPOffer message contains an unleased IP address and additional TCP/IP configuration information, such as the subnet mask and default gateway.
- More than one DHCP server can respond with a DHCPOffer message.
- The client accepts the best offer, which, for a Windows DHCP client, is the first DHCPOffer message that it receives.

DHCPRequest

- Broadcast by a DHCP client after it selects a DHCPOffer.
- The DHCPRequest message contains the IP address from the DHCPOffer that it selected. If the client is renewing or rebinding to a previous lease, this packet might be unicast directly to the server.

DHCPAck

- Broadcast by a DHCP server to a DHCP client acknowledging the DHCPRequest message.
- At this time, the server also forwards any options. Upon receipt of the DHCPAck, the client can use the leased IP address to participate in the TCP/IP network and complete its system startup.
- This message is typically broadcast, because the DHCP client does not officially have an IP address that it can use at this point.
- If the DHCPAck is in response to a DHCPInform, then the message is unicast directly to the host that sent the DHCPInform message.

DHCPNack

- Broadcast by a DHCP server to a DHCP client denying the client's DHCPRequest message.
- This might occur if the requested address is incorrect because the client moved to a new subnet or because the DHCP client's lease has expired and cannot be renewed.

DHCPDecline

- Broadcast by a DHCP client to a DHCP server, informing the server that the offered IP address is declined because it appears to be in use by another computer.

DHCPRelease

- ent by a DHCP client to a DHCP server, relinquishing an IP address and canceling the remaining lease. This is unicast to the server that provided the lease.

DHCPInform

- Sent from a DHCP client to a DHCP server, asking only for additional local configuration parameters; the client already has a configured IP address.
- This message type is also used by DHCP servers running Windows Server 2008 to detect unauthorized DHCP servers.

DHCP lease process

- A DHCP-enabled client obtains a lease for an IP address from a DHCP server.

- Before the lease expires, the DHCP client must renew the lease or obtain a new lease.
- Leases are retained in the DHCP server database for a period of time after expiration.
- By default, this grace period is four hours and cleanup occurs once an hour for a DHCP server running Windows Server 2008.
- This protects a client's lease in case the client and server are in different time zones, the internal clocks of the client and server computers are not synchronized, or the client is off the network when the lease expires.

7. What are the main functions of DHCP? Why is DHCP needed? Can it be used when nodes are mobile? Explain your answer. (Or) Explain the significance of Dynamic Host Configuration Protocol. Give examples of situations where it is useful.

Key Points

DHCP – Introduction

Benefits

- Reliable IP address configuration
- Reduced network administration

Why use DHCP - maintains a pool of IP addresses

Significance of Dynamic Host Configuration Protocol

DHCP supports three important mechanisms for IP address allocation

- Automatic allocation
- Dynamic allocation
- Manual allocation

Dynamic Host Configuration Protocol (DHCP)

- DHCP was developed based on bootstrap protocol (BOOTP). DHCP provides several types of information to a user including its IP address.
- To manage dynamic configuration information and dynamic IP addresses, IETF standardized an extension to BOOTP known as dynamic host configuration protocol (DHCP).
- The DHCP client and server work together to handle the roaming status and to assign IP address on a new network efficiently. The DHCP server allocates an IP address from a pool of IP addresses to a client.
- The BOOTP protocol is used for booting (starting) computers from the network. These are popularly used in case of diskless computers. Whenever a client requests an IP address from the server machine, BOOTP searches a table which matches to its physical address.

Benefits of DHCP

- **Reliable IP address configuration.** DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

- **Reduced network administration.** DHCP includes the following features to reduce network administration:
  - Centralized and automated TCP/IP configuration.
  - The ability to define TCP/IP configurations from a central location.
  - The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
  - The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.
  - The forwarding of initial DHCP messages by using a DHCP relay agent, thus eliminating the need to have a DHCP server on every subnet.

Why use DHCP

- Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources.
- Without DHCP, IP addresses must be configured manually for new computers or computers that are moved from one subnet to another, and manually reclaimed for computers that are removed from the network.
- DHCP enables this entire process to be automated and managed centrally. The **DHCP server maintains a pool of IP addresses** and leases an address to any DHCP-enabled client when it starts up on the network.
- Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.
- The network administrator establishes DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer.

The DHCP server stores the configuration information in a database, which includes:

- Valid TCP/IP configuration parameters for all clients on the network.
- Valid IP addresses, maintained in a pool for assignment to clients, as well as excluded addresses.
- Reserved IP addresses associated with particular DHCP clients. This allows consistent assignment of a single IP address to a single DHCP client.
- The lease duration, or the length of time for which the IP address can be used before a lease renewal is required.

A DHCP-enabled client, upon accepting a lease offer, receives:

- A valid IP address for the subnet to which it is connecting.
- Requested DHCP options, which are additional parameters that a DHCP server is configured to assign to clients. Some examples of DHCP options are Router (default gateway), DNS Servers, and DNS Domain Name. For a full list of DHCP options, see "DHCP Tools and Settings."

Significance of Dynamic Host Configuration Protocol

- DHCP is an extension to the BOOTP and compatible with it. For example, if a host is running BOOTP, it can also request configuration (example: static configuration) from a DHCP server node.

- The importance of DHCP in a mobile computing environment is that it provides temporary IP addresses whenever a host moves from one network to another network.

DHCP supports the following three important mechanisms for IP address allocation:

Automatic allocation: In automatic allocation, DHCP assigns a permanent IP address to a particular client.

Dynamic allocation: In dynamic allocation, DHCP assigns IP address to a client for a specific period of time.

Manual allocation: In manual allocation, a client's IP address is assigned by the network administrator, where the DHCP is used to inform the address assigned to clients.

Mobile Transport Layer

- In mobile computing applications, Transmission Control Protocol (TCP) is possibly the most popular transport layer protocol. In fact, TCP is the **de facto** standard transport layer protocol for applications that require guaranteed message delivery.
- TCP is a connection-oriented protocol. UDP (User Datagram Protocol), on the other hand, is a connectionless protocol in the TCP/IP protocol suite and does not guarantee reliable data delivery. However, when the traditional TCP is used in mobile computing networks, it operates in a highly inefficient and unsatisfactory manner.
- TCP needs several special adaptations to make it suitable for use in wireless networks.

8. Explain in detail about the basic concepts of Adhoc network.

Key Points

- Adhoc basic concepts – Schematic model of a mobile Adhoc Network
- Routing in a MANET

Adhoc Basics Concepts

How Is an Ad Hoc Network Set Up without the Infrastructure Support?

Adhoc network is defined as a set of mobile devices can communicate with each other in the **absence of** any form of fixed networking infrastructures such as **hubs, routers, base stations**, etc.

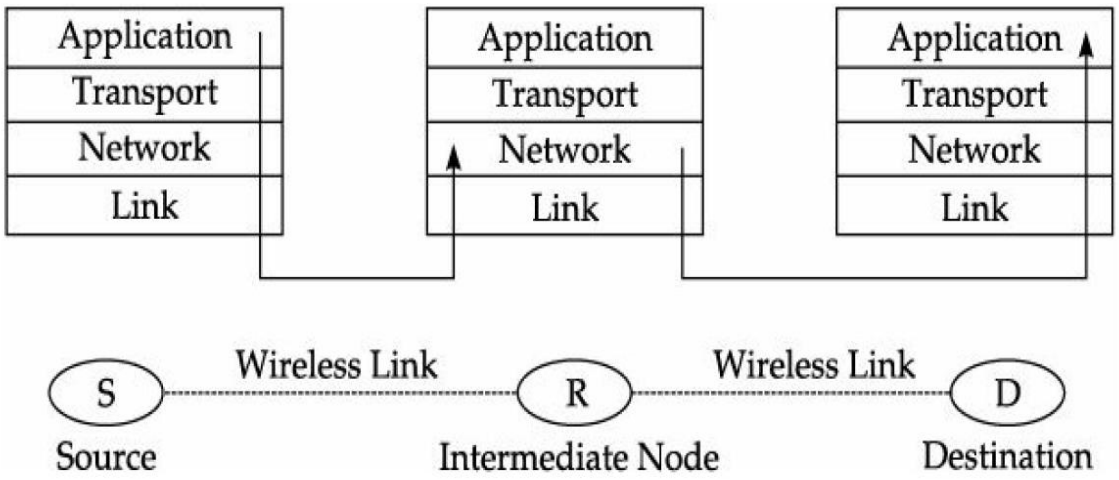


Figure 7.1 *A schematic model of a mobile ad hoc network.*

In this figure, suppose the mobile device S wants to communicate with the device D.

- Assume that S and D are not within the transmission range of each other and cannot directly communicate with each other.
- They can take the help of node R to relay packets from each other.
- R is primarily an independent device and not a networking infrastructure, yet R is acting as some sort of a router operating at the network (or Internet) layer to facilitate communication.

Routing in a MANET

- In a wired network, a router determines the path that needs to be followed by a packet based on the information contained within the IP address of the destination, and uses this information to forward a packet towards its destination.
- In an ad hoc network, such a simple and efficient routing protocol is difficult to deploy.
- In a MANET(Mobile Adhoc Network) the topology of the network and consequently the routes between different devices change dynamically as nodes move away or fail.
  Packet routing is a critical and complex issue in MANETs.

9. Explain in detail about characteristics of Mobile Adhoc Networks.
Explain characteristics, Applications of MANET. (4+4) [May 2016]

Key Points

- Lack of fixed infrastructure
- Dynamic topologies
- Bandwidth constrained, variable capacity links
- Energy constrained operation
- Increased vulnerability

Characteristics of Mobile Ad Hoc Networks (MANETs)

1. Lack of fixed infrastructure:

In the absence of any fixed networking infrastructure, a pair of nodes can either communicate directly when they are in the transmission range of each other, or they

can communicate using a multi-hop communication that gets set up through several devices located between them.

2. Dynamic topologies:

Since the devices in a MANET are allowed to move arbitrarily, the network topology can change unpredictably. The rate of topology change depends on the speed of movement of the mobile devices. The speed of movement of a mobile device can vary greatly with the time of the day and the specific MANET application being considered.

3. Bandwidth constrained, variable capacity links:

Wireless links have significantly lower capacity than their wired counterparts. Further, factors such as fading, noise, and interference can change the available bandwidth of a wireless link arbitrarily with time. Consequently, the bandwidth of a link can change arbitrarily with time.

4. Energy constrained operation:

The nodes in a MANET rely on battery power. These batteries are small and can store very limited amounts of energy. On the other hand, transmissions and processing required during routing involve expenditure of substantial amount of energy causing the batteries to get rapidly drained out, unless the routing protocol is carefully designed. Therefore, energy conservation is usually considered to be an important objective of MANET routing protocols.

5. Increased vulnerability:

MANETs are prone to many new types of security threats that do not exist in the case of their wired counterparts. Many of these threats arise due to the underlying wireless transmissions and the deployment of collaborative routing techniques.

There are increased possibilities of eavesdropping, spoofing, denial-of-service attacks in these networks. It is very difficult to identify the attacker since the devices keep moving and do not have a global identifier.

Other characteristics:

Other distinguishing characteristics of a MANET include a distributed peer-to-peer mode of operation, multi-hop routing, and relatively frequent changes to the concentration of nodes over any specific area.

MANET Operational Constraints

The nodes in a MANET have low processing capabilities and these are connected by low bandwidth wireless links.

An appropriate routing protocol for a MANET should keep the computational and communicational overheads low, since the nodes in a MANET have low computational capability, storage capacity and battery power.

10. Explain in detail about the Applications of Adhoc networks.

Key Points

- Communication among portable computers
- Environmental monitoring
- Military
- Emergency applications

Applications

1. Communication among portable computers

- Miniaturization has allowed the development of many types of portables and computerized equipment, which have become very popular.
- Many of these portables work meaningfully when connected to some network, possibly a LAN or the Internet. For this, the portables are typically required to be within the range of some wireless hub.
- Satisfaction of this requirement would, however, drastically reduce the flexibility and the mobility of the devices.
- In this case, using MANET the audience can exchange notes, and also can surf the Web if at least one of the hand-held devices has access to Internet, for example, through a data card.
- If the mobile devices are present in sufficient density, network connections among them can be established seamlessly to form a MANET over which the nodes can communicate and carry out the network operations.

2. Environmental monitoring

- Continuous data collection from remote locations is considered important for several applications such as environmental management, security monitoring, road traffic monitoring and management, etc.
- Miniaturized sensors have proved to be an effective means of gathering environmental information such as rainfall, humidity, presence of certain animals, etc.
- In this environmental monitoring application, a large number of sensors nodes are deployed in the environment.
- Such ad hoc sensor networks can be deployed to collect data from remote locations and the sensor nodes can even respond to some commands issued by the data collection centre.
- MANETs efficiently handle the introduction of new sensors into an already operational sensor network as well as can handle dynamic disconnections of nodes.
- Since each sensor acts as a hub, the range over which the sensors can be spread is tremendously increased.

3. Military

- Ad hoc networking of this equipment can allow a military setup to take advantage of an information network among the soldiers, vehicles, and military information headquarters.
- For example, an ad hoc network can be automatically set up at a battlefront among the equipment, and the hand-held devices can collect information from and disseminate command to the frontline personnel.

4. Emergency applications

- Ad hoc networks do not require any pre-existing infrastructure.
- These networks, therefore, can be deployed easily and rapidly in emergency situations such as a search and rescue operation after a natural disaster, and for applications such as policing and fire fighting.

11. Explain in detail about MANET Design Issues.

Explain the design issues in MANET and the applications of adhoc network. (13)[Apr 2018]

Explain the design issues of MANET routing protocols in detail. (16)

[May 2017]

Key Points
- Network size and node density
- Connectivity
- Network topology
- User traffic
- Operational environment
- Energy constraint

MANET Design Issues

Network size and node density

- Network size and node density are the two important parameters of a MANET that need to be considered while designing an appropriate routing protocol for a network.
- Network size refers to the geographical coverage area of the network and network density refers to the number of nodes present per unit geographical area.
- For larger networks, clustering is essential to keep the communication overheads low.
- The cluster size as well as a specific clustering solution for a network would, to a large extent, depend on node density.

Connectivity

- The term connectivity of a node usually refers to the number of neighbours it has.
- Here a neighbor of a node is one that is in its transmission range.
- The term connectivity is also sometimes used to refer to a link between the two nodes.
- The term link capacity denotes the bandwidth of the link. In a MANET, both the number of neighbouring nodes and the capacities of the links to different neighbours may vary significantly.

Network topology

- The topology of a network denotes the connectivity among the various nodes of the network. Mobility of the nodes affects the network topology.
- Due to node mobility, new links can form and some links may get dissolved. Other than mobility, nodes can become inoperative due to discharged batteries or hardware failures, and thereby cause changes to the topology.
- The rate at which the topology changes needs to be appropriately considered in the design of an effective network.

User traffic

- The design of a MANET is carried out primarily based on the anticipated node density, average rate of node movements, and the expected traffic.
- The traffic in a network can be of various types.
- A network protocol should leverage the characteristics of specific traffic types that are expected to improve its performance.

The common traffic types are the following:

- Bursty traffic

- Large packets sent periodically
- Combination of the above two types of traffic

Operational environment

- The operational environment of a mobile network is usually either urban, rural and maritime. These operational environments support the Line of Sight (LOS) communication.
- But, there can be a significant difference in the node density and mobility values in different operational environments, requiring different designs of mobile networks to suit an operational environment.

Energy constraint

- No fixed infrastructure exists in a MANET; the mobile nodes themselves store and forward packets. This additional role of mobile nodes as routers leads to nodes incurring perennial routing-related workload and this consequently results in continual battery drainage.
- Though this overhead is indispensable if the network is to be kept operational, the energy spent can be substantially reduced by allowing the nodes to go into a sleep mode whenever possible.

12. Explain in detail about popular MANET routing protocols and Proactive protocol-DSDV, Reactive Routing Protocols – DSR, AODV, Hybrid routing –ZRP, Multicast Routing- ODMRP.

Keypoints

1. Destination-Sequenced Distance-Vector Routing Protocol (DSDV) - table-driven (Proactive Protocol) approach
2. Dynamic Source Routing (DSR) Protocol - on-demand (or Reactive Routing Protocol) routing protocol.
   - Route Cache
   - Route discovery
   - Route maintenance
3. Ad Hoc On-demand Distance Vector (AODV)- on-demand (or Reactive Routing Protocol) routing protocol
   - Route Request
   - Route Reply
4. Zone Routing Protocol (ZRP) - both on-demand and proactive (Hybrid) routing protocol
5. Multicast Routing Protocols for MANET - delivery of a message to a group of destination nodes in a single transmission

Popular MANET Routing Protocols

- Destination-Sequenced Distance-Vector Routing Protocol(DSDV)
- Dynamic Source Routing (DSR) Protocol
- Ad Hoc On-demand Distance Vector (AODV)
- Zone Routing Protocol(ZRP)
- Multicast Routing Protocols for MANET

a) Destination-Sequenced Distance-Vector Routing Protocol(DSDV)

- Destination-Sequenced Distance-Vector Routing (DSDV) is an important MANET routing protocol. It is based on the table-driven (proactive) approach to packet routing.
- In DSDV, each node in a MANET maintains a routing table in which all of the possible destinations and the number of hops to each destination are recorded.
- Each node maintains information regarding routes to all the known destinations. The routing information is updated periodically.
- Also, there is traffic overhead even if there is no change in network topology. Nodes maintain routes which they may never use.
- A sequenced numbering system is used to allow mobile nodes to distinguish stale routes from new ones. Updated routing tables are exchanged periodically among the nodes of the network to maintain table consistency.
- DSDV uses two types of route update packets. The first is known as *full dump*. This type of packet carries all the available routing information and can require multiple network protocol data units (NPDUs) to be transmitted.
- The mobile nodes maintain an additional table where they store the data received through the incremental routing information packets from various nodes.

Important steps in the operation of DSDV

1. Each router (node) in the network collects route information from all its neighbours.
2. After gathering information, the node determines the shortest path to the destination based on the gathered information.
3. Based on the gathered information, a new routing table is generated.
4. The router broadcasts this table to its neighbours. On receipt by neighbours, the neighbor nodes recompute their respective routing tables.
5. This process continues till the routing information becomes stable.

Figure 7.3 shows an example of a MANET. Table 7.1 is the routing table of the node N 4 at the moment before the movement of nodes. The metric field in the routing table helps to determine the number of hops required for a packet to traverse to its destination.

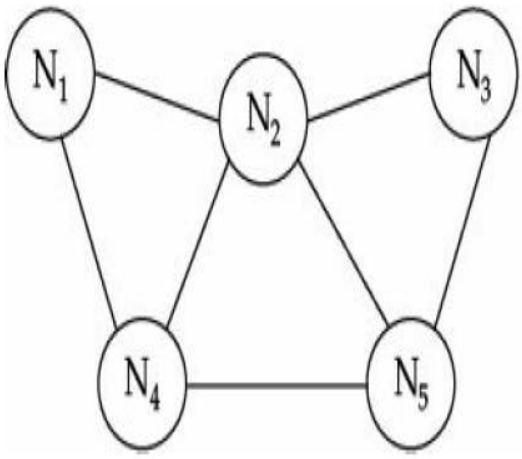


Figure 7.3 *An example of a MANET topology at a given instant of time.*

TABLE 7.1 DSDV Routing Table for the MANET of Figure 7.3 at Node N_4

Destination	Next hop	Metric	Sequence no.	Install time
N_1	N_1	1	321	001
N_2	N_2	1	218	001
N_3	N_2	2	043	002
N_5	N_5	1	163	002

2. Dynamic Source Routing (DSR) Protocol

- Dynamic Source Routing (DSR) protocol was developed to be suitable for use in a MANET having a reasonably small diameter of about 5 to 10 hops and when the nodes do not move very fast.
- DSR is a source initiated on-demand (or reactive) routing protocol for ad hoc networks.
- It uses source routing, a technique in which the sender of a packet determines the complete sequence of nodes through which a packet has to travel.
- The sender of the packet then explicitly records this list of all nodes in the packet's header. This makes it easy for each node in the path to identify the next node to which it should transmit the packet for routing the packet to its destination.
- In this protocol, the nodes do not need to exchange the routing table information periodically, which helps to reduce the bandwidth overhead associated with the protocol.
- Each mobile node participating in the protocol maintains a *routing cache* which contains the list of all routes that the node has *learnt*.
- Whenever a node finds a new route, it adds the new route to its *routing cache*. Each mobile node also maintains a sequence counter called *request id* to uniquely identify the last request it had generated.
- The pair < source address, request id > uniquely identifies any request in the ad hoc network.

Illustrate DSR routing in detail and compare it with DSDV. (13) [Nov 2018]
Explain DSR Routing Protocols in detail. (8) [May 2016]
Discuss Route Discovery and Route Maintenance mechanisms in DSR with illustrations. List its merits and demerits. (16) [Nov 2017]

DSR works in two phases:

(i) Route discovery and
(ii)Route maintenance.

Route discovery

- Route discovery allows any host to dynamically discover the route to any destination in the ad hoc network.
- When a node has a data packet to send, it first checks its own routing cache.
- If it finds a valid route in its own routing cache, it sends out the packet using this route.
- Otherwise, it initiates a route discovery process by broadcasting a route request packet to all its neighbours.
- The route request packet contains the source address, the request id and a route record in which the sequence of hops traversed by the request packet, before reaching the destination is recorded.

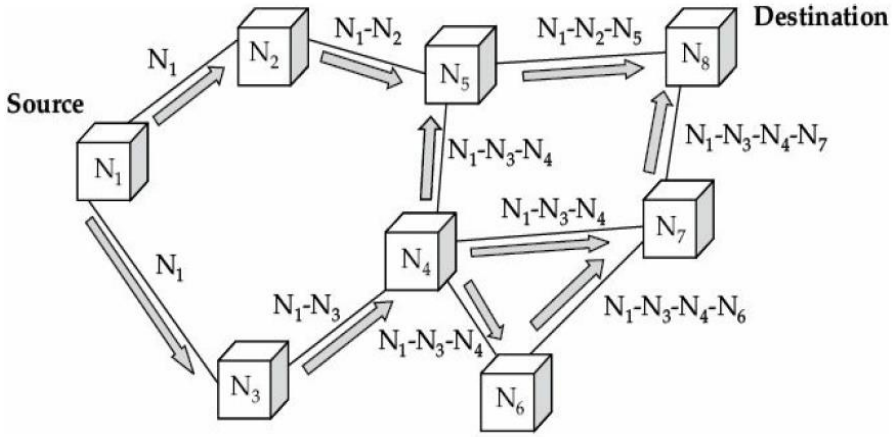


Figure 7.4 *An example of the route discovery process in DSR.*

- Suppose a node N1 wishes to send a message to the destination node N8. The intermediate nodes are N2, N3, N4, N5, N6, N7.
- The node N1 initiates the route discovery process by broadcasting a *route request* packet to its neighbours N2 and N3.
- Note that each node can have multiple copies of the route request packet arriving at it.
- The propagation of route reply is shown in Figure 7.5, and the acknowledgement messages from destination to source are indicated by thick arrows.

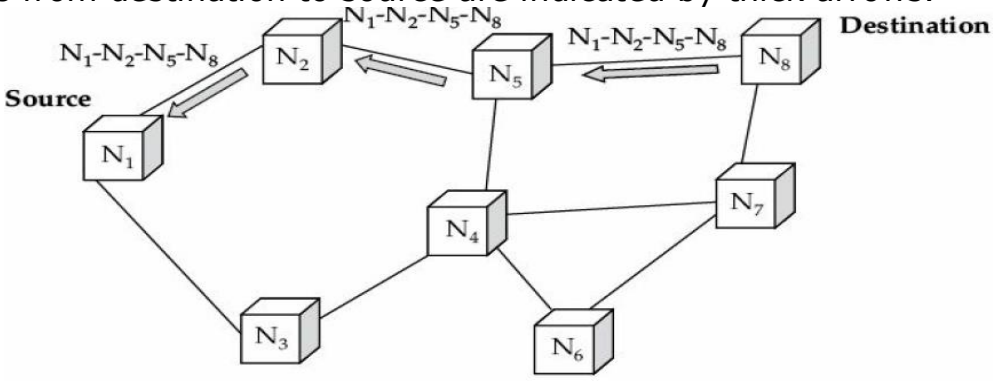


Figure 7.5 *An example of the propagation of route reply in DSR.*

Route maintenance

- Route maintenance is the process of monitoring the correct operation of a route in use and taking any corrective action when needed.
- When a host (source) while using a route, finds that it is inoperative, it carries out route maintenance.

- Whenever a node wanting to send a message finds that the route is broken, it would help if it already knows of some alternative routes.
- If it has another route to the destination, it starts to retransmit the packet using the alternative route. Otherwise, it initiates the route discovery process

again.

	DSR Advantages	*DSR Disadvantages*
1	No need to keep a routing table inside each node because the entire route is contained in the packet header of each data packet sent from the source to the destination.	DSR is not scalable to large networks and requires significantly more processing resources than most other protocols.
2	DSR allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example, for use in load balancing or for increased robustness.	Each node must spend a lot of time to process any control data it receives in order to obtain the routing information, even if it is not the intended recipient.
3	DSR protocol includes easily guaranteed loop-free routing, operation in networks containing unidirectional links, use of only "soft state" in routing, and rapid recovery when routes in the network change.	Route maintenance mechanism does not locally repair a broken link.
4	A node processes a route request packet only if it has not already seen the packet and its address is not present in the route record of the packet. This minimizes the number of route requests propagated in the network.	Stale route cache information could also result in inconsistencies during the route reconstruction phase because an intermediate node may send a Route Reply using a stale cached route, thus polluting other caches.
5	An intermediate node can use an alternate route from its own cache, when a data packet meets a failed link on its source route.	The connection setup delay is higher than in table-driven protocols.
6	DSR does not enforce any use of periodic messages from the mobile hosts for maintenance of routes.	Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility.
7	DSR enables multiple routes to be learnt for a particular destination. DSR does not require any periodic update messages, thus avoiding wastage of bandwidth.	Routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length and data load.
8	Route caching can further reduce route discovery	A flood of route requests may potentially reach all

3. Ad Hoc On-demand Distance Vector (AODV)

- The route discovery and route maintenance activities in AODV are very similar to those for the DSR protocol.

