JAYAM ARTS AND SCIENCE COLLEGE

NALLANUR, DHARMAPURI

SUB.TITLE: MOBILE COMPUTING
PAPER CODE:21UCAE03

UNIT- 1

Introduction - Mobile Computing - Mobile Computing Vs Wireless Networking - Mobile Computing Applications – Characteristic of mobile computing – Structure of Mobile Computing Application. MAC Protocols – Wireless MAC Issues – Fixed Assignment Schemes – Random Assignment Schemes – Reservation Schemes

UNIT- 2

Mobile Internet Protocol and Transport Layer – Over view of Mobile IP – Features of Mobile IP – Key Mechanism in Mobile IP – Route optimization. Overview of TCP/ IP – Architecture of TCP/IP -Adaptation of TCP Window – Improvement inTCP Performance.

UNIT- 3

Mobile Telecommunication System - Global System for Mobile Communication(GSM) – GeneralPacket Radio Service(GPRS) – Universal Mobile Tele communication System(UMTS)

UNIT- 4

Mobile Ad-Hoc Networks – Ad-Hoc Basic Concepts – Characteristic – Applications – DesignIssues – Routing – Essential of Traditional Routing Protocols – Vechicular Ad Hoc Networks (VANET) – MANET Vs VANET – Security.

UNIT- 5

Mobile Platforms and Applications – Mobile Device Operating Systems – Special Constrains & Requirements – Commercial Mobile Operating Systems – Software Development Kit: iOS, Android, BlackBerry, Windows Phone – M-Commerce – Structure – Pros& Cons – Mobile Payment System – Security Issues.

TEXT BOOKS

Prasant Kumar Pattnaik, Rajib Mall, "Fundamentals of Mobile Computing", PHI learning Pvt.Ltd,New Delhi 2012.

REFRENCE BOOKS

- **Jochen H. Schller, "Mobile communications", Pearson Education , New Delhi,2007, 2nd Edition.**

• **Dharma Prakash Agarval, Qing and Ad Zeng, "Wireless and Mobile Systems", Thomson Asia Pvt Ltd.2005.**

UNIT-1

INTRODUCTION

Mobile Computing is a technology that provides an environment that enables users to transmit data from one device to another device without the use of any physical link or cables.

Mobile computing allows transmission of data, voice and video via a computer orany other wireless-enabled device without being connected to a fixed physical link.

In this technology, data transmission is done wirelessly with the help of wirelessdevices such as mobiles, laptops etc.

Mobile computing technology provides a vast coverage diameter for communication. It is one of the fastest and most reliable sectors of the computing technology field.

The concept of Mobile Computing can be divided into three parts:

- Mobile Communication
- Mobile Hardware
- Mobile Software

Mobile Communication

Mobile communication refers to an infrastructure that ensures seamless and reliable communication among wireless devices.

This framework ensures the consistency and reliability of communication betweenwireless devices.

The mobile communication framework consists of communication devices such as protocols, services, bandwidth, and portals necessary to facilitate and support the stated services.

These devices are responsible for delivering a smooth communication process.

Mobile communication can be divided in the following four types:

- Fixed and Wired
- Fixed and Wireless
- Mobile and Wired
- Mobile and Wireless

Fixed and Wired: In Fixed and Wired configuration, the devices are fixed at a position,and they are connected through a physical link to communicate with other devices.

Example, Desktop Computer.

Fixed and Wireless: In Fixed and Wireless configuration, the devices are fixed at a position, and they are connected through a wireless link to make communication with other devices.

Example, Communication Towers, WiFi router

Mobile and Wired: In Mobile and Wired configuration, some devices are wired, andsome are mobile. They altogether make communication with other devices.

Example, Laptops.

Mobile and Wireless: In Mobile and Wireless configuration, the devices can communicate with each other irrespective of their position. They can also connect to any network without the use of any wired device.

Example, WiFi Dongle.

Mobile Hardware

Mobile hardware consists of mobile devices or device components that can be usedto receive or access the service of mobility.

Ex: smartphones, laptops, portable PCs, tablet PCs, Personal Digital Assistants, etc.

MOBILE COMPUTING Vs WIRELESS NETWORKING

The terms "mobile" and "wireless" are often used interchangeably but in reality, they are two very different concepts applied to modern computing and technology.

Mobile is a word that is commonly used to describe portable devices. A mobile device is one that is made to be taken anywhere.

Therefore, it needs an internal battery for power, and must be connected to a modern mobile network that can help it to send and receive data without attaching to a hardware infrastructure.

Wireless, on the other hand, does not mean mobile. Traditional computers or other non-mobile devices can access wireless networks.

One very common example is the use of a localized browser product in a local area network (LAN), where the router takes what used to be a cabled interaction and makes it wireless.

Other kinds of wireless networks called Wide Area Networks(WAN) can even use components of 3G or 4G wireless systems made specifically for mobile devices, but that doesn‘t mean that the devices on these networks are mobile. They may still be plugged in or require proximity to a router or network node.

Mobile and wireless systems accomplish two different things.

A wireless system provides a fixed or portable endpoint with access to a distributed network,

A mobile system offers all of the resources of that distributed network to something that can go anywhere, barring any issues with local reception or technical area coverage.

Difference between mobile and wireless

Think of businesses that offer Wi-Fi hotspots. A Wi-Fi hotspot is typically a resource for someone who has a relatively fixed device, such as a laptop computer that doesn‘t have its own internal Internet access built in.

Mobile devices already have inherent access to the Internet or other wireless

specifically for them. So mobile devices don‘t need Wi-Fi - they already have theirconnections.

APPLICATIONS OF MOBILE COMPUTING

- Web or Internet access.
- Global Position System (GPS).
- Emergency services.
- Entertainment services.
- Educational services.

CHARACTERISTICS OF MOBILE COMPUTING

- **Portability** - The Ability to move a device within a learning environment or todifferent 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 dataunique 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 smartphones 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.

