CS8601 MOBILE COMPUTING

UNIT – I
INTRODUCTION

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

COURSE OBJECTIVE: Understand the basic concepts of mobile computing.

PART – A

1. Define Mobile Computing.

Mobile Computing also called as Ubiquitous Computing or Nomadic Computing is described as the ability to compute remotely while on the move. It makes possible for people to access information from anywhere and at any time.

Mobile Computing = Mobility + Computing

2. What do you mean by the terms Mobility and Computing?

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

Computing: Capability to automatically carry out certain processing related to services invocation on a remote computer.

3. Name the type of Mobility.

a) User Mobility
b) Device Portability

4. List out the advantages of Mobile Computing. May/June 2016

(i) Location Flexibility
(ii) User Mobility
(iii) Device Portability
(iv) Saves Time
(v) Enhanced Productivity
(vi) Entertainment

5. Mention the disadvantages of Mobile Computing.

(i) Expensive
(ii) Power Consumption
(iii) Small Screen Display
(iv) Slow Internet Speed
(v) Risky to carry
(vi) Security Concerns
(vii) Communication depends upon network

6. 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

7. List out the differences between Mobile Computing and Wireless Networking.

S.No	Mobile Computing	Wireless Networking
1.	It is a technology that access data through wireless network	It is a network that uses wireless data connections for connecting network nodes
2.	It denotes accessing information and remote computational services while on the move	It provides the basic communication infrastructure necessary for mobile computing
3.	It refers to computing devices that are not restricted to a desktop. Eg: Smart Phone, PDA, Laptop etc.,	It is a method of transferring information between a computing devices such as PDA & data sources without a physical connection
4.	It refers to a device performing computation that is not always connected to a central network	It refers to the data communication without the use of a landline. Eg. Cellular Telephone, Two way radio, Satellite, Wireless Connection.

8. Name some of the Mobile Computing Devices.

- Mobile Phones
- Laptops
- PDA
- Notebook PCs

9. Point out the problems faced by devices in Wireless Transmission?

1. Lower Bandwidth
2. Bandwidth Fluctuations
3. Host mobility
4. Intermittent disconnections
5. High bit error rate
6. Poor link reliability
7. Higher delay
8. Power consumption

10. What are the classifications of Wireless Networks?

i) Extension of Wired Networks: Uses fixed infrastructures such as base stations to provide single hop wireless communication (or) two-hop wireless communication.
   a. Example: WLAN, Bluetooth

ii) Adhoc Networks: It does not use any fixed infrastructure and it is based on multi-hop wireless communication.

Example: MANET, VANET.

11. What are the applications of mobile computing?

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

12. List out the characteristics of Mobile Computing.

(i) Ubiquity
(ii) Location Awareness
(iii)Adaptation
(iv)Broadcast
(v) Personalization

13. Draw the structure of Mobile Computing Application.

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

14. Specify the functionalities of Application Tier.

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

15. What is the use of Data Tier?

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

16. Describe about MAC Protocol.

MAC Protocol is access control protocol which is responsible for regulating access to the shared channel when multiple nodes compete to access that channel. It is a sub layer of the data link layer protocol and it directly invokes the physical layer protocol.

17. What are the Objectives of MAC Protocol?

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

18. List out the properties required of MAC protocol.

(i) It should implement some rules to enforce discipline wen multiple nodes compete for a shared channel.
(ii) It should help maximize the channel utilization.
(iii) Channel allocation needs to be fair. No node should be discriminated against at any time and made wait for an long time for transmission.
(iv) It should be capable of supporting several types of traffic having different bit rates.
(v) It should be robust in the face of equipment failure and changing network conditions.

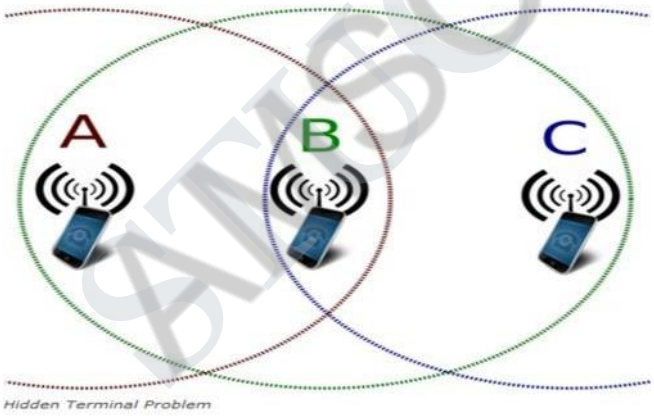
19. What is meant by Hidden Node and Exposed Node?

- Hidden Node: A hidden node is a node that does not hear the transmission that a node within its range is receiving and thus does not attempting to gain access.
- Exposed Node: An exposed node is a node that hears multiple disjoint sections of a network and never gets an opportunity to compete for transmission since it is always deferring to someone.

20. Explain hidden and exposed terminal problem in infrastructure-less network. May/June 2016

Hidden Terminal Problem:

The Hidden Terminal Problem arises when at least three nodes (A, B and C) communicating.

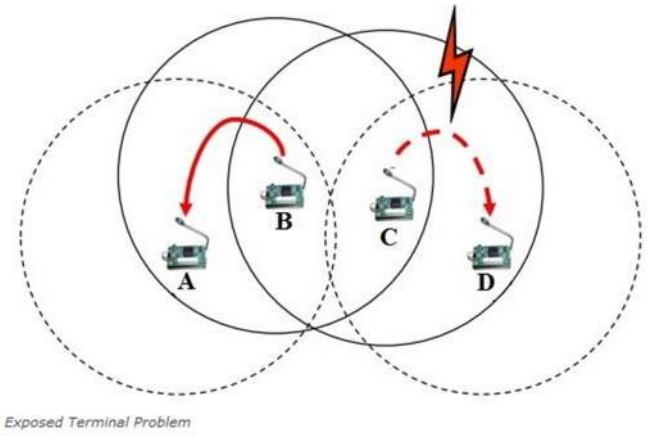


B is in the radio range of A, and B is also with the radio range of C. The nodes A and C are not in the radio range of each other. If both A and C start to transmit to B at the same time, the data received at B would get garbled. This situation arises because A and C are "hidden" from each other, because they are outside each other's transmission range.

Note:- Hidden Terminal causes Collisions.

Exposed Terminal Problem:

Exposed Terminal Problem arises when all the three nodes are in the radio range of all nodes.



Exposed Terminal Problem

Now B is transmitting to A, C wants to send to another terminal (not A or B) outside the range. C senses the carrier and detects that the carrier is busy, so C postpones the transmission until it detects the medium is free. But A is outside the radio range of C. This problem arises because "C is exposed to B".

Note:- Exposed Terminal leads to inefficient spectrum usage and unnecessary transmission delays.

21. What are the classifications of MAC Protocols?

Wireless MAC protocols are classified into

A. Fixed-assignment schemes (Circuit-switched)
B. Random-Assignment schemes(CL packet-switched)
C. Reservation-based schemes(CO packet-switched)

(i) Fixed Assignment
   a. FDMA
   b. TDMA
   c. CDMA

(ii) Random Assignment
   a. ALOHA
   b. Slotted ALOHA
   c. CSMA
   d. CSMA/CD
   e. CSMA/CA

(iii) Reservation Based
   a. RTS / CTS

22. Compare CSMA / CD and CSMA / CA.

S.No	CSMA / CD	CSMA / CA
1.	It takes effect after a collision	It takes effect before a collision
2.	It will not take steps to prevent transmission collision until it is taken place	It will take actions not to take place any collision

3.	It only minimizes the recovery time	It reduces the possibility of a collision
4.	Typically used in wired networks	Typically used in wireless networks & WLANs
5.	Standardized in IEEE 802.3	Standardized in IEEE 802.11

23. Summarize the steps involved in RTS / CTS scheme.

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

24. 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.

25. Assess why is the MAC protocol designed for infrastructure based wireless N/W may not work satisfactory in infrastructure-less environment. Justify your answer?

Because,

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

PART - B

1. Explain the characteristics of Mobile Computing. [An] **May/June 2016**

CHARACTERISTICS OF MOBILE COMPUTING

Portability - The Ability to move a device within a learning environment or to different environments with ease.

. **Social Interactivity** - The ability to share data and collaboration between users.

. **Context Sensitivity** - The ability to gather and respond to real or simulated data unique to a current location, environment, or time.

. **Connectivity** - The ability to be digitally connected for the purpose of communication of data in any environment.

. **Individual** - The ability to use the technology to provide scaffolding on difficult activities and lesson

customization for individual learners.

. **Small Size -** Mobile devices are also known as handhelds, palmtops and smart phones due to their roughly phone-like dimensions. A typical mobile device will fit in the average adult's hand or pocket. Some mobile devices may fold or slide from a compact, portable mode to a slightly larger size, revealing built-in keyboards or larger screens. Mobile devices make use of touch screens and small keypads to receive input, maintaining their small size and independence from external interface devices. The standard form of a mobile device allows the user to operate it with one hand, holding the device in the palm or fingers while executing its functions with the thumb.

Netbooks and small tablet computers are sometimes mistaken for true mobile devices, based on their similarity in form and function, but if the device's size prohibits one-handed operation or hinders portability, then it cannot be considered a true mobile device.

. **Wireless Communication -** Mobile devices are typically capable of communication with other similar devices, with stationary computers and systems, with networks and portable phones. Base mobile devices are capable of accessing the Internet through Bluetooth or Wi-Fi networks, and many models are equipped to access cell phone and wireless data networks as well. Email and texting are standard ways of communicating with mobile devices, although many are also capable of telephony, and some specialized mobile devices, such as RFID and barcode.

2. Explain the structure of Mobile Computing Applications with neat sketch. [An] **May/June 2016**

Programming languages are used for mobile system software. Operating system functions to run the software components onto the hardware. Middleware components deployment. Layered structure arrangement of mobile computing components is used. Protocols and layers are used for transmission and reception.

Programming Languages

The following are the programming languages used for Mobile Computing applications are:

- Java - J2SE.
- J2ME (Java2 Micro edition)
- JavaCard (Java for smart card)
- The Java enterprise edition (J2EE) used for web and enterprise server based applications of mobile services
  - C and C+
- Visual C++

- Visual Basic

Operating System

Symbian OS, Window CE, Mac OS are the operating systems used in Mobile computing applications. It offers the user to run an application without considering the hardware specifications and functionalities. It provides functions which are used for scheduling the multiple tasks in a system.

It provides the functions required for the synchronization of multiple tasks in the system. It uses multiple threads synchronization and priority allocation. Management functions (such as creation, activation, deletion, suspension, and delay) are used for tasks and memory. It provides Interfaces for communication between software components at the application layer, middleware layers, and hardware devices.

It facilitates the execution of software components on diversified hardware. It provides Configurable libraries for the GUI (graphic user interface) in the device. It provides

User application‘s GUIs, VUI (voice user interface) components, and phone API. It provides the device drivers for the keyboard, display, USB, and other devices.

Middleware

Software components that link the application components with the network-distributed components. It is used to discover the nearby device such as Bluetooth. It is used to discover the nearby hot spot for achieving device synchronization with the server or an enterprise server. It is used for retrieving data (which may be in Oracle or DB2) from a network database. It is used for service discovery at network. It is used for adaptation of the application to the platform and service availability.

Architecture of Mobile Computing Applications

Client/server architecture (and its variants) is often adopted for this kind of applications. However we have to take into consideration some specific aspects related to the mobile devices (clients), and their connectivity with servers.

Clients

There are many mobile device types, including RIM devices, cellular telephones, PDAs, Tablet, PCs, and Laptop PCs. These mobile devices can typically operate as thin clients or fat clients, or they can be developed so that they can host web pages

Thin Clients

Thin clients have no custom application code and completely rely on the server for their functionality. They do not depend as heavily on the mobile device‘s operating system or the mobile device type as fat clients. Thin clients typically use widely available web and Wireless Application Protocol (WAP) browsers to display the application content pages.

Fat Clients

Fat clients typically have one to three layers of application code on them and can operate independently from a server for some period of time. Typically, fat clients are most useful in situations where communication between a client and server cannot be guaranteed.

For example, a fat client application may be able to accept user input and store data in a local database until connectivity with the server is re-established and the data can be moved to the server.

This allows a user to continue working even if he/she is out of contact with the server. Fat clients depend heavily on the operating system and mobile device type and the code can be difficult to release and distribute. Fat clients can be implemented using one, two, or three layers of application code. However, if you only use one layer it is extremely difficult to isolate the individual areas of functionality and reuse and distribute the code over multiple device types.

3. Explain the various taxonomy of MAC protocols in detail. [U] **May/June 2016**

Three broad classes: • Channel partitioning • Divide channel into smaller "pieces" (time slots, frequency) • Allocate piece to node for exclusive use • Random access • Allow collisions • "Recover" from collisions • "Taking turns" • Tightly coordinate shared access to avoid collisions Goal: efficient, fair, simple, decentralized

• Random Access MAC Protocols • Ethernet MAC • Random Access Analysis • Other Ethernet Issues • "Taking Turns" MAC and Other LANs

When node has packet to send • Transmit at full channel data rate R. • No a priori coordination among nodes • Two or more transmitting nodes ‡ "collision", • Random access MAC protocol specifies: • How to detect collisions • How to recover from collisions (e.g., via delayed retransmissions) • Examples of random access MAC protocols: • Slotted ALOHA • ALOHA • CSMA and CSMA/CD

Aloha – Basic Technique

First random MAC developed • For radio-based communication in Hawaii (1970) • Basic idea: • When you're ready, transmit • Receiver's send ACK for data • Detect collisions by timing out for ACK • Recover from collision by trying after random delay • Too short ‡ large number of collisions • Too long ‡ underutilization

Slotted Aloha

Time is divided into equal size slots (= pkt trans. time) • Node (w/ packet) transmits at beginning of next slot • If collision: retransmit pkt in future slots with probability p, until successful Success (S), Collision (C), Empty

Pure (Unslotted) ALOHA • Unslotted Aloha: simpler, no synchronization • Pkt needs transmission: • Send without awaiting for beginning of slot • Collision probability increases: • Pkt sent at t0 collide with other pkts sent in [t0 -1, t0+1]

Ethernet

• First practical local area network, built at Xerox PARC in 70's • "Dominant" LAN technology: • Cheap $20 for 100Mbs! • Kept up with speed race: 10, 100, 1000 Mbps

Ethernet MAC – Carrier Sense

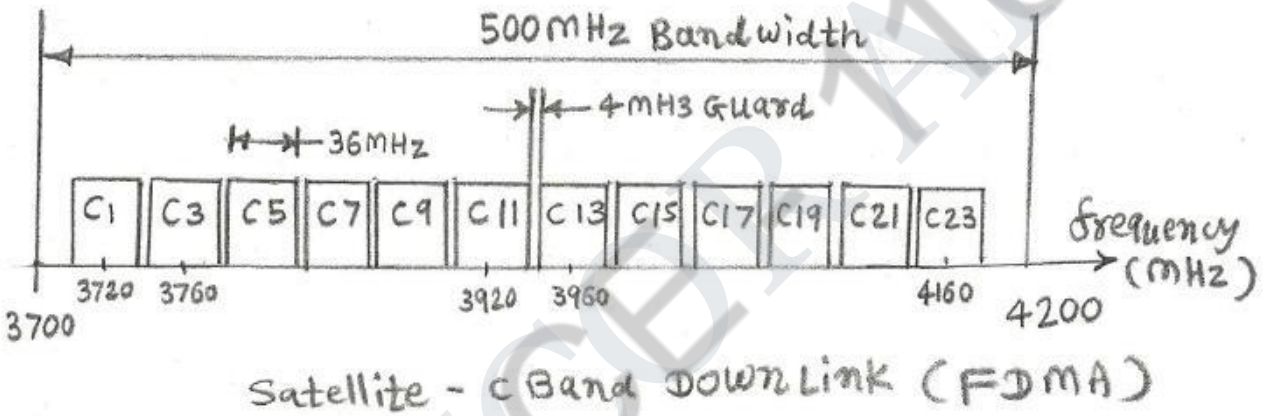
5: 9 -11-01 10 Ethernet MAC – Carrier Sense

4. Briefly explain FDMA, CDMA, and TDMA. [An] **Nov/Dec 2011, May/June 12, May /June 2013, Nov/Dec 2013, May/June 2014, Nov/Dec2014**

FDMA- Frequency Division Multiple Access, here entire band of frequencies is divided into multiple RF channels/carriers. Each carrier is allocated to different users.

For example in GSM entire frequency band of 25 MHz is divided into 124 RF carriers of bandwidth 200 KHz each. In Satellite applications entire transponder band of 500 MHz is divided into 24 channels each of bandwidth 40MHz (36 MHz useful and 4MHz guard band).

There are two main types of FDMA scheme used in satellite network. SCPC(Single channel per carrier) and MCPC(multiple channel per carrier). MCPC uses FDM or TDM as multiplexing scheme.



Satellite - C Band Down Link (FDMA)

FDMA Types

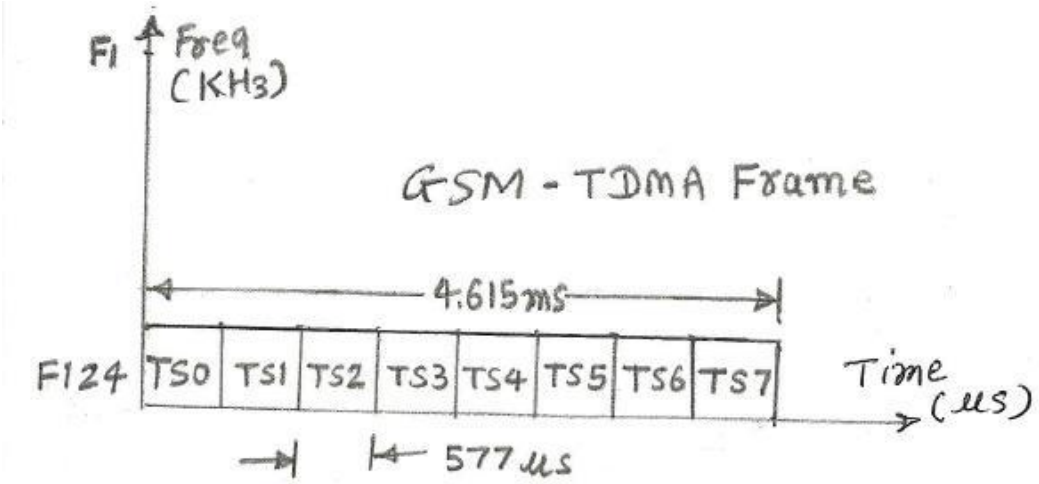
• **FAMA**- Fixed Assignment Multiple Access, here frequencies are pre-allocated to users/subscribers/VSATs.

• **DAMA**- Demand Assignment Multiple Access, here frequencies are dynamically allocated based on requests.

TDMA

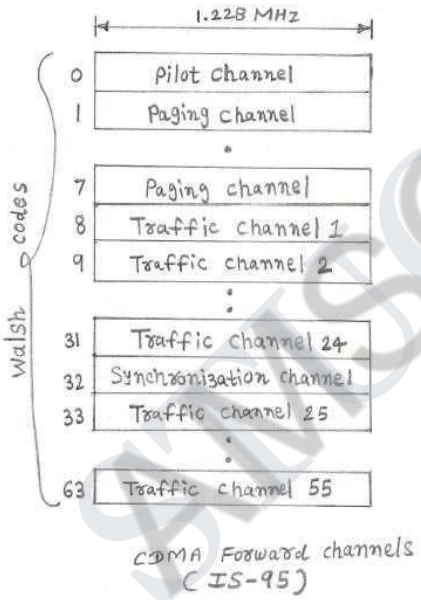
TDMA- Time Division Multiple Access, here entire bandwidth is shared among different subscribers at fixed predetermined or dynamically assigned time intervals/slots. For example in GSM each RF carrier is used/shared by 8 users at different time instants.

TDMA uses TDM multiplexing technique.



CDMA

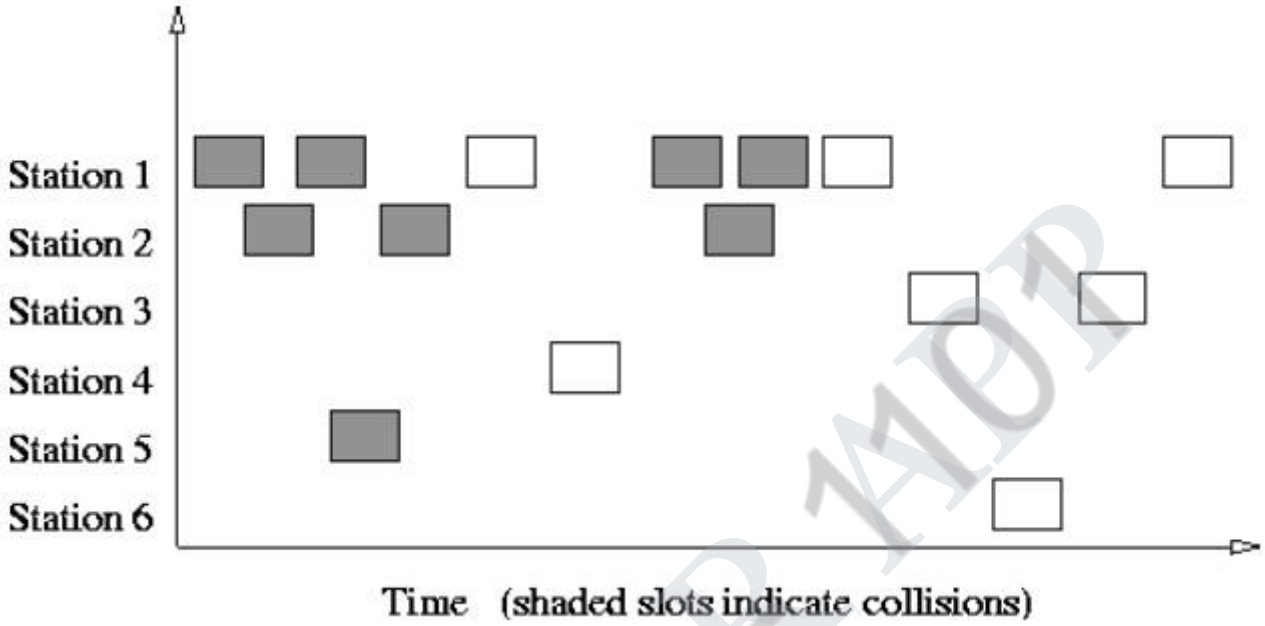
CDMA-Code Division Multiple Access, here entire bandwidth is shared among different users by assigning unique codes. For example in CDMA IS-95 standard entire bandwidth of 1.225 MHz is shared by various channels/users using unique 64 Walsh Codes. In CDMA entire bandwidth is being used by users all the time and each have their unique codes to recover the data. The system works based on spread spectrum concept.