- AODV does make use of hop-by-hop routing, sequence numbers and beacons.
- The node that needs a route to a specific destination generates a *route request*.
- The *route request* is forwarded by intermediate nodes which also learn a reverse route from the source to themselves.
- When the request reaches a node with route to destination, it generates a *route reply* containing the number of hops required to reach the destination.
- All nodes that participate in forwarding this reply to the source node create a forward route to destination.
- This route created from each node from source to destination is a hop-by-hop route.

Recollect that DSR includes the complete route in packet headers.

- The large headers can substantially degrade the performance, especially when the data content of packets is small.
- AODV attempts to improve upon DSR by maintaining routing tables at the nodes, so that the data packets do not have to contain the routes.
- AODV retains a positive feature of DSR, in that the routes are maintained only between those nodes that need to communicate.
- If a link break occurs while a route is being used to transmit a message, a route error message is sent to the source node by the node that observes that the next link in the route has failed.

4. Zone Routing Protocol

- The Zone Routing Protocol (ZRP) is a hybrid protocol. It incorporates the merits of both on-demand and proactive routing protocols.
- A routing zone comprises a few MANET nodes within a few hops from the central zone. Within a zone, a table-driven routing protocol is used.
- If a destination node happens to be outside the source's zone, ZRP employs an ondemand route discovery procedure which works as follows.
- The source node sends a route request to the border nodes of its zone, containing its own address, the destination address and a unique sequence number.
- Border nodes are those nodes which are some predefined number of hops away from the source. Each border node checks its local zone for the destination.

What Multicast routing protocols. (8) [Nov 2016]

5. Multicast Routing Protocols for MANET

Multicast is the delivery of a message to a group of destination nodes in a single transmission as shown in Figure 7.6.

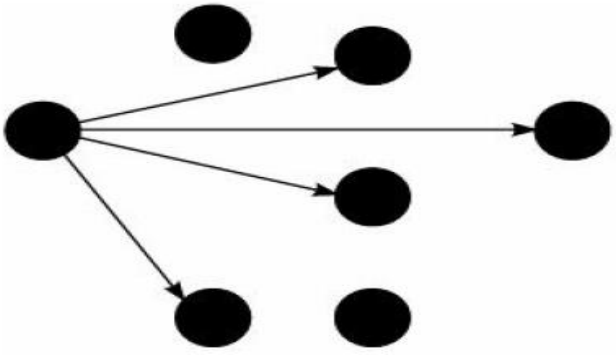


Figure 7.6 *Multicast transmission.*

For efficient operation of a multicast routing protocol, it is necessary to minimize the unnecessary packet transmissions as well as minimize the energy consumption.
In order to achieve this, a multicast transmission should not be approximated by multiple unicast transmissions.
The popular MANET multicasting protocols are either tree-based or mesh-based:

Tree-based protocol

Tree-based schemes establish a single path between any two nodes in the multicast group. These schemes require minimum number of copies per packet to be sent along the branches of the tree. Hence, they are bandwidth efficient.

Mesh-based protocol

Mesh-based schemes establish a mesh of paths that connect the sources and destinations. They are more resilient to link failures as well as to mobility.
The major disadvantage of this scheme is that multiple copies of the same packet are disseminated through the mesh, resulting in reduced packet delivery and increased control overhead under highly mobile conditions.

13. What are reactive and proactive protocols? Specify its advantages and Disadvantages. (8) [Nov 2016]

A Classification of Unicast MANET Routing Protocols

- Unicast routing protocols in MANETs are classified into proactive (table-driven), reactive (ondemand) and hybrid protocols.
- This classification is based on how a protocol manages to determine the route correctly in the presence of topology changes.

Proactive protocol:

- A proactive routing protocol is also known as a *table-driven* routing protocol.
- Each node in a *routing table maintains information about routes* to every other node in the network.
- These tables are *periodically updated* in the face of random network topology changes.
- Example protocol - Destination Sequenced Distance Vector (DSDV) protocol.

Reactive protocol:

- A reactive routing protocol is also known as an on-demand routing protocol, since in this protocol nodes do not *maintain up-to-date routes* to different destinations, and new routes are discovered only when required.
- When a node does not have knowledge about any route to a specific destination, it uses a flooding technique to determine the route.
- Two examples of on-demand routing protocols are:

(i) Dynamic source routing (DSR)
(ii) Ad hoc on-demand distance vector routing (AODV)

Hybrid routing protocols:

- Hybrid routing protocols have the characteristics of both proactive and reactive protocols. These protocols combine the good features of both the protocols.
- The hybrid routing protocols are designed to achieve increased scalability by allowing nodes with close proximity to work together to form some sort of a backbone to reduce the route discovery overheads.
- This is mostly achieved by proactively maintaining routes to nearby nodes and determining routes to far away nodes only when required using a route discovery strategy.
- Most hybrid protocols proposed to date are zone-based, which means that the network is partitioned or seen as a number of routing zones by each node.
- Example: Zone Routing Protocol (ZRP).

14. Explain in detail about Vehicular Adhoc Network. (VANET)

Key Points

- VANET – Introduction
- Uses

Vehicular Ad Hoc Networks (VANETs)

- A Vehicular Ad Hoc Network (VANET) is a special type of MANET in which moving automobiles form the nodes of the network.
- VANETs were initially introduced for vehicles of police, fire brigades, and ambulances for safe travelling on road.
- In this network, a vehicle communicates with other vehicles that are within a range of about 100 to 300 metres. Multi-hop communication often results in rather large networks.
- In a city or a busy highway, the diameter of the network can be several tens of kilometres.
- Any vehicle that goes out of the signal range of all other vehicles in the network is excluded from the network.
- A vehicle that was outside the communication range of all other vehicles of a VANET can come in the range of a vehicle that is already in the network and as a result can join the network.
- A VANET can offer a significant utility value to a motorist.

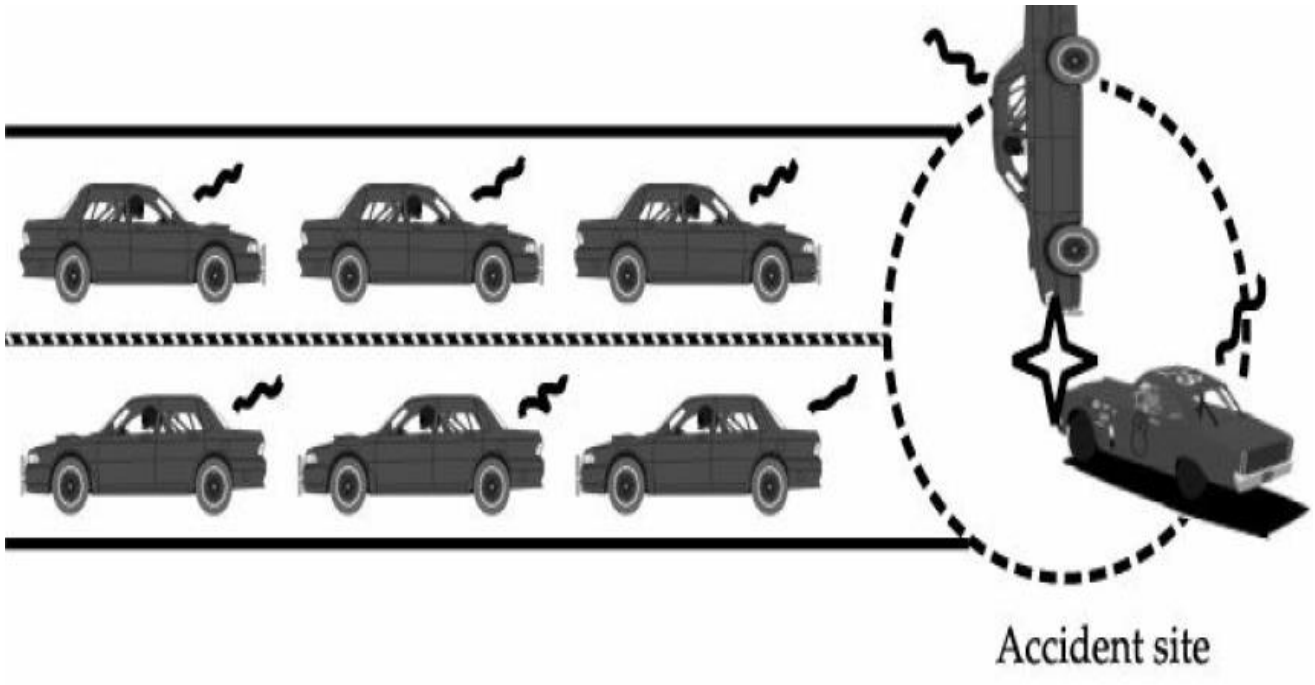


Figure 7.7 *A VANET use scenario.*

A few important uses of a VANET:

A VANET can help drivers to get advance information and warnings from a nearby environment via message exchanges.

For example two vehicles are involved in a collision in the fig.

- The trailing vehicles get advance notification of the collision ahead on the road.
- The driver can also get advance information on the road condition ahead, or a warning about the application of emergency electronic brake by a vehicle ahead in the lane.
- A VANET can help disseminate geographical information to the driver as he continues to drive. For example, the driver would be notified of the nearby food malls or petrol refilling stations, map display, etc.
- Drivers may have the opportunity to engage in other leisurely tasks, such as VoIP with family, watch news highlights, listen to series of media files known as podcasts, or even carry out some business activities such as participate in an office video conference session.

15. Describe the architecture of VANET with the functionality of the components. Compare VANET vs MANET. (16) [Nov 2017]
Describe the architecture of VANET with a neat diagram. (13) [Apr 2018]
Draw and explain the architecture of VANET. (8) [May 2016]

The system architecture of vehicular ad hoc networks

Main Components

- The mobile domain consists of two parts:
  - Vehicle domain
  - Mobile device domain
- The vehicle domain comprises all kinds of vehicles such as cars and buses.

- The mobile device domain comprises all kinds of portable devices like personal navigation devices and smart phones.
- Within the infrastructure domain, there are two domains:
  - Roadside infrastructure domain
  - Central infrastructure domain
- The roadside infrastructure domain contains roadside unit entities like traffic lights.
- The central infrastructure domain contains infrastructure management centers such as traffic management centers (TMCs) and vehicle management centers.

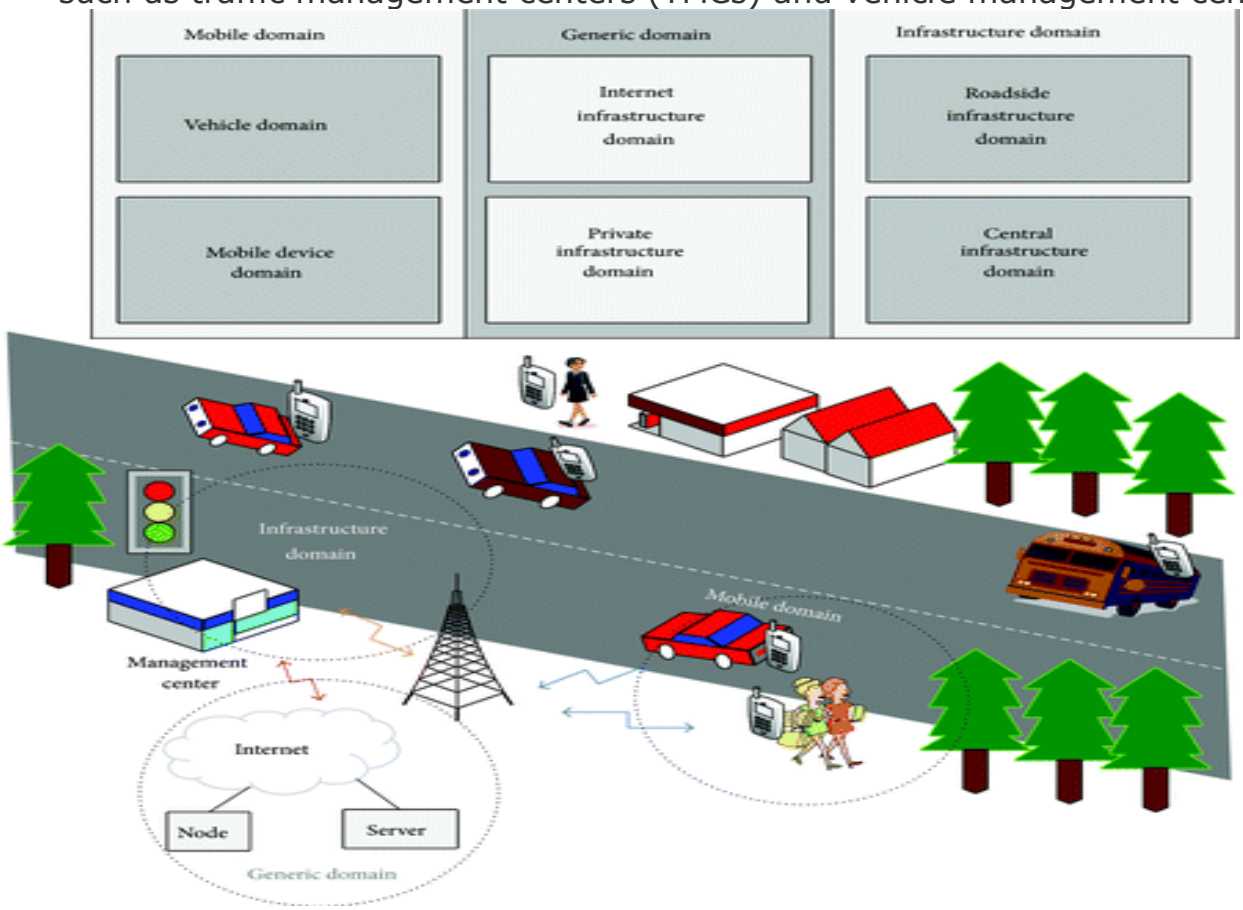
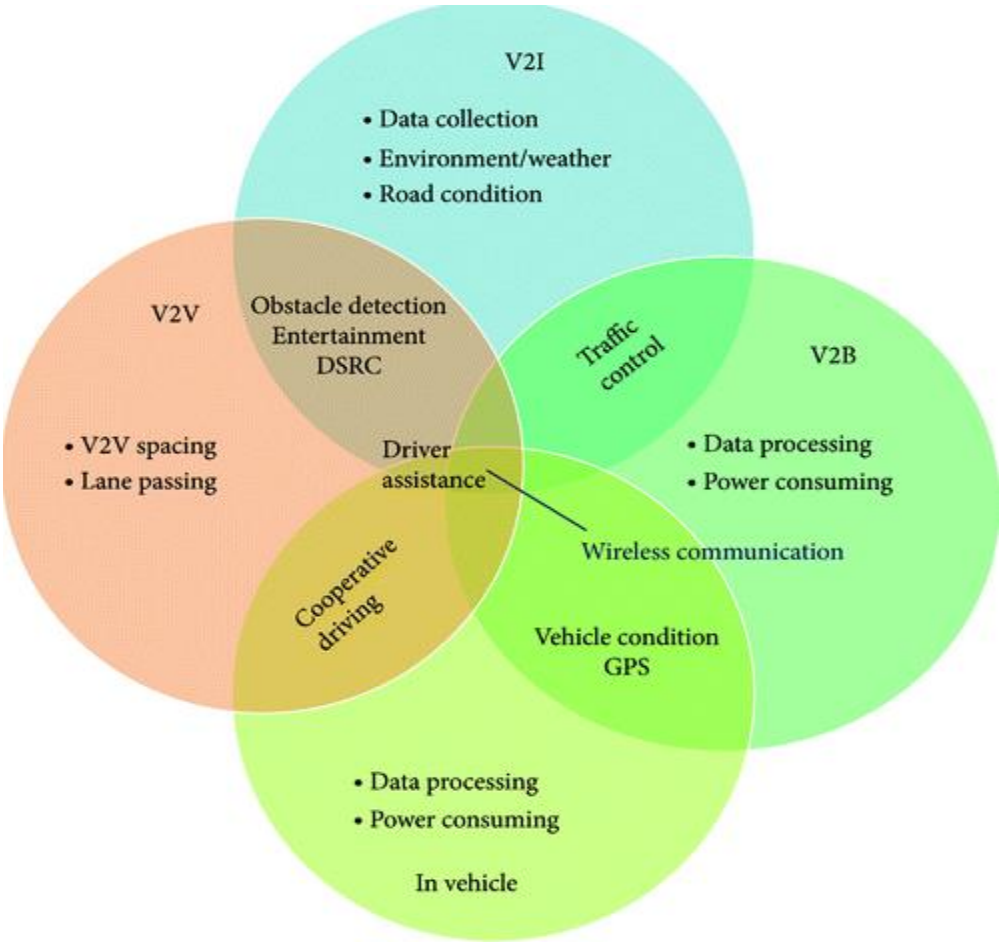


Figure 1 VANETs system domains.

- However, the development of VANETs architecture varies from region to region.
- In the CAR-2-X communication system which is pursued by the CAR-2-CAR communication consortium, the reference architecture is a little different.
- CAR-2-CAR communication consortium (C2C-CC) is the major driving force for vehicular communication in Europe and published its "manifesto" in 2007.
- This system architecture comprises three domains:
  - In-vehicle domain
  - Ad hoc domain
  - Infrastructure domain

Communication Architecture

Communication types in VANETs can be categorized into four types.



Key functions of each communication type.

In-vehicle communication

- Which is more and more necessary and important in VANETs research, refers to the in-vehicle domain.
- In-vehicle communication system can detect a vehicle's performance and especially driver's fatigue and drowsiness, which is critical for driver and public safety.

Vehicle-to-vehicle (V2V)

- *Communication* can provide a data exchange platform for the drivers to share information and warning messages, so as to expand driver assistance.

Vehicle-to-road infrastructure (V2I) communication

- It is another useful research field in VANETs.
- V2I communication enables real-time traffic/weather updates for drivers and provides environmental sensing and monitoring.

Vehicle-to-broadband cloud (V2B) communication

- It means that vehicles may communicate via wireless broadband mechanisms such as 3G/4G.
- As the broadband cloud may include more traffic information and monitoring data as well as infotainment, this type of communication will be useful for active driver assistance and vehicle tracking.

MANET Vs VANET

- A MANET is a collection of mobile nodes that communicate with each other over bandwidth constrained wireless links without any infrastructure support.
- Consider a VANET to be a special category of MANET.
- The nodes are mobile in VANETs as well as in MANETs. However, the VANET nodes (vehicles) can communicate with certain roadside infrastructures or base stations.
- Further, the node mobility in a VANET is constrained to the road topologies, whereas the movement of nodes in a MANET is more random in nature.
- Considering that vehicles move over large distances at relatively high speeds, a VANET undergoes fast topological changes.
- Another important difference is that in a MANET, power is a major constraint but in VANET the battery power available in a vehicle is quite adequate.
- The issues such as the relatively larger size of VANETs compared to MANETs and the relatively high speed with which vehicles move, need to be appropriately considered for the design of an effective VANET.

16. Explain any two VANET routing protocol with an example. (16) [May 17]

Key Points
- Unicast routing protocols
- Multicast/Geocast Routing Protocols

1. Unicast routing protocols
- Unicast routing protocols transmit data packets from a single source to a single destination.
- They are primarily required to support personalised comfort applications and commercial applications such as internet connectivity and multimedia access.
- Unicast routing protocols are the most fundamental protocols in ad hoc environment and they form the basis for constructing other types of protocols.
- Unicast routing protocols are further classified into topology based, position based, cluster based and hybrid protocols

a) Topology based Routing Protocols
- Topology based protocols utilise the global information about the network topology and the information about the communication links for making routing decisions.
- These protocols use either proactive or reactive approaches for routing. Proactive approaches maintain the topology information about all the nodes irrespective of the fact that whether they are presently participating in the communication or not.
- These methods discover network topology information through periodic control packets and operate independent of current communication needs and network conditions.
- This increases overhead of joining new nodes into the network and consumes the network resources for control messages.
- Whereas, reactive protocols determine the routing information for a destination on-demand, only when it is needed for current communication.

- Reactive routing can be classified either as source routing or hop-by-hop routing.
- In source routing complete route information from source to destination is included in data packets, whereas in hop-by-hop routing only the next hop address and the destination address are provided.
- Hop-by-hop routing is better in terms of overall packet delivery ratio and end-to-end delay than source routing and hence it is adopted by most of the routing protocols.
- Examples of proactive protocols are Fisheye State Routing (FSR), Destination-Sequenced Distance-Vector (DSDV) and Optimized Link State Routing (OLSR).
- These protocols maintain a next hop table, which is exchanged among the neighbours.
- Reactive protocols such as Ad hoc On Demand distance Vector (AODV) and Dynamic Source Routing (DSR) have been considered efficient for multi-hop wireless ad hoc networks.
- AODV is a reactive routing protocol, which supports both unicast and multicast routing.
- It uses a destination sequence number, which makes it different from other on-demand routing protocols.
- It reduces memory requirements and the route redundancy. AODV responds to the link failure in the network.

b) Position based Routing Protocols

- In position based protocols, the routing decisions are based on geographic position of the vehicles.
- This does not require establishment or maintenance of routes, but requires location services to determine the position of the destination.
- Some of the commonly used location services include Global Position System (GPS), DREAM Location Services (DLS), Reactive Location Services (RLS) and Simple Location Services (SLS).
- With the advancement of GPS based location services, position based routing protocols are gaining importance. In position based protocols, the packet is sent without any knowledge of digital map to the one-hop neighbour, which is the closest to the position of the destination.
- Every node continuously sends beacon packets with their position information and other node identification parameters.
- Position based protocols are suitable for VANETs since they offer higher delivery ratio than topology based routing protocols in a highly mobile environment.
- They provide minimum delay in establishing the route and achieve good scalability. However, privacy is compromised since navigation information is disclosed on the network.

c) Non-Delay Tolerant Network (Non-DTN)

- Non-DTN protocols are also referred as Mindelay protocols and they aim at minimising the delivery time of the packets from source to destination.

- These protocols are suitable for time critical safety applications, which demand real-time response during data dissemination.
- The delay time in the transmission is the major concern in the design of Non-DTN protocols and usually the shortest path method is adopted.
- However, the shortest path may not always ensure faster delivery, especially when the traffic condition is sparse.
- These protocols are further classified into beacon based, nonbeacon based and hybrid routing protocols.

d) Delay Tolerant Network (DTN) Delay

- Tolerant Network is an approach to networking, which addresses the technical issues related to heterogeneous network that lack continuous network connectivity.
- They are characterized by limitations of latency, bandwidth, error probability and/or path stability.
- DTN uses carry and forward strategy to overcome frequent disconnection of nodes in the network. When a node cannot contact other nodes it stores the packet information and forwards the same when an opportunity arises.

2. Multicast/Geocast Routing Protocols

- Multicast routing enables dissemination of messages from single source to a group of destination nodes of interest.
- Geocast routing is basically a location based multicast routing, which aims to deliver information from a source node to all other nodes within a specified geographical region called a Zone of Relevance (ZOR).
- A Zone of Forwarding (ZOF) is defined within which the packets are directed instead of simply flooding the packets everywhere in the network.
- This reduces the overhead and network congestion. This protocol is applicable for safety and convenience related applications.

a) Topology based Approaches

- Topology based approaches select forwarding nodes based on the network topology information, which can be either multicast tree or multicast mesh.
- A multicast group is not constrained by a particular location; a group of members can be defined by unique and logical group identification such as class-D IP address.
- Robust Vehicular Routing (ROVER) [89] is a reliable geographical multicast protocol, where only control packets are broadcasted in the network and the data packets are unicasted.
- The objective of the protocol is to send a message to all other vehicles within a specified ZOR. When a vehicle receives a message, it accepts the message if it is within the ZOR.
- It also defines a ZOF, which includes the source and the ZOR.
- All vehicles in the ZOF are used in the routing process.
- It uses a reactive route discovery process within a ZOR.
- This protocol creates lot of redundant messages in the network, which leads to congestion and delay in data transfer.

b) Location based Approaches

- Location based approaches select forwarding nodes based on location information such as the position of sending/receiving nodes, the position of neighbouring nodes, and the coordinates of a multicast region.
- Since forwarding nodes are selected during dissemination of each multicast packet, there is no need to maintain multicast trees and hence less overhead.
- These protocols are further divided into two schemes:
- approaches with location-independent and approaches with location-dependent.
- Inter-Vehicles Geocast protocol (IVG) is developed for disseminating safety messages to vehicles on highways.
- The multicast group is defined dynamically using vehicles within the risk area, which is determined by the driving direction and position of vehicles.
- This group is defined temporarily and dynamically by the location, speed, and driving direction of vehicles.
- This protocol uses a timer based mechanism for forwarding messages and periodic broadcasts are used to overcome network fragmentation for delivering messages to the multicast members.
- The rebroadcast period is calculated based on the maximum speed of vehicles.
- Besides, IVG protocol reduces the number of hops by using the deferring time.
- A vehicle, which is farthest from the source node, has less deferring time to rebroadcast.

17. Explain the various security and attacks on VANET. (8) [May 2016]
Explain the architecture of VANET and various security attacks on VANET. (13) [Nov 2018]

Architecture
Refer Q.No.15

- VANETs are themselves vulnerable against attacks that can directly lead to the corruption of networks and then possibly provoke big losses of time, money, and even lives.

VANET Security Requirements

- Confidentiality,
- Integrity,
- Availability.
- Privacy
- Traceability and revocability
- Non-repudiation
- Real-time constraints
- Low Overhead

ATTACKS AND COUNTERMESURES IN VANETS

Denial of Service Attack:

- It is the most serious level attack in vehicular network. In this attack attacker jams the main communication medium and network is no more available to legitimate user.

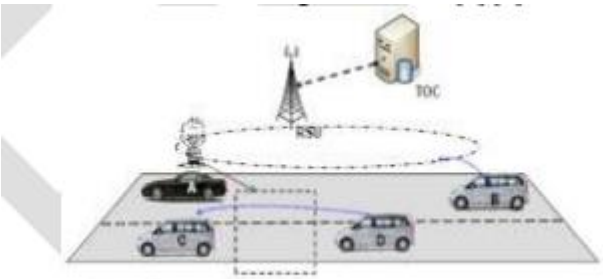


Fig. 2- Denial of Service Attack between V2V and V21

Fig. shows the whole scenario when the attacker A launches DOS attack in vehicular network as a result it Jams the whole communication medium between V2V and V2I and the authentic users (B, C, and D) cannot communicate with each other.