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

- **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,

STRUCTURE OF MOBILE COMPUTING APPLICATION

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 programming languages are used for Mobile Computing applications are:

- Java - J2SE.
- J2ME (Java2 Micro edition)
- JavaCard (Java for smart card)
- 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.

MAC PROTOCOLS

MAC (Medium Access Control) Layer

- MAC layers are above the physical layer, it transmits the frames over the medium and transmits the data by resolving if any issues occur regarding the source and destination address.
- It will specify the channel through which the frames will travel or access the resources, it supports more than one frame at a time.
- Collision-free transmission has happened here when in any situation collision occurs then it will retransmit the frame again to the destination.
- It also prevents transmission errors while transmitting the data and for every frame, it checks for the sequence to maintain the correct sequent order so that the users will receive the correct information

Classification of MAC Protocols

MAC protocols have been divided into 4 types

- Contention-based MAC protocol

- Channel polling-based MAC protocol
- Scheduling-based MAC protocol
- Hybrid MAC protocol

Four types of MAC protocols

- **Contention-based MAC Protocol**
    - It is used for accessibility purposes.
    - To transmit the data from one node to another node, before initiation it will check for the nearest nodes and their positions and also examine thecarrier status.
    - The accessibility of the channel is specified by the carrier status. If the value is ideal, then it can start the transmission of data. If it is not then the node has to wait for a while.
    - This mechanism will reduce the collision and simultaneous accessing of resources. It is flexible even the network grows or shrinks.
    - There is no guarantee of transmission of data and it is solely dependent on the sender. Under contention-based, there are sender-based and receiver-based sender- based transmissions that can start by the sender. The receiver initiates the Connection.

- **Channel polling-based MAC Protocol**
    - There is the keyword “preamble sampling”. Like the above before transmission, the sender will check for the receiver’s availability by sending apreamble.
    - A preamble is a byte that is added with the data packet prefix value. It will help the sender to activate the receiver when it is in sleep mode. If the receiver is active then it will take the packet otherwise this preamble will be in sleep mode. The receiver is in sleep mode until no more activation signals are sent by the sender.
    - This happens on an interval basis. For this scheduling is not needed. All nodes are synchronized. This channel polling is also represented as LPL in BMAC protocol.

- **Scheduling-Based MAC Protocol**
    - A schedule followed by the nodes while transmitting the data, all nodes must follow certain time slots.
    - As it is scheduled one packet will transfer as per the schedule only so there is no collision occurs while transmitting the data. Nodes don’t check for the availability or status of other nodes because they have their time slots. So before going to access the channel first they should get the timeslot.

- It has advantages like reduction of collision, and avoiding the checking of the status receiver randomly.
- It is also associated with the drawbacks like traffic, less throughput, reduce scalability, etc.

- **Hybrid MAC protocol**
  - It is the combination of MAC Protocols. It supports both synchronous and asynchronous.
  - As it is the combination of MAC protocols under this it has the advantage of remaining protocols. It will be like a new approach as it includes more than one MAC protocol.
  - An example of a hybrid MAC protocol is Z-MAC i.e; Zebra MAC.

WIRELESS MAC ISSUES

The three important issues are:

- Half Duplex operation –> either send or receive but not both at a given time
- Time varying channel
- Burst channel errors

- **Half Duplex Operation**

  In wireless, it's difficult to receive data when the transmitter is sending the data, because: When node is transmitting, a large fraction of the signal energy leaks into the receiver path.

  - The transmitted and received power levels can differ by orders of magnitude.

  Collision detection is not possible, while sending data. As collision cannot be detected by the sender, all proposed protocols attempt to minimize the probability of collision - Focus on collision avoidance.

- **Time Varying Channel**

  Three mechanisms for radio signal propagation

  - **Reflection** – occurs when a propagating wave impinges upon an object that has very large dimensions than the wavelength of the radio wave e.g. reflection occurs from the surface of the earth and from buildings and walls.
  - **Diffraction** – occurs when the radio path between the transmitter and the receiver is obstructed by a surface with sharp edges.
  - **Scattering** – occurs when the medium through which the wave travels consists of objects with.

- **Burst Channel Errors**

A consequence of time varying channel and varying signals strengths errors are introduced in the transmission (Very likely) for wire line networks the bit error rate (BER) is the probability of packet error is small .

- Smaller package
- Forward Error Correcting Codes
- Retransmissions (Acks)

FIXED ASSIGNMENT SCHEMES TDMA

Time Division Multiple Access (TDMA) is a digital wireless telephony transmission technique. TDMA allocates each user a different time slot on a given frequency. TDMA divides each cellular channel into three time slots in order to increase the amount of data that can be carried.

Advantages of TDMA:

TDMA can easily adapt to transmission of data as well as voice communication. TDMA has an ability to carry 64 kbps to 120 Mbps of data rates.

TDMA allows the operator to do services like fax, voice band data, and SMS as well as bandwidth-intensive application such as multimedia and video conferencing.

TDMA provides users with an extended battery life, since it transmits only portion of the time during conversations.

TDMA is the most cost effective technology to convert an analog system to digital.

Disadvantages of TDMA

TDMA technology is that the users has a predefined time slot. When moving from one cell site to other, if all the time slots in this cell are full the user might be disconnected.

Another problem in TDMA is that it is subjected to multipath distortion. To overcome this distortion, a time limit can be used on the system. Once the time limit is expired the signal is ignored.

CDMA

- Code Division Multiple Access (CDMA) is a digital wireless technology that uses spread-spectrum techniques.
- CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum.
- Individual conversations are encoded with a pseudo-random digital sequence. CDMA consistently provides better capacity for voice and data communications than other commercial mobile technologies, allowing more subscribers to

connect at any given time, and it is the common platform on which 3G technologies are built.

Advantages of CDMA

- One of the main advantages of CDMA is that dropouts occur only when the phone is at least twice as far from the base station. Thus, it is used in therural areas.
- Another advantage is its capacity; it has a very high spectral capacity that it can accommodate more users per MHz of bandwidth.