5. Explain in detail about the motivation for specialized MAC. [U] **May/June 2013**
6. Explain the following: [U]
   (i) Random Assignment Schemes
   (ii) Reservation-based schemes

Pure Aloha

With Pure Aloha, stations are allowed access to the channel whenever they have data to transmit. Because the threat of data collision exists, each station must either monitor its transmission on the rebroadcast or await an acknowledgment from the destination station. By comparing the transmitted packet with the received packet or by the lack of an acknowledgement, the transmitting station can determine the success of the transmitted packet. If the transmission was unsuccessful it is resent after a random amount of time to reduce the probability of re-collision.



Slotted Aloha

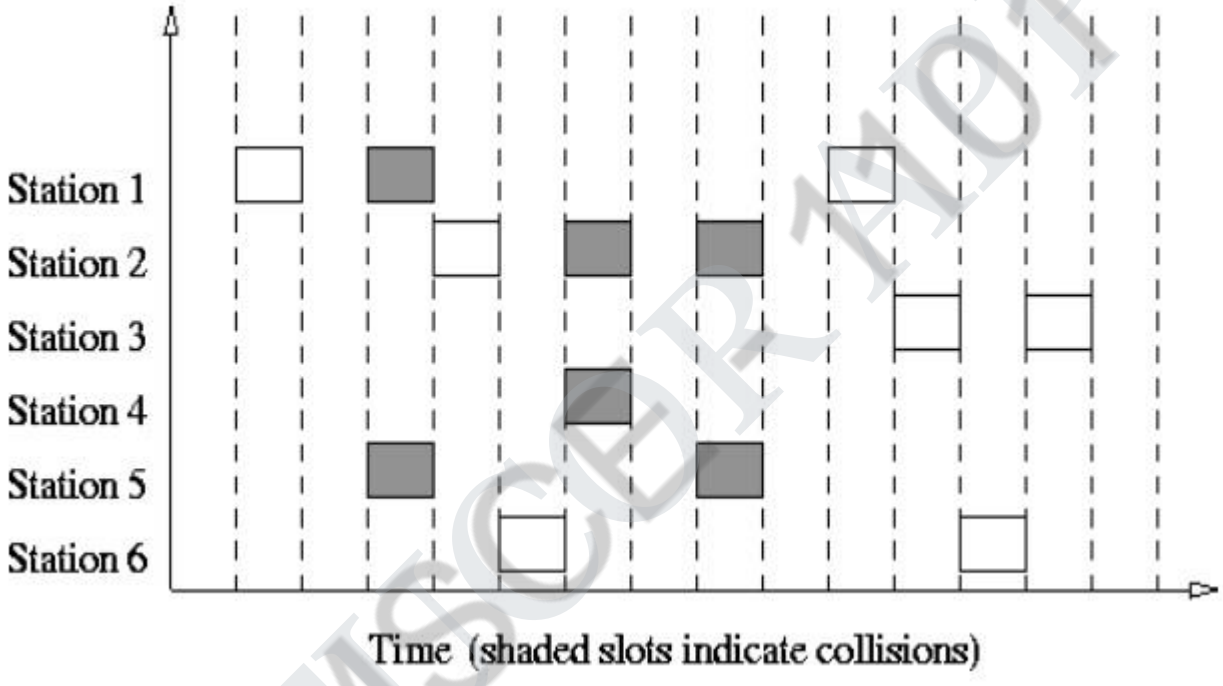
The first of the contention based protocols we evaluate is the Slotted Aloha protocol. The channel bandwidth is a continuous stream of slots whose length is the time necessary to transmit one packet. A station with a packet to send will transmit on the next available slot boundary. In the event of a collision, each station involved in the collision retransmits at some random time in order to reduce the possibility of recollision.

Obviously the limits imposed which govern the random retransmission of the packet will have an effect on the delay associated with successful packet delivery. If the limit is too short, the probability of recollision is high. If the limit is too long the probability of recollision lessens but there is unnecessary delay in the retransmission. For the Mars regional network studied here, the resending of the packet will occur at some random time not greater than the burst factor times the propagation delay.

Another important simulation characteristic of the Slotted Aloha protocol is the action which takes place on transmission of the packet. Methods include blocking (i.e. prohibiting packet generation) until verification of successful transmission occurs. This is known as "stop-and-wait". Another method known as "go-back-n" allows continual transmission of queued packets, but on the detection of a collision, will retransmit all packets from the point of the collision.

This is done to preserve the order of the packets. In this simulation model queued packets are continually sent and only the packets involved in a collision are retransmitted. This is called "selective-repeat" and allows out of order transmission of packets. By making a small restriction in the transmission freedom of the individual stations, the throughput of the Aloha protocol can be doubled.

Assuming constant length packets, transmission time is broken into slots equivalent to the transmission time of a single packet. Stations are only allowed to transmit at slot boundaries. When packets collide they will overlap completely instead of partially. This has the effect of doubling the efficiency of the Aloha protocol and has come to be known as Slotted Aloha.



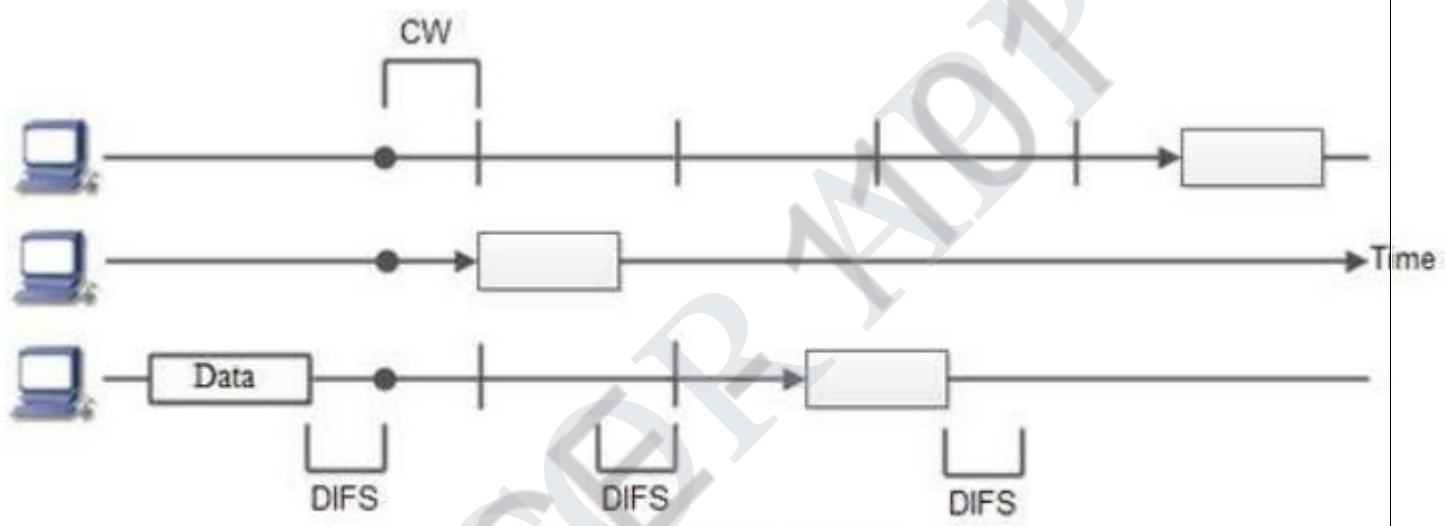
CSMA

CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.

In other words, a station that wants to communicate "listen" first on the media communication and awaits a "silence" of a preset time (called the Distributed Inter Frame Space or DIFS). After this compulsory period, the station starts a countdown for a random period considered. The maximum duration of this countdown is called the collision window

(Window Collision, CW). If no equipment speaks before the end of the countdown, the station simply deliver its package. However, if it is overtaken by another station, it stops immediately its countdown and waits for the next silence. She then continued his account countdown where it left off.

The waiting time random has the advantage of allowing a statistically equitable distribution of speaking time between the various network equipment, while making little unlikely (but not impossible) that both devices speak exactly the same time. The countdown system prevents a station waiting too long before issuing its package. It's a bit what place in a meeting room when no master session (and all the World's polite) expected a silence, then a few moments before speaking, to allow time for someone else to speak. The time is and randomly assigned, that is to say, more or less equally.



Sharing time with CSMA method.

Again, this is what we do naturally in a meeting room if many people speak exactly the same time, they are realizing account immediately (as they listen at the same time they speak), and they interrupt without completing their sentence. After a while, one of them speaks again. If a new collision occurs, the two are interrupted again and tend to wait a little longer before speaking again.

CSMA protocol was developed to overcome the problem found in ALOHA i.e. to minimize the chances of collision, so as to improve the performance. CSMA protocol is based on the principle of 'carrier sense'. The station senses the carrier or channel before transmitting a frame. It means the station checks the state of channel, whether it is idle or busy.

Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it.

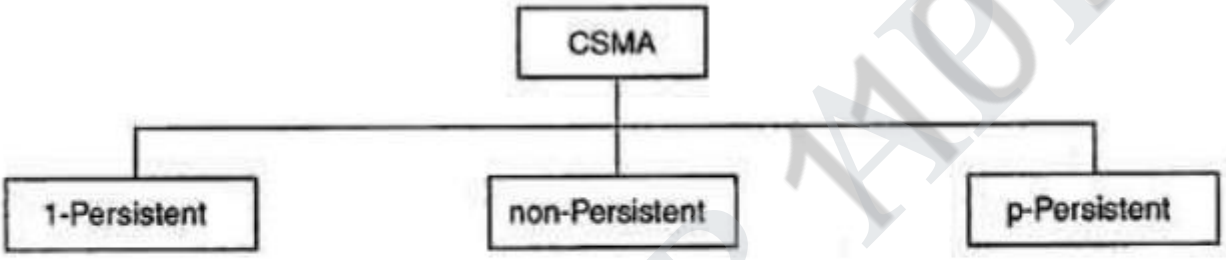
The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations. In the meantime, other stations may sense the channel to be idle and transmit their frames. This results in the collision.

There Are Three Different Type of CSMA Protocols

(I) I-persistent CSMA

(ii) Non- Persistent CSMA

(iii) p-persistent CSMA



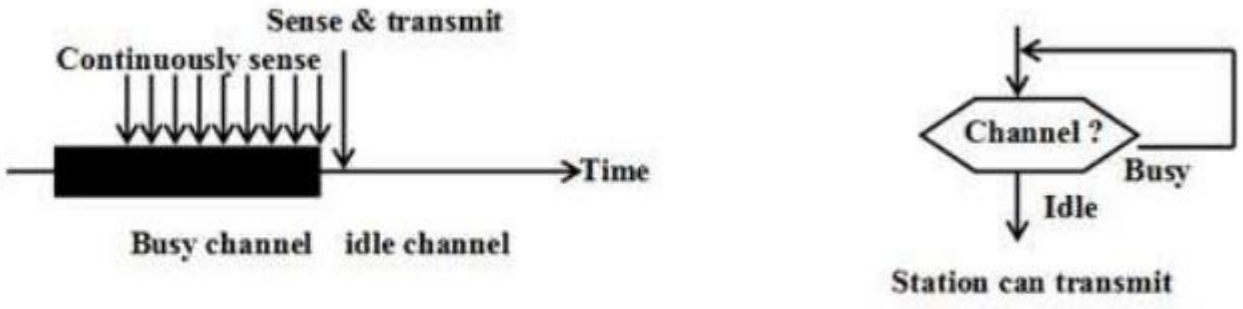
Types of CSMA

(i) I-persistent CSMA

In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy. If the channel is busy, the station waits until it becomes idle. When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called I-persistent CSMA. This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames. When the collision occurs, the stations wait a random amount of time and start all over again.

Drawback of I-persistent

The propagation delay time greatly affects this protocol. If after the station I begins its transmission, station 2 also became ready to send its data and senses the channel. If the station I signal has not yet reached station 2, station 2 will sense the channel to be idle and will begin its transmission. This will result in collision.



1-persistent CSMA

Even if propagation delay time is zero, collision will still occur. If two stations became .ready in the middle of third station's transmission, both stations will wait until the transmission of first station ends and then both will begin their transmission exactly simultaneously. This will also result in collision.

(ii) Non-persistent CSMA

In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time. After this time, it again checks the status of the channel and if the channel is free it will transmit. A station that has a frame to send senses the channel.

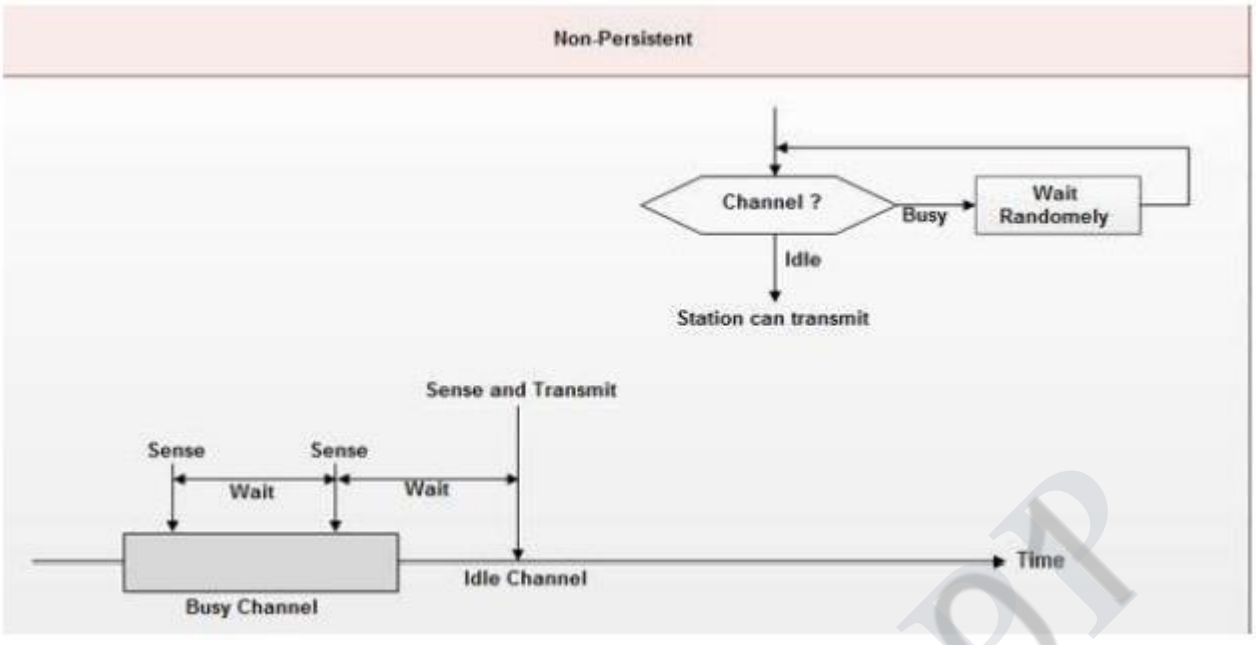
If the channel is idle, it sends immediately. If the channel is busy, it waits a random amount of time and then senses the channel again. In non-persistent CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

Advantage of non-persistent

It reduces the chance of collision because the stations wait a random amount of time. It is unlikely that two or more stations will wait for same amount of time and will retransmit at the same time.

Disadvantage of non-persistent

It reduces the efficiency of network because the channel remains idle when there may be stations with frames to send. This is due to the fact that the stations wait a random amount of time after the collision.



(iii) p-persistent CSMA

This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time. Whenever a station becomes ready to send, it senses the channel. If channel is busy, station waits until next slot. If channel is idle, it transmits with a probability p.

With the probability q=l-p, the station then waits for the beginning of the next time slot. If the next slot is also idle, it either transmits or waits again with probabilities p and q. This process is repeated till either frame has been transmitted or another station has begun transmitting. In case of the transmission by another station, the station acts as though collision

has occurred and it waits a random amount of time and starts again.

Advantage of p-persistent

• It reduces the chance of collision and improves the efficiency of the network.

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. Expand GSM, GPRS and UMTS.

GSM – Global System for Mobile Communication
GPRS – General Packet Radio Services
UMTS – Universal Mobile Telecommunication Systems

2. What is meant by GSM?

Global System for Mobile Communication (GSM) is a wide area wireless communications system that uses digital radio transmission to provide voice, data and multimedia communication services. A GSM system coordinates the communication between a mobile telephones (Mobile Stations), base stations (Cell Sites) and switching systems.

3. What is the important characteristic of GSM?

GSM provides data services in addition to voice services and it is compatible to 1G system.

4. What is the use of GSM in mobile telecommunication? Nov/Dec 2011&12 May/June 12

This system was soon named the Global System for Mobile communications (GSM), The primary goal of GSM was to provide a mobile phone system that allows users to roam and provides voice services compatible to ISDN and other PSTN systems

5. Specify the three different categories of services defined by GSM

- Bearer services
- Tele services
- Supplementary services

6. What is the use of emergency number?

Another service offered by GSM is the emergency number. This service is mandatory for all providers and free of charge. This connection also has the highest priority, possibly pre-empting other connections, and will automatically be set up with the closest emergency center.

7. List the important supplementary services offered by GSM.

- User Identification
- Call Forwarding (or Redirection)
- Automatic call-back
- Conferencing with up to 7 participants

8. What is meant by SMS and EMS?

- A useful service for very simple message transfer is the short message service(SMS), which offers transmission of messages of up to 160 characters
- The successor of SMS, the Enhanced Message Service (EMS), offers a larger message size (e.g., 760 characters, concatenating several SMs), formatted text, and the transmission of animated pictures

9. What are the sub systems available in GMS?

- Radio subsystem
- Network and switching subsystem
- Operation subsystem

10. What is RSS?

RSS stands for Radio Sub System. It comprises of all radio specific entities.

11. Name the entities of RSS.

1. Mobile Station (MS)
2. Base Station Subsystem (BSS)
3. Base Transceiver Station (BTS)
4. Base Station Controller (BSC)

12. Classify the functions of HLR and VLR.

Home Location Registers(HLR)	Visitor Location Registers(VLR)
HLR is a mobile operator database that includes details specific to each subscriber such as phone number, subscriber's IMSI, pre/postpaid, user's current location, billing details, phone status – parameters.	VLR is a temporary database that is updated whenever a new MS enters its area by roaming. The information is obtained from the corresponding HLR. i.e., VLR supports roaming functions for users outside the coverage area of their own HLR.
Basic Parameters stored in the HLR: • Subscriber ID (IMSI and MSISDN) • Current Locationo f the user • Supplementary Services Subscriber to (Caller Tone, Missed Call Alert, Any	The additional data stored in the VLR in telecom is listed below: 1. Location Area Identity (LAI). 2. Temporary Mobile Subscriber Identity (TMSI).

Other Services etc.) • Subscriber Status (Registered or Deregistered) • Authentication Key and AUC Functionality • Mobile Subscriber Roaming Number	3. Mobile Station Roaming Number (MSRN). 4. Mobile status (busy/free/no answer etc.).

13. List out the functions of OMC.

- Traffic Monitoring
- Subscribers
- Security Management
- Account Billing

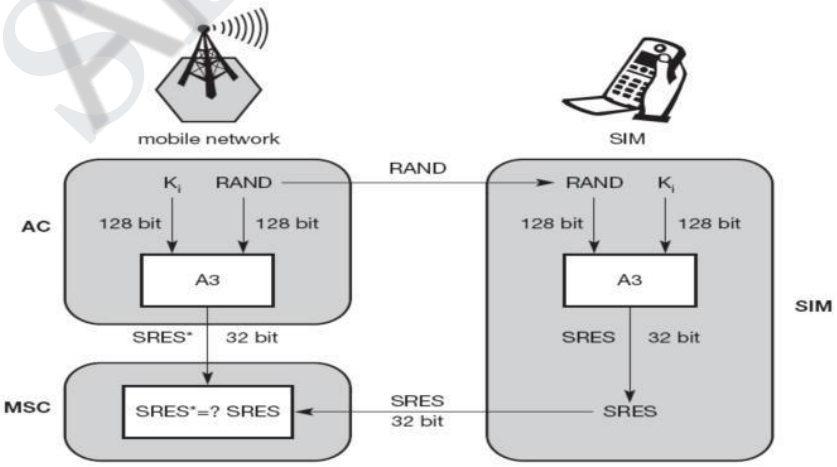
14. List the 3 important features of GSM Security. May/June 2016

1. **Authentication** – used to protect the network against unauthorized use.
2. **Confidentiality** – 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.
3. **Anonymity** – Anonymity is achieved by allocating Temporary Mobile Subscriber Identity (TMSI) instead of permanent identities to protect against tracking a user's location and obtaining information about a user's call log.

15. What are the characteristics of GSM?

1. Communication
2. Total Mobility
3. World Wide Connectivity
4. High Capacity
5. High Transmission Quality
6. Security Functions
7. SIM Card Bounded Service

16. Give the block diagram of GSM Authentication. May/June 2014



17. What is meant by GPRS? May/June 12

GPRS (General Packet Radio Services) is a packet-oriented mobile data service on the GSM of 3G and 2G cellular communication systems. It is a non-voice, high-speed and useful packet-switching technology for GSM networks.

18. List out the features of GPRS.

1. Speed
2. Immediacy
3. Packet Switched Resource Allocation (Spectrum Efficiency)
4. Flexible Channel Allocation
5. Traffic characteristics suitable for GPRS
6. Mobility
7. Localization

19. Explain in what ways is GPRS better than GSM?

GSM uses a billing system based on the time of connection whereas GPRS uses a billing system based on the amount of transmitted data.

20. What are the goals of GPRS?

1. Open Architecture
2. Consistent IP services
3. Same infrastructure for different air interfaces
4. Integrated telephony and Internet infrastructure
5. Service innovation independent of infrastructure

21. What are the services offered by GPRS?

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

1. Point-To-Point Service (PTP): It is between two users and can either be connectionless or connection-oriented.
2. Point-To-Multipoint Service (PTM): It is a data transfer service from one user to multiple users.