Distributed Denial of Service Attack (DDOS Attack):

- DDOS attacks are those attacks in which attacker attacks in distributed manner from different locations. Attacker may use different timeslots for sending the messages.
- Nature and time slot of the message can be varied from vehicle to vehicle of the attackers. The aim of attacker is same as DOS attack

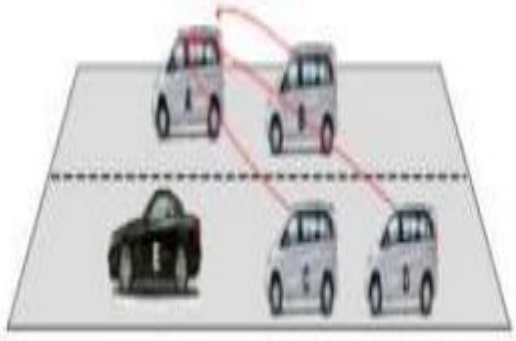


Fig. 3- DDOS Attack in vehicle to vehicle communication

Fig. explains the vehicle to vehicle (V2V) DDOS attack scenario in which attackers (B,C,D) launches DDOS on vehicle A.

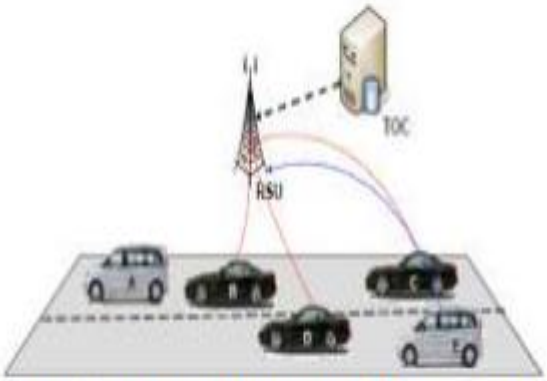


Fig. 4- DDOS Attack in vehicle to Infrastructure communication

Fig explains DDOS attack in vehicle to infrastructure communication. Here B,C,D are the attackers which attacks the infrastructure from different locations.
Whereas other vehicles (A,E) in the network want to access the network then the infrastructure is overloaded.

Sybil Attack:

- It is a critical attack. In this kind of attack attacker sends multiple messages to other vehicles. Each message contains different source identity.
- It creates confusion to other vehicles by sending wrong messages like traffic jam. So there is jam further and vehicles are forced to take another route.
- The main aim of the attacker is to provide an illusion of multiple vehicles to other vehicles so that vehicles can choose another route.

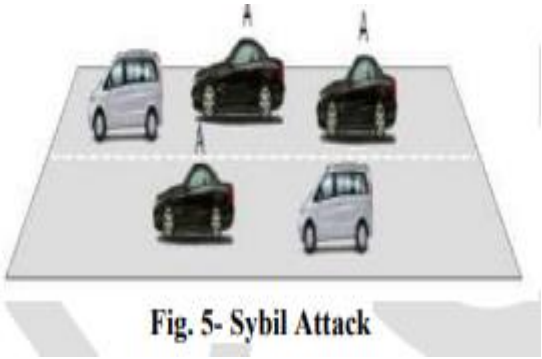


Fig. 5- Sybil Attack

Timing Attack:

- The main objective of attacker is to add some time slot in the original message that creates delay in the original message and these messages are received after these requires a time.
- AS we know safety applications are time critical applications if delay occurs in these applications then major objective of these applications is also finished.

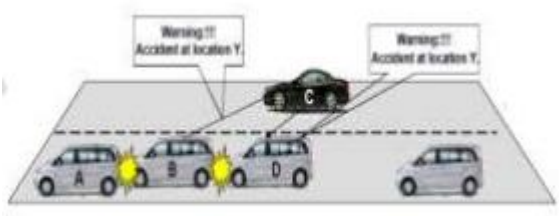


Fig. 9- Timing Attack

Fig. shows the complete scenario of the timing attack in which vehicle C is attacker which receives warning message from other vehicle B and then pass this message to other vehicle D by adding some time. Whenever the other D receives this message then accident actually occurs.

18. Explain in detail about MANET Vs VANET.

- A MANET is a collection of mobile nodes that communicate with each other over bandwidth constrained wireless links without any infrastructure support.
- Consider a VANET to be a special category of MANET.
- The nodes are mobile in VANETs as well as in MANETs. However, the VANET nodes (vehicles) can communicate with certain roadside infrastructures or base stations.
- Further, the node mobility in a VANET is constrained to the road topologies, whereas the movement of nodes in a MANET is more random in nature.
- Considering that vehicles move over large distances at relatively high speeds, a VANET undergoes fast topological changes.
- Another important difference is that in a MANET, power is a major constraint but in VANET the battery power available in a vehicle is quite adequate.
- The issues such as the relatively larger size of VANETs compared to MANETs and the relatively high speed with which vehicles move, need to be appropriately considered for the design of an effective VANET.

19. Explain in detail about Security issues.

Key Points

- Lack of physical boundary
- Low power RF transmissions
- Limited computational capabilities
- Limited power supply

Security Issues in a MANET

- MANETS are fundamentally different from both wired networks and infrastructure-based wireless networks.
- The nature of MANETs not only introduces new security concerns but also exacerbates the problem of detecting and preventing anomalous behaviour.
- In a wired network or in an infrastructure-based wireless network, an intruder is usually a host that is outside the network and therefore could be controlled through a firewall and subjected to access control and authentication.
- In a MANET, on the other hand, an intruder is part of the network, and therefore much more difficult to detect and isolate.
- Dynamic topological changes and the inherent wireless communications in a MANET, make it vulnerable to different types of attacks.
- Wireless links can get jammed and the batteries at the nodes can get depleted by such overloading, causing breakdowns of the network.
- Attackers can also disturb the normal operation of routing protocols by modifying the headers of packets.
- The intruder may insert spurious information while routing packets, causing erroneous routing table updates and thereby leading to frequent misroutings.

A few important characteristics of ad hoc networks that can be exploited to cause security vulnerabilities are the following:

Lack of physical boundary:
Each mobile node functions as a router and forwards packets from other nodes. As a result, network boundaries become blurred. The distinction between nodes that are internal or external to a network becomes meaningless, making it difficult to deploy firewalls or monitor the incoming traffic.

Low power RF transmissions:
It is possible for a malicious node to continuously transmit and monopolise the medium and cause its neighbouring nodes to wait endlessly for transmitting their messages. Also, signal jamming can lead to a denial-of-service (DoS) attack.

Limited computational capabilities:
Nodes in an ad hoc network usually have limited computational capabilities. It therefore becomes difficult to deploy compute-intensive security solutions such as setting up a public-key cryptosystem. Inability to encrypt messages invites a host of security attacks such as spoofing as well as several forms of routing attacks.

Limited power supply:
Since nodes normally rely on battery power, an attacker might attempt to exhaust batteries by causing unnecessary transmissions to take place or might cause excessive computations to be carried out by the nodes.

ANNA UNIVERSITY QUESTIONS

PART A

1. What is the key mechanism in mobile IP? [Nov 2018]
2. State the purpose of Home Location Register (HLR). [Nov 2018]
3. What is the purpose of DHCP? [Apr 2018]
4. What is the purpose of agent solicitation message? [Apr 2018]
5. To which layer do each of the following protocols belong to? What is their functionality? RARP, DNS [Nov 2017]
6. Differentiate the functionalities of a foreign agent and home agent.[Nov 2017]
7. What is Route Optimization? [May 2017]
8. List the modifications proposed in single-hop and multi-hop wireless network. [May 2017]
9. Define COA. [Nov 2016]
10. Illustrate the use of BOOTP protocol? [Nov 2016]
11. What is DHCP? [May 2016]
12. What is encapsulation in mobile IP? [May 2016]
13. Mention the two main design issues of MANET? [Nov 2018]
14. What are the important steps in destination sequence distance vector routing? [Nov 2018]
15. Compare VANET and MANET? [Apr 2018]
16. Differentiate cellular with adhoc networks? [Apr 2018]

17. List the applications of MANET's. [May 2017]
18. Distinguish proactive and reactive protocols. [May 2017]
19. Compare AODV and DSR protocols. [Nov 2017]
20. What are the contents of Link state Advertisement message? [Nov 2017]
21. Outline the concept of RTT? [Nov 2016]
22. Compare and contrast MANET Vs VANET [May 2016, Nov 2016]
23. List the characteristics of MANETs. [May 2016]

ANNA UNIVERSITY QUESTIONS

PART B

1. Explain about the key mechanism in Mobile IP. (16) [Nov 2016]
2. With a diagram explain DHCP and its protocol architecture. (8) [May 2016]
3. Explain IP in IP, minimal IP and GRE encapsulation methods. (8) [May 2016]
4. Illustrate packet delivery mechanism in mobile IP network with a neat Diagram. (16) [Nov 2017]
5. What is Encapsulation? Explain in detail the various encapsulation techniques in mobile IP. (16) [May 2017]
6. Explain mobile IP requirement and terminologies. (8) [Nov 2018]
7. Why the traditional IP cannot be used in the mobile network. In what way does mobile IP support mobile Hubs? (5) [Nov 2018]
8. Discuss Route Discovery and Route Maintenance mechanisms in DSR with Illustrations. List its merits and demerits. (16) [Nov 2017]
9. Describe the architecture of VANET with the functionality of the components. Compare VANET vs MANET. (16) [Nov 2017]
10. Explain the design issues of MANET routing protocols in detail. (16) [May 2017]
11. Explain any two VANET routing protocol with an example. (16) [May 2017]
12. Explain the Traditional Routing Protocols. (16) [Nov 2016]
13. What Multicast routing protocols. (8) [Nov 2016]
14. What are reactive and proactive protocols? Specify its advantages and Disadvantages. (8) [Nov 2016]

15. Explain characteristics, Applications of MANET. (4+4) [May 2016]
16. Explain DSR Routing Protocols in detail. (8) [May 2016]
17. Draw and explain the architecture of VANET. (8) [May 2016]
18. Explain the various security and attacks on VANET. (8) [May 2016]
19. Illustrate DSR routing in detail and compare it with DSDV. (13) [Nov 2018]
20. Explain the architecture of VANET and various security attacks on VANET. (13) [Nov 2018]
21. Describe the architecture of VANET with a neat diagram. (13) [Apr 2018]
22. Explain the design issues in MANET and the applications of adhoc network. (13) [Apr 2018]

UNIT II - MOBILE TELECOMMUNICATION SYSTEM

Introduction to Cellular Systems - GSM – Services & Architecture – Protocols – Connection Establishment – Frequency Allocation – Routing – Mobility Management – Security – GPRS- UMTS – Architecture – Handover – Security

PART A

1) List the subsystems of GSM. [Nov 2018]

Radio Subsystem (RSS) - MS, BSS, BTS, BSC
Networking and Switching Subsystem (NSS) - MSC
Operation Subsystem (OSS) - OMC, AuC, EIR

2) What is the function of Gateway GPRS support node? [Nov 2018]

- A Gateway GPRS Support Node (GGSN) is part of the core network that connects GSM- based 3G networks to the Internet.
- The GGSN, sometimes known as a wireless router, works in tandem with the Serving GPRS Support Node (SGSN) to keep mobile users connected to the Internet and IP-based applications.
- The GGSN converts incoming data traffic from mobile users (via the SGSN) and forwards it to the relevant network, and vice versa.
- The GGSN and the SGSN together form the GPRS support nodes (GSN). The GGSN is also linked into hosted services (such as voice and video) and to the billing, policy control, and user verification elements of the core network.

3) What is frequency range of uplink and downlink in GSM network? [Apr 2018]

- GSM-1800 uses 1710 - 1785 MHz to send information from the Mobile Station to the Base Transceiver Station (uplink) and 1805 - 1880 MHz for the other direction (downlink), providing 374 channels (channel numbers 512 to 885). Duplex spacing is 95 MHz.
- GSM-900 uses 890 - 915 MHz to send information from the Mobile Station to the Base Transceiver Station (uplink) and 935 - 960 MHz for the other direction (downlink), providing 124 RF channels (channel numbers 1 to 124) spaced at 200 kHz. Duplex spacing of 45 MHz is used.

4) What are the informations are stored in SIM? [Apr 2018]

- The SIM is a removable smart card.
- a SIM card is a very important component of a GSM network
- It contains all the subscription information of a subscriber and holds the key information that activates the phone after it is powered on.
- Identification information is stored in the SIM card's protected memory (ROM) that is not accessible or modifiable by the customer.
- The SIM card contains many other identifiers and tables such as card type, serial number, a list of subscribed services, and a Personal Identity Number (PIN).

5) List the services of GPRS? [Nov 2017]

i) Point-to-Point (PTP) service

- The PTP service is between two users and can either be connectionless or connection-oriented.

(ii) Point-to-Multipoint (PTM) service.

- The PTM is a data transfer service from one user to multiple users.
- Again, there are two types of PTM services.
    - One is multicast PTM where the data packets are broadcast in a certain area

Other is group call PTM where the data packets are addressed to a group of users.

6) Define Handoff. What are its types? [Nov 2017]

- Handover or handoff refers to the process of transferring an ongoing call or data session from one channel connected to the core network to another channel.
- In satellite communications it is the process of transferring satellite control responsibility from one earth station to another without loss or interruption of service.

Types:

- Hard Handoff
- Soft Handoff

7) Name the teleservices provided by GSM? [May 2017]

a. Telephony
b. Emergency number
c. Short message services
d. Fax

8) Write the suggestions of mobile phone with respect to human body. [May 2017]

- The effect of mobile phone radiation on human health is a subject of interest and study worldwide, as a result of the enormous increase in mobile phone usage throughout the world.
- As of 2015, there were 7.4 billion subscriptions worldwide, though the actual number of users is lower as many users own more than one mobile phone.
- Mobile phones use electromagnetic radiation in the microwave range (450–3800 MHz).
- Other digital wireless systems, such as data communication networks, produce similar radiation.

9) Write about the supplementary services in GSM? [Nov 2016]

Supplementary services are provided on top of teleservices or bearer services, and include features such as caller identification, call forwarding, call waiting, multi-party conversations, and barring of outgoing (international) calls, among others.

10) What is multitasking? [Nov 2016]

- Multitasking involves being able to rapidly switch between different apps and to combine multiple sources of information.
- Small mobile screens limit users' ability to see content from different apps at the same time, so current operating-system support for multitasking focuses mostly on switching between different apps.
- This increases users' memory load, so mobile designers must help users compare and rapidly retrieve recent items.

11) List the 3 important features of GSM security. [May 2016]

Key features of GSM

1. International Roaming -single subscriber number worldwide.
2. Superior speech quality -better than existing analog cellular technology.
3. High level of security -user's information is safe and secure.
4. Universal and Inexpensive Mobile handsets.
5. Digital Convenience -talk time is doubled per battery life and digital networks can handle higher volume of calls at any one time that analog networks.
6. New services - such as call waiting, call forwarding, Short Message Service (SMS), GSM Packet Radio Service (GPRS).
7. Digital compatibility – easily interfaces with existing digital networks i.e. Integrated Services Digital Network (ISDN).

12) What are the main elements of UMTS? [May 2016]

1. **User Equipment (UE):** The User Equipment or UE is the name given to what was previous termed the mobile, or cellphone. It could also be anything between a mobile phone used for talking to a data terminal attached to a computer with no voice capability.
2. **Radio Network Subsystem (RNS):** The RNS also known as the UMTS Radio Access Network, UTRAN, is the equivalent of the previous Base Station Subsystem or BSS in GSM. It provides and manages the air interface fort the overall network.
3. **Core Network:** The core network provides all the central processing and management for the system. It is the equivalent of the GSM Network Switching Subsystem or NSS.

13) Write about GSM?

GSM (Global System for Mobile Communications) is at present being used in India. It is possibly the most successful digital mobile system to have ever been used till now. An important characteristic of the GSM system is that it provides data services in addition to voice services, and yet is compatible to 1G system.

14) List out GSM radio frequencies?

- Operate either in the 900 MHz or in the 1800 MHz frequency bands.
- 850 MHz and 1900 MHz bands
- 400 MHz and 450 MHz frequency b

- uplink frequency band is 890–915 MHz, and the downlink frequency band is 935–960 MHz

15) List out GSM services?

(i) Bearer services
(ii) Teleservices
(iii) Supplementary services

16) Define Bearer services?

Bearer services give the subscribers the capability to send and receive data to/from remote computers or mobile phones. For this reason, bearer services are also known as data services

17) List out some of Teleservices?

- Telephony
- Emergency number
- Short message services
- Fax

18) What are all the radio frequency elements compressed by RSS?

- The mobile stations,
- The base station subsystems,
- The base transceiver station
- And the base station controller

19) Define Base Station Subsystem?(BSS)

- A GSM network comprises many BSSs. Each BSS consists of **A Base Station Controller (BSC)** and Several **Base Transceiver Stations (BTSs).**
- A BSS performs all functions necessary to **maintain radio connections to an MS**, as well **as does coding/decoding of voice**.

20) Define Base Transceiver Station?

(BTS):

A BTS **comprises all radio equipment** such as antenna, signal processors and amplifiers that are necessary for radio transmission.

- It encodes the received signal,
- modulates it on a carrier wave,
- and feeds the RF signals to the antenna.
- It communicates with both the mobile station and the BSC.

22) Define Base Station Controller? (BSC):

- A BSC manages the radio resource of the BTSs in the sense that **it assigns frequency and time slots for all MSs in the area**.
- It also manages the handoff from one BTS to another within the BSS. The BSC also multiplexes the radio channels onto the fixed network connection to the Mobile Switching Centre (MSC).

23) Define Network and switching subsystem? (NSS)

- This subsystem forms the heart of the GSM system.
- It connects the wireless networks to the standard public networks and carries out usage-based charging, accounting, and also handles roaming.
- NSS consists of a switching centre and several databases as described below.

24) Define Mobile Switching Center? (MSC):

- An MSC can be considered to form the heart of a GSM network. An MSC sets up connections to other MSCs and to other networks such as Public Data Network (PDN).
- An MSC is responsible for the connection setup, connection release, and call handoff to other MSCs.
- A Gateway MSC (GMSC) is responsible for gateway functions, while a customer roams to other networks. It also performs certain other supplementary services such as call forwarding, multiparty calls, etc.

25) Define Home Location Registers? (HLRs):

A HLR stores in a database important information that is specific to each subscriber. The information contains subscriber's IMSI, pre/post paid, user's current location, etc.

26) Define Visitor Location Register? (VLR):

- It is essentially a temporary database that is updated whenever a new MS enters its area by roaming.
- The information is obtained from the corresponding HLR database. The function of the VLR is to reduce the number of queries to the HLR and make the user feel as if he were in his home network.

27) Define Operation subsystem (OSS)?

- **Operation and Maintenance Centre (OMC):** It supervises all other network entities. Its functions are traffic monitoring, subscribers, security management and accounting billing.
- **Authentication Centre** (**AuC**)**:** It protects against intruders targeting the air interface. The AuC stores information concerned with security features such as user authentication and encryption. The AuC is related to the HLR.
- **Equipment Identity Register (EIR):** It is essentially a database that is used to track handsets using the IMEI. It helps to block calls from stolen, unauthorized, or defective mobiles.

28) List out 3 levels of GSM Security?

- Operator's level,
- Customer's level and
- System level.

29) Define General Packet Radio Service (GPRS)

It transfers data packets from GSM mobile stations to external packet data networks (PDNs). Packets can be directly routed from the GPRS mobile stations to packet switched networks making it easy to connect to the Internet.

30) Define Point-to-Point (PTP) service?

- **The PTP service** is between two users and can either be connectionless or connection-oriented.
-

31) Define Point-to-Multipoint (PTM) service?

- **The PTM** is a data transfer service from one user to multiple users.
- Again, **there are two types of PTM services**.
- **One is multicast PTM** where the data packets are broadcast in a certain area
- **Other is group call PTM** where the data packets are addressed to a group of users.

32) Define GSN & GGSN?

- **A GSN** is essentially a router. All GSNs are integrated into a standard GSM architecture.
- The **GGSN** is the interworking unit between the GPRS network and the external packet data network (PDN).
- The **GGSN** contains routing information for GPRS users, performs address connection and tunnels data to a user through encapsulation.

33) Dissimilarities between UTMS networks?

- Higher speech quality
- Higher data rate
- Virtual home environment

34) Define User Equipment? (UE):

- The User Equipment (UE) is the name by which a cell phone is referred to.
- The new name was chosen because of the considerably greater functionality that the UE incorporates compared to a cell phone.
- It can be thought of as both a mobile phone used for talking and a data terminal attached to a computer with no voice capability.

35) Define Radio Network Subsystem? (RNS):

The RNS is the equivalent of the Base Station Subsystem (BSS) in GSM. It provides and manages the wireless interface for the overall network.

36) Define Core Network?

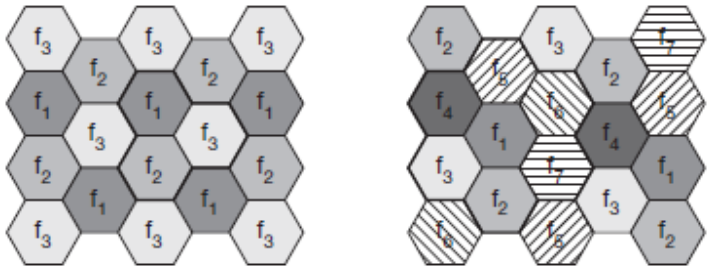
The core network is the equivalent of the GSM Network Switching Subsystem (NSS).

PART B

1) Explain in architecture of cellular mobile communication with neat diagram and its advantage and disadvantage of cellular system with small cells (NOV 2013)

- Cellular systems for mobile communications implement SDM. Each transmitter, typically called a **base station**, covers a certain area, a **cell**.
- Cell radii can vary from tens of meters in buildings, and hundreds of meters in cities, up to tens of kilometers in the countryside.
- The shape of cells are never perfect circles or hexagons (as shown in Figure 2.41), but depend on the environment (buildings, mountains, valleys etc.), on weather conditions, and sometimes even on system load.
- Typical systems using this approach are mobile telecommunication systems, where a mobile station within the cell around a base station communicates with this base station and vice versa

Figure 2.41
Cellular system with three and seven cell clusters



Advantages of cellular systems with small cells are the following:

- Higher capacity: Implementing SDM allows frequency reuse. If one transmitter is far away from another.
- less transmission power: While power aspects are not a big problem for base stations, they are indeed problematic for mobile stations. A receiver far away from a base station would need much more transmit power than the current few Watts.
- Local interference only: Having long distances between sender and receiver results in even more interference problems. With small cells, mobile stations and base stations only have to deal with „local" interference.
- Robustness: Cellular systems are decentralized and so, more robust against the failure single components. If one antenna fails, this only influences communication within a small area.

Small cells also have some disadvantages:

- Infrastructure needed: Cellular systems need a complex infrastructure to Connect all base stations.
- Handover needed: The mobile station has to perform a handover when changing from one cell to another. Depending on the cell size and the speed of movement, this can happen quite often.
- Frequency planning: To avoid interference between transmitters using the Same frequencies, frequencies have to be distributed carefully

2) Explain detail about Global System for Mobile Communications (GSM) services, Architecture and security with neat diagram?

Key Points

GSM (Global System for Mobile Communications) – Introduction

GSM Services

- Bearer services - (transparent or non-transparent)
- Teleservices - (voice-oriented teleservices and the non-voice teleservices)
- Supplementary services – (user identification, call redirection, and forwarding of ongoing calls)

System Architecture of GSM

- Radio Subsystem (RSS) - MS, BSS, BTS, BSC
- Networking and Switching Subsystem (NSS) - MSC
- Operation Subsystem (OSS)- OMC, AuC, EIR

GSM (Global System for Mobile Communications)

An important characteristic of the GSM system is that it provides **data services** in addition to **voice services**, and yet is compatible to 1G system.

GSM networks operate in **four different radio frequencies**.

- GSM networks **operate either in the 900 MHz or in the 1800 MHz** frequency bands.
- Some countries in the American continent use the **850 MHz and 1900 MHz** bands because the 900 MHz and 1800 MHz frequency bands are already allocated for other purposes.
- The relatively rarely used **400 MHz and 450 MHz** frequency bands are assigned in some countries
- In the 900 MHz band, the **uplink frequency band is 890–915 MHz**, and the **downlink frequency band is 935–960 MHz**

1) GSM Services

GSM provides three main categories of services.

(i) Bearer services
(ii) Teleservices
(iii) Supplementary services

i) Bearer services

- Bearer services give the subscribers the capability **to send and receive data to/from remote computers or mobile phones**. For this reason, **bearer services are also known as data services.**
- These services also enable the transparent transmission of data between GSM and other networks like PSTN, ISDN, etc. at rates from 300 bps to 9600 bps.
- These services are **implemented on the lower-three layers of the OSI reference model**. Besides supporting SMS, e-mail, voice mailbox, and Internet access, this service provides the users with the capability to execute remote applications. **GSM supports data transfer rates of up to 9.6 kbps.**
- Bearer services permit **either transparent or non-transparent**, **and either synchronous or asynchronous** modes of data transmission.

The transparent bearer services:

- The transparent bearer services use the functions of the physical layer of transmission of data leading to constant delay and throughput if no transmission errors occur.
- There is a mechanism called **FEC (Forward Error Correction)** to increase the quality of data transmission.

The non-transparent bearer services:

- The non-transparent bearer services use protocols of the second and third layers to implement error correction and flow control.
- They use transparent bearer services in addition to a Radio Link Protocol (RLP). This protocol comprises mechanisms of high level data link control.

BOX 2.1 GSM bearer services

The GSM data services are named *bearer* services.
Consider the following example: Suppose a customer requires to send a data file such as a picture to a computer at the office that is connected to a public telephone network.
In this example, the bearer service provides 9.6 kbps circuit switched data

transfer. The handset dials the office computer telephone number and establishes a connection with it via the modem. When the office computer modem accepts the call, the customer's handset begins to send data directly on the telephone line channel at 9.6 kbps.

ii) Teleservices

- GSM provides **both the voice-oriented teleservices and the non-voice teleservices**, as discussed below.

Telephony:

- The main goal of GSM was to provide high quality digital voice transmission, offering the bandwidth of 3.1 kHz of analog phone systems.
- Special codec's(**a device or program that compresses data to enable faster transmission and decompresses received data.)** are used for voice transmission, while other codec's are used for the transmission of analog data for communication with traditional computer modems used in fax machines.