Disadvantages of CDMA

Channel pollution, where signals from too many cell sites are present in the subscriber. s phone but none of them is dominant. When this situation arises, the quality of the audio degrades.
When compared to GSM is the lack of international roaming capabilities.

FDMA

FDMA is the process of dividing one channel or bandwidth into multiple individualbands, each for use by a single user.
Each individual band or channel is wide enough to accommodate the signal spectra of the transmissions to be propagated.
The data to be transmitted is modulated on to each subcarrier, and all of them are linearly mixed together.

FDMA divides the shared medium bandwidth into individual channels.
Subcarriers modulated by the information to be transmitted occupy each sub channel.
The best example of this is the cable television system. The medium is a single coax cable that is used to broadcast hundreds of channels of video/audio programming to homes.
The coax cable has a useful bandwidth from about 4 MHz to 1 GHz. This bandwidth is divided up into 6-MHz wide channels. Initially, one TV station or channel used a single 6-MHz band.
But with digital techniques, multiple TV channels may share a single band today thanks to compression and multiplexing techniques used in each channel.
This technique is also used in fibre optic communications systems. A single fibre optic cable has enormous bandwidth that can be subdivided to provide FDMA.
FDMA is called wavelength division multiple access (WDMA) or just wavelength division multiplexing (WDM).
One of the older FDMA systems is the original analog telephone system, which used a hierarchy of frequency multiplex techniques to put multiple telephone calls on single line. The analog 300-Hz to 3400-Hz voice signals were used to modulate subcarriers in 12 channels from 60 kHz to 108 kHz. Modulator/mixers

created single sideband (SSB) signals, both upper and lower sidebands. These subcarriers were then further frequency multiplexed on subcarriers in the 312-kHz to 552-kHz range using the same modulation methods.

SDMA

- Space-division multiple access (SDMA) is a channel access method based on creating parallel spatial pipes next to higher capacity pipes through spatial multiplexing and/or diversity, by which it is able to offer superior performance in radio multiple access communication systems.

In traditional mobile cellular network systems, the base station has no information on the position of the mobile units within the cell and radiates the signal in all directions within the cell in order to provide radio coverage. This results in wasting power on transmissions when there are no mobile units to reach, in addition to causing interference for adjacent cells using the same frequency, so called co-channel cells.

Likewise, in reception, the antenna receives signals coming from all directions including noise and interference signals. By using smart antenna technology and differing spatial locations of mobile units within the cell, space-division multiple access techniques offer attractive performance enhancements.

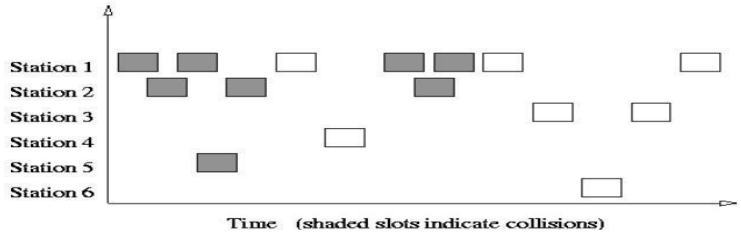
The radiation pattern of the base station, both in transmission and reception, is adapted to each user to obtain highest gain in the direction of that user.

This is often done using phased array techniques. In GSM cellular networks, the base station is aware of the distance (but not direction) of a mobile phone by use of a technique called "timing advance" (TA). The base transceiver station (BTS) can determine how distant the mobile station (MS) is by interpreting the reported TA.

RANDOM ASSIGNMENT SCHEMES

Pure Aloh

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.



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.

There Are Three Different Type of CSMA Protocols

- I-persistent CSMA
- (ii) Non- Persistent CSMA
- (iii) p-persistent 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.

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.

- **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

- **-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.

RESERVATION BASED SCHEMES

Polling

- Polling is the process where the computer or controlling device waits for an external device to check for its readiness or state, often with low-level hardware.
- Polling is sometimes used synonymously with busy-wait polling.
- In this situation, when an I/O operation is required, the computer does nothing other than check the status of the I/O device until it is ready, at which point the device is accessed.

Token Bus

- Token Bus is described in the IEEE 802.4 specification, and is a Local Area Network (LAN) in which the stations on the bus or tree form a logical ring.
- Each station is assigned a place in an ordered sequence, with the last station in the sequence being followed by the first, as shown below. Each station knows the address of the station to its "left" and "right" in the sequence.

- This type of network, like a Token Ring network, employs a small data frame only a few bytes in size, known as a token, to grant individual stations exclusive access to the network transmission medium.
- Token-passing networks are deterministic in the way that they control access to the network, with each node playing an active role in the process

**********UNIT- I **********

UNIT-2

MOBILE INTERNET PROTOCOL

Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue withoutthe user's sessions or connections being dropped.

Key Mechanisms in Mobile IP:

- **Agent Discovery:** Agents advertise their presence by periodically broadcastingtheir agent advertisement messages.
  The mobile node receiving the agent advertisement messages observes whether the message is from its own home agent and determines whether it is inthe home network or foreign network.

- **Agent Registration:** Mobile node after discovering the foreign agent sends a registration request (RREQ) to the foreign agent. The foreign agent, in turn, sendsthe registration request to the home agent with the care-of-address..

  - **Tunneling:** It establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation

TRANSPORT LAYER

The transport Layer is the second layer in the TCP/IP model and the fourth layer in the OSI model HYPERLINK "https://www.geeksforgeeks.org/layers-of-osi-model/". It is an end-to-end layer used to deliver messages to a host.

It is termed an end-to-end layer because it provides a point-to-point connection rather than hop-to-hop, between the source host and destination host to deliver the services reliably.