22. Point out the purpose of EIR in Mobile Computing.

Equipment Identity Register (EIR) is a database that used to track handsets using the IMEI. It helps to block calls from stolen, unauthorized, or defective mobiles.

23. What is the use of VOIP? May/June 2013

Voice over Internet protocol, a technology for making telephone calls over the Internet in which speech sounds are converted into binary.

24. What is meant by roaming?

In wireless telecommunications, roaming is a general term referring to the extension of connectivity service in a location that is different from the home location where the service was registered. Roaming ensures that the wireless device is kept connected to the network, without losing the connection

25. What is the function of GGSN? May/June 2014

- The gateway GPRS support node (GGSN) is the interworking unit between the GPRS network and external packet data networks (PDN). This node contains routing information for GPRS users, performs address conversion, and tunnels data to a user via encapsulation.
- The GGSN is connected to external networks (e.g., IP or X.25) via the Gi interface and transfers packets to the SGSN via an IP-based GPRS backbone network (Gn interface).

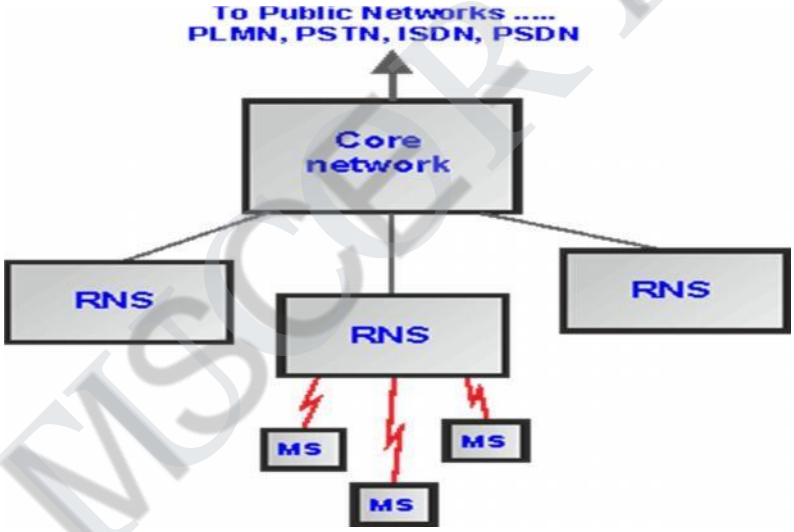
26. What is UMTS?

The Universal Mobile Telecommunications System (UMTS) is a 3G mobile communication system that provides a range of broadband services to wireless and mobile communications. The UMTS was developed mainly for countries with GSM networks.

27. What are the main elements of UMTS? May/June 2016

1. User Equipment / Mobile Station (MS): is the name by which a cell phone is referred to
2. Radio Network Subsystem (RNS): Equivalent of Base Station Subsystem (BSS) in GSM. It provides and manages the wireless interface for the overall network.
3. Core Network (CN): Equivalent of the Network Switching Subsystem (NSS) in GSM.

28. Draw Architecture of UMTS?



29. List out UMTS Problems.

- Require more battery power
- Can handoff UMTS to GSM but not GSM to UMTS
- Initial poor coverage
- More expensive than GSM

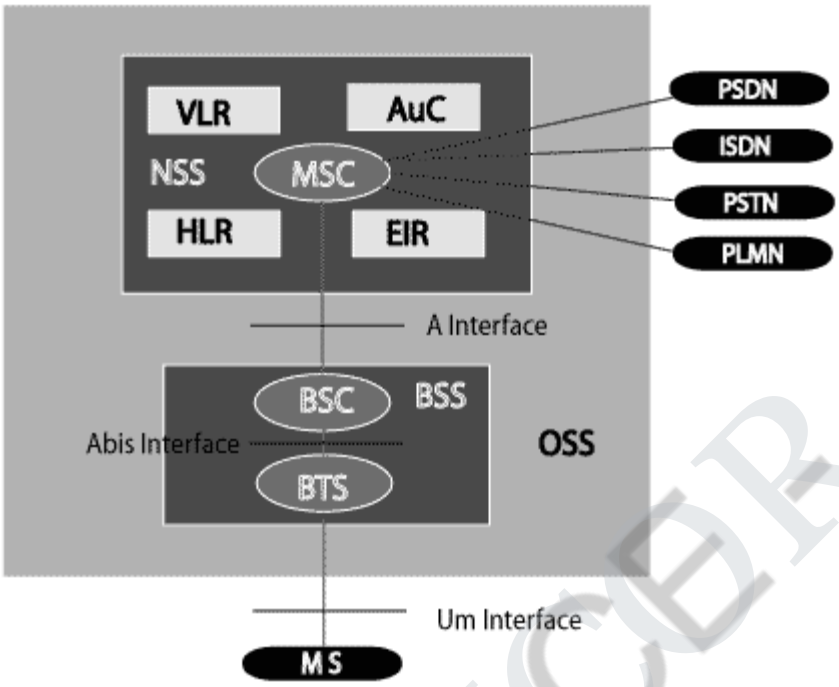
PART-B

1. Explain GSM architecture and its services with neat diagram. **[U] Nov/Dec2011&12, May/June 12, May /June 2013, Nov/Dec 2013, May/June 2014, Nov/Dec2014, May/June 2016**

A GSM network comprises of many functional units. These functions and interfaces are explained in this chapter. The GSM network can be broadly divided into:

- The Mobile Station (MS)
- The Base Station Subsystem (BSS)
- The Network Switching Subsystem (NSS)
- The Operation Support Subsystem (OSS)

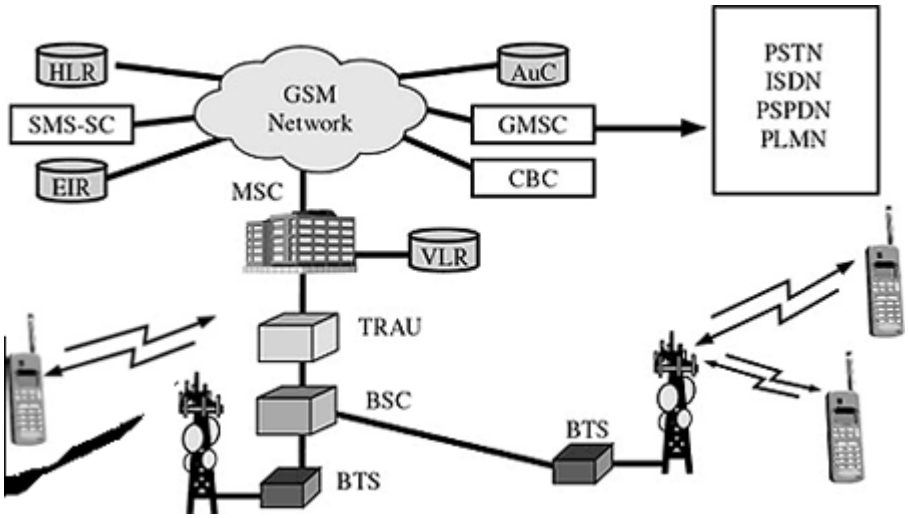
Given below is a simple pictorial view of the GSM architecture.



The additional components of the GSM architecture comprise of databases and messaging systems functions:

- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Equipment Identity Register (EIR)
- Authentication Center (AuC)
- SMS Serving Center (SMS SC)
- Gateway MSC (GMSC)
- Chargeback Center (CBC)
- Transcoder and Adaptation Unit (TRAU)

The following diagram shows the GSM network along with the added elements:



The MS and the BSS communicate across the Um interface. It is also known as the *air interface* or the *radio link*. The BSS communicates with the Network Service Switching (NSS) center across the *A* interface.

GSM network areas

In a GSM network, the following areas are defined:

- **Cell** : Cell is the basic service area; one BTS covers one cell. Each cell is given a Cell Global Identity (CGI), a number that uniquely identifies the cell.
- **Location Area** : A group of cells form a Location Area (LA). This is the area that is paged when a subscriber gets an incoming call. Each LA is assigned a Location Area Identity (LAI). Each LA is served by one or more BSCs.
- **MSC/VLR Service Area** : The area covered by one MSC is called the MSC/VLR service area.
- **PLMN** : The area covered by one network operator is called the Public Land Mobile Network (PLMN). A PLMN can contain one or more MSCs.

2. Explain security service in GSM. **[U] December 2012, Nov/Dec 2013**

GSM is the most secured cellular telecommunications system available today. GSM has its security methods standardized. GSM maintains end-to-end security by retaining the confidentiality of calls and anonymity of the GSM subscriber.

Temporary identification numbers are assigned to the subscriber's number to maintain the privacy of the user. The privacy of the communication is maintained by applying encryption algorithms and frequency hopping that can be enabled using digital systems and signalling.

This chapter gives an outline of the security measures implemented for GSM subscribers.

Mobile Station Authentication

The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit Random Number (RAND) is sent to the MS. The MS computes the 32-bit Signed Response (SRES) based on the encryption of the RAND with the authentication algorithm (A3) using the individual subscriber authentication key (Ki). Upon receiving the SRES from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.

The individual subscriber authentication key (Ki) is never transmitted over the radio channel, as it is present in the subscriber's SIM, as well as the AUC, HLR, and VLR databases. If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure is indicated to the MS.

The calculation of the signed response is processed within the SIM. It provides enhanced security, as confidential subscriber information such as the IMSI or the individual subscriber authentication key (Ki) is never released from the SIM during the authentication process.

Signalling and Data Confidentiality

The SIM contains the ciphering key generating algorithm (A8) that is used to produce the 64-bit ciphering key (Kc). This key is computed by applying the same random number (RAND) used in the authentication process to ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki).

GSM provides an additional level of security by having a way to change the ciphering key, making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required. As in case of the authentication process, the computation of the ciphering key (Kc) takes place internally within the SIM. Therefore, sensitive information such as the individual subscriber authentication key (Ki) is never revealed by the SIM.

Encrypted voice and data communications between the MS and the network is accomplished by using the ciphering algorithm A5. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the ciphering algorithm (A5) and the ciphering key (Kc).

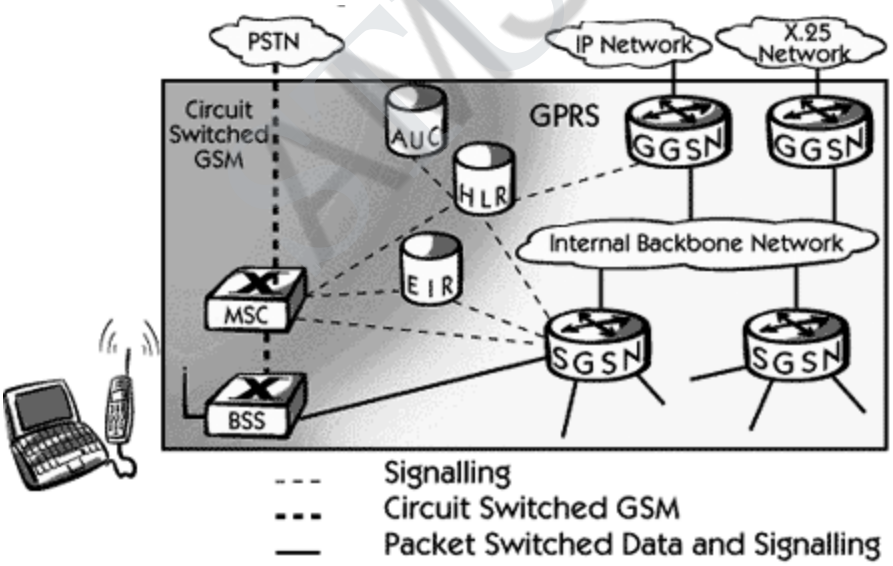
Subscriber Identity Confidentiality

To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity (TMSI) is used. Once the authentication and encryption procedures are done, the TMSI is sent to the mobile station. After the receipt, the mobile station responds. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) is necessary in addition to the TMSI.

3. Draw a neat diagram of GPRS and explain its protocol architecture and services. **[An] Nov/Dec 2011&12, May/June 12, May /June 2013, Nov/Dec 2013, May/June 2014, Nov/dec2014, May/June 2016**

GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.

Following is the GPRS Architecture diagram:



GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required.

Therefore, GPRS requires modifications to numerous GSM network elements as summarized below:

GSM Network Element	Modification or Upgrade Required for GPRS.
Mobile Station (MS)	New Mobile Station is required to access GPRS services. These new terminals will be backward compatible with GSM for voice calls.
BTS	A software upgrade is required in the existing Base Transceiver Station(BTS).
BSC	The Base Station Controller (BSC) requires a software upgrade and the installation of new hardware called the packet control unit (PCU). The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
GPRS Support Nodes (GSNs)	The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).
Databases (HLR, VLR, etc.)	All the databases involved in the network will require software upgrades to handle the new call models and functions introduced by GPRS.

GPRS Mobile Stations

New Mobile Stations (MS) are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data. A variety of MS can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers. These mobile stations are backward compatible for making voice calls using GSM.

GPRS Base Station Subsystem

Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade. The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber mobile, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call. However, at the output of the BSC, the traffic is separated; voice is sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

GPRS Support Nodes

Following two new components, called Gateway GPRS Support Nodes (GSNs) and, Serving GPRS Support Node (SGSN) are added:

Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node. The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

Serving GPRS Support Node (SGSN)

The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.

Internal Backbone

The internal backbone is an IP based network used to carry packets between different GSNs. Tunnelling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signalling from a GSN to a MSC, HLR or EIR is done using SS7.

Routing Area

GPRS introduces the concept of a Routing Area. This concept is similar to Location Area in GSM, except that it generally contains fewer cells. Because routing areas are smaller than location areas, less radio resources are used While broadcasting a page message.

4. Explain in detail about UMTS Architecture and its Services. [U] **May/June 2016**

The Universal Mobile Telecommunications System (UMTS), based on the GSM standards, is a mobile cellular system of third generation that is maintained by 3GPP (3rd Generation Partnership Project). It specifies a complete network system and the technology described in it is popularly referred as Freedom of Mobile Multimedia Access (FOMA). This tutorial starts off with a brief introduction to the history of mobile communication and cellular concepts and gradually moves on to explain the basics of GSM, GPRS, and EDGE, before getting into the concepts of UMTS.

UMTS - Radio Interface and Radio Network Aspects

After the introduction of UMTS the amount of wide area data transmission by mobile users had picked up. But for the local wireless transmissions such as WLAN and DSL, technology has increased at a much higher rate. Hence, it was important to consider the data transmission rates equal to the category of fixed line broadband, when WIMAX has already set high targets for transmission rates. It was clear that the new 3GPP radio technology Evolved UTRA (E-UTRA, synonymous with the LTE radio interface) had to become strongly competitive in all respect and for that following target transmission rates were defined −

- Downlink: 100 Mb/s
- Uplink: 50 Mb/s

Above numbers are only valid for a reference configuration of two antennas for reception and one transmit antenna in the terminal, and within a 20 MHz spectrum allocation.

UMTS – All IP Vision

A very general principle was set forth for the Evolved 3GPP system. It should “all IP”, means that the IP connectivity is the basic service which is provided to the users. All other layer services like voice, video, messaging, etc. are built on that.

Looking at the protocol stacks for interfaces between the network nodes, it is clear that simple model of IP is not applicable to a mobile network. There are virtual layers in between, which is not applicable to a mobile network. There are virtual layer in between, in the form of "tunnels", providing the three aspects - mobility, security, and quality of service. Resulting, IP based protocols appear both on the transport layer (between network nodes) and on higher layers.

UMTS – Requirements of the New Architecture

There is a new architecture that covers good scalability, separately for user plane and control plane. There is a need for different types of terminal mobility support that are: fixed, nomadic, and mobile terminals.

The minimum transmission and signaling overhead especially in air, in an idle mode of the dual mode UE signaling should be minimized, in the radio channel multicast capability. It is required to be reused or extended, as roaming and network sharing restrictions, compatible with traditional principles established roaming concept, quite naturally, the maximum transmission delay required is equivalent to the fixed network, specifically less than 5 milliseconds, set to control plane is less than 200 milliseconds delay target.

Looking at the evolution of the 3GPP system in full, it may not seem less complex than traditional 3GPP system, but this is due to the huge increase in functionality. Another strong desire is to arrive at a flat structure, reducing CAPEX/OPEX for operators in the 3GPP architecture carriers.

Powerful control functions should also be maintained with the new 3GPP systems, both real-time seamless operation (for example, VoIP) and non-real-time applications and services. The system should perform well for VoIP services in both the scenarios. Special attention is also paid to the seamless continuity with legacy systems (3GPP and 3GPP2), supports the visited network traffic local breakout of voice communications.

UMTS – Security and Privacy

Visitor Location Register (VLR) and SNB are used to keep track of all the mobile stations that are currently connected to the network. Each subscriber can be identified by its International Mobile Subscriber Identity (IMSI). To protect against profiling attacks, the permanent identifier is sent over the air interface as infrequently as possible. Instead, local identities Temporary Mobile Subscriber force (TMSI) is used to identify a subscriber whenever possible. Each UMTS subscriber has a dedicated home network with which it shares a secret key K_i long term.

The Home Location Register (HLR) keeps track of the current location of all the home network subscribers. Mutual authentication between a mobile station and a visited network is carried out with the support of the current GSN (SGSN) and the MSC / VLR, respectively. UMTS supports encryption of the radio interface and the integrity protection of signaling messages.

UNIT III

MOBILE AD-HOC NETWORKS

SYLLABUS: 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 meant by Ad-hoc network?**
   The term implies spontaneous or impromptu construction. An ad hoc network is a network that is composed of individual devices communicating with each other directly. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other.

2. **What are the basic principles of Ad-hoc networking?**
   - Mobile device communicate in peer-to-peer fashion
   - Self-organizing network without the need of fixed network infrastructure,,
   - Multi-hop communication,,
   - Decentralized, mobility-adaptive operation

3. **What are the needs of ad hoc networks?**
   - Ease of deployment
   - Speed of deployment
   - Decreased dependence on infrastructure

4. **What are the advantages of ad hoc networks?**
   The advantages of an ad hoc network include:
   1. Separation from central network administration.
   2. Self-configuring nodes are also routers.
   3. Self-healing through continuous re-configuration.
   4. Scalability incorporates the addition of more nodes.
   5. Mobility allows ad hoc networks created on the fly in any situation where there are multiple wireless devices.
   6. Flexible ad hoc can be temporarily setup at any time, in any place.
   7. Lower getting - started costs due to decentralized administration.
   8. The nodes in ad hoc network need not rely on any hardware and software. So, it can be connected and communicated quickly.

5. **What are the key challenges in ad hoc networks?**
   1. All network entities may be mobile ⇒ very dynamic topology
   2. Network functions must have high degree of adaptability (mobility, outage)
   3. No central entities ⇒ operation in completely distributed manner

.

6. Give the difference between cellular and ad-hoc networks.

S.No	Cellular Networks	Ad-hoc Networks
1	Infrastructure Networks	Infrastructure-less Networks
2	Fixed, pre-located cell sites and base stations	No base station and rapid deployment
3	Static backbone network topology	Highly dynamic network topologies
4	Relatively caring environment and stable connectivity	Hostile environment and irregular connectivity
5	Detailed planning before base station can be installed	Ad-hoc networks automatically forms and adapts to changes
6	High setup costs	Cost-effective
7	Large setup time	Less setup time

7. List out the characteristics of MANETs. May/June 2016

1) Lack of fixed infrastructure
2) Dynamic Topologies
3) Bandwidth constrained, variable capacity links
4) Energy Constrained Operation
5) Increased Vulnerability
6) Distributed peer-to-peer mode of operation
7) Multi-hop Routing
8) Autonomous Terminal
9) Lightweight Terminals
10) Shared Physical Medium

8. Analyze the operational constraints (challenges) associated with MANET.

1. Low Processing Capabilities & low bandwidth
2. Computational & Communication overhead
3. Mobility-induced route changes
4. Battery Constraints
5. Packet losses due to transmission errors
6. Security Threats
7. Dynamic Topology

9. What are the advantages of MANETs?

- They provide access to information and services regardless of geographic position.
- Independence from central network administration
- Self-configuring network, nodes are also act as routers. Less expensive as compared to wired network.
- Scalable—accommodates the addition of more nodes.
- Improved Flexibility.
- Robust due to decentralize administration.
- The network can be set up at any place and time.

10. What are the disadvantages of MANET?

1. Limited Resource
2. Limited Physical Security
3. Vulnerable to attacks. Lack of authorization facilitates
4. Variable network topology makes it hard to detect malicious nodes

5. Security protocols for wired network cannot work for adhoc network
6. Battery constraints
7. Frequent route changes leads to computational overhead

11. List out some of the applications of MANETs.

Some of the typical applications include:

1) Communication among portable computers
2) Environmental Monitoring
3) Sensor Networks
4) Military Sector
5) Personal Area Network and Bluetooth
6) Emergency Applications

12. Analyze and list out the various design issues associated with MANET.

1) Network Size and Node Density
2) Connectivity
3) Network Topology
4) User Traffic
5) Operational Environment
6) Energy Constraints

13. What is meant by routing in ad hoc networks?

"Routing is the process of finding the best path between the source and the destination for forwarding packets in any store-and-forward network. Routing is the mechanism of forwarding packet towards its destination using most efficient path. Efficiency of the path is measured in various metrics like, Number of hops, traffic, security, etc. In Ad-hoc network each host node acts as specialized router itself.