Emergency number:

- The same number is used throughout an area. This service is free of cost and mandatorily provided by all service providers. This connection will automatically be set up with the closest emergency centre.

Short message services:

- This service offers transmission of text messages of sizes up to 160 characters. SMS services use the signaling channels, making possible the duplex system of the sending and receiving the SMSs messages.

Fax:

- In this service, using modems fax data is transmitted as digital data over the analog telephone network according to the ITU-T Standards T.4 and T.30.

iii) Supplementary services

- GSM provides certain supplementary services such as user identification, call redirection, and forwarding of ongoing calls. In addition, standard ISDN features such as 'close user groups and 'multiparty' communication are available.

Describe GSM architecture and its services in detail. (8) [May 2016]
Explain GSM architecture and its services with neat diagram. (16) [May 2017][Nov 2017]
Describe about the system architecture of Global System for Mobile Communication. (13) [Nov 2018]

2) System Architecture of GSM

A GSM system consists of three main subsystems:

(i) Radio Subsystem (RSS)
(ii) Networking and Switching Subsystem (NSS)
(iii) Operation Subsystem (OSS)

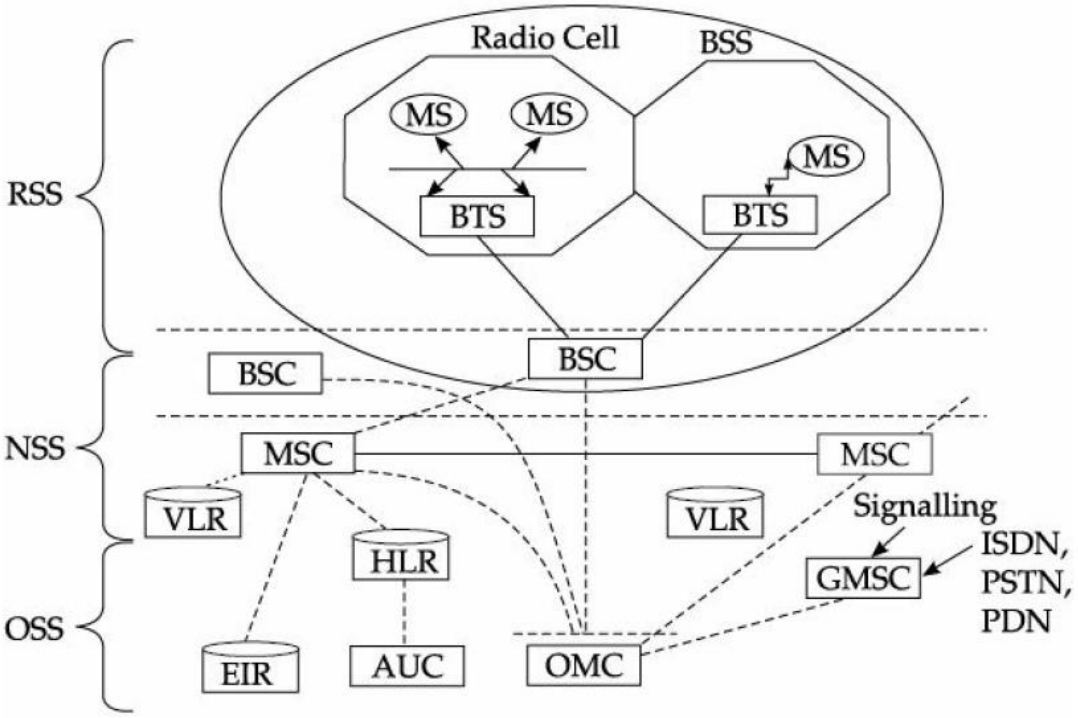


Figure 2.9 *Functional architecture of a GSM system.*

(i) Radio subsystem (RSS)

This subsystem **comprises** all the radio specific entities. That is,

i) The mobile stations,
ii) The base station subsystems,
iii) The base transceiver station
iv) And the base station controller.

The important components of **the radio subsystem** in the following:

Mobile Station (Ms)*:*

A mobile station (MS) or cell phone contains **two major components**:

a. The subscriber identity module **(SIM)**
b. And the **Mobile Device.**

a) The subscriber identity module (SIM)

- The SIM is a removable smart card.
- Each mobile device has a unique identifier that is known as its **IMEI (International Mobile Equipment Identity)**.
- Apart from the telephone interface, an **MS** also offers other types of interfaces to the users such as USB, Bluetooth, etc.
- Despite its small size, **a SIM card is a very important component of a GSM network**.
- It contains all the **subscription information of a subscriber** and holds **the key information that activates the phone** after it is powered on.
- It contains **a microcontroller** to primarily **store and retrieve data from the flash storage** on the SIM.
- **Identification information is stored in the SIM card's protected memory (ROM)** that is not accessible or modifiable by the customer.

- The SIM card contains many other identifiers and tables such as card type, serial number, a list of subscribed services, and a Personal Identity Number (PIN).

b) The Mobile Device

- **Additional flash memory** is included in the mobile device to allow storage of other information such as addresses, pictures, audio and video clips, and short messages.

Base Station Subsystem (BSS):

- A GSM network comprises many BSSs. Each BSS consists of **A Base Station Controller (BSC)** and Several **Base Transceiver Stations (BTSs).**
- A BSS performs all functions necessary to **maintain radio connections to an MS**, as well **as does coding/decoding of voice**.

Base Transceiver Station (BTS):

A BTS **comprises all radio equipment** such as antenna, signal processors and amplifiers that are necessary for radio transmission.

- It encodes the received signal,
- modulates it on a carrier wave,
- and feeds the RF signals to the antenna.
- It communicates with both the mobile station and the BSC.

Base Station Controller (BSC):

- A BSC manages the radio resource of the BTSs in the sense that **it assigns frequency and time slots for all MSs in the area**.
- It also manages the handoff from one BTS to another within the BSS. The BSC also multiplexes the radio channels onto the fixed network connection to the Mobile Switching Centre (MSC).

(ii) Network and switching subsystem (NSS)

- This subsystem forms the heart of the GSM system.
- It connects the wireless networks to the standard public networks and carries out usage-based charging, accounting, and also handles roaming.
- NSS consists of a switching centre and several databases as described below.

Mobile Switching Center (MSC):

- An MSC can be considered to form the heart of a GSM network. An MSC sets up connections to other MSCs and to other networks such as Public Data Network (PDN).
- An MSC is responsible for the connection setup, connection release, and call handoff to other MSCs.
- A Gateway MSC (GMSC) is responsible for gateway functions, while a customer roams to other networks. It also performs certain other supplementary services such as call forwarding, multiparty calls, etc.

Home Location Registers (HLRs):

- A HLR stores in a database important information that is specific to each subscriber. The information contains subscriber's IMSI, pre/post paid, user's current location, etc.

Visitor Location Register (VLR):

- It is essentially a temporary database that is updated whenever a new MS enters its area by roaming.

- The information is obtained from the corresponding HLR database. The function of the VLR is to reduce the number of queries to the HLR and make the user feel as if he were in his home network.

(iii) Operation subsystem (OSS)

The operation subsystem contains all the functions necessary for network operation and maintenance.

It consists of the following:

- **Operation and Maintenance Centre (OMC):** It supervises all other network entities. Its functions are traffic monitoring, subscribers, security management and accounting billing.
- **Authentication Centre** (**AuC**)**:** It protects against intruders targeting the air interface. The AuC stores information concerned with security features such as user authentication and encryption. The AuC is related to the HLR.
- **Equipment Identity Register (EIR):** It is essentially a database that is used to track handsets using the IMEI. It helps to block calls from stolen, unauthorized, or defective mobiles.

Explain GSM Authentication and security. (8) [May 2016]

3) GSM Security

Security in GSM is broadly supported at three levels:

- Operator's level,
- Customer's level and
- System level.

The following are a few important features associated with providing security in GSM networks.

Authentication

- The purpose of authentication is to protect the network against unauthorized use. In the GSM context, it helps protect the GSM subscribers by denying the possibility for intruders to impersonate authorized users.
- A GSM network operator can verify the identity of the subscriber, making it highly improbable to clone someone else's mobile phone identity.
- Authentication can be achieved in a simple way by using a password such as Personal Identification Number (PIN).

Confidentiality

- A GSM network protects voice, data and sensitive signaling information (e.g. dialed digits) against eavesdropping (**secretly listen to a conversation**) on the radio path.
- Confidentiality of subscriber-dialed information in the GSM network is achieved by using encryption techniques prescribed by the GSM designers.
- Data on the radio path is encrypted between the Mobile Equipment (ME) and the BTS which protects user traffic and sensitive signaling data against eavesdropping.

Anonymity (unknown or unacknowledged)

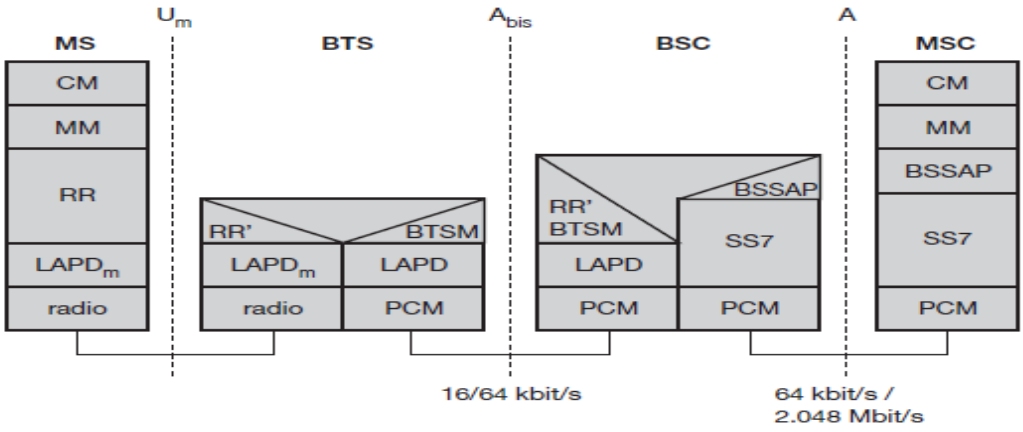
- A GSM network protects against someone tracking the location of a user or identifying calls made to (or from) the user by eavesdropping on the radio path.
- The anonymity of the subscriber on the radio access link in the GSM network is achieved by allocating Temporary Mobile Subscriber Identity (TMSIs) instead of permanent identities.
- This helps to protect against tracking a user's location and obtaining information about a user's calling pattern.

3) Explain in detail about GSM Protocol stack with neat diagram? Explain in detail about Radio Resource Management (RR), Connection Management (CM) and Mobility Management (MM).

GSM PROTOCOL STACK

GSM architecture is a layered model that is designed to allow communications between two different systems. The lower layers assure the services of the upper-layer protocols. Each layer passes suitable notifications to ensure the transmitted data has been formatted, transmitted, and received accurately.

The GMS protocol stacks diagram is shown below:



MS Protocols

Based on the interface, the GSM signaling protocol is assembled into three general layers:

- **Layer 1** : The physical layer. It uses the channel structures over the air interface.
- **Layer 2** : The data-link layer. Across the Um interface, the data-link layer is a modified version of the Link access protocol for the D channel (LAP-D) protocol used in ISDN, called Link access protocol on the Dm channel (LAP-Dm). Across the A interface, the Message Transfer Part (MTP), Layer 2 of SS7 is used.
- **Layer 3** : GSM signalling protocol's third layer is divided into three sublayers:
  - Radio Resource Management (RR),
  - Mobility Management (MM), and

- Connection Management (CM).

MS to BTS Protocols

- The RR layer is the lower layer that manages a link, both radio and fixed, between the MS and the MSC. For this formation, the main components involved are the MS, BSS, and MSC.
- The responsibility of the RR layer is to manage the RR-session, the time when a mobile is in a dedicated mode, and the radio channels including the allocation of dedicated channels.
- The MM layer is stacked above the RR layer. It handles the functions that arise from the mobility of the subscriber, as well as the authentication and security aspects.
- Location management is concerned with the procedures that enable the system to know the current location of a powered-on MS so that incoming call routing can be completed.
- The CM layer is the topmost layer of the GSM protocol stack. This layer is responsible for Call Control, Supplementary Service Management, and Short Message Service Management.
- Each of these services is treated as individual layer within the CM layer. Other functions of the CC sublayer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

BSC Protocols

- The BSC uses a different set of protocols after receiving the data from the BTS. The Abis interface is used between the BTS and BSC.
- At this level, the radio resources at the lower portion of Layer 3 are changed from the RR to the Base Transceiver Station Management (BTSM).
- The BTS management layer is a relay function at the BTS to the BSC.
- The RR protocols are responsible for the allocation and reallocation of traffic channels between the MS and the BTS.
- The BSC still has some radio resource management in place for the frequency coordination, frequency allocation, and the management of the overall network layer for the Layer 2 interfaces.
- To transit from the BSC to the MSC, the BSS mobile application part or the direct application part is used, and SS7 protocols is applied by the relay, so that the MTP 1-3 can be used as the prime architecture.

MSC Protocols

- At the MSC, starting from the BSC, the information is mapped across the A interface to the MTP Layers 1 through 3.
- Here, Base Station System Management Application Part (BSS MAP) is said to be the equivalent set of radio resources.
- The relay process is finished by the layers that are stacked on top of Layer 3 protocols; they are BSS MAP/DTAP, MM, and CM. This completes the relay process.
- Each GSM MS user is given a HLR that in turn comprises of the user's location and subscribed services.
- VLR is a separate register that is used to track the location of a user. When the users move out of the HLR covered area, the VLR is notified by the MS to find the location of the user.

- The VLR in turn, with the help of the control network, signals the HLR of the MS's new location. With the help of location information contained in the user's HLR, the MT calls can be routed to the user.

4) Explain in detail about the handovers of GSM. (8) [Nov 2016]
Write in detail about the various types of handover in GSM. Also discuss the timeline diagram of the intra MSC handover. (13) [Apr 2018]

Requirements for GSM handover

- 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.
- Accordingly GSM handover was an area to which particular attention was paid when developing the standard.

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: **Intra-cell 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 changes the channel or slot.

Inter-BTS Intra BSC handover: **Inter-cell, intra-BSC handover**

- This form of GSM handover or GSM handoff occurs when the mobile moves 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: **Inter-BSC, intra-MSC handover**

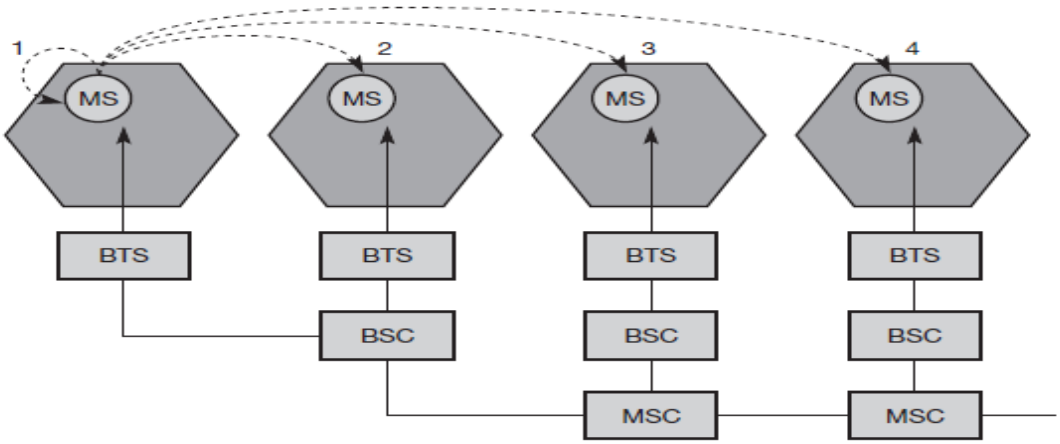
- When the mobile moves out of the range of cells controlled by one BSC, a more involved form of handover has to be performed, handing over not only from one BTS to another but one BSC to another. For this the handover is controlled by the MSC.

Inter-MSC handover: **Inter MSC handover**

- This form of handover occurs when changing between networks. The two MSCs involved negotiate to control the handover.

GSM handover process

- Although there are several forms of GSM handover as detailed above, as far as the mobile is concerned, they are effectively seen as very similar.
- There are a number of stages involved in undertaking a GSM handover from one cell or base station to another.
- In GSM which uses TDMA techniques the transmitter only transmits for one slot in eight, and similarly the receiver only receives for one slot in eight.



Types of HANDOVER IN GSM

- As a result the RF section of the mobile could be idle for 6 slots out of the total eight.
- This is not the case because during the slots in which it is not communicating with the BTS, it scans the other radio channels looking for beacon frequencies that may be stronger or more suitable.
- In addition to this, when the mobile communicates with a particular BTS, one of the responses it makes is to send out a list of the radio channels of the beacon frequencies of neighboring BTSs via the Broadcast Channel (BCCH).
- The mobile scans these and reports back the quality of the link to the BTS.
- In this way the mobile assists in the handover decision and as a result this form of GSM handover is known as Mobile Assisted Hand Over (MAHO).
- The network knows the quality of the link between the mobile and the BTS as well as the strength of local BTSs as reported back by the mobile.
- It also knows the availability of channels in the nearby cells. As a result it has all the information it needs to be able to make a decision about whether it needs to hand the mobile over from one BTS to another.
- If the network decides that it is necessary for the mobile to hand over, it assigns a new channel and time slot to the mobile.
- It informs the BTS and the mobile of the change. The mobile then retunes during the period it is not transmitting or receiving, i.e. in an idle period.
- A key element of the GSM handover is timing and synchronization. There are a number of possible scenarios that may occur dependent upon the level of synchronization.

Old and new BTSs synchronized:

- In this case the mobile is given details of the new physical channel in the neighboring cell and handed directly over.
- The mobile may optionally transmit four access bursts. These are shorter than the standard bursts and thereby any effects of poor synchronization do not cause overlap with other bursts.
- However in this instance where synchronization is already good, these bursts are only used to provide a fine adjustment.

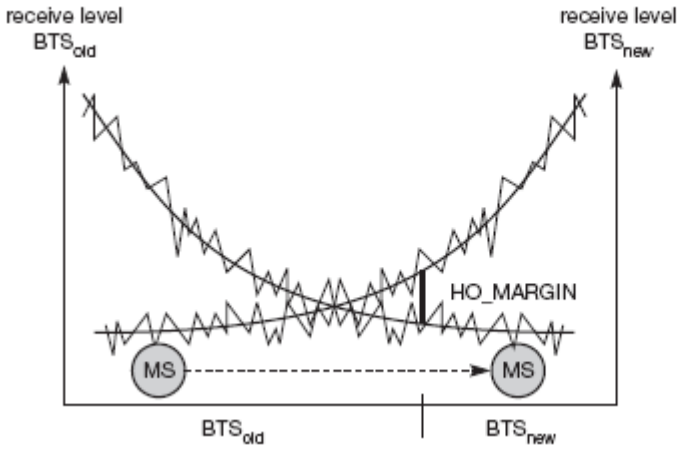


Figure 4.12 Handover decision depending on receive level

Time offset between synchronized old and new BTS:

- In some instances there may be a time offset between the old and new BTS. In this case, the time offset is provided so that the mobile can make the adjustment.
- The GSM handover then takes place as a standard synchronized handover.

Non-synchronized handover:

- When a non-synchronized cell handover takes place, the mobile transmits 64 access bursts on the new channel.
- This enables the base station to determine and adjust the timing for the mobile so that it can suitably access the new BTS. This enables the mobile to re-establish the connection through the new BTS with the correct timing.

Inter-system handover

- With the evolution of standards and the migration of GSM to other 2G technologies including to 3G UMTS / WCDMA as well as HSPA and then LTE, there is the need to handover from one technology to another.
- Often the 2G GSM coverage will be better then the others and GSM is often used as the fallback.
- When handovers of this nature are required, it is considerably more complicated than a straightforward only GSM handover because they require two technically very different systems to handle the handover.
- These handovers may be called intersystem handovers or inter-RAT handovers as the handover occurs between different radio access technologies.
- The most common form of intersystem handover is between GSM and UMTS / WCDMA. Here there are two different types:

UMTS / WCDMA to GSM handover:

There are two further divisions of this category of handover:

Blind handover:

- This form of handover occurs when the base station hands off the mobile by passing it the details of the new cell to the mobile without linking to it and setting the timing, etc of the mobile for the new cell.
- In this mode, the network selects what it believes to be the optimum GSM based station. The mobile first locates the broadcast channel of the new cell, gains timing synchronization and then carries out non-synchronized intercell handover.

Compressed mode handover:

- Using this form of handover the mobile uses the gaps I transmission that occur to analyze the reception of local GSM base stations using the neighbor list to select suitable candidate base stations.
- Having selected a suitable base station the handover takes place, again without any time synchronization having occurred.

Handover from GSM to UMTS / WCDMA:

This form of handover is supported within GSM and a "neighbor list" was established to enable this occur easily.

- As the GSM / 2G network is normally more extensive than the 3G network, this type of handover does not normally occur when the mobile leaves a coverage area and must quickly find a new base station to maintain contact.
- The handover from GSM to UMTS occurs to provide an improvement in performance and can normally take place only when the conditions are right.
- The neighbor list will inform the mobile when this may happen.

5) What are the functions of authentication and encryption in GSM? How is system security maintained? (8) [Nov 2016]

Authentication

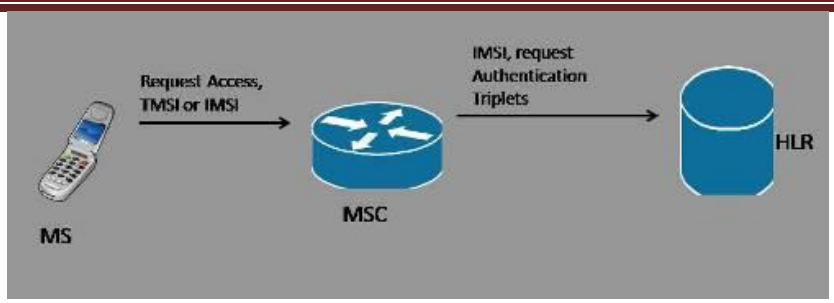
- Whenever a MS requests access to a network, the network must authenticate the MS.
- Authentication verifies the identity and validity of the SIM card to the network and ensures that the subscriber is authorized access to the network.

Encryption

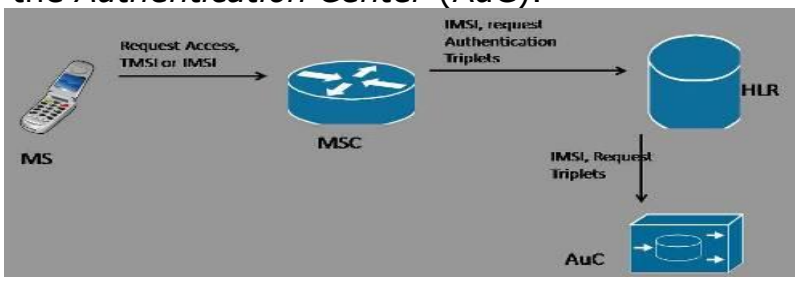
- In GSM, encryption refers to the process of creating authentication and ciphering crypto variables using a special key and an encryption algorithm.

Authentication Procedures

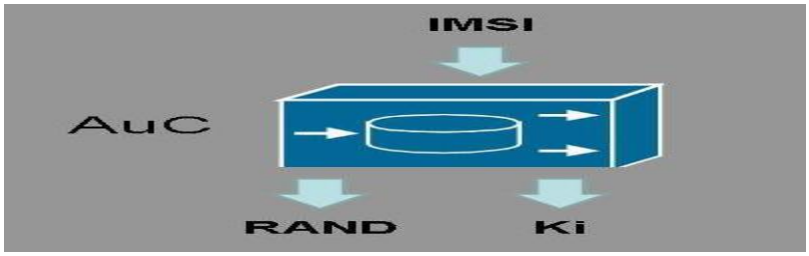
- When a MS requests access to the network, the MSC/VLR will normally require the MS to *authenticate*.
- The MSC will forward the IMSI to the HLR and request authentication *Triplets*.



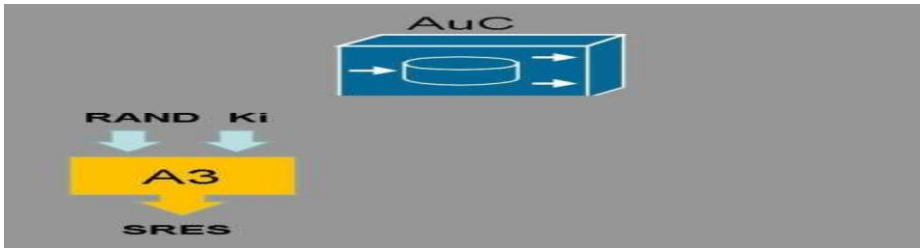
- When the HLR receives the IMSI and the authentication request, it first checks its database to make sure the IMSI is valid and belongs to the network.
- Once it has accomplished this, it will forward the IMSI and authentication request to the *Authentication Center* (AuC).



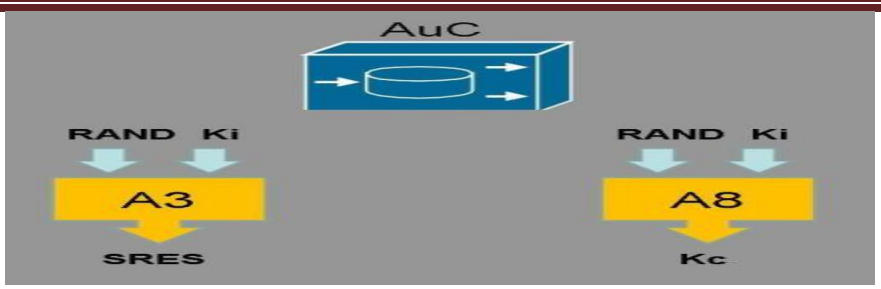
- The AuC will use the IMSI to look up the Ki associated with that IMSI.
- The Ki is the individual subscriber authentication key. It is a 128-bit number that is paired with an IMSI when the SIM card is created.
- The Ki is only stored on the SIM card and at the AuC. The Auc will also generate a 128-bit random number called the RAND.