Responsibilities of a Transport Layer

- The Process to Process Delivery
- End-to-End Connection between Hosts
- Multiplexing and Demultiplexing
- Congestion Control
- Data integrity and Error correction
- Flow control

OVERVIEW OF MOBILE IP

Mobile IP (Internet Protocol) enables the transfer of information to and from mobilecomputers, such as laptops and wireless communications

Mobile IP Functional Entities

Mobile IP introduces the following new functional entities:

- **Mobile Node (MN)**-Host or router that changes its point of attachment from one network to another.
- **Home Agent (HA)**-Router on a mobile node's home network that intercepts datagrams destined for the mobile node, and delivers them through the care-ofaddress. The home agent also maintains current location information for the mobile node.
- **Foreign Agent (FA)**-Router on a mobile node's visited network that provides routing services to the mobile node while the mobile node is registered.

FEATURES OF MOBILE IP

- **Roaming Connectivity**

  - Mobile IP allows mobile devices to connect to the Internet when they are not at their home network. This lets laptops connect to hotspots and it lets phones connect through 3G and other Internet network sources.
  - An IP address lets a network know where to send and receive information from on a network. Mobile IP uses an address that references its home network while finding a location on the newnetwork.

  This keeps Mobile IP from knocking other computers off of a network, because each computer comes from a unique network and has a unique number.

- **Compatibility**

  Mobile IP is compatible with most networks that offer the Internet. This include the 3G network used for mobile televisions; Internet hotspots found in cafes, airports and book stores; and all homenetwork devices.

  Early attempts at Mobile IP would only work with certain routers or certain types of networks.

  Mobile IP today has no special requirements because the system is universal and fits within the original IP infrastructure.

Tunnelling and Reverse Tunnelling

The method by which mobile IP receives information from a network is called tunnelling.

A network cannot directly send information to a mobile IP device. In order to get this information the mobile device must create an IP address within its new IP address.
This allows the network to send information to the IP address through the tunnel of the two new IPs.
Firewalls and routers can sometimes block tunnelling by enabling what is called ingress filtering. Mobile IP also can use the process of reverse tunnelling, which is a similar process that reverses the flow of information to achieve the same result as tunnelling.

Cordless

- The greatest feature of Mobile IP is that there are no cords needed to complete the network connection.

- The standard IP required that networks be connected by a phone line or Ethernet cord. With Mobile IP, the device finds the network automatically and attempts to establish a connection.
- Some mobile capable devices like laptop computers have the ability to connect using the Mobile IP or using the standard IP with an Ethernet or phone cord.

KEY MECHANISM IN MOBILE IP

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

• **Agent Discovery** - A Mobile Node discovers its Foreign and Home Agents during agent discovery.

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

• **Tunnelling** - A reciprocal tunnel is set up by the Home Agent to the care-of address (current location of the Mobile Node on the foreign network) to route packets to the Mobile Node as it roams.

• **Agent Discovery**

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)

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.
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

- **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.
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

- **Tunnelling**

Tunnelling has two primary functions: encapsulation of the data packet to reach the tunnel endpoint, and decapsulation when the packet is delivered at that endpoint. The default tunnel mode is IP Encapsulation within IP Encapsulation. Optionally, GRE and minimal encapsulation within IP may be used.Typically, the Mobile Node sends packets to the Foreign Agent, which routes them to their final destination, the Correspondent Node, as shown in Figure 2.

- A feature called reverse tunnelling solves this problem by having the Foreign Agenttunnel packets back to the Home Agent when it receives them from the Mobile Node.

ROUTE OPTIMIZATION

Mobile IPv4 route optimization

Mobile IPv4 route optimization is a proposed extension to the Mobile IPv4protocol. It provides enhancements to the routing of data grams between the mobile nodeand to the correspondent node.

The enhancements provide means for a correspondent node to tunnel datagrams directly to the mobile node or to its foreign agent care-of address.

Route optimization messages and data structures

The route optimization extension adds a conceptual data structure, the bindingcache, to the correspondent node and to the foreign agent.
The binding cache contains bindings for mobile nodes' home addresses andtheir current care-of addresses.
With the binding the correspondent node can tunnel data grams directly to themobile node's care-of address.
Direct routing with route optimization and foreign agent care-of address.

Smooth handoffs with route optimization

The static case the protocol is fairly simple, but handoffs somewhat complicate the situation.
When the correspondent node has an out of date entry for the mobile node's care-of address it tries to send the tunnelled datagram to the mobile node's previous location and the datagram is lost.

- To solve this problem the protocol includes the previous foreign agent notification mechanism, which adds a binding cache to the foreign agent.

OVERVIEW OF TCP / IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

TCP/IP is a two-layer program.

The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.

TCP/IP Protocols for the Web

Web browsers and servers use TCP/IP protocols to connect to the Internet. CommonTCP/IP protocols are:

- **HTTP - Hyper Text Transfer Protocol**

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

- **HTTPS - Secure HTTP**
  - HTTPS takes care of secure communication between a web server and a web browser. HTTPS typically handles credit card transactions and other sensitive data.
- **FTP - File Transfer Protocol**
  - FTP takes care of transmission of files between computers.

ARCHITECTURE OF TCP / IP

- The physical layer covers the physical interface between a data transmissiondevice (such as a workstation or computer) and a transmission medium or network.
- This layer is concerned with specifying the characteristics of the transmission medium, the nature of the signals, the data rate, and related matters.

- The network access layer is concerned with the exchange of data between an end system and the network to which it's attached. The sending computer must provide the network with the address of the destination computer, so that the network can route the data to theappropriate destination.

  The specific software used at this layer depends on the type of network to be used; different standards have been developed for circuit-switching, packet- switching (for example, frame relay), local area networks (such as Ethernet), and others.

- The network access layer is concerned with access to and routing data across anetwork for two end systems attached to the same network.

- The Internet protocol (IP) is used at this layer to provide the routing function across multiple networks. This protocol is implement not only in the end systems but also in routers. A router is a processor that connects two networks; its primary function is to relay data from one network to the other on its route from the source to the destination end system.

- Finally, the application layer contains the logic needed to support the various user applications. For each type of application, such as file transfer, a separate module is needed that's peculiar to that application.