14. Compare Link State and Distance Vector Routing.

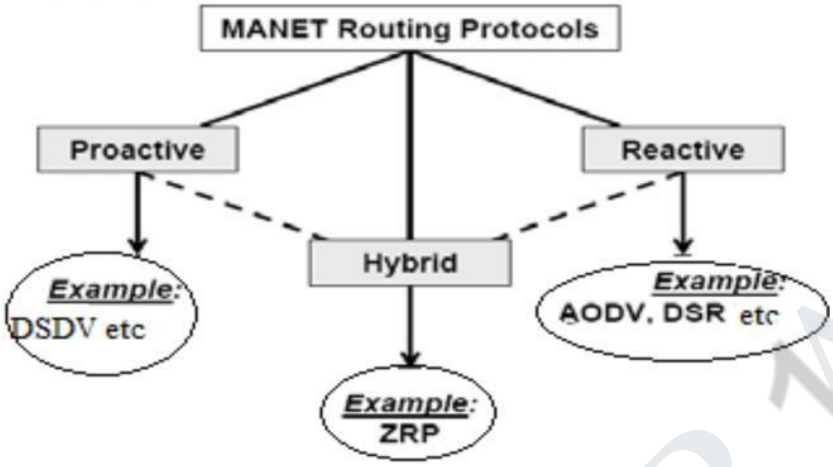
S.NO	Link Sate Routing	Distance Vector Routing
	It can be used in larger networks	It can be used in smaller networks
	It has unlimited number of hops	It has limited number of hops
	Convergence time is low	Convergence time is high
	Advertises only new changes	Periodically advertise updates
	Only advertise the updates and flood the advertisement	Advertises the entire routing tables to all its neighbors
	Metric used is cost	Metric used is hop count

15. Differentiate between MANET routing strategies with routing strategies of traditional networks.

S.NO	MANET routing strategies	Routing strategies of traditional networks
	In MANET, each node acts as a router	In traditional network, ordinary nodes do not participate in routing the packets.

	In MANET, the topology is dynamic because of the mobility of the nodes. Thus the routing table quickly becomes obsolete.	In traditional networks, the topology is static and the routing table is also constant during the data transmission.
	IP address encapsulated in the subnet structure does not work because of the node mobility	Simple IP-based addressing scheme is deployed in wired network.

16. Give the classification of MANET routing protocols.



17. List the types of communication in MANET.

- **Unicast:** Message is sent to a single destination node
- **Multicast:** Message is sent to a selected subset of network nodes
- **Broadcast:** Broadcasting is a special case of multicasting. Message is sent to all the nodes in the network.

18. What is meant by VANET?

A Vehicular Adhoc Network (VANET) is a special type of MANET in which moving automobiles form the nodes of the network. i.e., vehicles are connected to each other through an adhoc formation that forms a wireless network.

19. Mention the goals of VANET.

Improve traffic safety and comfort of driving
Minimize accidents, traffic intensity, locating vehicles
Up-to-date traffic information
Intersection collision warning
Weather information

20. What are the characteristics of VANETs?

1) High mobility of nodes
2) Rapidly changing network topology
3) Unbounded network size
4) Higher computational capacity
5) Time-sensitive data exchange
6) Potential support from infrastructure
7) Abundant Resources
8) Partitioned Network
9) Unlimited Transmission Power

21. Mention the uses of VANET.

1) A VANET can help drivers to get advance information and warnings from a nearby environment via message exchanges.
2) A VANET can help disseminate geographical information to the driver as he continues to drive.
3) Drivers may have the opportunity to engage in other task.

22. List out the applications of VANETs.

1) Safety oriented
a) Real-time traffic
b) Cooperative message transfer
c) Post-crash notification
d) Road hazard control notification
e) Traffic vigilance

2) Commercial oriented
a) remote vehicle personalization

b) internet access
c) digital map downloading
d) real time video relay
e) value-added advertisement

3) Convenience oriented
a) route diversion
b) electronic toll collection
c) parking availability

4) Productive Applications
a) Environmental Benefits
b) Time Utilization
c) Fuel Saving

23. Compare MANET Vs VANET. May/June 2016

S.No		VANET – Vehicular Adhoc Network	MANE – Mobile Adhoc Network
1	**Basic Idea**	It is a collection of nodes(vehicles) that communicate with each other over bandwidth constrained wireless links with certain road side infrastructure or base station	It is a collection nodes that communicate with each other over bandwidth constrained wireless links without any infrastructure support
2	**Production Cost**	Costly	Inexpensive
3	**Network Topology Change**	Frequent and very fast	Sluggish / Slow
4	**Mobility**	High	Low
5	**Density in Node**	Frequent variable and dense	Sparse
6	**Bandwidth**	1000 kbps	100 kbps
7	**Range**	Up to 600 m	Up to 100 m
8	**Node lifetime**	It is depend on vehicle life time	It is depend on power source
9	**Reliability**	High	Medium
10	**Nodes moving Pattern**	Regular	Random

PART – B

1. Explain the basic characteristics and applications of Mobile Ad hoc networks. [U]
May/June2016/ Nov/Dec 2014

It is an infrastructure-less IP based network of mobile and wireless machine nodes connected with radio. In operation, the nodes of a MANET do not have a centralized administration mechanism. It is known for its routable network properties where each node act as a "router" to forward the traffic to other specified nodes in the network.

Types of MANET

There are different types of MANETs including:

- InVANETs – Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.
- Vehicular ad hoc networks (VANETs) – Enables effective communication with another vehicle or helps to communicate with roadside equipment.
- Internet-Based Mobile Ad hoc Networks (iMANET) – helps to link fixed as well as mobile nodes.

Characteristics of MANET

- In MANET, each node act as both host and router. That is it is autonomous in behavior.
- Multi-hop radio relaying- When a source node and a destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
- Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
- The nodes can join or leave the network anytime, making the network topology dynamic in nature.
- Mobile nodes are characterized by less memory, power and lightweight 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.
- Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
- 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.

Manet Challenges

A Manet environment has to overcome certain issues of limitation and inefficiency. It includes:

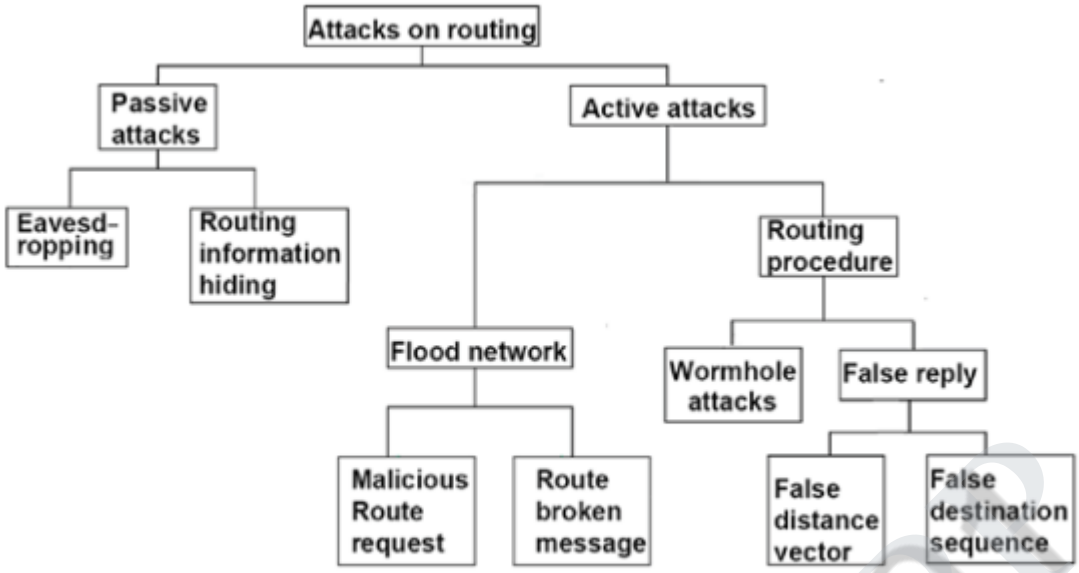
- The wireless link characteristics are time-varying in nature: There are transmission impediments like fading, path loss, blockage and interference that adds to the susceptible behavior of wireless channels. The reliability of wireless transmission is resisted by different factors.

- Limited range of wireless transmission – The limited radio band results in reduced data rates compared to the wireless networks. Hence optimal usage of bandwidth is necessary by keeping low overhead as possible.

- Packet losses due to errors in transmission – MANETs experience higher packet loss due to factors such as hidden terminals that results in collisions, wireless channel issues (high bit error rate (BER)), interference, frequent breakage in paths caused by mobility of nodes, increased collisions due to the presence of hidden terminals and uni-directional links.

- Route changes due to mobility- The dynamic nature of network topology results in frequent path breaks.

- Frequent network partitions- The random movement of nodes often leads to the partition of the network. This mostly affects the intermediate nodes.



2. Explain the various routing strategies in mobile ad-hoc networks. [U]

In Table-driven routing protocols each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables so as to maintain a consistent and up-to-date view of the network. When the network topology changes the nodes propagate update messages throughout the network in order to maintain a consistent and up-to-date routing information about the whole network. These routing protocols differ in the method by which the topology change information is distributed across the network and the number of necessary routing-related tables. The following sections discuss some of the existing table-driven ad hoc routing protocols.

2.1 Dynamic Destination-Sequenced Distance-Vector Routing Protocol

The Destination-Sequenced Distance-Vector (DSDV) Routing Algorithm is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements.

Every mobile station maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node. The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time-driven and event-driven. The routing table updates can be sent in two ways:- a "full dump" or an incremental update. A full dump sends the full routing table to the neighbors and could span many packets whereas in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet. If there is space in the incremental update packet then those entries may be included whose sequence number has changed. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent. In a fast-changing network, incremental packets can grow big so full dumps will be more frequent. Each route update packet, in addition to the routing table information, also contains a unique sequence number assigned by the transmitter. The route labeled with the highest (i.e. most recent) sequence number is used. If two routes have the same sequence number then the route with the best metric (i.e. shortest route) is used. Based on the past history, the stations estimate the settling time of routes. The stations delay the transmission of a routing update by settling time so as to eliminate those updates that would occur if a better route were found very soon.

2.2 The Wireless Routing Protocol (WRP)

The Wireless Routing Protocol (WRP) is a table-based distance-vector routing protocol. Each node in the network

maintains a Distance table, a Routing table, a Link-Cost table and a Message Retransmission list.

The Distance table of a node x contains the distance of each destination node y via each neighbor z of x. It also contains the downstream neighbor of z through which this path is realized. The Routing table of node x contains the distance of each destination node y from node x, the predecessor and the successor of node x on this path. It also contains a tag to identify if the entry is a simple path, a loop or invalid. Storing predecessor and successor in the table is beneficial in detecting loops and avoiding counting-to-infinity problems. The Link-Cost table contains cost of link to each neighbor of the node and the number of timeouts since an error-free message was received from that neighbor. The Message Retransmission list (MRL) contains information to let a node know which of its neighbor has not acknowledged its update message and to retransmit update message to that neighbor.

Node exchange routing tables with their neighbors using update messages periodically as well as on link changes. The nodes present on the response list of update message (formed using MRL) are required to acknowledge the receipt of update message. If there is no change in routing table since last update, the node is required to send an idle Hello message to ensure connectivity. On receiving an update message, the node modifies its distance table and looks for better paths using new information. Any new path so found is relayed back to the original nodes so that they can update their tables. The node also updates its routing table if the new path is better than the existing path. On receiving an ACK, the mode updates its MRL. A unique feature of this algorithm is that it checks the consistency of all its neighbors every time it detects a change in link of any of its neighbors. Consistency check in this manner helps eliminate looping situations in a better way and also has fast convergence.

2.3 Global State Routing

Global State Routing (GSR) is similar to DSDV described in section 2.1. It takes the idea of link state routing but improves it by avoiding flooding of routing messages.

In this algorithm, each node maintains a Neighbor list, a Topology table, a Next Hop table and a Distance table. Neighbor list of a node contains the list of its neighbors (here all nodes that can be heard by a node are assumed to be its neighbors.). For each destination node, the Topology table contains the link state information as reported by the destination and the timestamp of the information. For each destination, the Next Hop table contains the next hop to which the packets for this destination must be forwarded. The Distance table contains the shortest distance to each destination node.

The routing messages are generated on a link change as in link state protocols. On receiving a routing message, the node updates its Topology table if the sequence number of the message is newer than the sequence number stored in the table. After this the node reconstructs its routing table and broadcasts the information to its neighbors.

2.4 Fisheye State Routing

Fisheye State Routing (FSR) is an improvement of GSR. The large size of update messages in GSR wastes a considerable amount of network bandwidth. In FSR, each update message does not contain information about all nodes. Instead, it exchanges information about closer nodes more frequently than it does about farther nodes thus reducing the update message size. So each node gets accurate information about neighbors and the detail and accuracy of information decreases as the distance from node increases. Figure 1 defines the scope of fisheye for the center (red) node. The scope is defined in terms of the nodes that can be reached in a certain number of hops. The center node has most accurate information about all nodes in the white circle and so on. Even though a node does not have accurate information about distant nodes, the packets are routed correctly because the route information becomes more and more accurate as the packet moves closer to the destination. FSR scales well to large networks as the overhead is controlled in this scheme.

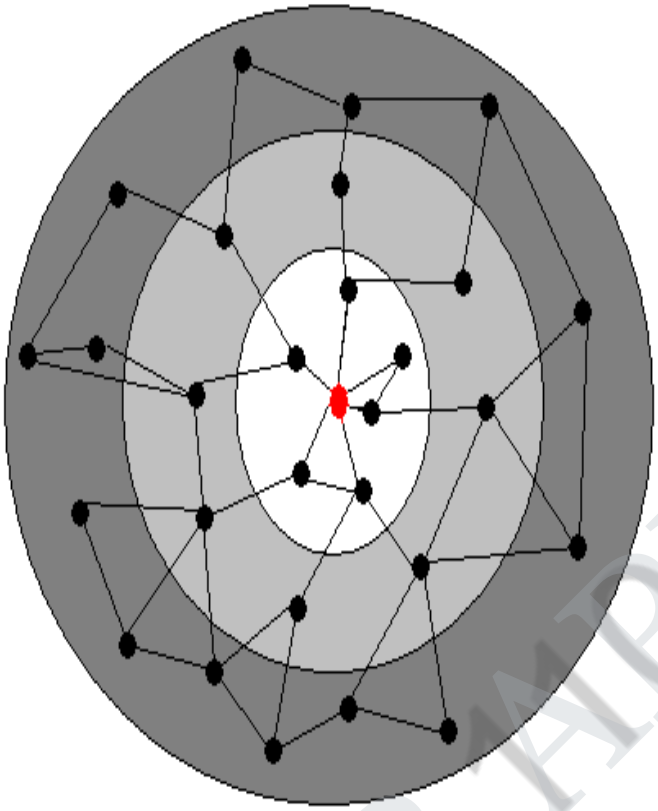


Figure 1. Accuracy of information in FSR

2.5 Hierarchical State Routing

The characteristic feature of Hierarchical State Routing (HSR) is multilevel clustering and logical partitioning of mobile nodes. The network is partitioned into clusters and a cluster-head elected as in a cluster-based algorithm. In HSR, the cluster-heads again organize themselves into clusters and so on. The nodes of a physical cluster broadcast their link information to each other. The cluster-head summarizes its cluster's information and sends it to neighboring cluster-heads via gateway (section 2.2). As shown in the figure 2, these cluster-heads are member of the cluster on a level higher and they exchange their link information as well as the summarized lower-level information among each other and so on. A node at each level floods to its lower level the information that it obtains after the algorithm has run at that level. So the lower level has a hierarchical topology information. Each node has a hierarchical address. One way to assign hierarchical address is the cluster numbers on the way from root to the node as shown in figure 2. A gateway can be reached from the root via more than one path, so gateway can have more than one hierarchical address. A hierarchical address is enough to ensure delivery from anywhere in the network to the host.

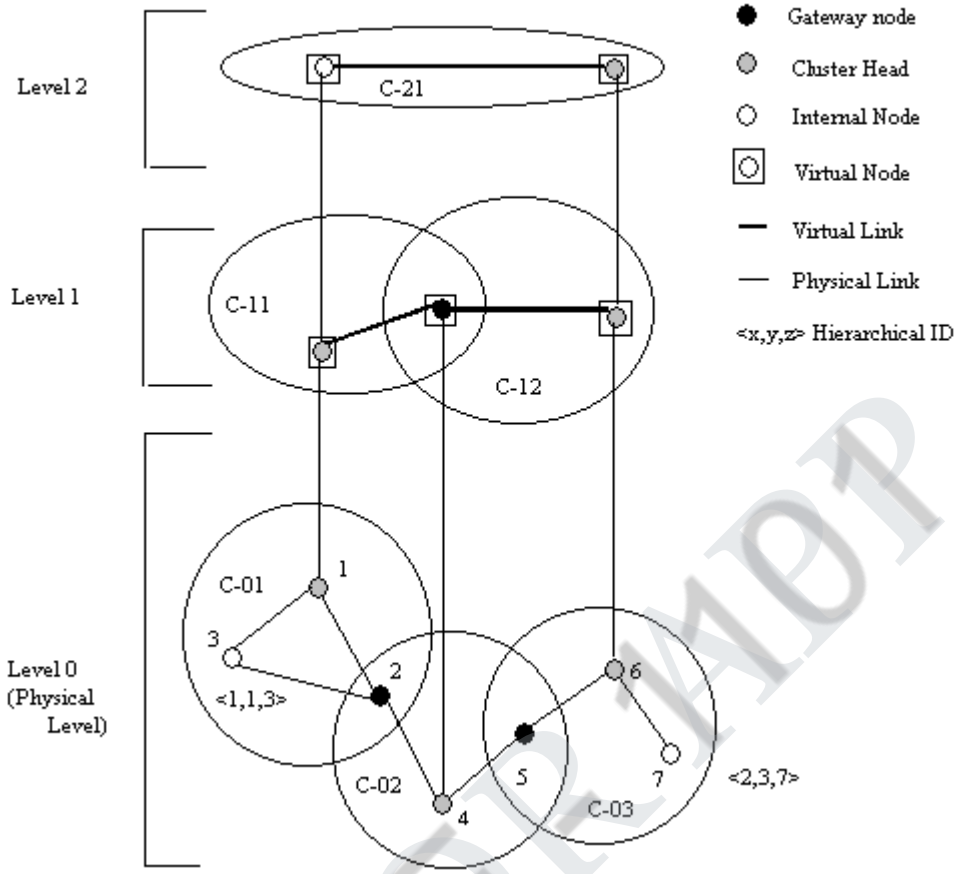


Figure 2. An example of clustering in HSR

In addition, nodes are also partitioned into logical subnetworks and each node is assigned a logical address <subnet, host>. Each subnetwork has a location management server (LMS). All the nodes of that subnet register their logical address with the LMS. The LMS advertise their hierarchical address to the top levels and the information is sent down to all LMS too. The transport layer sends a packet to the network layer with the logical address of the destination. The network layer finds the hierarchical address of the hierarchical address of the destinationÆs LMS from its LMS and then sends the packet to it. The destinationÆs LMS forwards the packet to the destination. Once the source and destination know each otherÆs hierarchical addresses, they can bypass the LMS and communicate directly. Since logical address/hierarchical address is used for routing, it is adaptable to network changes.

2.6 Zone-based Hierarchical Link State Routing Protocol

In Zone-based Hierarchical Link State Routing Protocol (ZHLS, the network is divided into non-overlapping zones. Unlike other hierarchical protocols, there is no zone-head. ZHLS defines two levels of topologies - node level and zone level. A node level topology tells how nodes of a zone are connected to each other physically. A virtual link between two zones exists if at least one node of a zone is physically connected to some node of the other zone. Zone level topology tells how zones are connected together. There are two types of Link State Packets (LSP) as well - node LSP and zone LSP. A node LSP of a node contains its neighbor node information and is propagated with the zone where as a zone LSP contains the zone information and is propagated globally. So each node has full node connectivity knowledge about the nodes in its zone and only zone connectivity information about other zones in the network. So given the zone id and the node id of a destination, the packet is routed based on the zone id till it reaches the correct zone. Then in that zone, it is routed based on node id. A <zone id, node id@gt; of the destination is sufficient for routing so it is adaptable to changing topologies.

2.7 Clusterhead Gateway Switch Routing Protocol

Clusterhead Gateway Switch Routing (CGSR) uses as basis the DSDV Routing algorithm described in the previous section.

The mobile nodes are aggregated into clusters and a cluster-head is elected. All nodes that are in the communication range of the cluster-head belong to its cluster. A gateway node is a node that is in the communication range of two or more cluster-heads. In a dynamic network cluster head scheme can cause performance degradation due to frequent cluster-head elections, so CGSR uses a Least Cluster Change (LCC) algorithm. In LCC, cluster-head change occurs only if a change in network causes two cluster-heads to come into one cluster or one of the nodes moves out of the range of all the cluster-heads.

The general algorithm works in the following manner. The source of the packet transmits the packet to its cluster-head. From this cluster-head, the packet is sent to the gateway node that connects this cluster-head and the next cluster-head along the route to the destination. The gateway sends it to that cluster-head and so on till the destination cluster-head is reached in this way. The destination cluster-head then transmits the packet to the destination. Figure 3 shows an example of CGSR routing scheme.

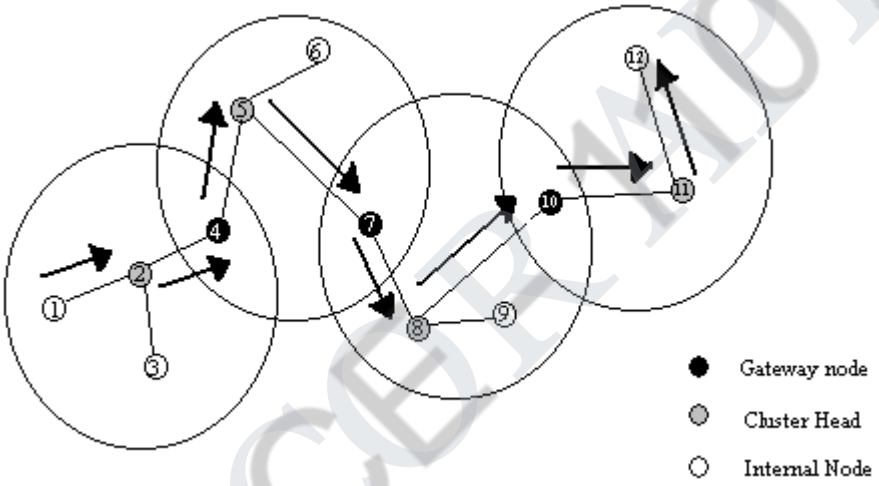


Figure 3. Example of CGSR routing from node 1 to node 12

Each node maintains a cluster member table that has mapping from each node to its respective cluster-head. Each node broadcasts its cluster member table periodically and updates its table after receiving other nodeÆs broadcasts using the DSDV algorithm. In addition, each node also maintains a routing table that determines the next hop to reach the destination cluster.