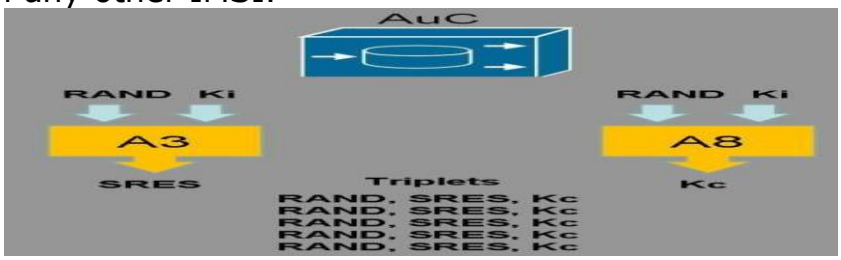
- The RAND and the Ki are inputted into the A3 encryption algorithm. The output is the 32-bit *Signed Response* (SRES).
- The SRES is essentially the "challenge" sent to the MS when authentication is requested.



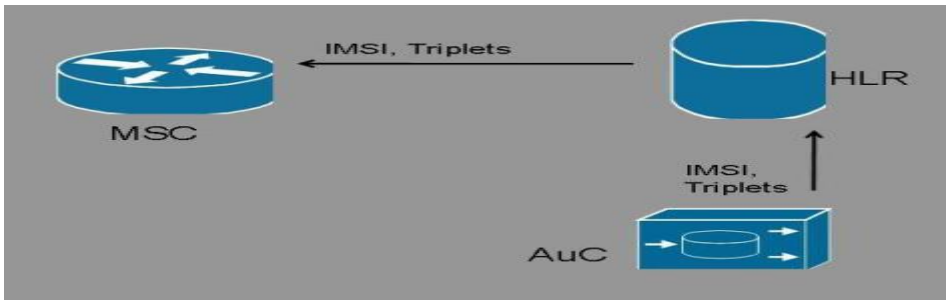
- The RAND and Ki are input into the A8 encryption algorithm. The output is the 64-bit Kc.
- The Kc is the ciphering key that is used in the A5 encryption algorithm to encipher and decipher the data that is being transmitted on the Um interface.



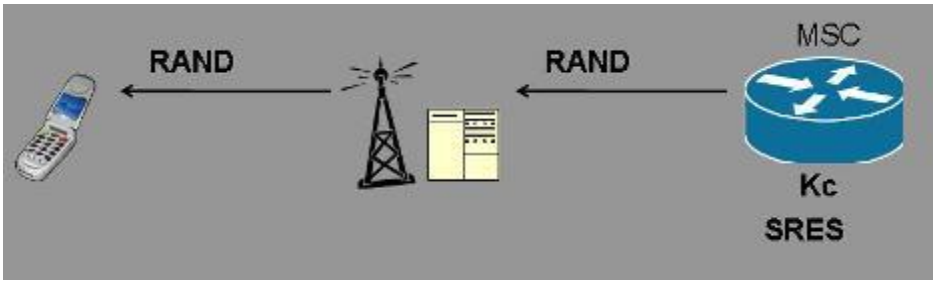
- The RAND, SRES, and Kc are collectively known as the *Triplets*. The AuC may generate many sets of Triplets and send them to the requesting MSC/VLR.
- This is in order to reduce the signaling overhead that would result if the MSC/VLR requested one set of triplets every time it wanted to authenticate the.
- It should be noted that a set of triplets is unique to one IMSI, it cannot be used with any other IMSI.



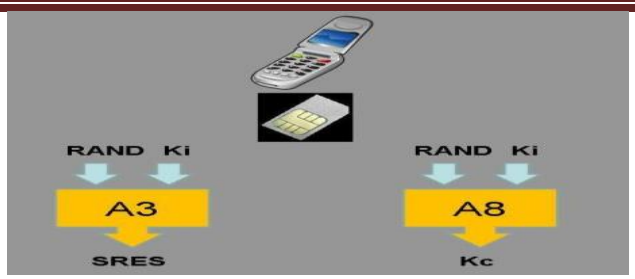
- Once the AuC has generated the triplets (or sets of triplets), it forwards them to the HLR. The HLr subsequently sends them to the requesting MSC/VLR



- The MSC stores the Kc and the SRES but forwards the RAND to the MS and orders it to authenticate.

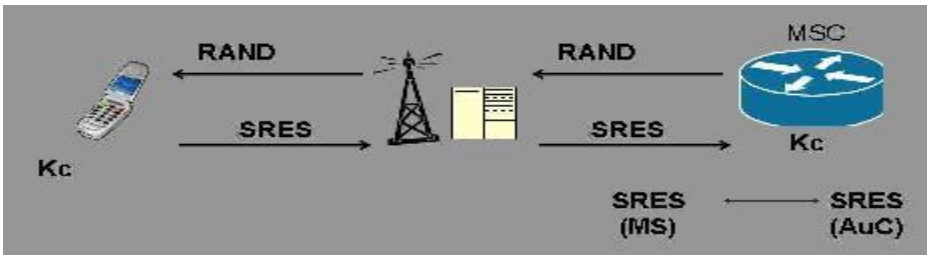


- The MS has the Ki stored on the SIM card. The A3 and A8 algorithms also reside on the SIM card. The RAND and Ki are inputted into the A3 and A8 encryption algorithms to generate the SRES and the Kc respectively.

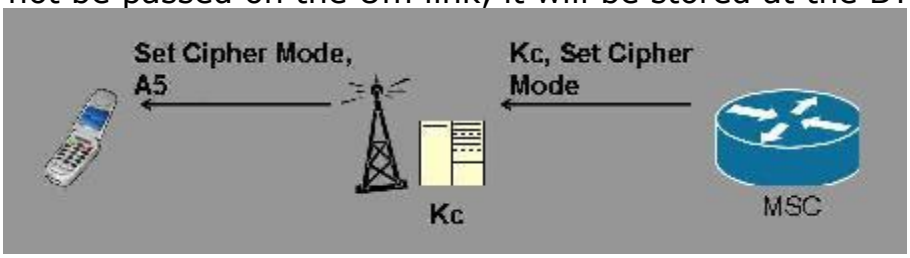


Ciphering Procedure

- The MS stores the Kc on the SIM card and sends the generated SRES back to the network. The MSC recieves the MS generated SRES and compares it to the ARES generated by the AuC. if they match, then the MS is authenticated.



- Once the MS is authenticated, it passes the Kc to the BSS (the BTS to be specific), and orders the BTS and MS to switch to *Cipher Mode*. The Kc should not be passed on the Um link, it will be stored at the BTS.



- The BTS inputs the Kc and the data payload into the A5 encryption algorithm resulting in an enciphered data stream.
- The MS also inputs the Kc and the data payload into the A5 encryption algorithm resulting in an enciphered data stream. It should be noted that the A5 algorithm is a function of the Mobile Equipment (ME) and not the SIM card.

6) Explain in detail about General Packet Radio Service (GPRS) with Architecture?

Explain GPRS and its Protocol architecture. (8) [May 2016]

Explain GPRS protocol architecture. (16) [May 2017]

Key Points
- GPRS – Introduction
- GPRS Services – Point to Point, Point to Multipoint
- GPRS Architecture – GSN, SGSN, GGSN, MS, BSS, MSC, VLR, HLR, EIR

General Packet Radio Service (GPRS)

- GPRS when integrated with GSM significantly improves and simplifies Internet access. It transfers data packets from GSM mobile stations to external packet data networks (PDNs).
- Packets can be directly routed from the GPRS mobile stations to packet switched networks making it easy to connect to the Internet.
- GSM uses a billing system based on the time (duration) of connection, whereas GPRS uses a billing system based on the amount of transmitted data rather than the duration of the connection.
- So, users can remain continuously connected to the system, and yet get charged only for the amount of transmitted data.

1. GPRS Services

GPRS offers end-to-end packet-switched data transfer services which can be categorized into the following two types:

i) Point-to-Point (PTP) service
- The PTP service is between two users and can either be connectionless or connection-oriented.

ii) Point-to-Multipoint (PTM) service.
- The PTM is a data transfer service from one user to multiple users.
- Again, there are two types of PTM services.
  - One is multicast PTM where the data packets are broadcast in a certain area
  - Other is group call PTM where the data packets are addressed to a group of users.

2. GPRS Architecture

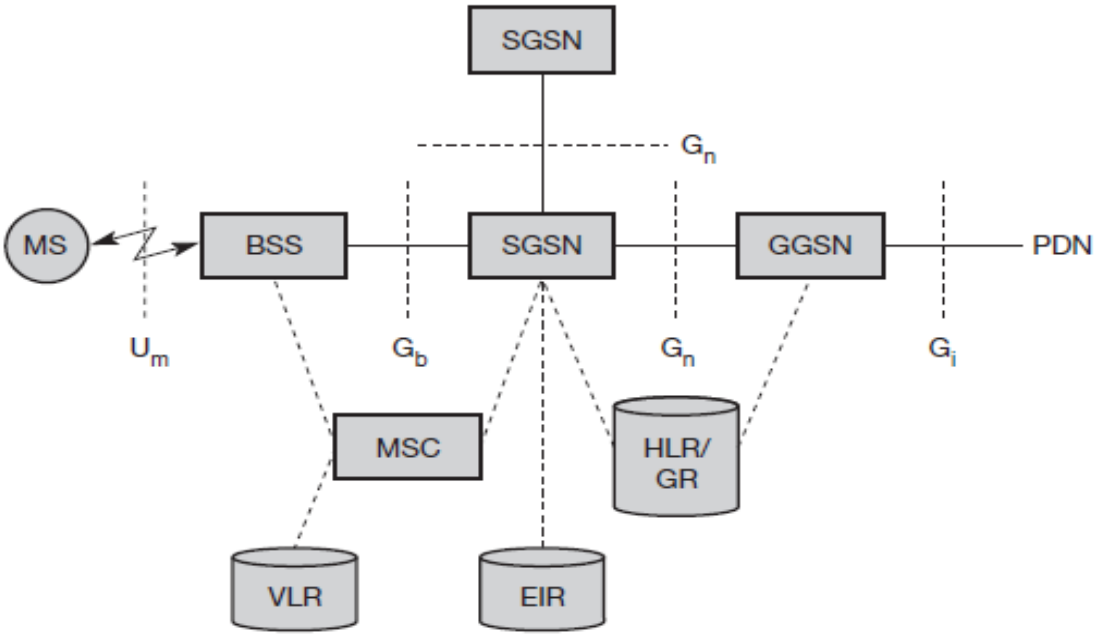
GPRS architecture introduces two new network elements, called
- GPRS Support Node (GSN) and
- The Gateway GPRS Support Node (GGSN).

GSN:
- A GSN is essentially a router. All GSNs are integrated into a standard GSM architecture.

GGSN:
- The GGSN is the interworking unit between the GPRS network and the external packet data network (PDN).
- The GGSN contains routing information for GPRS users, performs address connection and tunnels data to a user through encapsulation.

SGSN:

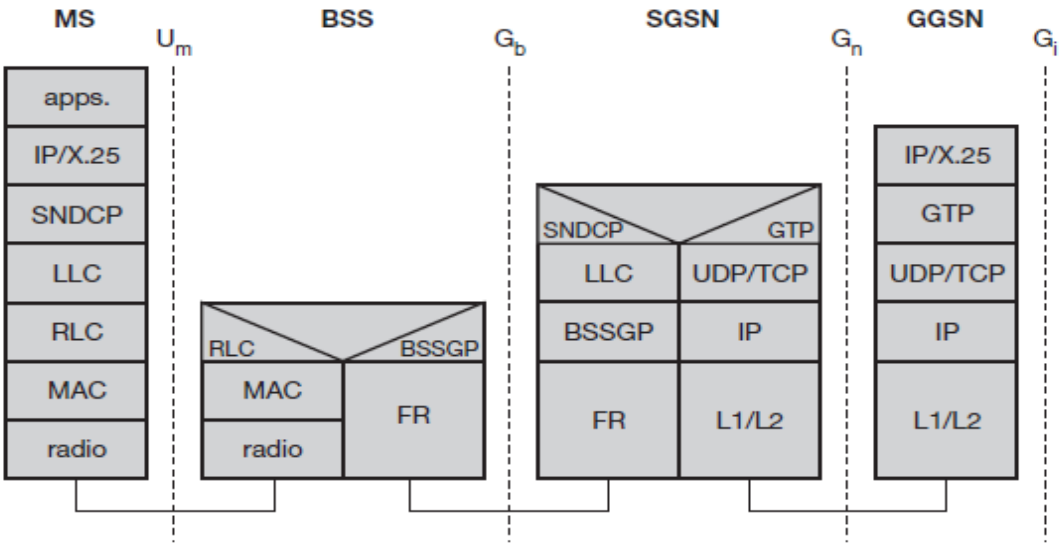
- SGSN (Serving GPRS Support Node) helps support MS. The SGSN is connected to BSC through frame relay and it is at the same hierarchy level as the MSC. The GPRS Register (GR) is a part of HLR which stores all the relevant GPRS data.
- In a part of HLR which stores all the relevant data of GPRS in a mobile IP network, GGSN and SGSNs can be compared with home agent and foreign agent respectively. The data packets are transmitted to the BSS and finally to the MS through the GGSN and SGSN.
- The MSC as we have already discussed is responsible for data transport in the traditional circuit-switched GSM.



GPRS architecture reference model

7) Explain the functions of GPRS protocol stack with a diagram and Applications of GPRS. (8) [Nov 2016]

The flow of GPRS protocol stack and end-to-end message from MS to the GGSN is displayed in the below diagram. GTP is the protocol used between the SGSN and GGSN using the Gn interface. This is a Layer 3 tunneling protocol.



GPRS transmission plane protocol reference model

- The process that takes place in the application looks like a normal IP sub-network for the users both inside and outside the network.
- The vital thing that needs attention is, the application communicates via standard IP, that is carried through the GPRS network and out through the gateway GPRS.
- The packets that are mobile between the GGSN and the SGSN use the GPRS tunneling protocol, this way the IP addresses located on the external side of the GPRS network do not have deal with the internal backbone. UDP and IP are run by GTP.
- Sub Network Dependent Convergence Protocol (SNDCP) and Logical Link Control (LLC) combination used in between the SGSN and the MS.
- The SNDCP flattens data to reduce the load on the radio channel. A safe logical link by encrypting packets is provided by LLC and the same LLC link is used as long as a mobile is under a single SGSN.
- In case, the mobile moves to a new routing area that lies under a different SGSN; then, the old LLC link is removed and a new link is established with the new Serving GSN X.25.
- Services are provided by running X.25 on top of TCP/IP in the internal backbone.

Applications

- **Communications:** E-mail, fax, unified messaging and intranet/Internet access, etc.
- **Value-added services:** Information services and games, etc.
- **E-commerce:** Retail, ticket purchasing, banking and financial trading, etc.
- **Location-based applications:** Navigation, traffic conditions, airline/rail schedules and location finder, etc.
- **Vertical applications:** Freight delivery, fleet management and sales-force automation.

- **Advertising:** Advertising may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

8) Explain in detail about Universal Mobile Telecommunications System (UMTS) and its dissimilarity?
What is UMTS? Describe the function of HLR and VLR in call routing and roaming. (13) [Nov 2018]
Explain in detail about UMTS architecture. (8) [Nov 2016]
Explain in detail network architecture of UMTS with a neat diagram? (13) [Apr 2018]
Explain in detail about UMTS architecture and its services. (16) [Nov 2017]
Explain in detail about UMTS architecture. (8) [May 2016]

Key Points
UMTS – Introduction
UMTS – Network Architecture – Elements - UE, RNS, RNC, Core Network.

Universal Mobile Telecommunications System (UMTS)

CDMA2000 and UMTS were developed separately and are two separate ITU approved 3G standards.

- In these networks, coverage is provided by a combination of various cell sizes, ranging from "in building" Pico cells to global cells provided by satellites, giving service to the remote regions of the world.
- The UMTS was developed mainly for countries with GSM networks, and it is expected that all GSM networks will be upgraded to UMTS networks.
- Because it is a new technology, a whole new radio access network has to be built. An important advantage of UMTS is that it gives significantly enhanced capacities to operators.
- The UMTS specification has been designed so that the UMTS systems are compatible with GSM networks.
- Therefore, the UMTS networks can easily work with any existing GSM/GPRS network.
- The UMTS systems use different frequency bands, so the BTSs do not interfere with each other.

The dissimilarities between these networks, The UMTS networks are different from the 2G networks in the following respects:

- ***Higher speech quality:*** In addition to speech traffic, the UMTS supports the advanced data and information services and can be called a true multimedia network.
- ***Higher data rate:*** The UMTS supports 2 Mbps data rate, which is much higher than that supported by the 2G mobile systems.
- ***Virtual home environment (VHE):*** A user roaming from his network to other UMTS networks will not feel any discontinuity or service difference, thus giving a "feeling" of being in the home network. In contrast, in a 2G network, a user is registered to a visitor location and is also charged a roaming overhead.

UMTS Network Architecture

The UMTS network architecture can be divided into three main elements:

User Equipment (UE):

- The User Equipment (UE) is the name by which a cell phone is referred to.
- The new name was chosen because of the considerably greater functionality that the UE incorporates compared to a cell phone.
- It can be thought of as both a mobile phone used for talking and a data terminal attached to a computer with no voice capability.

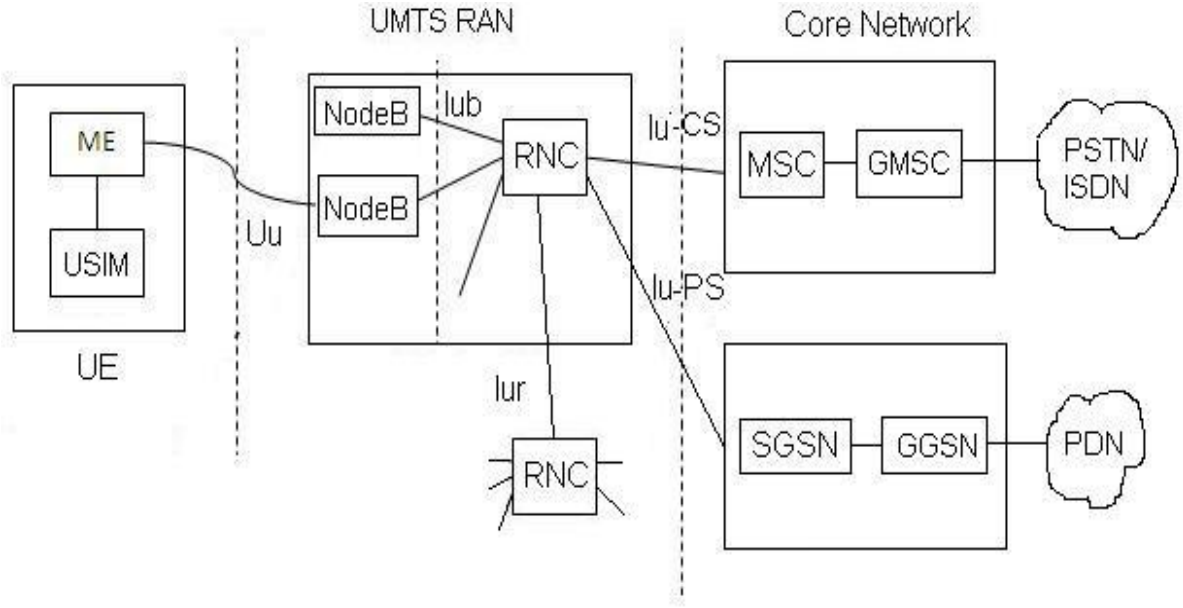
Radio Network Subsystem (RNS):

- The RNS is the equivalent of the Base Station Subsystem (BSS) in GSM. It provides and manages the wireless interface for the overall network.

Core Network:

- The core network is the equivalent of the GSM Network Switching Subsystem (NSS).

UMTS network architecture



User Equipments is composed of Mobile Equipment (ME) and USIM.

- Radio Access Network is composed of NodeB and RNC (**Radio Network Controller)**.

- The Radio Network Controller (or RNC) is a governing element in the UMTS radio access network (UTRAN) and is responsible for controlling the Node Bs that are connected to it.
- Core Network is composed of circuit switched and packet switched functional modules.
- For Circuit switched (CS) operations MSC and GMSC along with database modules such as VLR, HLR will be available.
- For packet switched (PS) operations SGSN and GGSN will serve the purpose.
- GMSC will be connected with PSTN/ISDN in CS case.
- GGSN is connected with Packet data Network (PDN) for PS case.

Interfaces between these entities are summarized below.

- Uu interface between UE and NodeB
- Iub interface between NodeB and RNC
- Iur interface between RNC and RNC
- Iu-CS interface between RNC and MSC
- Iu-PS interface between RNC and SGSN

9) Explain in detail about Universal Mobile Telecommunications System (UMTS) Handover and its similarity?

Handover in UMTS

For purely inter W-CDMA technology, there are three basic types of handover:

- Hard Handover
- Soft Handover
- Softer Handover

Hard Handover

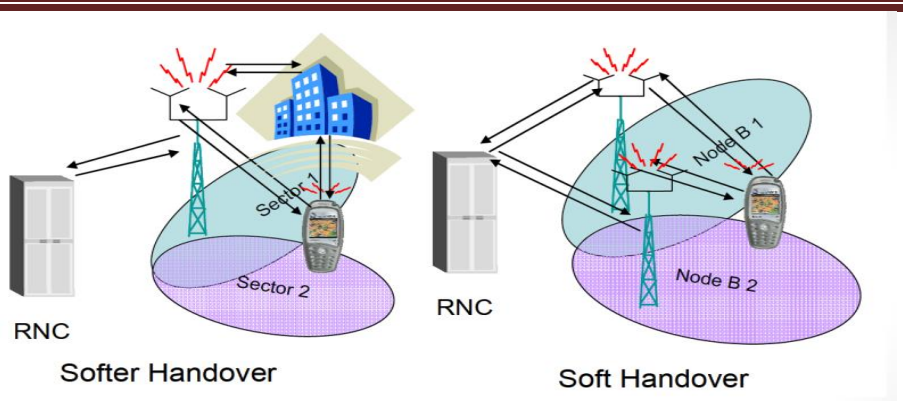
- Break before Make
- The network decides a handover is required dependent upon the signal Strengths of the existing link, and the strengths of broadcast channels of Adjacent cells.
- The link between the existing NodeB and the UE is broken.
- A new link is established between the new NodeB and the UE.

Soft Handover

- Occurs when the ME is moving in the overlapping coverage area.
- The ME communicate and receive the signals from the NodeB's which their Signals are overlapping.
- The rake receiver is needed in the UE (ME) to combine the two signals
- In the uplink, the best quality frame of the two signals is selected. The Selection is made by the outer loop power control algorithm measurement.
- Negatives: It needs to indicate resources (capacity) on both NodeBs

Softer Handover

- Softer handover is a special case of soft handover where the radio links That are added and removed belong to the same Node B.
- In softer Handover, the NodeB can receive the signal in macro diversity With maximum ratio combining.
- In soft handover macro diversity with selection combining is selected.



10) Explain in detail about Universal Mobile Telecommunications System (UMTS) Security Mechanisms?

UMTS Security Mechanisms

The UMTS access security standards, in particular the new authentication mechanism, are based on research work conducted by the European Union funded USECA project.

4.1 Enhancements in UMTS vs. GSM

- Mutual Authentication
  - o provides enhanced protection against false base station attacks by allowing the mobile to authenticate the network
- Data Integrity
  - o provides enhanced protection against false base station attacks by allowing the mobile to check the authenticity of certain signaling messages
- Network to Network Security
  - o Secure communication between serving networks. MAPSEC or IPsec can be used
- Wider Security Scope
  - o Security is based within the RNC rather than the base station
- Flexibility
  - o Security features can be extended and enhanced as required by new threats and services
- Longer Key Length
  - o Key length is 128 as against 64 bits in GSM

4.2 Entity authentication

UMTS provides mutual authentication between the UMTS subscriber, represented by a smart card application known as the USIM (Universal Subscriber Identity Module), and the network in the following sense:

- Subscriber authentication: the serving network corroborates the identity of the subscriber.
- Network authentication: the subscriber corroborates that he is connected to a serving network that is authorized, by the subscriber's home network, to provide him with services; this includes the guarantee that this authorization is recent.

4.3 Signaling data integrity and origin authentication

The following security features are provided with respect to integrity of data on the network access link: • Integrity algorithm agreement: the mobile station (MS) and the serving network (SN) can securely negotiate the integrity algorithm that they use.

• Integrity key agreement: the MS and the SN agree on an integrity key that they may use subsequently; this is realized as part of the protocol which also provides entity authentication.

• Data integrity and origin authentication of signaling data: the receiving entity (MS or SN) is able to verify that signaling data has not been modified in an unauthorized way since it was sent by the sending entity (SN or MS) and that the data origin of the signaling data received is indeed the one claimed.

4.4 Mutual authentication and key agreement between user and network

The design of the authentication and key agreement (AKA) protocol for UMTS reflects the results of an analysis of the threats and risks in GSM.

The main changes with respect to the GSM authentication and key agreement protocol are:

• The challenge is protected against replay by a sequence number and it is also 'signed' (integrity-protected).

• The AKA generates an integrity key in addition to a ciphering key.