ADAPTATION OF TCP WINDOW

- The first phase of a TCP session is establishment of the connection.
- This requires a three-way handshake, ensuring that both sides of the connection have an unambiguous understanding of the sequence number space of the remote side for this session.

- The local system sends the remote end an initial sequence number to the remote port, using a SYN packet.
  - The remote system responds with an ACK of the initial sequence number and the initial sequence number of the remote end in a response SYN packet.
- The local end responds with an ACK of this remote sequence number.
- The performance implication of this protocol exchange is that it takes one and a half round-trip times (RTTs) for the two systems to synchronize state before any data can be sent.

  - The TCP protocol manages the reliable exchange of data between the two systems.
  - The algorithms that determine the various retransmission timers have been redefined numerous times.
  - TCP is a sliding-window protocol, and the general principle of flow control is based on the management of the advertised window size and the management of retransmission timeouts, attempting to optimize protocol performance within the observed delay and loss parameters of the connection.
  - Tuning a TCP protocol stack for optimal performance over a very low- delay, high-bandwidth LAN requires different settings to obtain optimal performance over a dialup Internet connection, which in turn is different for the requirements of a high-speed wide-area network.
  - TCP attempts to discover the delay bandwidth product of the connection, and attempts to automatically optimize its flow rates within the estimated parameters of the network path, some estimates will not be accurate, and the corresponding efforts by TCP to optimize behavior may not be completely successful.
  - Another critical aspect is that TCP is an adaptive flow-control protocol. TCP uses a basic flow-control algorithm of increasing the data-flow rate until the network signals that some form of saturation level has been reached (normally indicated by data loss).
  - When the sender receives an indication of data loss, the TCP flow rate is reduced; when reliable transmission is reestablished, the flow rate slowly increases again.

  - If no reliable flow is reestablished, the flow rate backs further off to an initial probe of a single packet, and the entire adaptive flow- control process starts again.This process has numerous results relevant to service quality.

- First, TCP behaves adaptively , rather than predictively . The flow- control algorithms are intended to increase the data-flow rate to fill all available network path capacity, but they are also intended to quickly back off if the available capacity changes because of interaction with other traffic, or if a dynamic change occurs in the end-to-end network path.

IMPROVEMENT IN TCP PERFORMENCE

The protocols to improve the performance of TCP are:

Link-layer protocols

- There have been several proposals for reliable link-layer protocols.
- The two main classes of techniques employed by these protocols are:
    - Error correction (using techniques such as forward error correction (FEC)),
    - Retransmission of lost packets in response to automatic repeatrequest (ARQ) messages.

Indirect-TCP (I-TCP) protocol

- One of the early protocols to use the split-connection approach.
- It involves splitting each TCP connection between a sender and receiver into two separate connections at the base station — one TCP connection between the sender and the base station, and the other between the base station and the receiver.
- Classification of protocols, TCP is a split-connection solution that uses regular TCP for its connection over wireless link

The Snoop Protocol

- The snoop protocol introduces a module, called the snoop agent, at the base station.

- The agent monitors every packet that passes through the TCP connection in both directions and maintains a cache of TCP segments sent across the link that have not yet been acknowledged by the receiver.
- A packet loss is detected by the arrival of a small number of duplicate acknowledgments from the receiver or by a local timeout.
- The snoop agent retransmits the lost packet if it has it cached and suppresses the duplicate acknowledgments.
- In classification of protocols, the snoop protocol is a link-layer protocol that takes advantage of the knowledge of the higher-layer transport protocol (TCP).
- The main advantage of this approach is that it suppresses duplicate acknowledgments for TCP segments lost and retransmitted locally, thereby avoiding unnecessary fast retransmissions and congestion control invocations by the sender.

********** UNIT - II**********

UNIT-3

Mobile Telecommunications System

The Universal Mobile Telecommunications System (UMTS) is a broadband, packet-based, 3G mobile cellular system based upon GSM standards. The specifications of UMTS covers the entire network system, including the radio access network, the corenetwork and user authentication.

Features

- UMTS is a component of IMT-2000 standard of the International Telecommunications Union (ITU), developed by 3GPP.
- It uses wideband code division multiple access (W-CDMA) air interface.
- It provides transmission of text, digitized voice, video and multimedia.
- It provides high bandwidth to mobile operators.
- It gives a high data rate of 2Mbps. For High-Speed Downlink Packet Access (HSDPA) handsets, the data-rate is as high as 7.2 Mbps in the downlink connection.
- It is also known as Freedom of Mobile Multimedia Access (FOMA).
- It encompasses specifications for the entire mobile network system –
- Radio access network specified by UTRAN (UMTS Terrestrial Radio Access Network)
- Core network specified by MAP (Mobile Application Part)
- Authentication of the users by SIM (Subscriber Identity Module) cards.

Universal Mobile Telecommunications System (UMTS)
architectureUE: user equipment;
USIM: UMTS subscriber identity module ; ME: mobile equipment; RNC: radio network controller; MSC/VLR: mobile switching center/visitor location register; GMSC: gateway mobile switching center; PSTN: public switched telephone network; PLMN: public landmobile network ; ISDN: integrated services digital network; HLR/AuC: home location register/authentication center

GSM –Global system for mobile communication

GSM stands for **Global System for Mobile Communication.**
GSM is an open and digital cellular technology used for mobile communication.
It uses 4 different frequency bands of 850 MHz, 900 MHz, 1800 MHz and1900 MHz .
It uses the combination of FDMA and TDMA. This article includes all the concepts of GSM architecture and how it works.

GSM is having 4 different sizes of cells are used in GSM :

- Macro : In this size of cell, Base Station antenna is installed.
- Micro : In this size of cell, antenna height is less than the average roof level.
- Pico : Small cells' diameter of few meters.
- Umbrella : It covers the shadowed (Fill the gaps between cells) regions.

Features of GSM are :

- Supports international roaming
- Clear voice clarity
- Ability to support multiple handheld devices.
- Spectral / frequency efficiency
- Low powered handheld devices.
- Ease of accessing network
- International ISDN compatibility.
- Low service cost.
- New features and services.