On receiving a packet, a node finds the nearest cluster-head along the route to the destination according to the cluster member table and the routing table. Then it consults its routing table to find the next hop in order to reach the cluster-head selected in step one and transmits the packet to that node.

---

3. On-Demand Routing Protocols

These protocols take a lazy approach to routing. In contrast to table-driven routing protocols all up-to-date routes are not maintained at every node, instead the routes are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. The route remains valid till the destination is reachable or until the route is no longer needed. This section discusses a few on-demand routing protocols.

3.1 Cluster based Routing Protocols

In Cluster Based Routing protocol (CBRP) , the nodes are divided into clusters. To form the cluster the following algorithm is used. When a node comes up, it enters the "undecided" state, starts a timer and broadcasts a Hello message.

When a cluster-head gets this hello message it responds with a triggered hello message immediately. When the undecided node gets this message it sets its state to "member". If the undecided node times out, then it makes itself the cluster-head if it has bi-directional link to some neighbor otherwise it remains in undecided state and repeats the procedure again. Cluster heads are changed as infrequently as possible.

Each node maintains a neighbor table. For each neighbor, the neighbor table of a node contains the status of the link (uni- or bi-directional) and the state of the neighbor (cluster-head or member). A cluster-head keeps information about the members of its cluster and also maintains a cluster adjacency table that contains information about the neighboring clusters. For each neighbor cluster, the table has entry that contains the gateway through which the cluster can be reached and the cluster-head of the cluster.

When a source has to send data to destination, it floods route request packets (but only to the neighboring cluster-heads). On receiving the request a cluster-head checks to see if the destination is in its cluster. If yes, then it sends the request directly to the destination else it sends it to all its adjacent cluster-heads. The cluster-heads address is recorded in the packet so a cluster-head discards a request packet that it has already seen. When the destination receives the request packet, it replies back with the route that had been recorded in the request packet. If the source does not receive a reply within a time period, it backs off exponentially before trying to send route request again.

In CBRP, routing is done using source routing. It also uses route shortening that is on receiving a source route packet, the node tries to find the farthest node in the route that is its neighbor (this could have happened due to a topology change) and sends the packet to that node thus reducing the route. While forwarding the packet if a node detects a broken link it sends back an error message to the source and then uses local repair mechanism. In local repair mechanism, when a node finds the next hop is unreachable, it checks to see if the next hop can be reached through any of its neighbor or if hop after next hop can be reached through any other neighbor. If any of the two works, the packet can be sent out over the repaired path.

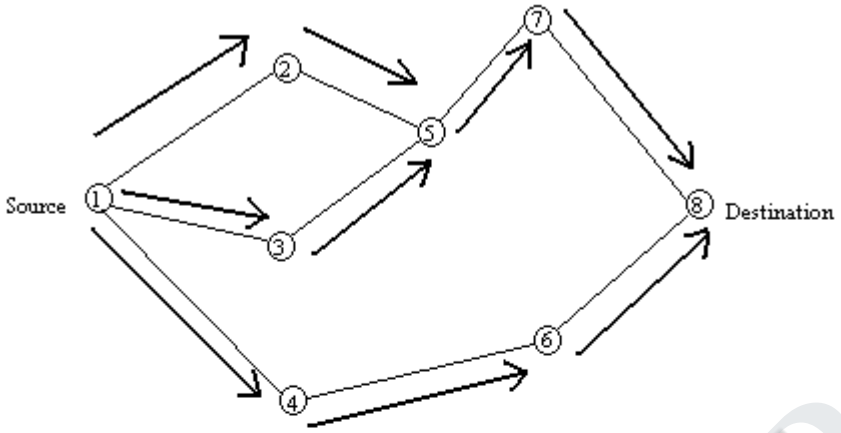
3.2 Ad hoc On-demand Distance Vector Routing

Ad hoc On-demand Distance Vector Routing (AODV) is an improvement on the DSDV algorithm discussed in section 2.1. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes.

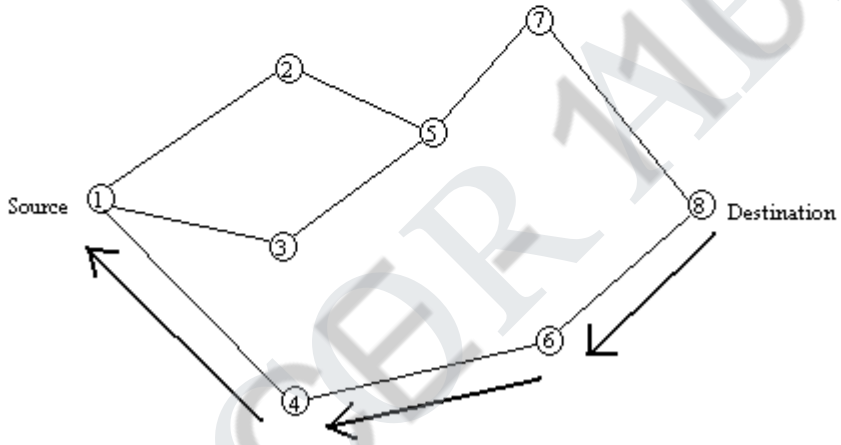
To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has a recent route information about the destination or till it reaches the destination (Figure 4a). A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only.

When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. As the route reply packet traverses back to the source (Figure 4b), the nodes along the path enter the forward route into their tables.

If the source moves then it can reinitiate route discovery to the destination. If one of the intermediate nodes move then the moved nodes neighbor realizes the link failure and sends a link failure notification to its upstream neighbors and so on till it reaches the source upon which the source can reinitiate route discovery if needed.



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

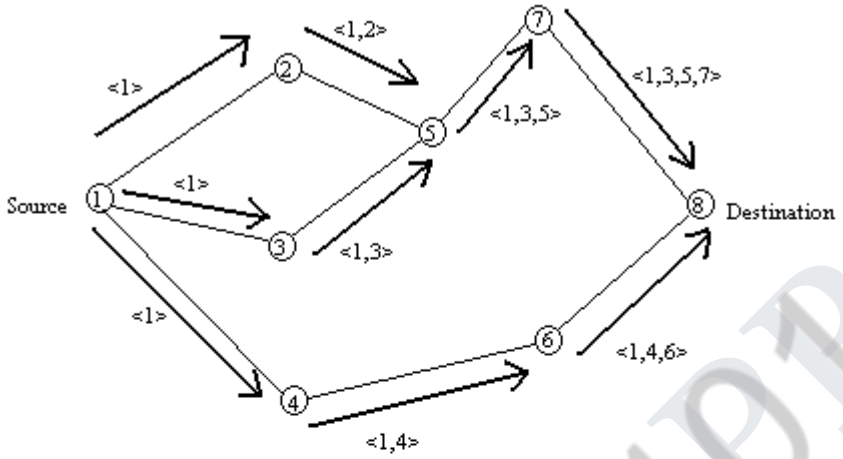
Figure 4. Route discovery in AODV

3.3 Dynamic Source Routing Protocol

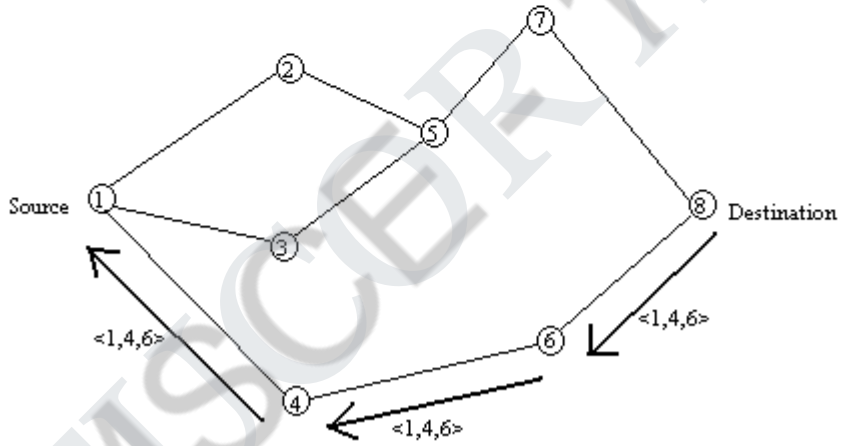
The Dynamic Source Routing Protocol is a source-routed on-demand routing protocol. A node maintains route caches containing the source routes that it is aware of. The node updates entries in the route cache as and when it learns about new routes.

The two major phases of the protocol are: route discovery and route maintenance. When the source node wants to send a packet to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the packet. But if the node does not have such a route, then it initiates the route discovery process by broadcasting a route request packet. The route request packet contains the address of the source and the destination, and a unique identification number. Each intermediate node checks whether it knows of a route to the destination. If it does not, it appends its address to the route record of the packet and forwards the packet to its neighbors. To limit the number of route requests propagated, a node processes the route request packet only if it has not already seen the packet and it's address is not present in the route record of the packet.

A route reply is generated when either the destination or an intermediate node with current information about the destination receives the route request packet . A route request packet reaching such a node already contains, in its route record, the sequence of hops taken from the source to this node.



(a) Building Record Route during Route Discovery



(b) Propogation of Route Reply with the Route Record

Figure 5. Creation of record route in DSRP

As the route request packet propagates through the network, the route record is formed as shown in figure 5a. If the route reply is generated by the destination then it places the route record from route request packet into the route reply packet. On the other hand, if the node generating the route reply is an intermediate node then it appends its cached route to destination to the route record of route request packet and puts that into the route reply packet. Figure 5b shows the route reply packet being sent by the destination itself. To send the route reply packet, the responding node must have a route to the source. If it has a route to the source in its route cache, it can use that route. The reverse of route record can be used if symmetric links are supported. In case symmetric links are not supported, the node can initiate route discovery to source and piggyback the route reply on this new route request.

DSRP uses two types of packets for route maintenance:- Route Error packet and Acknowledgements. When a node encounters a fatal transmission problem at its data link layer, it generates a Route Error packet. When a node receives a route error packet, it removes the hop in error from its route cache. All routes that contain the hop in error are are

truncated at that point. Acknowledgment packets are used to verify the correct operation of the route links. This also includes passive acknowledgments in which a node hears the next hop forwarding the packet along the route.

3.4 Temporally Ordered Routing Algorithm

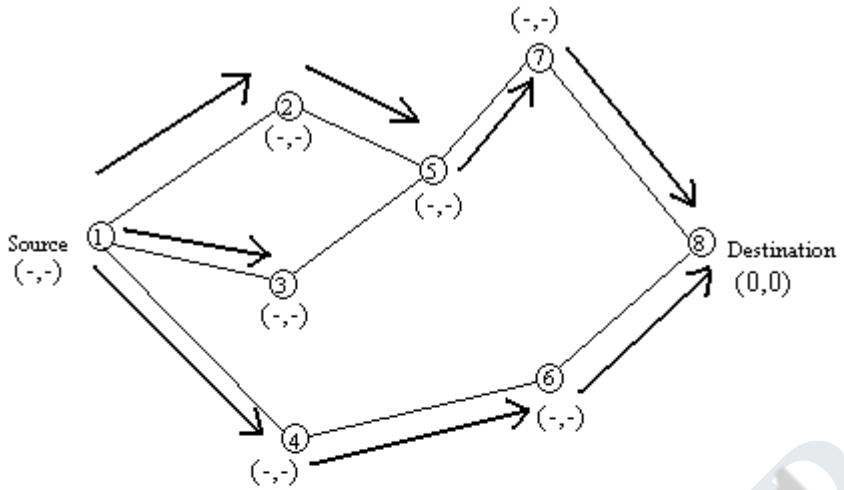
The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive, efficient and scalable distributed routing algorithm based on the concept of link reversal . TORA is proposed for highly dynamic mobile, multihop wireless networks. It is a source-initiated on-demand routing protocol. It finds multiple routes from a source node to a destination node. The main feature of TORA is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. To achieve this, the nodes maintain routing information about adjacent nodes. The protocol has three basic functions: Route creation, Route maintenance, and Route erasure.

Each node has a quintuple associated with it -

- Logical time of a link failure
- The unique ID of the node that defined the new reference level
- A reflection indicator bit
- A propagation ordering parameter
- The unique ID of the node

The first three elements collectively represent the reference level. A new reference level is defined each time a node loses its last downstream link due to a link failure. The last two values define a delta with respect to the reference level.

Route Creation is done using QRY and UPD packets. The route creation algorithm starts with the height (propagation ordering parameter in the quintuple) of destination set to 0 and all other node's height set to NULL (i.e. undefined). The source broadcasts a QRY packet with the destination node's id in it. A node with a non-NULL height responds with a UPD packet that has its height in it. A node receiving a UPD packet sets its height to one more than that of the node that generated the UPD. A node with higher height is considered upstream and a node with lower height downstream. In this way a directed acyclic graph is constructed from source to the destination. Figure 6 illustrates a route creation process in TORA. As shown in figure 6a, node 5 does not propagate QRY from node 3 as it has already seen and propagated QRY message from node 2. In figure 6b, the source (i.e. node 1) may have received a UPD each from node 2 or node 3 but since node 4 gives it lesser height, it retains that height.



(a) Propogation of QRY message through the network

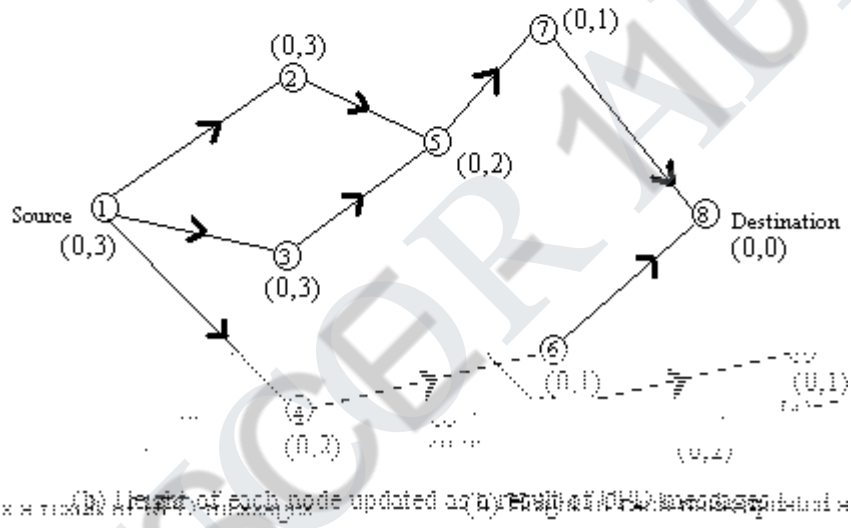


Figure 6. Route creation in TORA. (Numbers in braces are reference level, height of each node)

When a node moves the DAG route is broken, and route maintenance is needed to reestablish a DAG for the same destination. When the last downstream link of a node fails, it generates a new reference level. This results in the propagation of that reference level by neighboring nodes as shown in figure 7. Links are reversed to reflect the change in adapting to the new reference level. This has the same effect as reversing the direction of one or more links when a node has no downstream links.

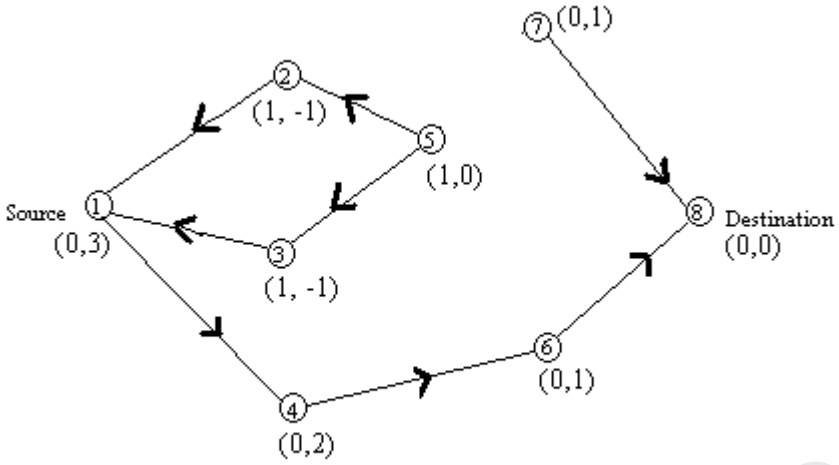


Figure 6. Re-establishing route on failure of link 5-7. The new reference level is node 5.

In the route erasure phase, TORA floods a broadcast clear packet (CLR) throughout the network to erase invalid routes.

In TORA there is a potential for oscillations to occur, especially when multiple sets of coordinating nodes are concurrently detecting partitions, erasing routes, and building new routes based on each other. Because TORA uses internodal coordination, its instability problem is similar to the "count-to-infinity" problem in distance-vector routing protocols, except that such oscillations are temporary and route convergence will ultimately occur.

3.5 Associativity Based Routing

The Associativity Based Routing (ABR) protocol is a new approach for routing proposed in ABR defines a new metric for routing known as the degree of association stability. It is free from loops, deadlock, and packet duplicates. In ABR, a route is selected based on associativity states of nodes. The routes thus selected are liked to be long-lived. All node generate periodic beacons to signify its existence. When a neighbor node receives a beacon, it updates its associativity tables. For every beacon received, a node increments its associativity tick with respect to the node from which it received the beacon. Association stability means connection stability of one node with respect to another node over time and space. A high value of associativity tick with respect to a node indicates a low state of node mobility, while a low value of associativity tick may indicate a high state of node mobility. Associativity ticks are reset when the neighbors of a node or the node itself move out of proximity. The fundamental objective of ABR is to find longer-lived routes for ad hoc mobile networks. The three phases of ABR are Route discovery, Route reconstruction (RRC) and Route deletion.

The route discovery phase is a broadcast query and await-reply (BQ-REPLY) cycle. The source node broadcasts a BQ message in search of nodes that have a route to the destination. A node does not forward a BQ request more than once. On receiving a BQ message, an intermediate node appends its address and its associativity ticks to the query packet. The next succeeding node erases its upstream node neighbors' associativity tick entries and retains only the entry concerned with itself and its upstream node. Each packet arriving at the destination will contain the associativity ticks of the nodes along the route from source to the destination. The destination can now select the best route by examining the associativity ticks along each of the paths. If multiple paths have the same overall degree of association stability, the route with the minimum number of hops is selected. Once a path has been chosen, the destination sends a REPLY packet back to the source along this path. The nodes on the path that the REPLY packet follows mark their routes as valid. All other routes remain inactive, thus avoiding the chance of duplicate packets arriving at the destination.

RRC phase consists of partial route discovery, invalid route erasure, valid route updates, and new route discovery, depending on which node(s) along the route move. Source node movement results in a new BQ-REPLY process because the routing protocol is source-initiated. The route notification (RN) message is used to erase the route entries associated with downstream nodes. When the destination moves, the destination's immediate upstream node erases its route. A localized query (LQ [H]) process, where H refers to the hop count from the upstream node to the destination, is initiated

to determine if the node is still reachable. If the destination receives the LQ packet, it selects the best partial route and REPLYs; otherwise, the initiating node times out and backtracks to the next upstream node. An RN message is sent to the next upstream node to erase the invalid route and inform this node that it should invoke the LQ [H] process. If this process results in backtracking more than halfway to the source, the LQ process is discontinued and the source initiates a new BQ process.

When a discovered route is no longer needed, the source node initiates a route delete (RD) broadcast. All nodes along the route delete the route entry from their routing tables. The RD message is propagated by a full broadcast, as opposed to a directed broadcast, because the source node may not be aware of any route node changes that occurred during RRCs.

3.6 Signal Stability Routing

Signal Stability-Based Adaptive Routing protocol (SSR) presented in is an on-demand routing protocol that selects routes based on the signal strength between nodes and a node's location stability. This route selection criterion has the effect of choosing routes that have "stronger" connectivity. SSR comprises of two cooperative protocols: the Dynamic Routing Protocol (DRP) and the Static Routing Protocol (SRP).

The DRP maintains the Signal Stability Table (SST) and Routing Table (RT). The SST stores the signal strength of neighboring nodes obtained by periodic beacons from the link layer of each neighboring node. Signal strength is either recorded as a strong or weak channel. All transmissions are received by DRP and processed. After updating the appropriate table entries, the DRP passes the packet to the SRP.

The SRP passes the packet up the stack if it is the intended receiver. If not, it looks up the destination in the RT and forwards the packet. If there is no entry for the destination in the RT, it initiates a route-search process to find a route. Route-request packets are forwarded to the next hop only if they are received over strong channels and have not been previously processed (to avoid looping). The destination chooses the first arriving route-search packet to send back as it is highly likely that the packet arrived over the shortest and/or least congested path. The DRP reverses the selected route and sends a route-reply message back to the initiator of route-request. The DRP of the nodes along the path update their RTs accordingly.

Route-search packets arriving at the destination have necessarily arrived on the path of strongest signal stability because the packets arriving over a weak channel are dropped at intermediate nodes. If the source times out before receiving a reply then it changes the PREF field in the header to indicate that weak channels are acceptable, since these may be the only links over which the packet can be propagated.

When a link failure is detected within the network, the intermediate nodes send an error message to the source indicating which channel has failed. The source then sends an erase message to notify all nodes of the broken link and initiates a new route-search process to find a new path to the destination.

3. Explain DSR Routing Protocol in detail. [An] **May/June 2016**

DYNAMIC SOURCE ROUTING (DSR)

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes.

DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration.

It is a reactive protocol and all aspects of the protocol operate entirely on-demand basis. It works on the concept of source routing. Source routing is a routing technique in which

the sender of a packet determines the complete sequence of nodes through which, the packets are forwarded.

The advantage of source routing is : intermediate nodes do not need to maintain up to date routing information in order to route the packets they forward.

The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance".

DSR requires each node to maintain a route – cache of all known self – to – destination pairs. If a node has a packet to send, it attempts to use this cache to deliver the packet.

If the destination does not exist in the cache, then a route discovery phase is initiated to discover a route to destination, by sending a route request.

This request includes the destination address, source address and a unique identification number.