4.5 Protection against false base station attacks

While designing UMTS security mechanisms, emphasis was laid on providing protection against false base station attacks, where attacker masquerades as base station to the user. No security was provided for these attacks in GSM, as previously cost involved in carrying out such attacks made this impossibility. The advantages that the attacker can gain by carrying out these attacks are,

1) By suppressing encryption between the target user and the intruder
2) By suppressing encryption between the target user and the true network
3) By forcing the use of a compromised cipher key

ANNA UNIVERSITY QUESTIONS

PART A

1. List the subsystems of GSM. [Nov 2018]
Refer Q.No.1

2. What is the function of Gateway GPRS support node (GGSN)? [Nov 2018]
Refer Q.No.2

3. What is frequency range of uplink and downlink in GSM network? [Apr 2018]
Refer Q.No.3

4. What are the information's are stored in SIM? [Apr 2018]
Refer Q.No.4

5. List the services of GPRS? [Nov 2017]
Refer Q.No.5

6. Define Handoff. What are its types? [Nov 2017]
Refer Q.No.6

7. Name the teleservices provided by GSM? [May 2017]
Refer Q.No.7

8. Write the suggestions of mobile phone with respect to human body. [May 2017]
Refer Q.No.8

9. Write about the supplementary services in GSM? [Nov 2016]
Refer Q.No.9

10. What is multitasking? [Nov 2016]
Refer Q.No.10

11. List the 3 important features of GSM security. [May 2016]
Refer Q.No.11

12. What are the main elements of UMTS? [May 2016]
Refer Q.No.12

ANNA UNIVERSITY QUESTIONS

PART B

1. Explain GSM architecture and its services with neat diagram. (16) [May 2017],[Nov 2017]
2. Explain in detail about UMTS architecture and its services. (16) [Nov 2017]
3. Explain GPRS protocol architecture. (16) [May 2017]
4. What are the functions of authentication and encryption in GSM? How is system security maintained? (8) [Nov 2016]
5. Explain in detail about the handovers of GSM. (8) [Nov 2016]
6. Explain the functions of GPRS protocol stack with a diagram. (8) [Nov 2016]
7. Explain in detail about UMTS architecture. (8) [Nov 2016]
8. Describe GSM architecture and its services in detail. (8) [May 2016]
9. Explain GSM Authentication and security. (8) [May 2016]
10. Explain GPRS and its Protocol architecture. (8) [May 2016]
11. Explain in detail about UMTS architecture. (8) [May 2016]
12. Describe about the system architecture of Global System for Mobile Communication. (13) [Nov 2018]
13. What is UMTS? Describe the function of HLR and VLR in call routing and Roaming. (13) [Nov 2018]
14. Write in detail about the various types of handover in GSM. Also discuss the Timeline diagram of the intra MSC handover. (13) [Apr 2018]
15. Explain in detail network architecture of UMTS with a neat diagram? (13) [Apr 2018]

CS8601 - MOBILE COMPUTING

UNIT I INTRODUCTION 9

Introduction to Mobile Computing – Applications of Mobile Computing- Generations of Mobile Communication Technologies- Multiplexing – Spread spectrum -MAC Protocols – SDMA- TDMA- FDMA- CDMA

UNIT II MOBILE TELECOMMUNICATION SYSTEM 9

Introduction to Cellular Systems - GSM – Services & Architecture – Protocols – Connection Establishment – Frequency Allocation – Routing – Mobility Management – Security – GPRS- UMTS – Architecture – Handover – Security

UNIT III MOBILE NETWORK LAYER 9

Mobile IP – DHCP – AdHoc– Proactive protocol-DSDV, Reactive Routing Protocols – DSR, AODV , Hybrid routing –ZRP, Multicast Routing- ODMRP, Vehicular Ad Hoc networks (VANET) –MANET Vs VANET – Security.

UNIT IV MOBILE TRANSPORT AND APPLICATION LAYER 9

Mobile TCP– WAP – Architecture – WDP – WTLS – WTP –WSP – WAE – WTA Architecture – WML

UNIT V MOBILE PLATFORMS AND APPLICATIONS 9

Mobile Device Operating Systems – Special Constraints & Requirements – Commercial Mobile Operating Systems – Software Development Kit: iOS, Android, BlackBerry, Windows Phone – MCommerce – Structure – Pros & Cons – Mobile Payment System – Security Issues

TOTAL 45 PERIODS

TEXT BOOKS:

1. Jochen Schiller, —Mobile Communications‖, PHI, Second Edition, 2003.
2. Prasant Kumar Pattnaik, Rajib Mall, —Fundamentals of Mobile Computing‖, PHI Learning Pvt.Ltd, New Delhi – 2012

REFERENCES

1. Dharma Prakash Agarval, Qing and An Zeng, "Introduction to Wireless and Mobile systems",Thomson Asia Pvt Ltd, 2005.
2. Uwe Hansmann, Lothar Merk, Martin S. Nicklons and Thomas Stober, —Principles of Mobile Computing‖, Springer, 2003.
3. William.C.Y.Lee,—Mobile Cellular Telecommunications-Analog and Digital Systems‖, Second Edition,TataMcGraw Hill Edition ,2006.
4. C.K.Toh, —AdHoc Mobile Wireless Networks‖, First Edition, Pearson Education, 2002.
5. Android Developers : http://developer.android.com/index.html
6. Apple Developer : https://developer.apple.com/
7. Windows Phone DevCenter : http://developer.windowsphone.com
8. BlackBerry Developer : http://developer.blackberry.com

UNIT I - INTRODUCTION

Introduction to Mobile Computing – Applications of Mobile Computing- Generations of Mobile Communication Technologies- Multiplexing – Spread spectrum -MAC Protocols – SDMA- TDMA- FDMA- CDMA

2 Marks

1) What are the challenges in mobile communication? [Nov 2018]

- **Portability**
  Portable computers face physical challenges (volume, weight, power consumption, cost), pragmatic challenges (increased chance of data loss, small user-interface issues), and systems issues.
- **Wireless communications**
- **Mobility**

2) State the objectives of MAC protocols. [Nov 2018]

- Collision avoidance
- Energy efficiency
- Scalability
- Latency
- Throughput
- Bandwidth utilization

3) List the issues of wireless MAC? [Apr 2018]

- The three important issues are:
  - Half Duplex operation –> either send or receive but not both at a given time
  - Time varying channel
  - Burst channel errors

4) "MAC protocol designed for infrastructure based wireless network may not work satisfactory in infrastructure-less environment." – Justify. [Nov 2017]

Because,

- Hidden and Exposed terminal problems makes MAC protocols inefficient.
- It is for a transmitting node to detect collisions.

5) Distinguish between mobile computing and wireless networking?
List out the difference between Mobile Computing and Wireless Networking. [Nov 2017][May 2017] [Apr 2018]

Mobile Computing	Wireless Networking

• Accessing information and remote computational services while on the move. • That **mobile computing is based on wireless networking** and helps one to invoke computing services on remote servers while on the move.	• Provides the basic communication infrastructure necessary to make this possible. • **wireless networking is an important ingredient of mobile computing.**

6) List some random assignment schemes. [May 2017]

- ALOHA
- Slotted ALOHA
- CSMA
- CSMA/CD
- CSMA/CA

7) What are the limitations of Mobile Computing? [Nov 2016]

- Insufficient bandwidth
- Security standards
- Power consumption
- Transmission interferences
- Potential health hazards
- Human interface with device

8) What are the different Random Assignment Scheme in MAC? [Nov 2016]

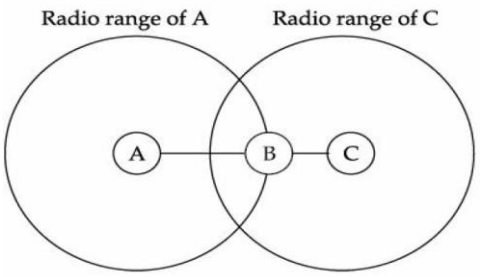
- ALOHA
- Slotted ALOHA
- CSMA
- CSMA/CD
- CSMA/CA

9) List the advantages of Mobile Computing. [May 2016]

- Location Flexibility
- Saves Time
- Enhanced Productivity
- Ease of Research
- Entertainment
- Streamlining of Business Processes

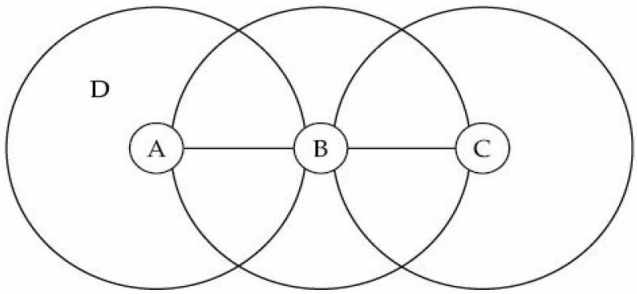
10) Explain hidden and exposed terminal problems in infrastructure less network. [May 2016]

Hidden Terminal problem



- Note that if both A and C start to transmit to B at the same time, the data received at node B would get garbled.
- Such a situation can arise because A and C are "hidden" from each other, because they are outside each other's transmission range.

Exposed Terminal problem



- Node A will not be able to transmit to any node when B is transmitting to C.
- On the other hand, had A transmitted to D, it would have been received correctly by D and B's transmission would have also been correctly received at C.
- The problem arose only because A and B are within each other's transmission range, though the destination nodes are in the transmission range of only one of the nodes.
- In other words, the problem occurs because A is exposed to B's transmission.

11) What is Mobile Computing?

- Mobile computing **(sometimes called ubiquitous computing and also at times called nomadic computing)** is the ability to compute remotely while on the move.
- This is a new and fast emerging discipline that has made it possible for people to access information from anywhere and at anytime.

Mobile computing as encompassing two separate and distinct concepts:

- Mobility and Computing.

12) Define computing?

Computing denotes the capability to automatically carry out certain processing related to service invocations on a remote computer.

13) Formulate a reason why Collision Detection is based protocol not suitable for wireless networks?

- Because, in a wireless network, it is very difficult for a transmitting node to detect a collision, since any received signal from other nodes would be too weak compared to its original signal and can easily be masked by noise.
- As a result the transmitting node would continue to transmit the frame which leads to corrupted frame. In wired network, when a node detects a

collision, it immediately stops transmitting, thereby minimizing channel wastage.

14) Define Mobility?

Mobility, on the other hand, provides the capability to change location while communicating to invoke computing services at some remote computers.

15) What is main advantage of mobile computing?

- The tremendous **flexibility** it provides to the users.
- The user need not be tethered to the chair in front of his desktop, but can move locally or even to faraway places and at the same time achieve what used to be performed while sitting in front of a desktop.

16) Compare Wired Networks and Mobile Networks.

S.No	Wired Networks	Mobile Networks
1	Users cannot get any information at any place (does not support mobility)	Users can get information at any place (Supports Mobility)
2	Bandwidth is high	Bandwidth is low
3	Low bandwidth variability	High bandwidth variability
4	Listen on wire	Hidden Terminal problem
5	Productivity is low	Productivity is high
6	High Power Machines	Low Power machines
7	High Resource machines	Low Resource machines
8	Need physical access	Need proximity
9	Low delay	Higher delay
10	Connected Operations	Disconnected Operations

17) What are the applications of mobile computing?

- Credit Card Verification
- Stock Information Collection/Control
- In companies
- In courts
- For Estate Agents
- Vehicles
- Stock Broker
- Emergency services
- Taxi/Truck Dispatch
- Electronic Mail/Paging

18) Point out the problems faced by devices in Wireless Transmission?

- Lower Bandwidth
- Bandwidth Fluctuations
- Host mobility
- Intermittent disconnections
- High bit error rate
- Poor link reliability
- Higher delay
- Power consumption

19) List out various forms of Wireless networks?

- WLANs (Wireless LANs),
- Mobile Cellular Networks,
- Personal Area Networks (Pans),
- And Ad Hoc Networks, etc.

20) What are the two basic types of wireless network?

Wireless networks can be classified into two basic types.

1. One is an extension of **wired networks**. It uses fixed infrastructures such as
2. The other type of **wireless network is an ad hoc network**

21) List out types of computer network?

1. Controller Area Networks (CANs)
2. Local Area Networks (LANs)
3. Internetworks.

22) Define CAN?

- A Controller Area Network (CAN) is essentially a very small network that is typically used to connect the different components of an embedded controller.
- The end-to-end length of a CAN is usually less than 50 meters. Since the propagation time of a CAN is very small, it behaves more like a local bus in a computer.

23) Define LANs?

- A Local Area Network (LAN) is typically deployed in a building or a campus and is usually privately owned.

For example,

- LAN can be used to connect a number of computers within an organization to share data and other resources such as files, printers, FAX services, etc.
- LANs typically operate at data rates exceeding 10 Mbps and many present-day LANs (gigabit Ethernets) operate at 1 Gbps.

24) Define Internetwork?

Several LANs can be interconnected using switches to realize internetworks or internet in short. In an internet, a node in a LAN communicates with a node in another LAN using packet switching.

25) List out Component of wireless System?

A wireless communication system is built from various types of basic components. The following are some of these basic types of components.

- *Transmitter*
- *Receiver*
- *Antenna*
- *Filters*
- *Amplifiers*
- *Mixers*

26) Write short notes about WLANs?

Wireless Local Area

- Networks (WLANs) provide connectivity between computers over short distances using the wireless medium.

- Typical indoor applications of WLANs may be in educational institutes, office buildings and factories where the required coverage distances are usually restricted to less than a few hundred feet.

27) Brief about Access point?

- It is a radio receiver/transmitter (also called transceiver) that connects to the wired network. These are typically mounted on the roofs at different locations of a building.
- The transceiver exchanges signals with the wireless LAN card in desktop or notebook PCs.
- A single access point can support a small group of users. It is connected to a wired network through cables and provides the connectivity between wireless devices and the wired network.

28) Write short notes about Wireless LAN cards?

Wireless LAN cards*:* End-users access the WLAN through WLAN adapters (wireless network interface cards) in their hand-helds. The LAN card used to be mounted on the motherboard of a computer. Now, it is inbuilt into the motherboards.

29) Define Bridge?

Bridge*:* It is used for connecting two LANs that may be in two different buildings or on two separate floors within the same building.

30) Write Advantages of Wireless LANs over Wired LANs?

Advantages of Wireless LANs over Wired LANs

1. Mobility- users get information at any place
2. Simplicity and speedy deployment
3. Flexibility: Wireless technology allows the network to be accessible where wiring is difficult to lay
4. Cost effectiveness

31) Write Bluetooth technology?

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs)

32) Define PANs?

- A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants.
- PANs can be used for communication among the personal devices themselves (intrapersonal communication)

33) What is piconet?

- A **piconet** is a computer network which links a wireless user group of devices using Bluetooth technology protocols.

- A piconet consists of two or more devices occupying the same physical channel (synchronized to a common clock and hopping sequence).
- It allows one *master* device to interconnect with up to seven active *slave* devices.

34) Describe Mobile ad hoc network?

- An ad hoc network is also known as a **Mobile Ad hoc Network(MANET)**. It is a collection of mobile nodes that form a network on the fly without requiring the support of any fixed infrastructure.
- Wireless sensor networks are a special type of wireless ad hoc networks.

35) List out the Characteristics of Mobile computing?

- Ubiquity
- Location awareness
- Adaptation
- Broadcast

36) List out the three tiers of a mobile computing application?

- Presentation (Tier-1)
- Application (Tier-2)
- Data (Tier-3)

37) Specify the functionalities of Application Tier.

- Moves and Process data between the presentation and data layers.
- Responsible for making logical decisions and performing calculations.

38) What is the use of Data Tier?

- Contains a database where the information is stored and retrieved.
- Responsible for providing the basic facilities of data storage, access and manipulation.

39) Write about MAC protocol?

- MAC protocol is to enforce discipline in the access of a shared channel when multiple nodes contend to access that channel.
- At the same time, two other objectives of any MAC protocol are maximization of the utilization of the channel and minimization of average latency of transmission.

40) Write some of issues of MAC protocol?

- Hidden Terminal Problems
- Exposed Terminal Problems

41) List out classification of MAC protocol?

- Fixed assignment schemes-
- Random assignment schemes
- Reservation-based schemes

42) Define fixed assignment schemes?

In fixed assignment schemes, the resources required for a call are assigned for the entire duration of the call.

43) Define random assignment schemes?

In random assignment schemes are comparable to the connection-less packet-switching schemes. In this, no resource reservations are made, the nodes simply start to transmit as soon as they have a packet to send.

44) Summarize the steps involved in RTS / CTS scheme.

- Sender transmits an RTS packet to the receiver before the actual data Receiver will send acknowledgement to the sender.
- Actual data transfer commences between the sender and receiver.
- Receiver sends a CTS packet to the sender.
- Transmission.

45) What are the Objectives of MAC Protocol?

- Maximization of the channel utilization
- Minimization of average latency of transmission

46) Define reservation assignment schemes?

In the reservation schemes, a node makes explicit reservation of the channel for an entire call before transmitting. This is analogous to a connection-based packet-switching scheme.

PART B

1) What is Mobile Computing?(4 marks)

Key Points
- Definition
- Mobility
- Computing
- Advantage - flexibility

Definition

Mobile computing **(sometimes called ubiquitous computing and also at times called nomadic computing)** is the ability to compute remotely while on the move. This is a new and fast emerging discipline that has made it possible for people to access information from anywhere and at anytime.

Mobile computing as encompassing two separate and distinct concepts:
- Mobility and Computing.

Computing denotes the capability to automatically carry out certain processing related to service invocations on a remote computer.

Mobility provides the capability to change location while communicating to invoke computing services at some remote computers.

The main advantage of this type of mobile computing is :
- The tremendous flexibility it provides to the users.
- The user need not be tethered to the chair in front of his desktop, but can move locally or even to far away places and at the same time achieve what used to be performed while sitting in front of a desktop.

2) Compare Mobile Computing vs. Wireless Networking.

Distinguish Between Mobile Computing And Wireless Networking.
- While **mobile computing** essentially denotes accessing information and remote computational services while on the move
- **Wireless networking** provides the basic communication infrastructure necessary to make this possible.
- That **mobile computing is based on wireless networking** and helps one to invoke computing services on remote servers while on the move: be it be office, home, conference, hotel, and so on.
- It should be clear **that wireless networking is an important ingredient of mobile computing,** but forms only one of the necessary ingredients of mobile computing.
- Mobile computing also requires the applications themselves— their design and development, and the hardware at the client and server sides.
- Wireless networking is increasingly replacing traditional networks because of the low setup time and low initial investment required to set up the wireless network.

WIRELESS NETWORKS

Wireless networks appear in various forms such as
- WLANs (Wireless LANs),
- Mobile Cellular Networks,

- Personal Area Networks (Pans),
- And Ad Hoc Networks, etc.

Wireless networks can be **classified into two basic types**.

1. One is an extension of **wired networks**. It uses **fixed infrastructures** such as
   Base stations to provide essentially single hop wireless communication with a wired network as illustrated in Fig. 2.1 A two-hop **wireless cellular communication** with another mobile.
2. The other type of wireless network is an ad hoc network. An ad hoc network does not use any fixed infrastructure and is based on multi-hop wireless communication as shown in Fig. 2.2.

One popular example of a fixed infrastructure wireless network is a Wireless LAN (WLAN) that implements the IEEE 802.11 protocol.

Access Point:

- Observe from Fig. 2.1 that only the last hop is through the wireless medium.
- An access point (AP) provides the last hop connectivity of the mobile nodes to a wired network.
- All communication goes through APs which perform bridging* between the wireless and the wired mediums. A station must be recognized by an AP to be able to connect to the network.
- The AP may require authentication and this in turn is used as the basic means to keep out the unauthorized users.
- In an infrastructureless network, the communication between hosts occurs directly or via a few intermediate nodes that form the hops.

For example, station A in **Fig. 2.2** can communicate with station C using either the hops A–B, B– C or A–D, D–C. * A network bridge connects multiple network segments at the data link layer (Layer 2) of the OSI reference model.

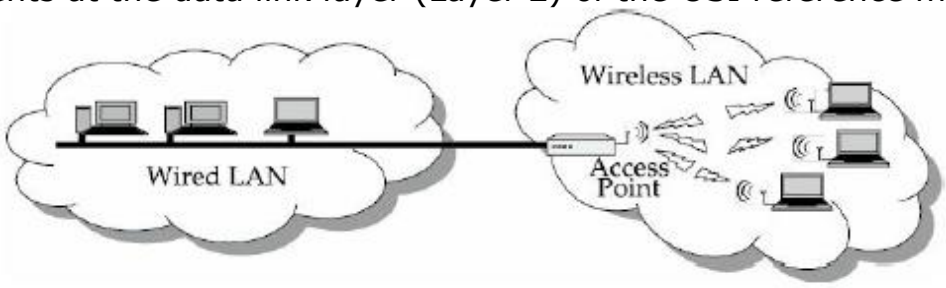


Figure 2.1 Wireless network based on fixed infrastructures.

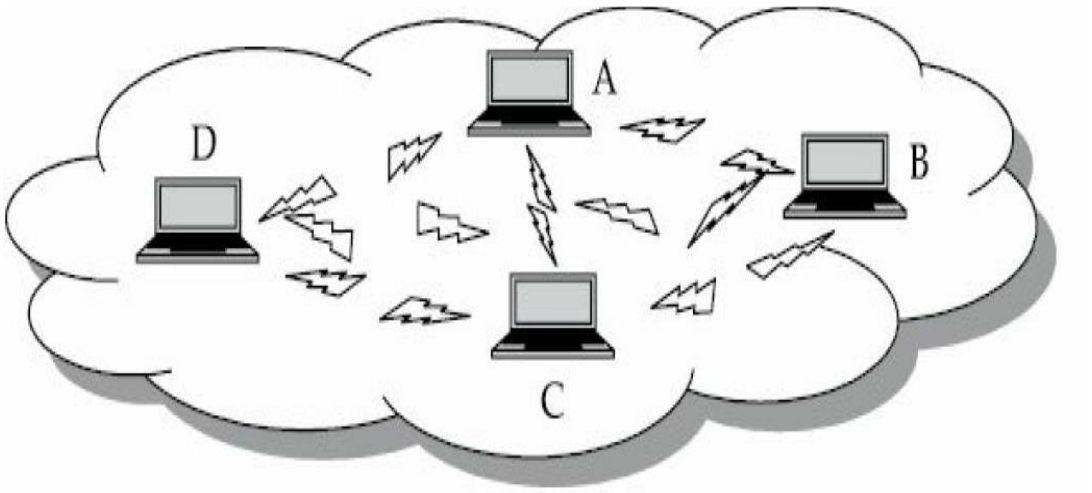


Figure 2.2 *Wireless network having no fixed infrastructures.*

Recent Development

A recent development wireless networking of various types of devices using the

Bluetooth technology,

- The Bluetooth technology can also be used to establish direct wireless connection of cell phones with devices such as printers, cameras, scanners, laptop and desk computers.
- Bluetooth is gradually replacing cables and infrared as the dominant way of exchanging information between devices.
- One of the objectives of the Bluetooth technology is to enable users to easily connect to a wide range of personal computing and telecommunication devices, without the need to buy, carry, or lay out cables.
- In fact, the Bluetooth technology enables setting up of personal area networks (PANs) known as **piconets** and ad hoc networks known as **scatternets**. It provides opportunities for rapid deployment of ad hoc connections, and the possibility of automatic, transparent connections between devices. It promises to eliminate the need to purchase additional or proprietary cabling and configuration exercises needed to connect the individual devices.

Ad Hoc Network

- An ad hoc network is also known as a **Mobile Ad hoc Network(MANET)**. It is a collection of mobile nodes that form a network on the fly without requiring the support of any fixed infrastructure.
- Wireless sensor networks are a special type of wireless ad hoc networks.

3) Explain in detail of Mobile Computing Applications?(4 marks)
Explain the various applications of Mobile Computing. (8) [May 2017]
Describe the applications of Mobile Computing. (8) [Nov 2016]

Key Points

- For Estate Agents
- Emergency Services
- In courts
- In companies
- Stock Information Collation/Control
- Credit Card Verification
- Taxi/Truck Dispatch
- Electronic Mail/Paging

Mobile Computing Applications

Mobile computing technology makes **it possible for people to send or extract information while on the move.**

For example,

A stock broker travelling in a car may wish to issue stock transaction orders from a mobile phone or to receive share price quotations.

Positive Points

It eases of deployment and scalability is two important positive points in favor of data transmissions over the wireless medium.

Difficult

But when data is being transmitted on air, all the wireless devices present in the transmission range can receive the data. This, therefore, opens up very difficult security issues that must be overcome to ensure privacy of data.

For Estate Agents

- Estate agents can work either at home or out in the field. With mobile computers they can be more productive. They can obtain current real estate information by accessing multiple listing services, which they can do from home, office or car when out with clients.
- They can provide clients with immediate feedback regarding specific homes or neighborhoods, and with faster loan approvals, since applications can be submitted on the spot. Therefore, mobile computers allow them to devote more time to clients.

Emergency Services

- Ability to receive information on the move is vital where the emergency services are involved.
- Information regarding the address, type and other details of an incident can be dispatched quickly, via a CDPD system using mobile computers, to one or several appropriate mobile units which are in the vicinity of the incident.
- Here the reliability and security implemented in the CDPD system would be of great advantage.

In courts

- Defense counsels can take mobile computers in court. When the opposing counsel references a case which they are not familiar, they can use the computer to get direct, real-time access to on-line legal database services, where they can gather information on the case and related precedents.
- Therefore mobile computers allow immediate access to a wealth of information, making people better informed and prepared.

In companies

- Managers can use mobile computers in, say, critical presentations to major customers. They can access the latest market share information.
- At a small recess, they can revise the presentation to take advantage of this information. They can communicate with the office about possible new offers and call meetings for discussing responds to the new proposals.
- Therefore, mobile computers can leverage competitive advantages.

Stock Information Collation/Control

- In environments where access to stock is very limited ie: factory warehouses. The use of small portable electronic databases accessed via a mobile computer would be ideal.
- Data collated could be directly written to a central database, via a CDPD network, which holds all stock information hence the need for transfer of data to the central computer at a later date is not necessary.
- This ensures that from the time that a stock count is completed, there is no inconsistency between the data input on the portable computers and the central database.

Credit Card Verification

- At Point of Sale (POS) terminals in shops and supermarkets, when customers use credit cards for transactions, the intercommunication required between the bank central computer and the POS terminal, in order to effect verification of the card usage, can take place quickly and securely over cellular channels using a mobile computer unit.
- This can speed up the transaction process and relieve congestion at the POS terminals.

Taxi/Truck Dispatch

- Using the idea of a centrally controlled dispatcher with several mobile units (taxis), mobile computing allows the taxis to be given full details of the dispatched job as well as allowing the taxis to communicate information about their whereabouts back to the central dispatch office.
- This system is also extremely useful in secure deliveries i.e. Securicor. This allows a central computer to be able to track and receive status information from all of its mobile secure delivery vans. Again, the security and reliability properties of the CDPD system shine through.

Electronic Mail/Paging

- Usage of a mobile unit to send and read emails is a very useful asset for any business individual, as it allows him/her to keep in touch with any colleagues as well as any urgent developments that may affect their work.
- Access to the Internet, using mobile computing technology, allows the individual to have vast arrays of knowledge at his/her fingertips.
- Paging is also achievable here, giving even more intercommunication capability between individuals, using a single mobile computer device.

4) Detail about Characteristics of Mobile Computing?