GSM is nothing but a larger system which is divided into further 3 subsystems.

- **BSS :** BSS stands for Base Station Subsystem. BSS handles traffic and signaling between a mobile phone and the network switching subsystem.BSS having two components **BTS** and **BSC.**

- **NSS :** NSS stands for Network and Switching Subsystem. NSS is the core network of GSM. That carried out call and mobility management functions formobile phone present in network. NSS have different components like **VLR, HLR** and **EIR.**
- **OSS :** OSS stands for Operating Subsystem. OSS is a functional entity which the network operator monitor and control the system. **OMC** is the partof OSS. Purpose of OSS is to offer the customer cost-effective support for allGSM related maintenance services.

Suppose there are 3 Mobile stations which are connected with the tower andthat tower is connected to BTS through TRX, then further connected to BSC and MSC.

The functionality of different components.

- **MS :** MS stands for Mobile System. MS comprises user equipment and software needed for communication with a mobile network.

Mobile Station (MS)= Mobile Equipment(ME) + Subscriber Identity Module (SIM). Now, these mobile stations are connected to tower and that tower connected with BTS through TRX. TRX is a transceiver which comprises transmitter and receiver. Transceiver has two performance of sending and receiving.

- **BTS :** BTS stands for Base Transceiver Station which facilitates wireless communication between user equipment and a network. Every tower has BTS.

- **BSC :** BSC stands for Base Station Controller. BSC has multiple BTS. Youcan consider the BSC as a local exchange of your area which has multiple towers and multiple towers have BTS.

- **MSC :** MSC stands for Mobile Switching Center. MSC is associated with communication switching functions such as call setup, call release and routing.Call tracing, call forwarding all functions are performed at the MSC level. MSCis having further components like VLR, HLR, AUC, EIR and PSTN.

    - **VLR :** VLR stands for Visitor Location Register. VLR is a database which contains the exact location of all mobile subscribers currently present in the service area of MSC. If you are going from one state toanother state then your entry is marked into the database of VLR.

  HLR : HLR stands for Home Location Register. HLR is a database containing pertinent data regarding subscribers authorized to use a GSM network.. If you purchase SIM card from in the HLR. HLR is like a home which contains all data like your ID proof, which plan you are taking, whichcaller tune you are using etc.

  AUC : AUC stands for Authentication Center. AUC authenticates the mobile subscriber that wants to connect in the network.

  EIR : EIR stands for Equipment Identity Register. EIR is a database that keeps the record of all allowed or banned in the network. If you are bannedin the network then you can't enter the network, and you can't make the calls.

  PSTN : PSTN stands for Public Switched Telephone Network. PSTN connects with MSC. PSTN originally a network of fixed line analog telephonesystems. Now almost entirely digital in its core network and includes mobile and other networks as well as fixed telephones. The earlier landline phones which places at our home is nothing but PSTN.

- **OMC** : OMC stands for Operation Maintenance Center. OMC monitor and maintain the performance of each MS, BSC and MSC within a GSM system. Three subsystem BSS, NSS and OSS are connected with each other via someinterfaces. Total three interfaces are there:

- **Air Interface :** Air interface is also known as UM interface.
  Interface between MS and BTS is called as UM interface because it ismobile analog to the U interface of ISDN.
- **Abis Interface :** It is a BSS internal interface linking with BTS and BSC.
- **A interface :** It provides communication between BSS and MSC.

Services of GSM:

- **Bearer services/ data services:**

GSM specifies different mechanism for data transmission, The originalGSM allowing for data rates of up to 9600 bits/s.

Bearer services permit transparent or non transparent data transmission.

Transparent bearer services:

Transparent bearer services only use the physical layer to transmitdata. Data transmission has a constant delay at throughput if no transmission error occurs.

Non-transparent bearer services:

Non-transparent bearer services use protocols of layer two and threetwo three to implement error correction and flow control.(data link layer and network layer).

- **Tele services**:

  Tele services are nothing but we use now as at also.

  Video calls.
  Video text and face
  emoji. short text
  message(SMS).

- **Supplementary services:**

  supplementary services it means advanced services.

  Conference
  calls. Call
  waiting.
  Call forwarding.

GSM security:

GSM offers several security using confidential information stored in the AUCand in the individual SIM.
The SIM stores personal secret data and is protected with a pin against unauthorized use.

Advantages:

Compatibility: GSM is widely used around the world, so it is compatible withmany different networks and devices.
Security: GSM offers enhanced security features such as authentication, encryption and confidentiality, which helps to protect the user's privacy anddata.

Efficient use of bandwidth: GSM uses a time-division multiplexing (TDM) technique which enables many users to share the same frequency channel atdifferent times, making it an efficient use of the available bandwidth.

Roaming: GSM allows users to roam internationally and use their mobile phones in other countries that use the same GSM standard.
Wide range of features: GSM supports a wide range of features, including call forwarding, call waiting, voicemail, conference calling, and more.

Disadvantages:

Limited coverage: GSM networks may have limited coverage in some remoteareas, which can make it difficult for users to make calls or access the internet.**Network congestion:** GSM networks may become congested during peak hours, which can lead to dropped calls or poor call quality.
Security vulnerabilities: Although GSM offers enhanced security features, it isstill vulnerable to certain types of attacks, such as eavesdropping and spoofing.**Data transfer speed:** GSM networks offer relatively slow data transfer speeds compared to newer technologies such as 3G and 4G.
Limited capacity: GSM networks have a limited capacity for handling large volumes of data, which can be a disadvantage for users who require high- speed internet access or other data-intensive applications.

GPRS- General Packet Radio System

General Packet Radio System is also known as **GPRS** is a third-generation step toward internet access. GPRS is also known as GSM-IP that is a Global-System Mobile Communications Internet Protocol as it keeps the users of this system online, allows to make voice calls, and access internet on-the-go.

Even Time-Division Multiple Access (TDMA) users benefit from this system as it provides packet radio access.