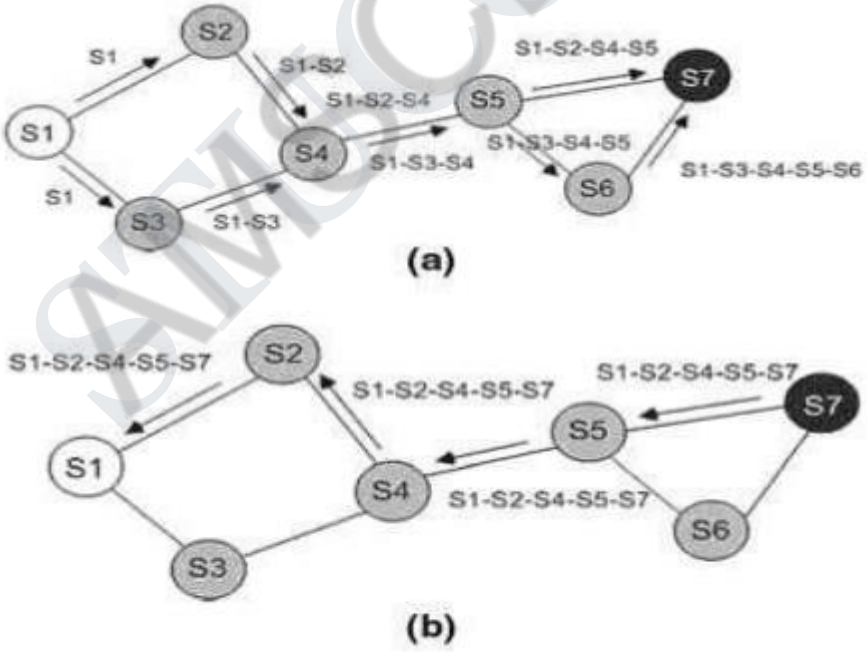
If a route is available from the route – cache, but is not valid any more, a route maintenance procedure may be initiated.

A node processes the route request packet only if it has not previously processes the packet and its address is not present in the route cache.

A route reply is generated by the destination or by any of the intermediate nodes when it knows about how to reach the destination.

Example

In the following example, the route discovery procedure is shown where S1 is the source node and S7 is the destination node.



(a) Route Discovery **(b)** Using route record to send the route reply

In this example, the destination S7, gets the request through two paths. It chooses one path based on the route records in the incoming packet and sends a reply using the reverse path to the source node. At each hop, the best route with minimum hop is stored. In this example, it is shown the route record status ate each hop to reach the destination from the source node. Here, the chosen route is S1-S2-S4-S5-S7.

Advantages and Disadvantages:

a) DSR uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.

b) The disadvantage of DSR is that the route maintenance mechanism does not locally repair a broken down link. The connection setup delay is higher than in table- driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source- routing mechanism employed in DSR. This routing overhead is directly proportional to the path length.

4. Explain about Hybrid Routing protocols in MANETs. [U]
5. Demonstrate how multicast routing is carried out in ad-hoc networks. [An]
6. Define VANET? Explain how does it differ from MANET? Explain any one application of VANET. [An]

Vehicular ad-hoc networks (**VANETs**) are created by applying the principles of mobile ad hoc networks (MANETs) – the spontaneous creation of a wireless network of mobile devices – to the domain of vehicles.[1] VANETs were first mentioned and introduced [2] in 2001 under "car-to-car ad-hoc mobile communication and networking" applications, where networks can be formed and information can be relayed among cars. It was shown that vehicle-to-vehicle and vehicle-to-roadside communications architectures will co-exist in VANETs to provide road safety, navigation, and other roadside services. VANETs are a key part of the intelligent transportation systems (ITS) framework. Sometimes, VANETs are referred as Intelligent Transportation Networks[3]

While, in the early 2000s, VANETs were seen as a mere one-to-one application of MANET principles, they have since then developed into a field of research in their own right. By 2015,[4](p3) the term VANET became mostly synonymous with the more generic term **inter-vehicle communication** (**IVC**), although the focus remains on the aspect of spontaneous networking, much less on the use of infrastructure like Road Side Units (RSUs) or cellular networks.

VANETs support a wide range of applications – from simple one hop information dissemination of, e.g., cooperative awareness messages (CAMs) to multi-hop dissemination of messages over vast distances. Most of the concerns of interest to mobile ad hoc networks (MANETs) are of interest in VANETs, but the details differ.[5] Rather than moving at random, vehicles tend to move in an organized fashion. The interactions with roadside equipment can likewise be characterized fairly accurately. And finally, most vehicles are restricted in their range of motion, for example by being constrained to follow a paved highway.

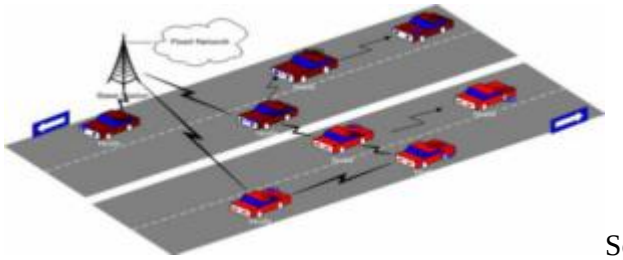
Example applications of VANETs are:[4](p56)

- **Electronic brake lights**, which allow a driver (or an autonomous car or truck) to react to vehicles breaking even though they might be obscured (e.g., by other vehicles).
- **Platooning**, which allows vehicles to closely (down to a few inches) follow a leading vehicle by wirelessly receiving acceleration and steering information, thus forming electronically coupled "road trains".

- **Traffic information systems**, which use VANET communication to provide up-to-the minute obstacle reports to a vehicle's satellite navigation system[6]
- **Road Transportation Emergency Services**[7] – where VANET communications, VANET networks, and road safety warning and status information dissemination are used to reduce delays and speed up emergency rescue operations to save the lives of those injured.
- **On-The-Road Services**[8] – it is also envisioned that the future transportation highway would be "information-driven" or "wirelessly-enabled". VANETs can help advertise services (shops, gas stations, restaurants, etc.) to the driver, and even send notifications of any sale going on at that moment.

7. Draw and explain the architecture of VANET. [U] **May/June 2016**

Architecture of Vanet



Source: Research Gate

Main Components

Vanets can be divided into three domains

- **The Mobile Domain**– It consists of two parts.

1. Mobile Device Domain- consists of all kinds of portable devices such as personal navigation devices and smartphone
2. Vehicle Domain- consists of all kinds of vehicles such as cars and buses

- **Infrastructure Domain**– It consists of two domains

1. Roadside Infrastructure Domain- Contains roadside entities like traffic lights
2. Central Infrastructure Domain- Contains Infrastructure management centres such as traffic management centres and vehicle management centre.

- **Generic Domain-** Although the architecture of VANET varies from region to region. In V2X (Vehicle to Anything) communication mainly V2V communication, the architecture is a little different. It further comprises three domains

1. In-Vehicle: It is composed of an onboard unit (OBU) and one or multiple application units. The connections between them are usually wired and sometimes wireless

1. Ad-hoc- It consists of vehicles which have OBUs and RSUs (Roadside Unit). An OBU is a non-stationary unit and the RSU is the stationary unit. RSUs can communicate with each other directly or via multihop as well.
2. Infrastructure Domain- There are two types of infrastructure domain access

- Road Side Unit (RSU)
- Hotspot (HS)

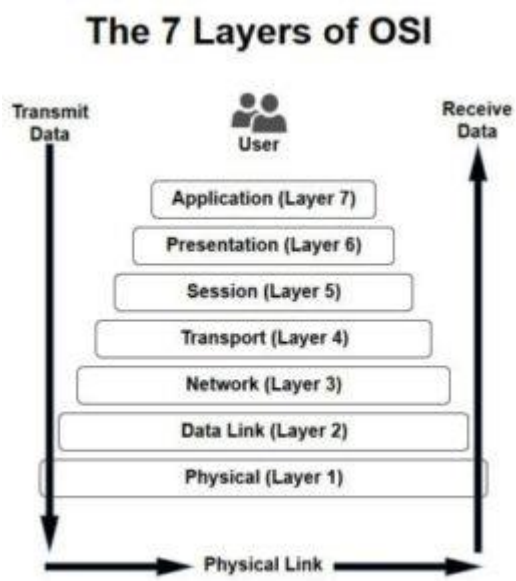
OBUs communicate with internet through RSU or HS. OBUs can communicate with each other via cellular network when RSU or HSU are not present.

Communication Architecture

There are 4 types of communication architecture in Vanets

1. **In-Vehicle Communication**– In vanet research, this is the most important domain. It can detect a vehicle's performance and more importantly driver's drowsiness and fatigue which is crucial in the safety of the driver and public.
2. **Vehicle to Vehicle Communication**– It provides data exchange platform so that vehicle can share information among themselves to assist the driver.
3. **Vehicle to Infrastructure Communication**– It allows the vehicle to communicate with the environment and infrastructure for real time traffic or weather updates. It provides environmental sensing and monitoring. It is one of the most important fields in Vanets.
4. **Vehicle to Broadband cloud communication**– Vehicles communicate through cellular data mechanisms such as 3G/4G. Broadband cloud includes more traffic information and it monitors data and infotainment. It is useful for the driver in assistance and vehicle tracking.

Layered Architecture



Source: Webopedia

The Open System Interconnection (OSI) model classifies similar communication functions into one of seven logical layers. The architecture varies in every region and hence there are different protocols and interfaces designed for them. For example DSRC in the US has a set of standard protocols and interfaces. Different protocols are designed to use at different layers. After amending IEEE 802.11 to IEEE 802.11p which adds standard Wireless Access in Vehicular Environments (WAVE), mainly to the physical (PHY) layer and the MAC sublayer. IEEE 1609 is a higher layer standard based on the IEEE 802.11p. IEEE 1609, represents a set of protocols that operates in the middle layers of protocol stack to support safety applications in vanets. Non safety applications are presented by another set of protocols which are IPv6 (Internet Protocol version 6), UDP (User Datagram Protocol) and TCP (Transmission Control Protocol) for network layer services and transport layer services.

Characteristics of Vanet

1. **High Dynamic Topology**– The topology of vanet changes because of the movement of vehicles at high speed.
2. **Frequent Disconnected Network**– As the network of vehicles widens the disconnection between vehicles become frequent when they exchange information.
3. **Mobility Modelling**– The mobility of vehicle depends upon the traffic environment, roads structure, the speed of other vehicles, driver's driving pattern etcetera.
4. **Battery Power and Storage Capacity**– Due to high battery power and storage, vanets are helpful for making effective communication and making routing decision unlike manet (Mobile Ad-hoc Network)
5. **Communication Environment**– Due to difference in communication environment between dense and sparse network, the routing approach of the dense and sparse network will be different. For example in dense areas, trees are considered to be obstacles and in sparse areas like highways trees are absent.
6. **Interaction with On-Board Sensors-** For effective communication and routing decisions, the movement and current position of these nodes can easily be sensed by On-Board sensors like GPS.

8. Discuss about various schemes in VANET routing. [An]

9. Explain the various security attacks on VANET. [U] **May/June 2016**

Types of Attackers

For secure VANET communication first we have to discover who are the attackers, their capacity and nature to spoil the network communication. Based on their nature we divided attackers into following five categories:

Active and Passive Attacker: Based on the participation nature of attackers we can categories attackers into two categories: Active and Passive Attacker. Active Attacker takes active part in communication by replying the message, by changing the content of message or dining the available services to legitimate users. Passive Attacker does not disturb the communication, but only observes the communication and monitors the traffic and position details of other vehicles.

Insider and Outsider attacker: Based on the Network knowledge we can categories the attacker in two categories: Insider and Outsider Attacker. Insider attacker is having all the communication details running inside the network and outside attackers haven't such details or having very less details. Insider attackers are the authenticated type of attacker, whom has details knowledge of network. These types of attacker learn about the design and structure of network and launches attack based on gain knowledge to disturb communication. Outsider attackers are also authenticated user of system but have a less knowledge of internal system. These types of attacker have limited scope compare to insider attacker.

Area Attacker: Such attackers are targeting some specific area before spreading such attacks in network. Total reflected area is depends on type of attack. It can be reflect communication of V2V or V2I in specific area. It can affect single or multiple OBU/RSU communication which is area specific.

Communication Attacker: This type of attacker attacks on specific communication like RSU to RSU communication, RSU to OBU Communication, and OBU to OBU Communication. Attackers want to deny user or the group of users by not allowing specific type of communication like denying of specific type of services.

Malicious and Rational Attacker: Malicious attackers are not having any personal benefits by disturbing the network. Such attackers only want to disturb the running network. Rational attackers are having any personal reason or profit for doing such malicious activities inside the network.

Timing Attacker: In this type of attack, attackers involve unnecessary delay in transmitted messages. Legitimate user will get the important message after required time. Due to such type of delay message becomes useless and some time it becomes very harmful in safety related messages.

. Security Requirement (Services) The security services increase the security of processing and data exchange in VANET. The security requirement includes: Authentication: It ensures that message is generated through legitimate user. Receiver will only trust on data which are coming from the authenticated source.

UNIT IV
MOBILE TRANSPORT AND APPLICATION LAYER

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

1. Define Mobile IP.

Mobile IP is a standard protocol created by extending Internet Protocol (IP) to enable users to keep the same IP address while travelling from one network to a different network.
Mobile IP = Mobility + Internet Protocol (IP)

2. Specify the goals of Mobile IP.

- Allows mobile hosts to stay connected to the internet regardless of their location and without changing their IP address.
- Enable packet transmission efficiently without any packet loss and disruptions in the presence of host and/or destination mobility.

3. What are the main requirements needed for mobile IP?

- Compatibility
- Transparency
- Scalability and efficiency
- Security

4. List out the various terminologies involved in Mobile IP.

a) Mobile Node
b) Home Network
c) Home Address
d) Foreign Agent
e) Correspondent Node
f) Care-of-Address
g) Tunnel
h) Foreign Network
i) Home Agent

5. Define COA.

It is an address that identifies the mobile node's current location. The packets sent to the Mobile Node are delivered to COA. COA is associated with the mobile node's Foreign Agent (FA).

6. Define Tunneling.

Tunneling is the process of delivering the packet sent by the Home Agent(HA) to foreign agent(COA) and frm COA to the mobile node via tunnel. Tunneling has two primary functions:

1. Encapsulation of data packet to reach the tunnel endpoint

2. Decapsulation when the packet is delivered at that endpoint.

7. What is encapsulation in Mobile IP.

Encapsulation refers to arranging a packet header and data and putting it into the data part of a new packet. Thus the encapsulated packet will contain the new destination address as "Address of COA" and the new source address as "Address of HA".

8. What are the two types of COA?

1. Foreign Agent COA: It is an IP address of Foreign Agent(FA).
2. Co-located COA: Temporary IP address that is assigned to MN.

9. What is meant by Agent Discovery?

Agent Discovery is a process by which a mobile node determines its Foreign Agent(FA) during call establishment.

Two methods of Agent Discovery:

(i) Agent Advertisement

(ii) Agent Solicitation

10. What is meant by Agent Advertisement?

Foreign agents and home agents advertise their presence periodically using special agent advertisement messages. An Agent Advertisement Message lists one or more COA and a flag indicating whether

11. What is meant by Agent Solicitation?

Agent Solicitation is an Agent Discovery process which is used to search for a foreign agent. Agent Solicitation message is sent if a mobile node does not receive any COA.

12. What are the mechanisms used for forwarding the packet?

- CN does not need to know anything about the MN's current location and sends the packet as usual to the IP address of MN
- The packet is not forwarded into the subnet as usual, but encapsulated and tunnelled to the COA
- The foreign agent now decapsulates the packet, i.e., removes the additional header, and forwards the original packet with CN as source and MN as destination to the MN

13. What are the key mechanisms associated with Mobile IP?

1. Discovering the Care-of-Address
2. Registering the Care-of-Address
3. Tunneling to the Care-of-Address

14. What do you mean by the term binding of mobile node?

The association of the home address of a mobile node with a Care-Of-Address (COA) is called binding of mobile node.

15. What is DHCP? May/June 2016

DHCP (Dynamic Host Configuration Protocol) is a communication protocol that network administrators use to centrally manage and automate the network configuration of devices attaching to an Internet Protocol (IP) network.

16. Elaborate on TCP/IP protocol.

TCP/IP is a combination of two separate protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). The Internet Protocol standard dictates the logistics of packets sent out over networks; it tells packets where to go and how to get there.

The Transmission Control Protocol is responsible for ensuring the reliable transmission of data across Internet-connected networks. TCP checks packets for errors and submits requests for re-transmissions if any are found.

17. Mention the layers involved in TCP/IP Protocol Suite

1. Application Layer
2. Transport Layer
3. Internet Layer
4. Network Access Layer

18. Name the protocols in Application Layer.

1. HTTP (HyperText Tranfer Protocol)
2. FTP (File Transfer Protocol)
3. SMTP (Simple Mail Transfer Protocol)
4. SNMP (Simple Network Management Protocol)
5. DNS (Domain Name System)
6. TELNET

19. Mention the Transport Layer Protocols.

1. TCP (Transmission Control Protocol)
2. UDP (User Datagram Protocol)

20. List out the Internet Layer Protocols.

1. IGMP (Internet Group Management Protocol)
2. ICMP (Internet Control Message Protocol)
3. IP (Internet Protocol)
4. ARP (Address Resolution Protocol)
5. RARP (Reverse Address Resolution Protocol)

21. What is the use of HTTP and FTP?

- **HTTP:**

➢ HTTP stands for HyperText Transfer Protocol

➢ HTTP takes care of the communication between a web server and a web browser.

➢ It is used for sending requests from a web client (a browser) to a web server, returning web content (web pages) from the server back to the client.

- **FTP:**

➢ FTP stands for File Transfer Protocol

➢ FTP takes care of file transmission between computers.

22. What is BOOTP?

BOOTP stands for Boot Protocol. It used for booting (starting) computers from the network.

23. What are the various mechanisms used to improve traditional TCP performance?

1. Slow Start
2. Congestion Avoidance
3. Fast Retransmit / Fast Recovery

24. What are the various mechanisms used to improve TCP performance in Mobile Networks?

1. TCP in Single-hop Wireless Networks:
   - Indirect TCP (I-TCP)
   - Fast Retransmission
   - Snooping TCP (S-TCP)
   - Mobile TCP (M-TCP)
   - Freeze TCP (F-TCP)

2. TCP in Multi-hop Wireless Networks:
   - TCP-F (TCP Feedback)

25. List out indirect TCP advantages. May/June 2013

- I-TCP does not require any changes in the TCP protocol as used by the hosts in the fixed network or other hosts in a wireless network that do not use this optimization. All current optimizations for TCP still work between the foreign agent and the correspondent host.
- Due to the strict partitioning into two connections, transmission errors on the wireless link, i.e., lost packets cannot propagate into the fixed network

26. Define disadvantage of I-TCP.

- The loss of the end-to-end semantics of TCP might cause problems if the foreign agent partitioning the TCP connection crashes.
- The foreign agent must be a trusted entity because the TCP connections end at this point. If users apply end-to-end encryption.

27. What is meant by Snooping TCP?

- The main function of the enhancement is to buffer data close to the mobile host to perform fast local retransmission in case of packet loss.
- In this approach, the foreign agent buffers all packets with destination mobile host and additionally 'snoops' the packet flow in both directions to recognize acknowledgements

28. List out advantage of M-TCP.

- It maintains the TCP end-to-end semantics. The SH does not send any ACK itself but forwards the ACKs from the MH.
- If the MH is disconnected, it avoids useless retransmissions, slow starts or breaking connections by simply shrinking the sender's window to 0

29. Define fast retransmit and fast recovery.

- The mechanisms of fast recovery/fast retransmit a host can use after receiving duplicate acknowledgements, thus concluding a packet loss without congestion.
- As soon as the mobile host registers at a new foreign agent using mobile IP, it starts sending duplicated

30. Define time out freezing. May/June 12 and May/June 2013 Nov/Dec 2014

The MAC layer can inform the TCP layer of an upcoming loss of connection or that the current interruption is not caused by congestion. TCP can now stop sending and 'freezes' the current state of its congestion window and further timers

31. Define Selective retransmission. Nov / Dec 2012

- If a single packet is lost, the sender has to retransmit everything starting from the lost packet (go-back-n retransmission). This obviously wastes bandwidth, not just in the case of a mobile network, but for any network (particularly those with a high path capacity, i.e., bandwidth delay- product
- The advantage of this approach is obvious: a sender retransmits only the lost packets

32. List out disadvantage of M-TCP.

- As the SH does not act as proxy as in I-TCP, packet loss on the wireless link due to bit errors is propagated to the sender. M-TCP assumes low bit error rates, which is not always a valid assumption.
- A modified TCP on the wireless link not only requires modifications to the MH protocol software but also new network elements like the bandwidth manager

33. What are the possible locations for care of address? Nov/Dec 2013

The COA defines the current location of the MN from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the MN is done using a tunnel, as explained later. To be more precise, the COA marks the tunnel endpoint, i.e., the address where packets exit the tunnel

There are two different possibilities for the location of the COA:

- Foreign agent COA
- Co-located COA

34. What are the possible locations of Tunnel end point of Mobile IP? May/June 2014

A tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel is achieved by using encapsulation.

The possible locations of Tunnel end point are

1. Home Agent (HA)
2. Foreign Agent (FA)

35. How does M-TCP split the connections?

- **Unmodified TCP**

Used to handle wired part of connection and used in between the Fixed Host (FH) and the Supervisory Host (SH).

- **Optimized TCP**

Used to handle wireless part of connection and used in between the Supervisory Host (SH) and the Mobile Host (MH).

36. What should the value of TTL Filed in the IP packet of agent advertisement? Why? May/June 2014

The TTL field of the IP packet is set to 1 for all advertisements to avoid forwarding them. The IP destination address according to standard router advertisements can be either set to 224.0.0.1, which is the multicast address for all systems on a link or to the broadcast address 255.255.255.255.

37. Differentiate snoopy TCP and mobile TCP. Nov/Dec 2014

- The Snoop protocol is a TCP-aware link layer protocol designed to improve the performance of TCP over networks of wired and single-hop wireless links. The main problem with TCP performance in networks that have both wired and wireless links is that packet losses that occur because of bit-errors are mistaken by the TCP sender as being due to network congestion, causing it to drop its transmission window and often time out, resulting in degraded throughput.
- In wireless systems, WTCP is placed on a base station or intermediate gateway between a source host and a mobile (wireless) host. The base station is a wireless transmitter and receiver for the mobile host, and acts as a gateway to the internet for the host.