List the characteristics of mobile systems? (6) [Apr 2018]
Explain the characteristics of Mobile Computing. (8) [May 2016]

Characteristics of Mobile Computing

Key Points
- Ubiquity
- Location awareness
- Adaptation
- Broadcast
- Personalization

A **computing environment** is said to be **"mobile",** when either the sender or the receiver of information can be on the move while transmitting or receiving information.

Characteristics

Ubiquity:
- The dictionary **meaning of ubiquity is present everywhere**. In the context of mobile computing, ubiquity means the ability of a user to perform computations from anywhere and at anytime.
- **For example**, a business executive can receive business notifications and issue business transactions as long he is in the wireless coverage area.

Location awareness:
- A hand-held device equipped with global positioning system (GPS) can transparently provide information about the current location of a user to a tracking station.
- Many applications, ranging from strategic to personalized services, require or get value additions by location-based services
- **For example,** a person travelling by road in a car, may need to find out a car maintenance service that may be available nearby. He can easily locate such a service through mobile computing where an application may show the nearby maintenance shop.

A few other example applications include traffic control, fleet management and emergency services.

1. In a traffic control application, the density of traffic along various roads can be dynamically monitored, and traffic can be directed appropriately to reduce congestions.
2. In a fleet management application, the manager of a transport company can have up-to-date information regarding the position of its fleet of vehicles, thus enabling him to plan accurately and provide accurate information to customers regarding the state of their consignments.
3. Location awareness can also make emergency services more effective by automatically directing the emergency service vehicles to the site of the call.

Adaptation:
- Adaptation in the context of mobile computing implies the ability of a system to adjust to bandwidth fluctuation without inconveniencing the user.

- In a mobile computing environment, adaptation is crucial because of intermittent disconnections and bandwidth fluctuations that can arise due to a number of factors such as handoff, obstacles, environmental noise, etc.

Broadcast:

- Due to the broadcast nature of the underlying communication network of a mobile computing environment, efficient delivery of data can be made simultaneously to hundreds of mobile users.
- **For example**, all users at a specific location, such as those near a railway station, may be sent advertising information by a taxi service operator.

Personalization:

- Services in a mobile environment can be easily personalized according to a user's profile. This is required to let the users easily avail information with their hand-held devices.
- **For example**, a mobile user may need only a certain type of information from specific sources. This can be easily done through personalization.

5) Explain in detail of Structure of Mobile Computing Application?
Discuss in detail the structure of mobile computing? (6) [Apr 2018]
Explain the structure of Mobile Computing Application. (8) [May 2016]
Describe architecture of Mobile Computing. (8) [Nov 2017]

Key Points

1. Presentation (Tier-1) - user interface
2. Application (Tier-2) - making logical decisions and performing calculations
3. Data (Tier-3) - data storage, access, and manipulation

Structure of Mobile Computing Application

A mobile computing application is usually structured in terms of the functionalities implemented.

- The simple three-tier structure of a mobile computing application is depicted in Fig. 2.3.
- Figure 2.4 shows a specific scenario of the types of functionalities provided by each tier.
- The three tiers are named presentation tier, application tier and data tier.

1. Presentation (Tier-1)
2. Application (Tier-2)
3. Data (Tier-3)

Figure 2.3 The three tier structure of a mobile computing application.

Presentation tier

- The topmost level of a mobile computing application concerns the user interface. A good user interface facilitates the users to issue requests and to present the results to them meaningfully.
- Obviously, the programs at this layer run on the client's computer. This layer usually includes web browsers and customized client programs for dissemination of information and for collection of data from the user.

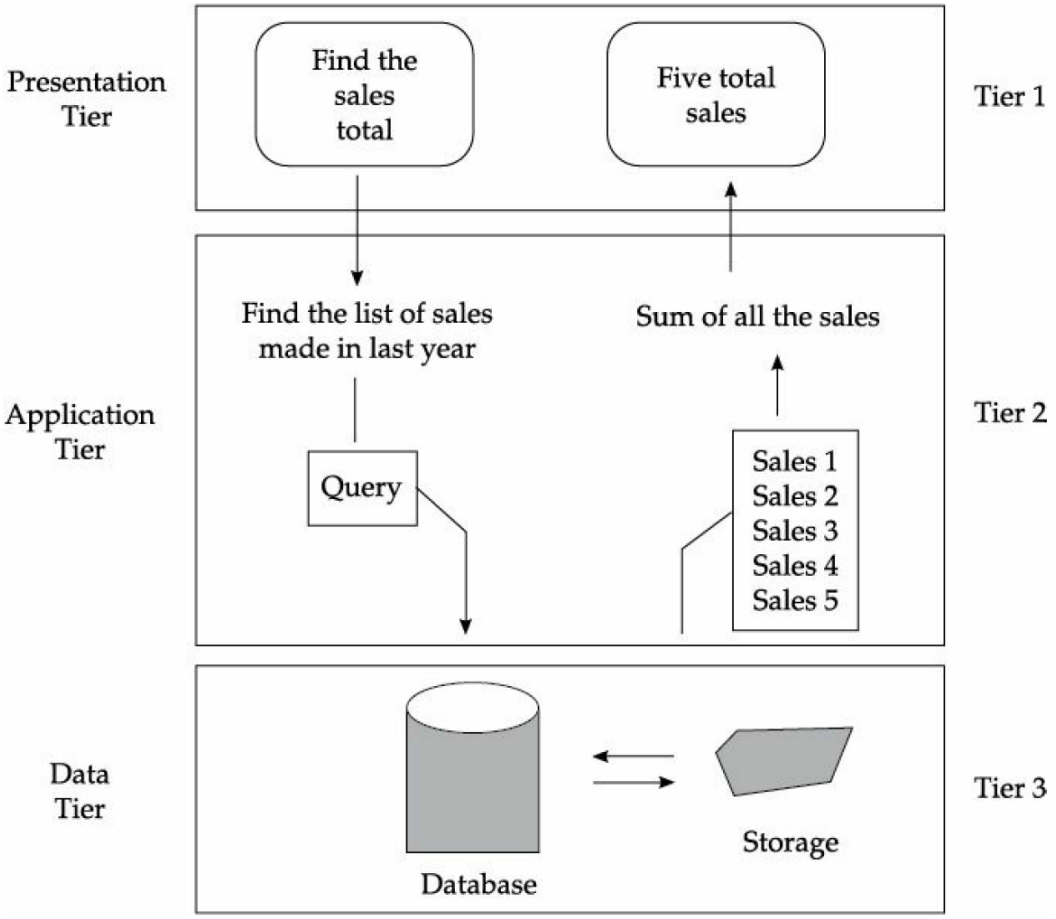


Figure 2.4 Functionalities provided by each tier structure of a mobile computing application.

Application tier

- This layer has the vital responsibility of making logical decisions and performing calculations. It also moves and processes data between the presentation and data layers.
- We can consider the middle tier to be like an "engine" of an automobile. It performs the processing of user input, obtaining information and then making decisions.
- This layer is implemented using technology like Java, .NET services, cold fusion, etc.
- The implementation of this layer and the functionality provided by this layer should be database independent.
- This layer of functionalities is usually implemented on a fixed server.

Data tier

- The data tier is responsible for providing the basic facilities of data storage, access, and manipulation. Often this layer contains a database. The information is stored and retrieved from this database.
- But, when only small amounts of data need to be stored, a file system can be used.
- This layer is also implemented on a fixed server.

6) Explain in detail about the generations of Mobile Communications Technologies and explain the distinguishing features of various generations of wireless networks. (8) [Nov 2016]

First Generation (1G)

- 1G, which stands for "first generation," refers to the first generation of wireless telecommunication technology, more popularly known as cellphones. A set of wireless standards developed in the 1980's,

1G technology replaced 0G technology, which featured mobile radio telephones and such technologies as

- Mobile Telephone System (MTS),
- Advanced Mobile Telephone System (AMTS),
- Improved Mobile Telephone Service (IMTS),
- Push to Talk (PTT).

Second Generation (2G)

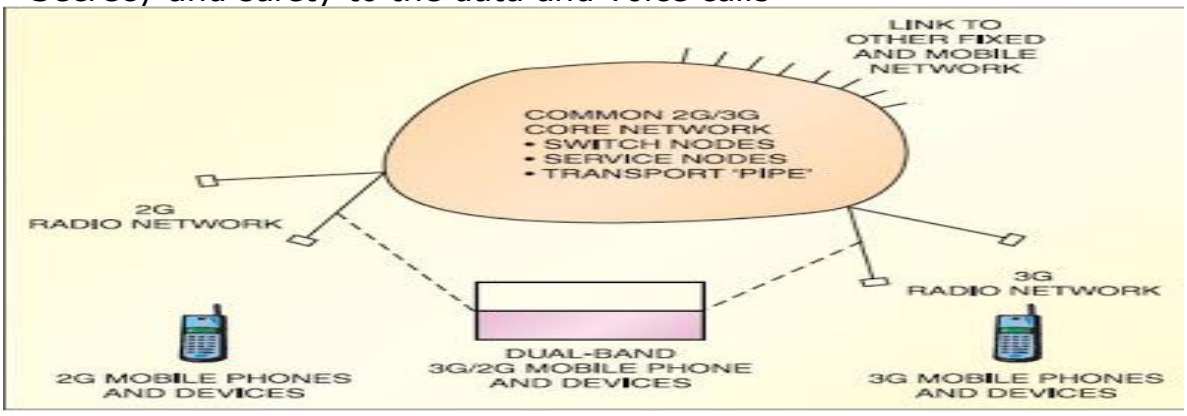
Second generation (2g) telephone **technology** is based on GSM or in other words global system for mobile communication. Second generation was launched in Finland in the year 1991.

How 2G works, Uses of 2G technology

- **2G network** allows for much greater penetration intensity.
- **2G technologies** enabled the various mobile phone networks to provide the services such as text messages, picture messages and MMS (multi media messages).
- **2G technology** is more efficient.
- **2G technology** holds sufficient security for both the sender and the receiver. All text messages are digitally encrypted. This digital encryption allows for the transfer of data in such a way that only the intended receiver can receive and read it

Benefits

- Voice clarity and Reduces noise
- Environment friendly
- Short Message Service
- Secrecy and safety to the data and voice calls



2.5G

- The mobile technology using general packet radio service (GPRS) standard has been termed as 2.5G. 2.5G systems enhance the data capacity of GSM and mitigate some of its limitations.
- GPRS adds packet-switched capabilities to existing GSM and TDMA networks. Working on the basis of emails, it sends text and graphics-rich data as packets at very fast speed.
- The circuit-switched technology has a long and successful history but it is inefficient for short data transactions and always-on service.

3G technology

- It make use of TDMA and CDMA. 3G (Third Generation Technology) technologies make use of value added services like mobile television, GPS (global positioning system) and video conferencing.
- It is expected that 2mbit/sec for stationary users, while 348kbits when moving or traveling.
- There are many **3G** technologies as W-CDMA, GSM EDGE, UMTS, DECT, WiMax and CDMA 2000.Enhanced data rates for GSM evolution or EDGE is termed to as a backward digital technology, because it can operate with older devices.

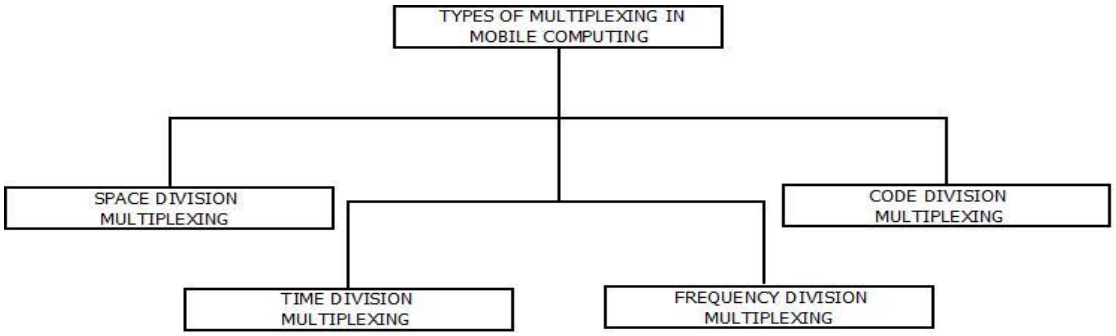
4G Technology

- **4G Technology** is basically the extension in the **3G technology** with more bandwidth and services offers in the 3G.
- The expectation for the 4G technology is basically the high quality audio/video streaming over end to end Internet Protocol.
- **WiMAX** or mobile structural design will become progressively more translucent, and therefore the acceptance of several architectures by a particular network operator ever more common.

7) Explain in detail about Multiplexing techniques in Mobile Computing?

Multiplexing: Introduction

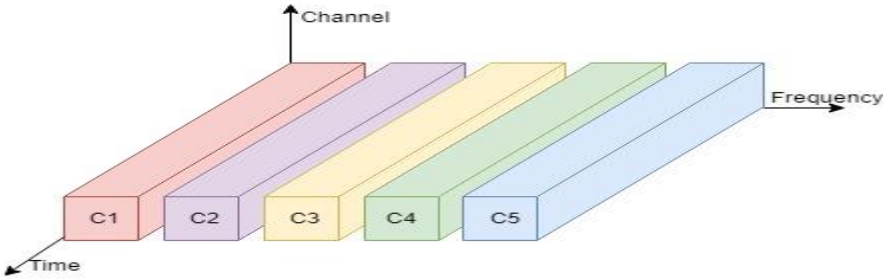
- Multiplexing is a technique in which, multiple simultaneous analog or digital signals are transmitted across a single data link.
- The concept behind it is very simple: Proper Resource Sharing and its Utilization.
- It can be classified into four types. These are:



Multiplexing : Mobile Computing

Multiplexing: Frequency Division Multiplexing(FDM)

- In Frequency Division, the frequency dimension spectrum is split into bands of smaller frequency.
- FDM is used because of the facts that, a number of frequency band can work simultaneously without any time constraint.



Frequency Division

Advantages of FDM

- This concept is applicable on both analog signals as well as digital signals.
- Simultaneous signal transmission feature.

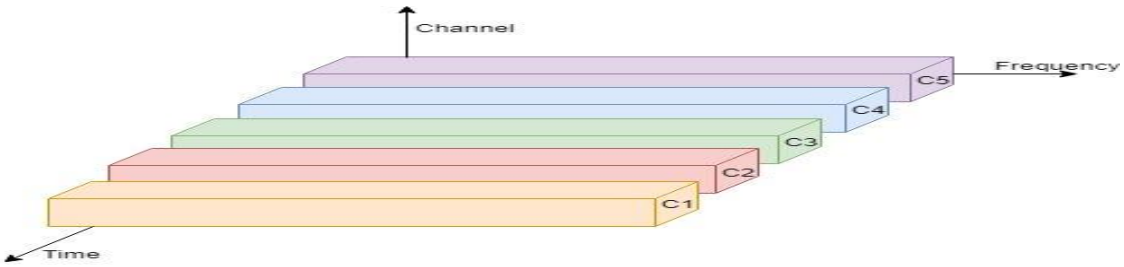
Disadvantages of FDM

- Less Flexibility.
- Bandwidth wastage is high and can be an issue.

For Example: Frequency Division Multiplexing can be used for radio station in a particular region as every radio station will have their own frequency and can work simultaneously without having any constraint of time.

Multiplexing: Time Division Multiplexing(TDM)

- Time Division is used for a particular amount of time in which the whole spectrum is used.
- Time frames of same intervals are made such that the entire frequency spectrum can be accessed at that time frame.



Time Division

Advantages of TDM

- Single user at a time.
- Less complex and more flexible architecture.

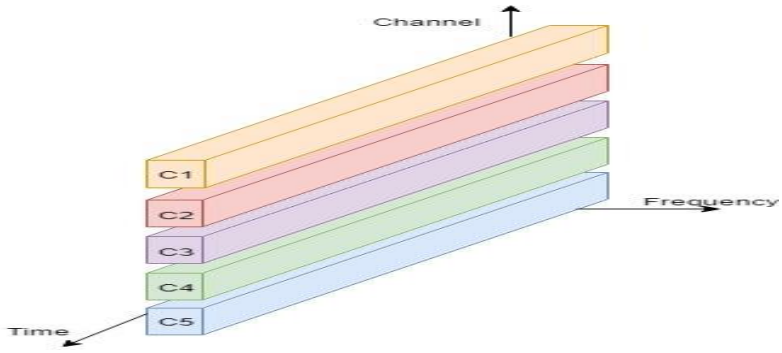
Disadvantages of TDM

- Difficult to implement.

For Example: ISDN(Integrated Service for Digital Network) telephonic service.

Multiplexing: Code Division Multiplexing (CDM)

- In Code Division Multiplexing, every channel is allotted with a unique code so that each of these channels can use the same spectrum simultaneously at same time.



Code Division

Advantages of CDM

- Highly Efficient.
- Less Inference.

Disadvantages of CDM

- Less data transmission rates.
- Complex in nature.

For Example: Cell Phone Spectrum Technology(2G, 3G etc.).

Multiplexing: Space Division Multiplexing(SDM)

- Space Division can be called as the combination of concepts of Frequency Division Multiplexing and Time Division Multiplexing.
- In SDM, the goal is to pass messages or data parallelly with the use of specific frequency at certain interval of time.
- It means, a particular channel for some amount of time will be used against a certain frequency band.

Advantages of SDM

- High Data transmission rate.
- Optimal Use of Time and Frequency bands.

Disadvantages of SDM

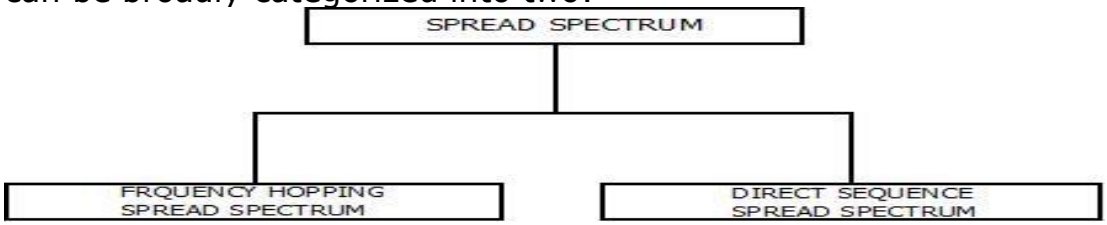
- Inference Problems.
- High inference losses.

For Example: GSM(Global Service For Mobile) Technology.

8) Explain in detail about Spread Spectrum used in Mobile Computing?

Spread Spectrum: Introduction

- When transmitted signals of certain frequencies are varied slightly in order to obtain greater bandwidth as compared to initial bandwidth is known as Spread Spectrum.
- Spread Spectrum technology helps in transmission of radio signals because they can easily reduce the noise and other issues that are data resistant.
- It can be broadly categorized into two:

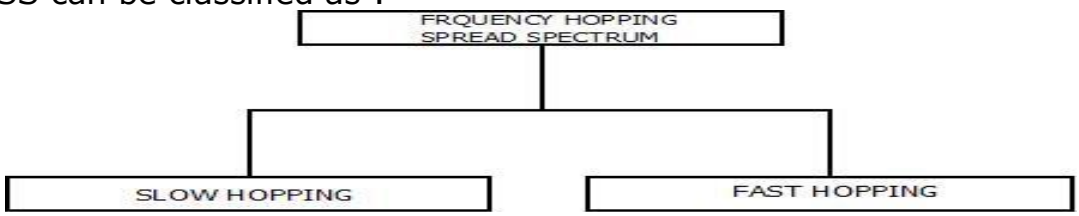


Spread Spectrum

- The major reason of spectrum technology being used is because of its proper bandwidth utilization ability.

Spread Spectrum: Frequency Hopping Spread Spectrum (FHSS)

- The logic behind the use of Frequency hopping Spread spectrum is, in order to utilize bandwidth properly, we need to divide the whole available bandwidth into many channels and spread them between channels which are arranged in a continuous manner.
- The selection of frequency slots is done on random basis and based on their occupancy, frequency signals are transmitted.
- The transmitters and receivers keeps on hopping on channels available for a particular amount of time in milliseconds.
- Hence, frequency division multiplexing and time division multiplexing are implemented simultaneously in FHSS.
- FHSS can be classified as :



Frequency Hopping Spectrum

- **Slow hopping**: In slow hopping, multiple bits are transmitted on a particular or same frequency.
- **Fast Hopping**: In fast hopping, individual bits are split and are transmitted on different frequencies.

Advantages of FHSS

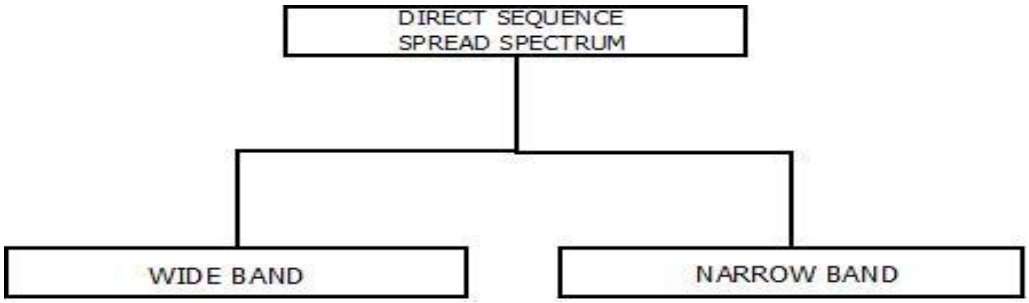
- Secure.
- Simple implementation as compared to DsSS.
- High efficiency.

Disadvantages of FHSS

- Less Robust.

Spread Spectrum: Direct Sequence Spread Spectrum (DSSS)

- Direct Sequence Spread Spectrum is another type of spread spectrum in which data that needs to be transmitted is split into smaller blocks.
- Then, each data block is attached with a high data rate bit sequence and is transmitted from sender end to receiver end.
- At the receiver's end with the help of data rate bit sequence, data blocks are recombined again to generate the original data which was sent by the sender.
- If in case the data is lost, with the help of those data rate bits data blocks can be recovered.
- This split of data into smaller blocks is done to reduce noise and unintentional inference.



Direct Sequence Spectrum

Advantages of DSSS

- Signals are difficult to detect.
- Less chances of jamming.
- Less reluctant to noise.

Disadvantages of DSSS

- Slow.
- Requirement of wide-band channels.

Applications of Spread Spectrum

- LAN technology
- Satellite communication technology.

9) Explain in detail about MAC Protocols and its properties?

Key Points
Responsibility
Two objectives
Features

MAC Protocols

- In a wireless network, multiple nodes may contend to transmit on the same shared channel at the same time.
- It is the **responsibility** of the medium access control (MAC) protocol to perform this task.
- The MAC protocol is a sub layer of the data link layer protocol and it directly invokes the physical layer protocol.
- The primary responsibility of a MAC protocol is to enforce discipline in the access of a shared channel when multiple nodes contend to access that channel.
- At the same time, **two other objectives** of any MAC protocol are maximization of the utilization of the channel and minimization of average latency of transmission.
- However, a MAC protocol must be fair and ensure that no node has to wait for an unduly long time, before it is allowed to transmit.

Properties Required of MAC Protocols

In a general sense a good MAC protocol needs to possess the following features:

- It should implement some rules that help to enforce discipline when multiple nodes contend for a shared channel.
- It should help maximize the utilization of the channel.
- Channel allocation needs to be fair. No node should be discriminated against at any time and made to wait for an unduly long time for transmission.

- It should be capable of supporting several types of traffic having different maximum and average bit rates.
- It should be robust in the face of equipment failures and changing network conditions.

10) Write in detail of Wireless MAC Protocols: Some Issues
Explain the wireless MAC issues in detail. (8) [May 2017]
Wireless MAC Protocols: Some Issues

Key Points
Hidden Terminal Problems
Exposed Terminal Problems in an Infrastructure-less Network

- A MAC protocol in a wireless medium is much more complex than its wired counterpart.
- First, a collision detection scheme is difficult to implement in a wireless environment, since collisions are hard to be detected by the transmitting nodes.
- Also, in infrastructure-less networks, the issue of hidden and exposed terminals make a MAC protocol extremely inefficient unless special care is taken to overcome these problems.

Explain Hidden and exposed terminal problem in infrastructure-less network . (8) [Nov 2017]
Explain in detail about hidden terminal problem and exposed terminal problem. (13) [Nov 2018]
The Hidden and Exposed Terminal Problems in an Infrastructure-less Network

The **Hidden Terminal** problem arises when at least three nodes (A, B, and C), as shown in Fig. 3.1, communicate among each other.

- As shown in this figure, B is in the radio range of A, and B is also within the radio range of C. However, the nodes A and C are not in the radio range of each other.
- Note that if both A and C start to transmit to B at the same time, the data received at node B would get garbled.
- Such a situation can arise because A and C are "hidden" from each other, because they are outside each other's transmission range. In this situation, when one node starts to sense the medium before transmission, it cannot sense that the other node is also transmitting. This creates a very difficult and important arbitration problem that a MAC protocol needs to resolve.

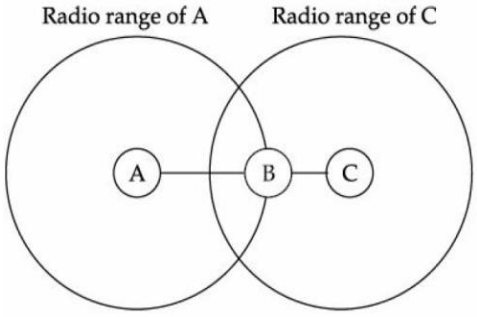


Figure 3.1 Hidden terminal problem

A related problem called **Exposed Terminal** could arise in a scenario such as that depicted in Fig. 3.2.

- MAC protocols usually inhibit transmission when transmission from another terminal is detected.
- As a result, node A will not be able to transmit to any node when B is transmitting to C.
- On the other hand, had A transmitted to D, it would have been received correctly by D and B's transmission would have also been correctly received at C.
- The problem arose only because A and B are within each other's transmission range, though the destination nodes are in the transmission range of only one of the nodes.
- In other words, the problem occurs because A is exposed to B's transmission.

The overall effect of **this problem is** that it leads to **inefficient spectrum usage** as well as **unnecessary transmission delays** unless these are carefully **addressed by a wireless MAC protocol**.