GPRS also permits the network operators to execute an Internet Protocol (IP) based core architecture for integrated voice and data applications that will continue to be used and expanded for 3G services.

GPRS supersedes the wired connections, as this system has simplified access to the packet data networks like the internet. The packet radio principle is employed by GPRS to transport user data packets in a structure way between GSM mobile stations and external packet data networks.

These packets can be directly routed to the packet switched networks from the GPRS mobile stations.

In the current versions of GPRS, networks based on the Internet Protocol (IP) like the global internet or private/corporate intranets and X.25 networks are supported.

Who owns GPRS ?

The GPRS specifications are written by the European Telecommunications Standard Institute (ETSI), the European counterpart of the American National Standard Institute (ANSI).

Key Features

Following three key features describe wireless packet data:

The always online feature - Removes the dial-up process, making applicationsonly one click away.
An upgrade to existing systems - Operators do not have to replace theirequipment; rather, GPRS is added on top of the existing infrastructure.
An integral part of future 3G systems - GPRS is the packet data core networkfor 3G systems EDGE and WCDMA.

Goals of GPRS

GPRS is the first step toward an end-to-end wireless infrastructure and has the following goals:

Open architecture
Consistent IP
services
Same infrastructure for different air
interfaces Integrated telephony and
Internet infrastructure Leverage
industry investment in IP
Service innovation independent of infrastructure

Benefits of GPRS

Higher Data Rate

GPRS benefits the users in many ways, one of which is higher data rates in turn of shorter access times. In the typical GSM mobile, setup alone is a lengthy process and equally, rates for data permission are restrained to 9.6 kbit/s. The session establishment time offered while GPRS is in practice is lower than one second and ISDN-line data rates are up to many 10 kbit/s.

Easy Billing

GPRS packet transmission offers a more user-friendly billing than that offered by circuit switched services. In circuit switched services, billing is based on the duration of the connection. This is unsuitable for applications with bursty traffic. The user must pay for the entire airtime, even for idle periods when no packets are sent (e.g., when the user reads a Web page).

In contrast to this, with packet switched services, billing can be based on the amount of transmitted data. The advantage for the user is that he or she can be "online" over a long period of time but will be billed based on the transmitted data volume.

UMTS(Universal Mobile Telecommunication System

UMTS or **Universal Mobile Telecommunications Framework**, is the 3G successor to the GSM family of measures counting GPRS and EDGE.

3G UMTS employments a completely diverse radio interface based around the utilize of Coordinate Grouping Spread Range as CDMA orCode Division Multiple Access.

Although 3G UMTS employments a completely distinctive radio get to standard, the center arrange is the same as that utilized for GPRS and EDGE to carry partitioned circuit exchanged voice and bundle data.

UMTS employments a wideband adaptation of CDMA possessing a 5 MHz wide channel.

Being more extensive than its competition CDMA2000 which as it was utilized a 1.25MHz channel, the tweak conspire was known as widebandCDMA or WCDMA/W-CDMA.

This title was regularly utilized to allude to the total framework. It could bea frame of media transmission utilized for remote gathering and transmission.

It is an advancement in speed boost from the more seasoned 2G standard of transmission speed and can increment information transmission times between gadgets and servers.

UMTS Applications

Streaming / Download (Video, Audio)
Videoconferences.
Fast Internet / Intranet.
Mobile E-Commerce (M-Commerce)
Remote Login
Background Class
applications Multimedia-
Messaging, E-Mail

- FTP Access
- Mobile Entertainment (Games)

Features of UMTS

- UMTS could be a component of IMT-2000 standard of the Universal Broadcast communications Union (ITU), created by 3GPP.

- It employments wideband code division multiple access (W-CDMA) discuss interface.
- It gives transmission of content, digitized voice, video and multimedia.
- It gives tall transmission capacity to portable operators.
- It gives a tall information rate of 2Mbps.
- For High-Speed Downlink Parcel Get to (HSDPA) handsets, the data-rate isas tall as 7.2 Mbps within the downlink connection.

It is additionally known as Flexibility of Mobile Multimedia Access (FOMA).

Advantages of UMTS

UMTS could be a successor to 2G based GSM advances counting GPRS and EDGE . Gaining a 3rd title 3GSM since it could be a 3G relocation for GSM
Support 2Mbit/s information rates.
Higher Information rates at lower incremental costs.
Benefits of programmed universal wandering also necessarily security and charging capacities, permitting administrators emigrate from 2G to 3G whereas holding numerous of their existing back-office frameworks
Gives administrators the adaptability to present unused mixed media administrations to trade clients and buyers
This not as it were gives client a valuable phone but moreover deciphershigher incomes for the administrator.

Disadvantages of UMTS

It is more expensive than GSM.
Universal Mobile Telecommunication System has poor video experience.
Universal Mobile Telecommunication System still not broadband.

Comparison of GSM and UMTS

Features	**GSM**	**UMTS**
Network Architecture	Circuit-switched	Circuit-switched and packet-switched
Radio Access Technology	FDMA and TDMA	Wideband CDMA (W-CDMA)
Bandwidth	200 kHz	5 MHz
Data Rate	Up to 384 kbps	Up to 2 Mbps for HSDPA; up to 7.2 Mbps forHSDPA
Applications	Voice and SMS	Multimedia applications
Roaming Support	Limited	Automatic international roaming
Video Quality	Poor	Improved compared to GSM
Cost	Affordable	More expensive than GSM
Broadband	Not broadband	Offers broadband capabilities

********** UNIT - III **********

UNIT-4

Mobile Ad hoc Network (MANET)

- MANET stands for Mobile Adhoc Network also called a wireless Adhoc network or Adhoc wireless network that usually has a routable networking environment on top of a Link Layer ad hoc network.
- They consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently.
- Each node behaves as a router as they forward traffic to other specifiednodes in the network.
- MANET may operate a standalone fashion or they can be part of larger internet.
- They form a highly dynamic autonomous topology with the presence ofone or multiple different transceivers between nodes.
- The main challenge for the MANET is to equip each device to continuously maintain the information required to properly route traffic.MANETs consist of a peer-to-peer, self-forming, self-healing network MANET's circa 2000-2015 typically communicate at radio frequencies (30MHz-5GHz).
- This can be used in road safety, ranging from sensors for the environment, home, health, disaster rescue operations, air/land/navydefense, weapons, robots, etc.