PART – B

1. Explain entities and terminology of Mobile IP. [U]

Mobile Node (MN):

1. A mobile node is an end-system or router that can change its point of attachment to the internet using mobile IP.
2. The MN keeps its IP address and can continuously communicate with any other system in the internet as long as link-layer connectivity is given. Examples are laptop, mobile phone, router on an aircraft etc.

Correspondent node (CN):

1. At least one partner is needed for communication. In the following the CN represents this partner for the MN.
2. The CN can be a fixed or mobile node.

Home network:

The home network is the subnet the MN belongs to with respect to its IP address. No mobile IP support is needed within the home network.

Foreign network:

The foreign network is the current subnet the MN visits and which is not the home network.

Foreign agent (FA):

1. The FA can provide several services to the MN during its visit to the foreign network.
2. The FA can have the COA, acting as tunnel endpoint and forwarding packets to the MN.
3. The FA can be the default router for the MN.
4. FAs can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.
5. FA is implemented on a router for the subnet the MN attaches to.

Care-of address (COA):

1. The COA defines the current location of the MN from an IP point of view.
2. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN.
3. Packet delivery toward the MN is done using a tunnel, i.e., the COA marks the tunnel endpoint, i.e., the address where packets exit the tunnel.
4. There are two different possibilities for the location of the COA:

   a. Foreign agent COA:

   1. The COA could be located at the FA, i.e., the COA is an IP address of the FA.
   2. The FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as common COA.

   b. Co-located COA:

   3. The COA is co-located if the MN temporarily acquired an additional IP address which acts as COA.
   4. This address is now topologically correct, and the tunnel endpoint is at the MN. Co-located addresses can be acquired using services such as DHCP. IP packet delivery

2. Describe the following terms in detail: [An]
   i) Corresponding Node
   ii) Care of Address

Mobile IP provides the following alternative modes for the acquisition of a care-of address:

- A foreign agent provides a **foreign agent care-of address**, which is advertised to the mobile node through agent advertisement messages. The care-of address is usually the IP address of the foreign agent that sends the advertisements. The foreign agent is the endpoint of the tunnel. When the foreign agent receives datagrams through a tunnel, the foreign agent de-encapsulates the datagrams. Then, the foreign agent delivers the inner datagram to the mobile node. Consequently, many mobile nodes can share the same care-of address. Bandwidth is important on wireless links. Wireless links are good candidates from which foreign agents can provide Mobile IP services to higher bandwidth-wired links.

- A mobile node acquires a **colocated care-of address** as a local IP address through some external means. The mobile node then associates with one of its own network interfaces. The mobile node might acquire the address through DHCP as a temporary address. The address might also be owned by the mobile node as a long-term address. However, the mobile node can only use the address while visiting the subnet to which this care-of address

belongs. When using a colocated care-of address, the mobile node serves as the endpoint of the tunnel. The mobile node performs de-encapsulation of the datagrams that are tunneled to the mobile node.

A colocated care-of address enables a mobile node to function without a foreign agent. Consequently, a mobile node can use a colocated care-of address in networks that have not deployed a foreign agent.

If a mobile node is using a colocated care-of address, the mobile node must be located on the link that is identified by the network prefix of the care-of address. Otherwise, datagrams that are destined to the care-of address cannot be delivered.

iii) Agent Discovery

A mobile node uses a method known as agent discovery to determine the following information:

- When the node has moved from one network to another
- Whether the network is the node's home or a foreign network
- What is the foreign agent care-of address offered by each foreign agent on that network

Mobility agents transmit **agent advertisements** to advertise their services on a network. In the absence of agent advertisements, a mobile node can solicit advertisements. This is known as **agent solicitation**.

iv) Tunneling and Encapsulation.

3. Explain in detail about the key mechanisms associated with Mobile IP. [U]

The Mobile IP process has three main phases, which are discussed in the following sections.

i.Agent Discovery - A Mobile Node discovers its Foreign and Home Agents during agent

discovery.

ii.Registration - The Mobile Node registers its current location with the Foreign Agent and Home Agent during registration.

iii.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.

i.Agent Discovery

During the agent discovery phase, the Home Agent and Foreign Agent advertise their services on the network by using the ICMP Router Discovery Protocol (IRDP). The Mobile Node listens to these advertisements to determine if it is connected to its home network or foreign network.

The IRDP advertisements carry Mobile IP extensions that specify whether an agent is a Home Agent, Foreign Agent, or both; its care-of address; the types of services it will provide such as reverse tunnelling and

generic routing encapsulation (GRE); and the allowed registration lifetime or roaming period for visiting Mobile Nodes. Rather than waiting for agent advertisements, a Mobile Node can send out an agent solicitation. This solicitation forces any agents on the link to immediately send an agent advertisement.

If a Mobile Node determines that it is connected to a foreign network, it acquires a care-of address. Two types of care-of addresses exist:

- Care-of address acquired from a Foreign Agent
- Co-located care-of address

A Foreign Agent care-of address is an IP address of a Foreign Agent that has an interface on the foreign network being visited by a Mobile Node. A Mobile Node that acquires this type of care-of address can share the address with other Mobile Nodes. A co-located care-of address is an IP address temporarily assigned to the interface of the Mobile Node itself.

A co-located care-of address represents the current position of the Mobile Node on the foreign network and can be used by only one Mobile Node at a time. When the Mobile Node hears a Foreign Agent advertisement and detects that it has moved outside of its home network, it begins registration.

ii.Registration

The Mobile Node is configured with the IP address and mobility security association (which includes the shared key) of its Home Agent. In addition, the Mobile Node is configured with either its home IP address, or another user identifier, such as a Network Access Identifier.

The Mobile Node uses this information along with the information that it learns from the Foreign Agent advertisements to form a Mobile IP registration request. It adds the registration request to its pending list and sends the registration request to its Home Agent either through the Foreign Agent or directly if it is using a co-located care-of address and is not required to register through the Foreign Agent.

If the registration request is sent through the Foreign Agent, the Foreign Agent checks the validity of the registration request, which includes checking that the requested lifetime does not exceed its limitations, the requested tunnel encapsulation is available, and that reverse tunnel is supported. If the registration request is valid, the Foreign Agent adds the visiting Mobile Node to its pending list before relaying the request to the Home Agent. If the registration request is not valid, the Foreign Agent sends a registration reply with appropriate error code to the Mobile Node.

The Home Agent checks the validity of the registration request, which includes authentication of the Mobile Node. If the registration request is valid, the Home Agent creates a mobility binding (an association of the Mobile Node with its care-of address), a tunnel to the care-of address, and a routing entry for forwarding packets to the home address through the tunnel.

The Home Agent then sends a registration reply to the Mobile Node through the Foreign Agent (if the registration request was received via the Foreign Agent) or directly to the Mobile Node. If the registration request is not valid, the Home Agent rejects the request by sending a registration reply with an appropriate error code.

The Foreign Agent checks the validity of the registration reply, including ensuring that an associated registration request exists in its pending list. If the registration reply is valid, the Foreign Agent adds the Mobile Node to its visitor list, establishes a tunnel to the Home Agent, and creates a routing entry for forwarding packets to the home address. It then relays the registration reply to the Mobile Node.

Finally, the Mobile Node checks the validity of the registration reply, which includes ensuring an associated request is in its pending list as well as proper authentication of the Home Agent. If the registration reply is not valid, the Mobile Node discards the reply. If a valid registration reply specifies that the registration is accepted, the Mobile Node is confirmed that the mobility agents are aware of its roaming. In the co-located care-of address case, it adds a tunnel to the Home Agent. Subsequently, it sends all packets to the Foreign Agent.

The Mobile Node reregisters before its registration lifetime expires. The Home Agent and Foreign Agent update their mobility binding and visitor entry, respectively, during re-registration. In the case where the registration is denied, the Mobile Node makes the necessary adjustments and attempts to register again. For example, if the registration is denied because of time mismatch and the Home Agent sends back its time stamp for synchronization, the Mobile Node adjusts the time stamp in future registration requests.

Thus, a successful Mobile IP registration sets up the routing mechanism for transporting packets to and from the Mobile Node as it roams.

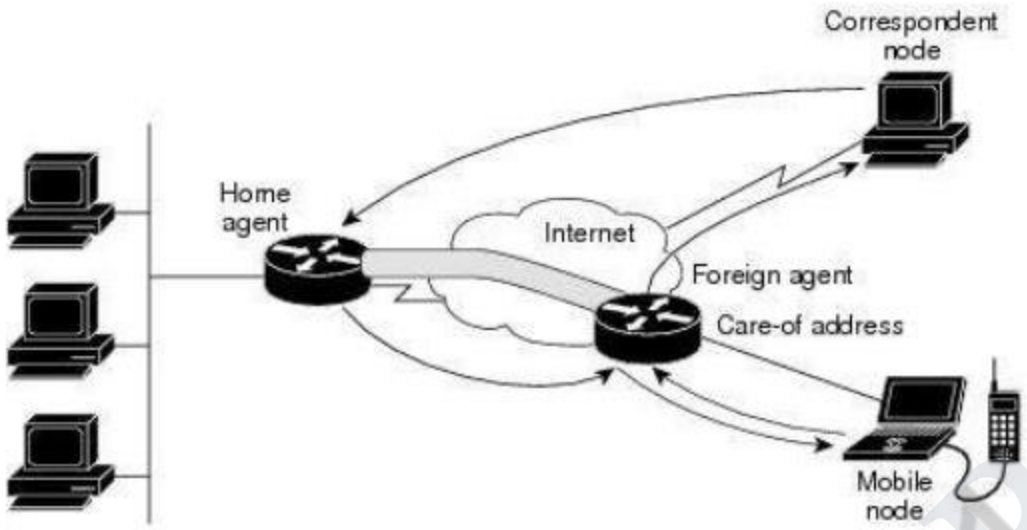
iii.Tunnelling

The Mobile Node sends packets using its home IP address, effectively maintaining the appearance that it is always on its home network. Even while the Mobile Node is roaming on foreign networks, its movements are transparent to correspondent nodes.Data packets addressed to the Mobile Node are routed to its home network, where the Home Agent now intercepts and tunnels them to the care-of address toward the Mobile Node.

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.

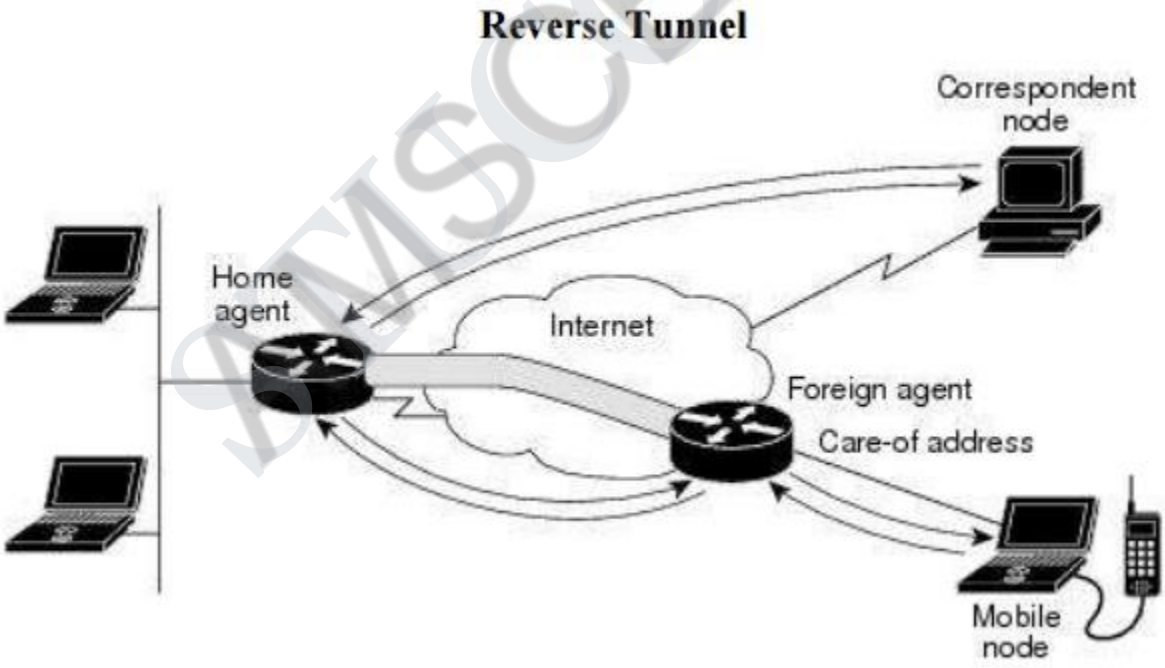
The default tunnel mode is IP Encapsulation within IP Encapsulation.

Packet Forwarding



However, this data path is topologically incorrect because it does not reflect the true IP network source for the data — rather, it reflects the home network of the Mobile Node. Because the packets show the home network as their source inside a foreign network, an access control list on routers in the network called ingress filtering drops the packets instead of forwarding them. A feature called reverse tunnelling solves this problem by having the Foreign Agent tunnel packets back to the Home Agent when it receives them from the Mobile Node.

Reverse Tunnel



Tunnel MTU discovery is a mechanism for a tunnel encapsulator such as the Home Agent to participate in path MTU discovery to avoid any packet fragmentation in the routing path between a Correspondent Node and Mobile Node. For packets destined to the Mobile Node, the Home Agent maintains the MTU of the tunnel to the care-of address and

informs the Correspondent Node of the reduced packet size. This improves routing efficiency by avoiding fragmentation and reassembly at the tunnel endpoints to ensure that packets reach the Mobile Node.

Security

Mobile IP uses a strong authentication scheme for security purposes. All registration messages between a Mobile Node and Home Agent are required to contain the Mobile-Home Authentication Extension (MHAE).

The integrity of the registration messages is protected by a preshared 128-bit key between a Mobile Node and Home Agent. The keyed message digest algorithm 5 (MD5) in "prefix+suffix" mode is used to compute the authenticator value in the appended MHAE, which is mandatory. Mobile IP also supports the hash-based message authentication code (HMAC-MD5). The receiver compares the authenticator value it computes over the message with the value in the extension to verify the authenticity.

Optionally, the Mobile-Foreign Authentication Extension and Foreign-Home Authentication Extension are appended to protect message exchanges between a Mobile Node and Foreign Agent and between a Foreign Agent and Home Agent, respectively.

Replay protection uses the identification field in the registration messages as a timestamp and sequence number. The Home Agent returns its time stamp to synchronize the Mobile Node for registration.

Cisco IOS software allows the mobility keys to be stored on an authentication, authorization, and accounting (AAA) server that can be accessed using TACACS+ or RADIUS protocols. Mobile IP in Cisco IOS software also contains registration filters, enabling companies to restrict who is allowed to register

4. Express brief account of route optimization in Mobile IP. [U]

Route Optimization has been designed within the IETF to ameliorate the problem of triangle routing, a routing artifact introduced by Mobile IP's requirement to route packets destined for a mobile node by way of its home network. In this article, we describe the current protocol specification for the Route Optimization protocol, concentrating on design decisions and justifications. Once the basic mechanisms are explained, we show how they are applied to enable foreign agents to offer smooth handoffs for mobile nodes, and describe the security operations that enable reliable operation of this handoff between foreign agents with which a mobile node has no pre-existing security relationship.

5. With a diagram explain DHCP and its protocol architecture. [R] **May/June 2016**

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to any new node entering the network. DHCP permits a node to be configured automatically, thereby avoiding the necessity of involvement by a network administrator.

DHCP does the following:

1. Manages the provision of all the nodes added or dropped from the network
2. Maintains the unique IP address of the host using a DHCP server
3. Sends a request to the DHCP server whenever a client/node, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node.

Dynamic Host Configuration Protocol is also known as RFC 2131.

node in a network can be assigned or reassigned an IP address instantly. Without DHCP, the network administrators would be forced to assign IP address manually for every node in a network.

A DHCP server has many duties:

1. A DHCP server is configured to manage the provision of IP addresses and is an essential requirement to run DHCP protocol. The server manages the record of all the IP addresses it allocates to the nodes. If the node rejoins or is relocated in the network, the server identifies the node using its MAC address. This helps to prevent the accidental configuration of same IP address to two different nodes.
2. For DHCP to operate, the clients need to be configured with it. When a DHCP-aware client connects to the network, the client broadcasts a request to the DHCP server for the network settings.
3. The server responds to the client's request by providing the necessary IP configuration information.
4. The DHCP server is ideally suited in scenarios where there is a regular inclusion and exclusion of network nodes like wireless hotspots. In these cases, the DHCP server also assigns a lease time to each client, after which the assigned IP address in invalid

6. Explain IP-in-IP, Minimal IP and GRE encapsulation methods. [U] **May/June 2016**

7. With a neat diagram explain the architecture of TCP/IP. [U] **May/June 2016**

The two main protocols defined in this architecture are:

• **IP (Internet Protocol)** network level, which provides connectionless service.

• **TCP (Transmission Control Protocol)** transport level, which provides a service with reliable connection.

TCP / IP define a layered architecture that also includes, without being explicitly defined, an access interface to the network. Indeed, many separate subnets can be taken into account in the TCP / IP architecture, both local type than extended.

This architecture is illustrated in FIG. Note in this figure the appearance of another level protocol message (layer 4), UDP (User Datagram Protocol). This protocol uses a connectionless mode, which allows you to send messages without the recipient's permission

8. Explain the layered architecture of the TCP/IP protocol suite and compare it with the ISO/OSI Architecture. [An]

9. Explain indirect TCP. [U] **Nov /Dec 2011&12, May/June 12, May /June 2013, Nov/Dec2014**

The two **competing insights** are

1) TCP performs poorly together with wireless links

2) TCP within the fixed network cannot be changed

Working:

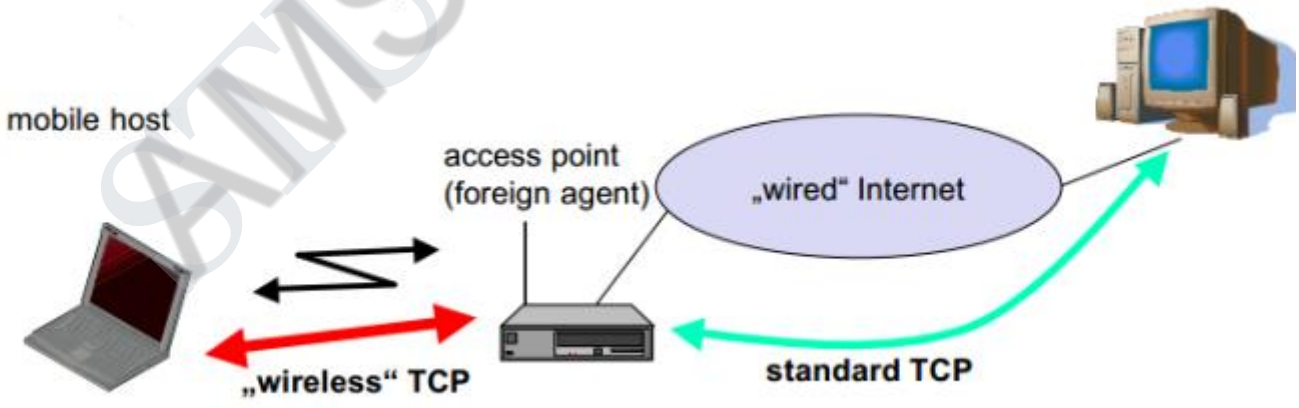
Indirect TCP or I-TCP segments the connection (figure 1)

- no changes to the TCP protocol for hosts connected to the wired Internet, millions of computers use (variants of) this protocol
- optimized TCP protocol for mobile hosts
- splitting of the TCP connection at, e.g., the foreign agent into 2 TCP connections, no real end-to-end connection any longer
- hosts in the fixed part of the net do not notice the characteristics of the wireless part

Packet delivery (CN to MN)

- If CN sends packet, FA acknowledges packet and forwards packet to MN
- If MN receives packet,it acknowledges
- This acknowledgement only used by CN

Similarly if MN sends packet, FA acknowledges packet and forwards it to CN



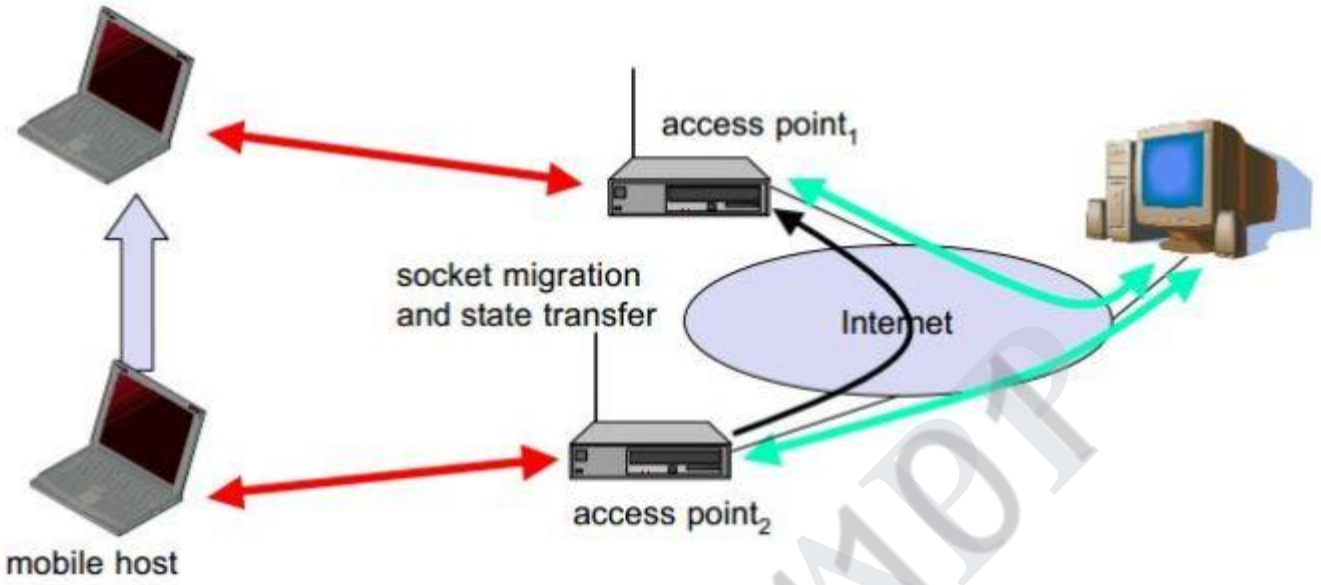
F

ig 1:I-TCP segments a TCP connection into two parts

I-TCP requires several actions as soon a handover takes place:

- The packets have to be redirected using mobile IP
- The access point acts as a proxy bufferering packets for retransmission

- After handover, the old proxy forwards data to new proxy
- The sockets(current state of TCP) of old proxy also migrate to new foreign agent



Socket migration after handover of a mobile host (I-TCP)
Data transfer to the mobile host o FA buffers data until it receives ACK of the MH, FA detects packet loss via duplicated ACKs or time-out o fast retransmission possible, transparent for the fixed network θ Data transfer from the mobile host o FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a NACK to the MH o MH can now retransmit data with only a very short delay θ Advantages: o Maintain end-to-end semantics o No change to correspondent node o No major state transfer during handover θ Problems o Snooping TCP does not isolate the wireless link well o May need change to MH to handle NACKs o Snooping might be useless depending on encryption schemes

10. Short notes on Snooping and Mobile TCP. [R] **Nov /Dec 2011&12, May/June 12, May /June 2013, Nov/Dec 2013, May/June2014, Nov/Dec 2014**

Snooping TCP I θ Transparent extension of TCP within the foreign agent θ buffering of packets sent to the mobile host θ lost packets on the wireless link (both directions!) will be retransmitted immediately by the mobile host or foreign agent, respectively (so called "local" retransmission) θ the foreign agent therefore "snoops" the packet flow and recognizes acknowledgements in both directions, it also filters ACKs θ changes of TCP only within the foreign agent (+min. MH change) „wired" Internet buffering of data end-to-end TCP connection local retransmission correspondent foreign host agent mobile host snooping of ACKs Snooping TCP II θ Data transfer to the mobile host o FA buffers data until it receives ACK of the MH, FA detects packet loss via duplicated ACKs or time-out o fast retransmission possible, transparent for the fixed network θ Data transfer from the mobile host o FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a NACK to the MH o MH can now retransmit data with only a very short delay θ Advantages: o Maintain end-to-end semantics o No change to correspondent node o No major state transfer during handover θ Problems o Snooping TCP does not isolate the wireless link well o May need change to MH to handle NACKs o Snooping might be useless depending on encryption schemes
Mobile TCP θ Special handling of lengthy and/or frequent disconnections θ M-TCP splits as I-TCP does o unmodified TCP fixed network to supervisory host (SH) o optimized TCP SH to MH θ Supervisory host o no caching, no retransmission o monitors all packets, if disconnection detected • set

sender window size to 0 • sender automatically goes into persistent mode o old or new SH reopen the window θ Advantages o maintains semantics, supports disconnection, no buffer forwarding θ Disadvantages o loss on wireless link propagated into fixed network o adapted TCP on wireless link

11. Write short notes on (i) TCP Tahoe (ii) TCP Reno [R]

Versions of TCP

There have been many (and increasingly sophisticated) congestion avoidance mechanims added to TCP since Jacobson's founding work.