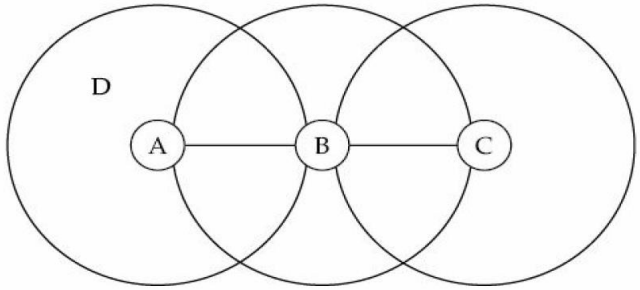


Figure 3.2 Exposed terminal problem.

11) Explain about Taxonomy of MAC Protocols?
Explain the various taxonomy of MAC protocols in detail. (16) [May 2016]
Explain MAC protocols for Adhoc Network. (8) [May 2017]

Key Points

- Fixed assignment schemes - are usually called circuit-switched schemes
  - Frequency Division Multiple Access (FDMA)
  - Time Division Multiple Access (TDMA)
  - Code Division Multiple Access (CDMA)
- Random assignment schemes are called packet-switched schemes
  - ALOHA
  - Slotted ALOHA
  - CSMA
  - CSMA/CD
  - CSMA/CA
- Reservation-based schemes - are called packet-switched schemes
  - MACA

Taxonomy of MAC Protocols

A large number of MAC protocols have been proposed. These MAC protocols can be broadly divided into the following three categories:

1. Fixed assignment schemes - are usually **called circuit-switched schemes**
2. Random assignment schemes
3. Reservation-based schemes -are **called packet-switched schemes**

- **In fixed assignment schemes**, the resources required for a call are assigned for the entire duration of the call.
- **In random assignment schemes** are comparable to the connection-less packet-switching schemes. In this, no resource reservations are made, the nodes simply start to transmit as soon as they have a packet to send.
- **In the reservation schemes**, a node makes explicit reservation of the channel for an entire call before transmitting. This is analogous to a connection-based packet-switching scheme.
- **The reservation-based MAC schemes are suitable to handle calls with widely varying traffic characteristics.**

12) What are the Fixed Assignment schemes of MAC protocol? Explain their mechanism in detail. Compare and contrast them FDMA, TDMA AND CDMA. (16) [Nov 2017]
Explain fixed assignment scheme with neat diagram. (8) [May 2017]

Fixed Assignment Schemes

A few important categories of fixed assignment MAC protocols are the following:

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

An analogy to the fixed assignment solution to the multiple access issues of a shared medium
An analogy may be drawn to the fixed assignment solution to the multiple access issues of a shared medium in the following way: Consider a students' common room (channel) in which many students want to communicate with each other. If the students want to avoid cross-talk in the ongoing process, then either the students could take turns in speaking (i.e. time division), or they could speak at different pitches (i.e. frequency division), or they could speak in different languages (i.e. code division). The last analogy captures the essence of CDMA, when the students who are speaking the same language understand each other, but the rest of the students cannot. In CDMA, each communicating pair shares a decryption code using which lets them understand only the communication between them. In this case many codes occupy the same channel, but only the users who share a specific code will be able to understand each other.

1) Frequency Division Multiple Access (FDMA)

- In FDMA, the available bandwidth (frequency range) is divided into many narrower frequency bands called channels. Figure 3.3 shows a division of the existing bandwidth into many channels (showns as Ch 1, Ch 2, etc.).

- For full duplex communication to take place, each user is allocated a forward link (channel) for communicating from it (mobile handset) to the base station (BS), and a reverse channel for communicating from the BS to it.
- Thus, each user making a call is allocated two unique frequency bands (channels), one for transmitting and the other for receiving signals during the call. Obviously, when a call is underway, no other user would be allocated the same frequency band to make a call.
- Unused transmission time in a frequency band that occurs when the allocated caller pauses between transmissions, or when no user is allocated a band, goes idle and is wasted. FDMA, therefore, does not achieve a high channel utilization.

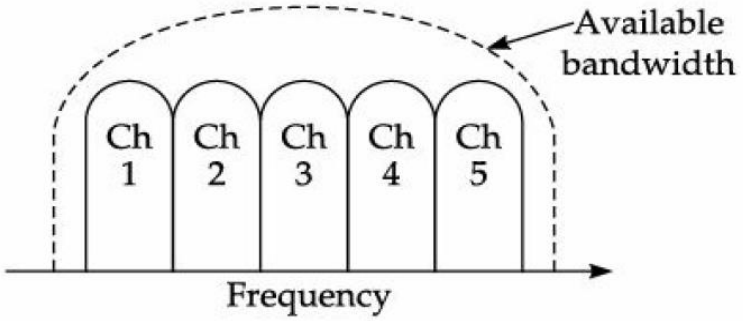


Figure3.3 Channels in Frequency Division Multiple Access (FDMA) scheme.

2) Time Division Multiple Access (TDMA)

- TDMA is an access method in which multiple nodes are allotted different time slots to access the same physical channel. That is, the timeline is divided into fixed-sized time slots and these are divided among multiple nodes who can transmit.
- Note that in this case, all sources use the same channel, but take turns in transmitting. Figure 3.4 shows the situation where time slots are allocated to users in a round robin manner, with each user being assigned one time slot per frame. See Box 3.2. Obviously, unused time slots go idle, leading to low channel utilization.

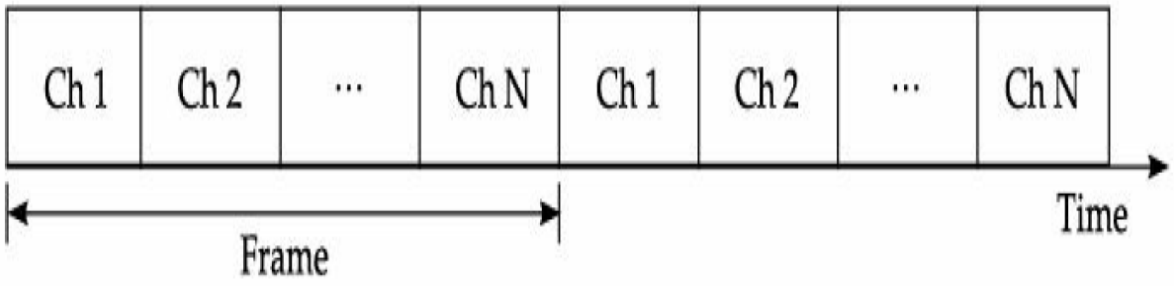


Figure 3.4 Channels in Time Division Multiple Access (TDMA) scheme.

3) Code Division Multiple Access (CDMA)

- In CDMA, multiple users are allotted different codes that consist of sequences of 0 and 1 to access the same channel.
- As shown in Fig. 3.5, a special coding scheme is used that allows signals from multiple users to be multiplexed over the same physical channel.
- As shown in the figure, three different users who have been assigned separate codes are multiplexed on the same physical channel.

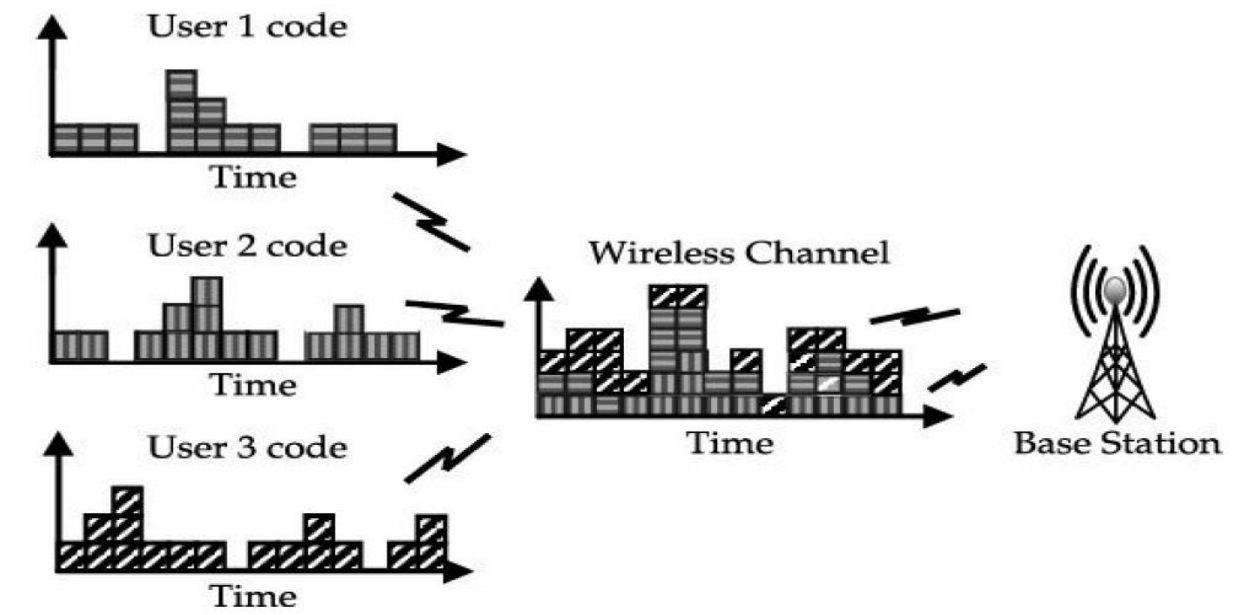


Figure 3.5 *Schematic of operation of Code Division Multiple Access (CDMA).*

13) Describe the various random assignment schemes that are used in MAC protocol? (8) [Nov 2018]

I) Random Assignment Schemes

There are a number of random assignment schemes that are used in MAC protocols.

i) ALOHA
ii) Slotted ALOHA
iii) CSMA
iv) CSMA/CD
v) CSMA/CA

i) ALOHA Scheme

- It is a simple communication scheme, the basic (also called pure) ALOHA scheme, is a simple protocol. If a node has data to send, it begins to transmit.

Note that the first step implies that Pure ALOHA does not check whether the channel is busy before transmitting.

- If the frame successfully reaches the destination (receiver), the next frame is sent.
- If the frame fails to be received at the destination, it is sent again.

The simple ALOHA scheme works acceptably,

- When the chances of contention are small (i.e., when a small number of senders send data infrequently).
- However, the collisions can become **unacceptably** high if the number of contenders for transmission is high.

An **improvement** over the pure **ALOHA scheme is the slotted ALOHA**.

- In the slotted ALOHA scheme, the chances of collisions are attempted to be reduced by enforcing the following restrictions.
- The time is divided into equal-sized slots in which a packet can be sent.

- Thus, the size of the packet is restricted. A node wanting to send a packet, can start to do so only at the beginning of a slot.
- The slotted ALOHA system employs beacon signals that are sent at precise intervals that mark the beginning of a slot, at which point the nodes having data to send can start to transmit.
- Again, this protocol does not work very well if the number of stations contending to send data is high. **In such cases, the CSMA scheme (described next) works better.**

What is CSMA? What are the categories of CSMA? Explain their working with advantages and disadvantages? (7) [Apr 2018]

ii) The CSMA Scheme

- A popular MAC arbitration technique is the Carrier Sense Multiple Access (CSMA).
- In this technique, a node senses the medium before starting to transmit.
- If it senses that some transmission is already underway, it defers its transmission.

Two popular extensions of the basic CSMA technique are

- The collision detection (CSMA/CD) and the collision avoidance (CSMA/CA) techniques.
- In the CSMA/CD technique, the sender starts to transmit if it senses the channel to be free. But, even if it senses the channel to be free, there can be a collision (why?) during transmission.
- In a **wired network**, the implementation of a **collision detection scheme is simple**.
- However, in a **wireless network** it is very **difficult** for a transmitting node to **detect a collision**, since any received signal from other nodes would be too feeble compared to its own signal and can easily be masked by noise.
- As a result, a transmitting node would continue to transmit the frame, and only the destination node would notice the corrupted frame after it computes the checksum. This leads to retransmissions and severe wastage of channel utilization.
- **In contrast**, in a **wired network when a node detects a collision**, it immediately stops transmitting, thereby minimizing channel wastage.
- **In a wireless network, a collision avoidance scheme works much better** compared to a collision detection-based scheme.
- A collision avoidance scheme is based on the idea that it is necessary to prevent collisions at the moment they are most likely to occur, that is, when the bus is released after a packet transmission.

Advantages and Disadvantages of CSMA

Advantages	Disadvantages
Helps prevent data collisions	Longer waiting times
Thanks to feedback, no data is	Causes additional traffic

Advantages	Disadvantages
unnoticeably lost	
Avoids unnecessary data traffic with the RTS/CTS extension	Solves the hidden station problem only by using RTS/CTS extension
	Creates the exposed station problem through using RTS/CTS

14) Discuss the various reservation based schemes in MAC protocol. (5) [Nov 2018]

II) Reservation-based Schemes

- A basic form of the reservation scheme is the RTS/CTS scheme.
- In an RTS/CTS scheme, a sender transmits an RTS (Ready to Send) packet to the receiver before the actual data transmission. On receiving this, the receiver sends a CTS (Clear to Send) packet, and the actual data transfer commences only after that.
- When the other nodes sharing the medium sense the CTS packet, they refrain from transmitting until the transmission from the sending node is complete.
- In a contention-based MAC protocol, a node wanting to send a message first reserves the medium by using an appropriate control message.
- **For example**, reservation of the medium can be achieved by transmitting a "Ready To Send" (RTS) message and the corresponding destination node accepting this request answers with a "Clear To Send" (CTS) message.
- Every node that hears the RTS and CTS messages defers its transmission during the specified time period in order to avoid a collision.
- **A few examples of RTS-CTS based** MAC protocols are MACA, MACAW, MACA-BI, PAMAS, DBTMA, MARCH, S-MAC protocols which have specifically been designed for sensor networks.

Explain in detail about hidden terminal problem and exposed terminal problem. (13) [Nov 2018]

MACA: MACA stands for Multiple Access Collision Avoidance

- MACA solves the hidden/exposed terminal problems by regulating the transmitter power. A node running MACA requests to use the medium by sending an RTS to the receiver.
- Since radio signals propagate omni-directionally every terminal within the sender's radio range will hear this and then refrain from transmitting. As soon as the receiver is ready to receive data, it responds with a CTS.

Figure 3.6 schematically shows how MACA avoids the hidden terminal problem. Before the start of its transmission, it sends a **Request To Send (RTS).**

- B receives the RTS that contains the sender's name and the receiver's name, as well as the length of the future transmission**.**

- In response to the RTS, an acknowledgment from B is triggered indicating **Clear To Send** (CTS).
- The CTS contains the names of the sender and receiver, and the length of the planned transmission.
- This CTS is heard by C and the medium is reserved for use by A for the duration of the transmission.

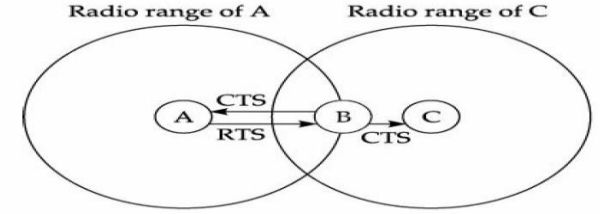


Figure 3.6 Hidden terminal solutions in MACA.

Some other technology that can be employed to solve hidden node problem are :

Increase Transmitting Power from the Nodes:

With the enhancement of the transmission power of access point can solve the hidden terminal problem by allowing the cell around each node to increase in size, encompassing all of the other nodes.

Use Omni directional antennas:

Since nodes using directional antennas are nearly invisible to nodes that are not positioned in the direction the antenna is aimed at, directional antennas should be used only for very small networks.

Remove obstacles:

Keep away the obstacles that affect the performance of access point accessibility.

Move the node:

Provide the mobility features to the nodes.

Use protocol enhancement software:

Pooling and token passing strategy should be used before start data transformation.

- On receipt of a CTS from B, C refrains from transmitting anything for the time indicated in the CTS.
- Thus a collision cannot occur at B during data transmission, and the hidden terminal problem is solved.
- **Figure 3.7** schematically shows how the exposed terminal problem is solved in MACA. Assume that B needs to transmit to A.
- B has to transmit an RTS first as shown in Fig. 3.7.
- The RTS would contain the names of the receiver (A) and the sender (B).
- C does not act in response to this message as it is not the receiver, but A responds with a CTS.
- C does not receive this CTS and concludes that A is outside the detection range.
- Thus C can start its transmission assuming that no collision would occur at A.

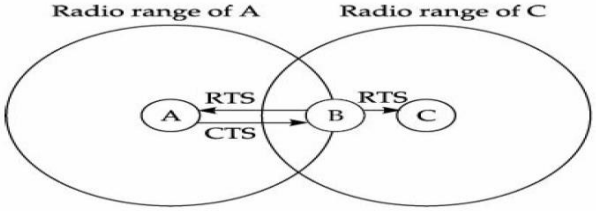


Figure 3.7 Exposed terminal solution in MACA.

15) Differentiate between SDMA, FDMA, TDMA and CDMA.(16)[Nov 2016]

Comparison SDMA/TDMA/FDMA/CDMA

Approach	SDMA	TDMA	FDMA	CDMA
Idea	segment space into cells/sectors	segment sending time into disjoint time-slots, demand driven or fixed patterns	segment the frequency band into disjoint sub-bands	spread the spectrum using orthogonal codes
Terminals	only one terminal can be active in one cell/one sector	all terminals are active for short periods of time on the same frequency	every terminal has its own frequency, uninterrupted	all terminals can be active at the same place at the same moment, uninterrupted
Signal separation	cell structure, directed antennas	synchronization in the time domain	filtering in the frequency domain	code plus special receivers
Advantages	very simple, increases capacity per km²	established, fully digital, flexible	simple, established, robust	flexible, less frequency planning needed, soft handover
Dis-advantages	inflexible, antennas typically fixed	guard space needed (multipath propagation), synchronization difficult	inflexible, frequencies are a scarce resource	complex receivers, needs more complicated power control for senders
Comment	only in combination with TDMA, FDMA or CDMA useful	standard in fixed networks, together with FDMA/SDMA used in many mobile networks	typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	still faces some problems, higher complexity, lowered expectations; will be integrated with TDMA/FDMA

Prof. Dr.-Ing. Jochen Schiller, http://www.jochenschiller.de/ MC SS05 3.26

<u>Frequency division multiple access</u> (FDMA):

- It is a technology by which the total bandwidth available to the system is divided into frequencies. This division is done between non overlapping frequencies that are then assigned to each communicating pair (2 phones)
- FDMA is used mainly for analog transmission. Its not that this technology is not capable of carrying digital information, but just that it is not considered to be an efficient method for digital transmission.
- Because just imagine if the frequencies to handle the customers gets over? What if more capacity is required? The only option would be to drill down the existing frequencies to a much narrower amount which will not be very competent.
- In FDMA all users share the satellite simultaneously but each user transmits at single frequency.
- To understand this technology better, just imagine how FM radio works. All the radios have their own frequency bands and they send their signals at the carefully allocated unique frequencies within the available bands.

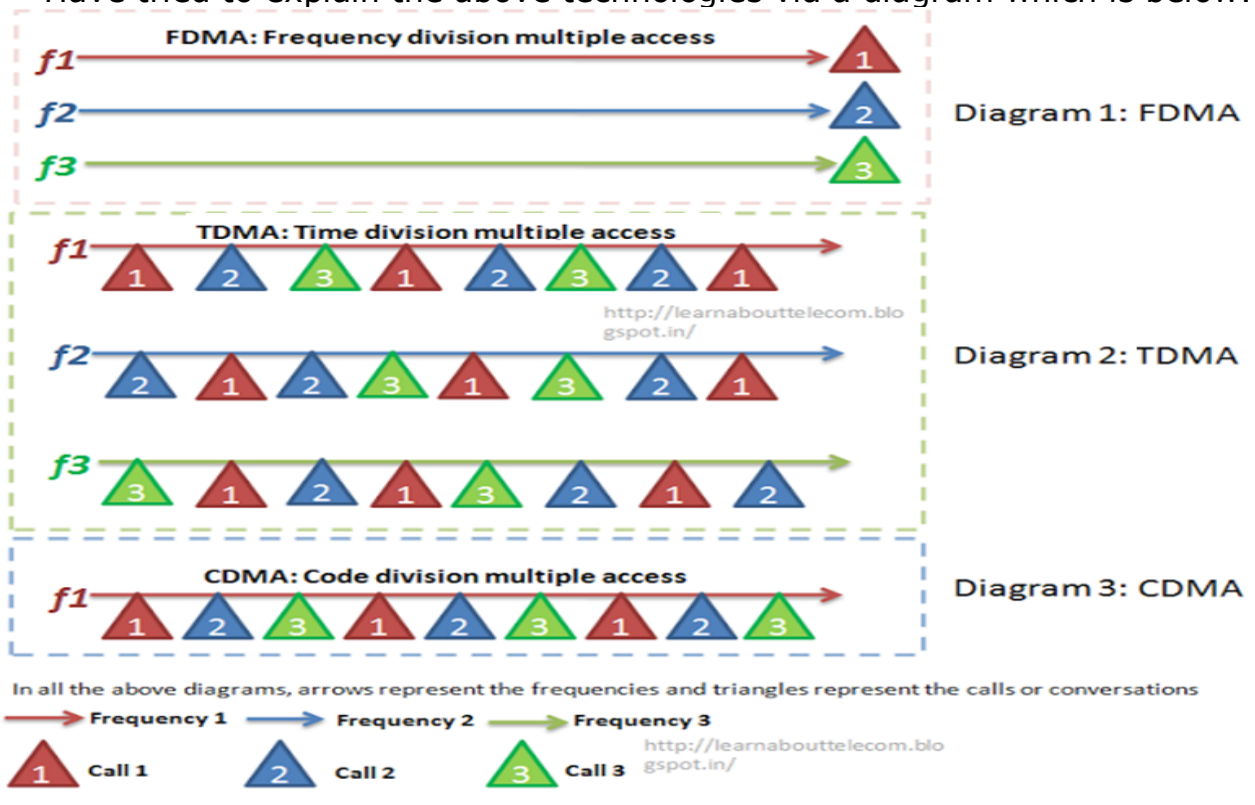
<u>Code division multiple access</u> (CDMA):

- Unlike FDMA, CDMA separates calls by code. Every bit of a conversation is been tagged with a specific and unique code.
- The system gets a call, it allocates a unique code to that particular conversation, now the data is split into small parts and is tagged with the unique code given to the conversation of which they are part of.

- Now, this data in small pieces is sent over a number of the discrete frequencies available for use at any time in the specified range. The system then at the end reassembles the conversation from the coded bits and deliver it.

Time division multiple access (TDMA):

- Unlike FDMA and CDMA, In TDMA the division of calls happens on time basis.
- The system first digitizes the calls, and then combines those conversations into a unified digital stream on a single radio channel.
- Now it divides each cellular channel into three time slots that means three calls get put on a single frequency and then, a time slot is assigned to each call during the conversation, a regular space in a digital stream.
- The users transmit in rapid succession, one after the other, each using its own time slot. This allows multiple stations to share the same transmission medium (e.g. radio frequency channel) while using only a part of its channel capacity.
- This technology enables three different users to use one frequency at the same time.
- Here there is no need for three separate frequencies like in FDMA. As in FDMA, instead of monopolizing a single radio channel for a single call, TDMA efficiently carries three calls at the same time☺
- BTW, this technology is the one used in our GSM system
- Have tried to explain the above technologies via a diagram which is below:



In the above diagram, you will observe:

FDMA: Single frequency is used for single call
CDMA: Single frequency is used for multiple calls

TDMA: Multiple frequencies are used for multiple calls

ANNA UNIVERSITY QUESTIONS

PART A

1. List the issues of wireless MAC? [Apr 2018]
   Refer Q.No.1
2. Distinguish between mobile computing and wireless networking? [Apr 2018]
   Refer Q.No.2
3. What are the challenges in mobile communication? [Nov 2018]
   Refer Q.No.3
4. State the objectives of MAC protocols. [Nov 2018]
   Refer Q.No.5
5. List out the difference between Mobile Computing and Wireless Networking.
   Refer Q.No.6 [Nov 2017][May 2017]
6. "MAC protocol designed for infrastructure based wireless network may not work satisfactory in infrastructure-less environment." – Justify. [Nov 2017]
   Refer Q.No.7
7. List some random assignment schemes. [May 2017]
   Refer Q.No.8
8. What are the limitations of Mobile Computing? [Nov 2016]
   Refer Q.No.9
9. What are the different Random Assignment Scheme in MAC? [Nov 2016]
   Refer Q.No.10
10. List the advantages of Mobile Computing. [May 2016]
    Refer Q.No.11
11. Explain hidden and exposed terminal problems in infrastructure less network.
    Refer Q.No.12 [May 2016]

ANNA UNIVERSITY QUESTIONS

PART B

1. Differentiate between FDMA, TDMA and CDMA. (16) [Nov 2016]
2. Explain the distinguishing features of various generations of wireless networks. (8) [Nov 2016]
3. Describe the applications of Mobile Computing. (8) [Nov 2016]
4. Explain the characteristics of Mobile Computing. (8) [May 2016]
5. Explain the structure of Mobile Computing Application. (8) [May 2016]
6. Explain the various taxonomy of MAC protocols in detail. (16) [May 2016]
7. Explain Hidden and exposed terminal problem in infrastructure-less network. (8) [Nov 2017]
8. Describe architecture of Mobile Computing. (8) [Nov 2017]
9. What are the Fixed Assignment schemes of MAC protocol? Explain their Mechanism in detail. Compare and contrast them. (16) [Nov 2017]
10. Explain the wireless MAC issues in detail. (8) [May 2017]
11. Explain the various applications of Mobile Computing. (8) [May 2017]
12. Explain fixed assignment scheme with neat diagram. (8) [May 2017]
13. Explain MAC protocols for Adhoc Network. (8) [May 2017]
14. Describe the various random assignment schemes that are used in MAC Protocol? (8) [Nov 2018]
15. Discuss the various reservation based schemes in MAC protocol. (5) [Nov 2018]
16. Explain in detail about hidden terminal problem and exposed terminal Problem. (13) [Nov 2018]
17. Discuss in detail the structure of mobile computing? (6) [Apr 2018]
18. Apply mobile computing to design taxi dispatcher and monitoring service. Explain the components in detail. (7) [Apr 2018]
19. List the characteristics of mobile systems? (6) [Apr 2018]
20. What is CSMA? What are the categories of CSMA? Explain their working with Advantages and disadvantages? (7) [Apr 2018]