There are3 versions of TCP - named after cities in Nevada:

- **TCP Tahoe**
  - This is the original version of TCP congestion avoidance as implemented by Jacobson
  - Uses: Slow Start)
  - and: Fast Retransmit
- **TCP Reno**
  - is equal to TCP Tahoe plus
  - Fast Recovery
- **TCP Vegas**
  - This is completely new implementation based on delay variation (instead of packet loss as in the previous2 versions of TCP)

11. Explain WAP Architecture in detail

L ayers of WAP Protocol

Application Layer

Wireless Application Environment (WAE). This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WMLScript.

Session Layer

Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.

Transaction Layer

Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

Security Layer

Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

Transport Layer

Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.

The WAP protocol architecture is shown below alongside a typical Internet Protocol stack.

12. Explain WTA Architecture

WTA is a collection of telephony specific extensions for call and feature control mechanisms, merging data networks and voice networks.

It is an Extension of basic WAE application model with following features

–network model for interaction

- client requests to server
- event signaling: server can push content to the client

– event handling

- table indicating how to react on certain events from the network
- client may now be able to handle unknown events

–telephony functions

- some application on the client may access telephony functions

WTAI (Wireless Telephony Application Interface) includes:

–Call control

–Network text messaging

–Phone book interface

–Event processing

Security model: segregation

–Separate WTA browser

–Separate WTA port

UNIT V

MOBILE PLATFORMS AND APPLICATIONS

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

COURSE OBJECTIVE: Gain knowledge about different mobile platforms and application development.

PART – A

1. What is meant by Mobile Operating System?

A mobile operating system, also called a mobile OS, is software that is specifically designed to run on mobile devices such as mobile phones, smartphones, PDAs, tablet computers and other handheld devices. Much like the Linux or Windows operating system controls your desktop or laptop computer, a mobile operating system is the software platform on top of which other programs can run on mobile devices.

2. List out the features of Mobile Operating Systems.

1. Multitasking
2. Scheduling
3. Memory Allocation
4. File System Interface
5. Keypad Interface
6. I/O Interface
7. Protection and Security
8. Multimedia features

3. Draw the architecture of Mobile OS.

Applications
OS Libraries
Device Operating System Base, Kernel
Low-Level Hardware, Manufacturer Device Drivers

4. What are the constraints in Mobile OS?

Design and capabilities of a Mobile OS (Operating System) is very different than a general purpose OS running on desktop machines:

- Mobile devices have constraints and restrictions on their physical characteristic such as screen size, memory, processing power and etc.
- Scarce availability of battery power
- Limited amount of computing and communication capabilities

5. List out various Mobile Operating Systems.
Give four examples of Mobile OS. May/June 2016

There are many mobile operating systems. The followings demonstrate the most important ones:

- Java ME Platform
- Palm OS
- Symbian OS
- Linux OS
- Windows Mobile OS
- BlackBerry OS
- iPhone OS
- Google Android Platform

6. Define Android SDK.

Android SDK is a software development kit that enables developers to create applications for the Android platform. The Android SDK includes sample projects with source code, development tools, an emulator, and required libraries to build Android applications.

7. What are the advantages and disadvantages of Android Mobile OS?

Advantages	Disadvantages
• Large number of devices using Android • Frequent Enhancement • Larger number of applications availability • Excellent UI • Multi-tasking • Free developer tools • No restrictions on applications • Phones are available from every service provider • Many devices can be unlocked with third-party applications	• Some device manufacturers add alternative UI front-ends which reduces OS consistency • Updates are controlled by device manufacturers and may be slow or non-existent • Applications are not validated

8. What are the advantages and disadvantages of Apple IOS?

Advantages	Disadvantages
• Excellent UI • Larger number of applications availability • Apple validates applications • Consistent UI across devices • Frequent free OS updates	• Closed architecture • Limited number of devices to choose from – all from apple • No multi-tasking for applications • Applications must be approved by Apple before being made available via the Marketplace • Can't be unlocked

9. What are the advantages and disadvantages of BlackBerry OS?

Advantages	Disadvantages
• Secure send and receive email using proprietary encryption • Multi-tasking • Phones available form most service	• Closed architecture • Limited number of devices to choose from – all from Research In Motion • Limited number of applications

providers	available • Application development is more complex and difficult than other Operating Systems • Applications tend to be more costly

10. What are the advantages and disadvantages of Windows Phone OS?

Advantages	Disadvantages
• Built in support for Windows Office documents • Multi-tasking • Phones available form most service providers • Excellent development tools, with free versions available to students • Updates available directly from Microsoft	• Closed architecture • Small number of applications available • Browser is a mix of IE7 and IE8 (a bit dated) • Applications must be approved by Microsoft before being

11. What is M-Commerce? May/June 2016

M-commerce (mobile commerce) is the buying and selling of goods, services or information by using Wireless handheld devices such as cellular telephone and personal digital assistants (PDAs). It is an important application of Mobile Computing. This includes purchases on Websites or apps, in-store or from vending machines; paying for travel, events or bills; or redeeming a coupon… any type of commerce that is conducted using a mobile device.

12. What are the characteristics of M-Commerce?

1. Fast Processing
2. Reduced Business Costs
3. Little Need for Maintenance

13. List out the applications of M-Commerce.

M-Commerce applications broadly categorized into

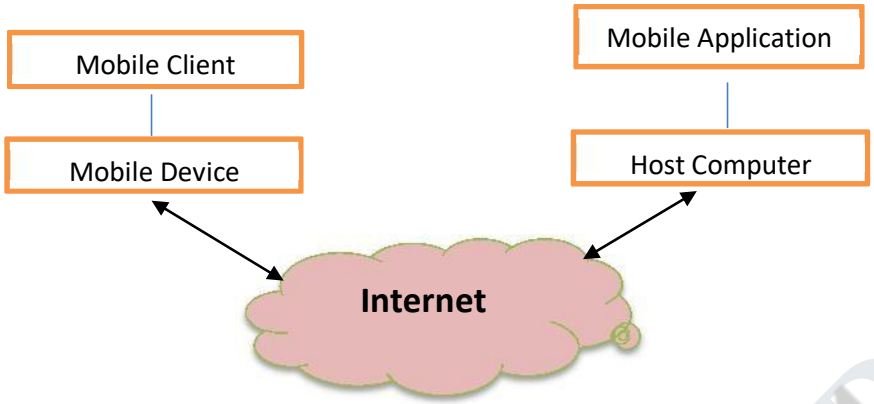
1. Business-to-Consumer (B2C) Applications

(i) Advertising
(ii) Comparison Shopping
(iii) Information about a product
(iv) Mobile Ticketing
(v) Content Purchase and Delivery
(vi) Loyalty and Payment Services
(vii) Mobile Banking
(viii) Catalogue Shopping
(ix) Mobile Brokerage

2. Business-to-Business (B2B) Applications

(i) Ordering and Delivery Conformation
(ii) Stock Tracking and Control
(iii) Supply Chain Management
(iv) Mobile Inventory Management

14. Draw the structure of Mobile Commerce.



15. What are the features required for a mobile device to enable mobile commerce?

To enable M-Commerce to be used widely, a mobile device should support the following features:

i) Good internet connectivity
ii) Ability to display rich content such as images
iii) Have a good quality camera with auto focus
iv) Screen should be able to properly display the bar codes
v) Ability to read the RFID tags
vi) MMS (Multimedia Message Service), SMS (Short Message Service)
vii) Ability to communicate between the mobile device and the supporting network
viii) Ability to scan bar codes
ix) Ability to interact with the Point-of-Sale (PoS) terminals

16. What are pros of M-Commerce?

1. For the business organizations, the benefits of using M-commerce include customer convenience, cost savings and new business opportunities.
2. For customers, M-commerce provides the flexibility of anytime, anywhere shopping using a lightweight device. Customers can save substantial time compared to visiting several stores to identify a right product at lowest price.
3. Cover wild distance: Mobile is the only technology which is now become necessary for any person in social and business life than computers. So, it is easy to reach users through mCommerce.
4. Consumer deals : As more users use mCommerce, there are lots of companies use mCommerce site to reach them by giving different and better deals in comparison of their competitor.
5. Savings : Companies try to reach to the consumer directly through mCommerce, so users have no need to go far to the store physically and at the end it saves user's time and money.
6. Easy to use : There is no need of skilled consumer. Buyers can have look thousands of items on their cell phones and there is no need of online checkout process.

17. What are the cons of M-Commerce?

1. Smart phone limitation (Small Screen): Mobile has no big screen like desktop or laptops, so sometimes users tried to navigate more and more to choose just one item from thousands. It affects shopping rates.

2. Habituate: Every new technology has some problem at the starting phase. Here mCommerce is new application, so sometimes people avoid to change which are rapidly change. As they are habituate to buy products from eCommerce.
3. The underlying network may impose several types of restrictions. For example, the available bandwidth is restricted, international calls and SMS may be expensive. Therefore ubiquity of E-commerce is hard to achieve.
4. Security: unless a customer is extremely careful, he may fall to various types of frauds and may get billed for the items he did not purchase.
5. Risk factor: Each business has its own risk. Same Mobile commerce is the growing field and a lot of investment in this field is become risky. Because technology change day by day. Moreover, there less security in wireless network, so in data transfer hacking chances are more.
6. Connectivity: Mobile commerce needs high speed connectivity of 3G. Otherwise it is become hectic for user to go through entire product purchase process.

18. What is meant by M-Payment (Mobile Payment)?

A Mobile Payment (m-payment) may be defined as initiation, authorization and confirmation of a financial transaction using a mobile devices like mobile phones, PDAs and other devices that connects to a mobile network for making payments.

19. What are the characteristics/properties of Mobile Payment System?

1. Simplicity and Usability
2. Universality
3. Interoperability
4. Security, privacy and Trust
5. Cost
6. Speed / Swiftness
7. Cross border payments

20. What are the different Mobile Payment System models?

There are three different models available for mobile payment solutions on the basis of payment:

1. Bank account based
2. Credit card based
3. Micro Payment

21. List out the various technologies used for M-Payment systems.

a) SMS (Short Message Service)
b) USSD (Unstructured Supplementary Services Delivery)
c) WAP/GPRS
d) Phone based applications (J2ME/BREW)
e) SIM-based Application
f) Near Field Communication (NFC)
g) Dual Chip
h) Mobile Wallet

22. Who are the stakeholders of M-Payment systems?

The mobile payment ecosystem involves the following types of stakeholders:

- Consumers
- Financial service providers (FSPs)
- Payment service providers (PSPs)

- In-service providers (merchants), including content providers
- Network service providers (NSPs)
- Device manufacturers
- Regulators
- Standardization and industry bodies
- Trusted service managers (TSMs)
- Application developers

23. What are the advantages of M-Payment System?

✓ **Security**: Mobile payments are more secure than traditional credit or debit cards. The retailer's system never has direct access to the cardholder's account number, so current point-of-sale malware doesn't work against it.

✓ **Speed**: Most mobile payments are fast. Customers simply pass their mobile device over a near-field communication (NFC) reader connected to the POS system. Some systems require entering a password or PIN, but others are just scan-and-go.

✓ **Fewer cards to carry around**: Instead of a wallet full of credit cards, customers can simply carry an identification card and mobile device.

✓ **Not limited to POS stations**: Some retailers have already started experimenting with mobile payment kiosks mounted around the retail floor. Customers can avoid long lines and use their mobile devices to pay from anywhere.

✓ **Tested and proven overseas**: Consumers in Kenya, Japan, Hong Kong, and Taiwan have been using mobile payment technology for over a decade. Japanese consumers can use their cell phones to buy at vending machines, ticket booths, and 1.8 million retailers.

24. List out the disadvantages of M-Payment System.

- **Cost**: In most cases, accepting mobile payments requires additional POS hardware. The NFC readers are not cheap, but because of upcoming changes to the credit card system that will start next year, your business will probably need to upgrade soon. The cost of an NFC reader included with the new hardware will probably be much less than current NFC readers.
- **Competing systems**: There are at least three major companies that offer mobile wallet services and dozens of smaller ones. Some systems require NFC readers, while others use bar codes displayed on the screen. A few retailers offer their branded mobile wallets that deduct funds from gift cards.
- **Mobile hardware incompatibility**: Not all systems work with all mobile hardware. Many older and low-end smartphones lack NFC capabilities.
- **Rewards**: Some mobile wallets don't give customers the same rewards as scanning their credit card would. For example, Google Wallet sets up a MasterCard debit account that charges the customer's credit card on the back end. Suppose a customer has a branded rewards card that gives double points for shopping at the issuing retailer. They would not get a double reward since the card was charged by Google and not a retailer.

25. What are the risks associated with M-Payment systems?

- Inability to adapt to mobile payments can put a company at a competitive disadvantage.
- New processes create new security vulnerabilities. Over-the-air provisioning of payment credentials and applications, for example, potentially creates new attack vectors for eavesdroppers to steal and misuse customer data.
- Attackers can steal and misuse data, leading to painful disclosures, adverse publicity, and fines.

- Failure to understand exactly where and how sensitive account data is stored and transmitted can prevent organizations from clearly defining and implementing data protection solutions.
- Rising transaction volumes can lead to performance bottlenecks as inefficient processing limits capacity and degrades the customer experience.
- Overly cumbersome and costly security schemes can hinder an organization's ability to adapt quickly to new opportunities or to scale its business processes to meet rising service demand.

PART – B

1. Explain in detail about the architecture of Mobile Operating system. [U]

Much like the Linux or Windows operating system controls your desktop or laptop computer, a mobile operating system is the software platform on top of which other programs can run on mobile devices. The operating system is responsible for determining the functions and features available on your device, such as thumb wheel, keyboards, WAP, synchronization with applications, email, text messaging and more. The mobile OS will also determine which third-party applications (mobile apps) can be used on your device.

Types of Mobile Operating Systems

When you purchase a mobile device the manufacturer will have chosen the operating system for that specific device. Often, you will want to learn about the mobile operating system before you purchase a device to ensure compatibility and support for the mobile applications you want to use.

2. Explain the components of Mobile Operating Systems. [U] **May/June 2016**
3. Explain the following: [An]
    a) Android OS
    b) Windows Phone OS
    c) Apple IOS
    d) Blackberry OS

Apple products have a strong reputation for security. iOS's walled garden means that iPhones can only run apps that are pre-approved by Apple, whereas Android is an open platform.

Apple also has control over rolling out updates to all iOS devices.

In addition, in terms of user experience for both users and companies, iOS is popular. 78 percent of IT professionals said in a survey by JAMF software in December 2015 that iPhone and iPad are easier to manage than other mobile device platforms.

Due to Apple's popularity within the enterprise, companies have developed many workplace and productivity apps for the platform, so there will be no shortage of tools for your employees using iOS devices.

The main concern about Apple devices is cost. The flagship iPhones can cost over £500 apiece, with the iPhone 6s being sold in some places for around £600, meaning that they are really only suitable as devices for executives or in the small business market.

However, Apple has aimed to address this with some of the products announced at its 21 March event.

The new iPhone SE aims to provide a more affordable smartphone for businesses looking to equip their workforce with fully featured iPhones.

The smaller device claims to offer some fundamentals that may appeal to businesses: faster LTE and wi-fi speeds and better battery life. In terms of specifications, it is the equivalent of the iPhone 5S.

The 16GB model is priced at $399, and the 64GB one at $499.

Apple also cut the price of the Apple Watch at the event, which could see further roll-out in the enterprise as a result.

2. Android

Android devices have a relatively poor reputation for security. There have been several major revelations of vulnerabilities in the Android code such as Stagefright and Certifi-gate.

Android updates have to go through telcos and mobile operators to get to the end-user, which means that a given device has not always got the latest vulnerability patched.

There has been some progress in this area, however. Following the StageFright revelation, Samsung Electronics and Google both announced that they will provide monthly security updates to their devices to tackle security vulnerabilities as and when they arise.

In addition, many of the device makers including Samsung are taking more direct control over the security of their proprietary devices.

For example, Samsung devices are now equipped with Samsung Knox, while LG smartphones, including the V10, G4, G3 and G2, as well as several of its tablets, have LG's Guarded Access to Enterprise (GATE) solution built in. Google also launched the Android for Work platform last year.

Cost-wise, Android devices straddle a broader range than Apple devices, and it is possible to get them far cheaper than the average iPhone. However, it is the premium devices or at least the premium vendors that provide the sort of enterprise-grade security mentioned above. Taking Samsung as an example, a Galaxy S7 will cost £569 and a Galaxy S7 Edge £639.

On user experience, Android also varies considerably because the device makers have so much control over the code. However, the premium devices will again have user experiences that rival Apple's while the lower-end ones may not. Android as a whole is also well served by productivity applications.

Essentially, an Android phone can be as secure and usable as an iPhone but you have to buy the right one, and it is unlikely to be much cheaper.

3. BlackBerry OS

BlackBerry has the strongest reputation for security, especially with the integration of secure containers from Good Technology

Where BlackBerry falls down is in user experience. BlackBerry OS devices are targeted at the enterprise and unlike Apple and the iOS are little used by consumers in their personal lives.

While the high level of control that they provide, including the management capabilities of BlackBerry's enterprise mobility management solution might make them a dream for IT, but this does not necessarily translate for users.

A survey by Computing found that BlackBerry had the strongest disparity between the overall satisfaction levels of end-users and IT, with 61 percent satisfaction in IT and 44 percent for users, a gap of 17 percentage points. iOS and Android had gaps of 1 and 10 respectively.

BlackBerry for example does not necessarily have access to the same apps as iOS and Android.

There have been signs of BlackBerry moving to address this, with a recent update to BBM adding some WhatsApp-esque features. BlackBerry retains a die-hard base of users and the physical keyboard seems to remain an attraction for many who find it difficult to accomplish work tasks using the virtual touch screen keyboard.

Currys currently sells the BlackBerry Classic outright for £299, so it is significantly cheaper than some of the more expensive Apple and Android phones.

4. Windows Phone

Windows Phone is considered very secure, with security experts from Kaspersky having said that the operating system has been clean of malware.

There are several reasons for this. In some ways, Windows Phone has been less of a cyber security target due to its low market penetration.

In the same Computing survey, Windows had a 16 percentage point disparity between the satisfaction of the IT department and that of workers, suggesting that user experience might be a concern since Windows Phone is another operating system that is less used than Android and iOS by consumers.

On the other hand, Microsoft benefits from its apps, which most consumers will be used to using and many of which are essentially the industry standard. These include the Microsoft Office suite, which comes equipped on the devices, as well as communications apps such as Skype.

In terms of cost, Microsoft's devices also span a range; the higher-end Microsoft Lumia 950 is currently selling on the Microsoft website for £419, with its larger 'XL' version selling for £469.99.

There is also the Microsoft Lumia 650, which definitely sits within the range where enterprises might be able to roll it out across their workforce: £159.99.

4. Write short notes on Android SDK. [U] **May/June 2016**

Android Studio is the official integrated development environment for Google's Android operating system, built on JetBrains' IntelliJ IDEA software and designed specifically for Android development. It is available for download on Windows, macOS and Linux based operating systems. It is a replacement for the Eclipse Android Development Tools as the primary IDE for native Android application development.

The **Android SDK** provides you the API libraries and developer tools necessary to build, test, and debug apps for Android.

If you're a new Android developer, we recommend you download the ADT Bundle to quickly start developing apps. It includes the essential Android SDK components and a version of the Eclipse IDE with built-in ADT (Android Developer Tools) to streamline your Android app development.