Characteristics of MANET

- **Dynamic Topologies:**
  Network topology which is typically multihop may change randomly and rapidly with time, it can form unidirectional or bi-directional links.
- **Bandwidth constrained, variable capacity links:**
  Wireless links usually have lower reliability, efficiency, stability, and capacityas compared to a wired network

  Autonomous Behavior:
  Each node can act as a host and router, which shows its autonomousbehavior.

  Energy Constrained Operation:
  As some or all the nodes rely on batteries or other exhaustible means for their energy. Mobile nodes are characterized by less memory, power, andlightweight features.

  Limited Security:
  Wireless networks are more prone to security threats. A centralized firewall is absent due to the distributed nature of the operation for security, routing, and host configuration.

  Less Human Intervention:

They require minimum human intervention to configure the network, therefore they are dynamically autonomous in nature.

Pros and Cons of MANET –

Pros:

- Separation from central network administration.
- Each node can play both the roles ie. of router and host showing autonomous nature.
- Self-configuring and self-healing nodes do not require human intervention.
- Highly scalable and suits the expansion of more network hub.

Cons:

- Resources are limited due to various constraints like noise, interference conditions, etc.
- Lack of authorization facilities.
- More prone to attacks due to limited physical security.
- High latency i.e. There is a huge delay in the transfer of data between two sleeping nodes.

Improvement in MANET:

- **Quality of Service (QoS):** Researchers are working to improve the qualityof service of MANET by developing efficient routing protocols that provide better bandwidth, throughput, and latency.
- **Security:** To ensure the security of the MANET, researchers are developing efficient security mechanisms that provide encryption, authentication, and authorization facilities.
- **Power management:** To enhance the lifetime of MANET nodes, researchers are working on developing efficient power management techniques that reduce the energy consumption of nodes.
- **Multimedia support:** Researchers are working to provide multimedia support to MANET by developing efficient routing protocols that can handlemultimedia traffic efficiently.
- **Standardization:** To ensure the interoperability of different MANET devices, researchers are working on developing standard protocols and interfaces that can be used by different MANET devices.

Mobile Adhoc Network (MANET) is a wireless network made up of a collection of mobile nodes connected wirelessly and free of any fixed infrastructure.
It is self-configuring and self-healing. MANET provides a lot of benefits,but it also has several drawbacks that need to be fixed

Advantages:

Flexibility: MANETs are highly flexible, as they can be easily deployed in various environments and can be adapted to different applications and scenarios. This makes them ideal for use in emergency situations or militaryoperations, where there may not be a pre-existing network infrastructure.

Scalability: MANETs can easily scale to accommodate a large number of nodes, making them suitable for large-scale deployments. They can also handledynamic changes in network topology, such as the addition or removal of nodes.

Cost-effective: Since MANETs do not require any centralized infrastructure, they are often more cost-effective than traditional wired or wireless networks.They can also be used to extend the range of existing networks without the need for additional infrastructure.

Rapid Deployment: MANETs can be rapidly deployed in areas where infrastructure is not available, such as disaster zones or rural areas.

Disadvantages:

Security: MANETs are vulnerable to security threats, such as attacks by malicious nodes, eavesdropping, and data interception. Since the network is decentralized, there is no central authority to ensure the security of the network.

Reliability: MANETs are less reliable than traditional networks, as they are subject to interference, signal attenuation, and other environmental factors thatcan affect the quality of the connection.

Bandwidth: Since MANETs rely on wireless communication, bandwidth can be limited. This can lead to congestion and delays, particularly when multiple nodes are competing for the same channel.

Routing: Routing in MANETs can be complex, particularly when dealing withdynamic network topologies. This can result in inefficient routing and longer delays in data transmission.

Power Consumption: Since MANETs rely on battery-powered devices, power consumption can be a significant issue. Nodes may need to conserve power toextend the life of the battery, which can limit the amount of data that can be transmitted.

ADHOC BASIC CONCEPTS

A wireless ad hoc network (WANET) is a decentralized type of wireless network.
The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks.

- Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity.

- To the classic routing, ad hoc networks can use flooding for forwarding data. Wireless mobile ad hoc networks are self-configuring, dynamic networks in which nodes are free to move.
- Wireless networks lack the complexities of infrastructure setup and administration, enabling devices to create and join networks "on the fly" - anywhere, anytime.
- A wireless ad-hoc network, also known as IBSS - Independent Basic Service Set, is a computer network in which the communication links are wireless.

- The network is ad-hoc because each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity.

- This is in contrast to older network technologies in which some designated nodes, usually with custom hardware and variously known as routers, switches, hubs, and firewalls, perform the task of forwarding the data.

- Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts.

- The earliest wireless ad-hoc networks were called "packet radio" networks, and were sponsored by Defense Advanced Research Projects Agency (DARPA) in the early 1970s.

- Bolt, Beranek and Newman Technologies (BBN) and SRI International designed, built, and experimented with these earliest systems.
- Experimenters included Jerry Burchfield, Robert Kahn, and Ray Tomlinson of later TEN-EXtended (TENEX), Internet and email fame.
- Similar experiments took place in the Ham radio community. It is interesting to note that these early packet radio systems predated the Internet, and indeed were part of the motivation of the original Internet Protocol suite.

- Later DARPA experiments included the Survivable Radio Network (SURAN) project, which took place in the 1980s.

- Another third wave of academic activity started in the mid-1990s with the advent of inexpensive 802.11 radio cards for personal computers. Current wireless ad-hoc networks are designed primarily for military utility.

CHARACTERISTIC

The characteristics are:

- In MANET, each node act as both host and router. That is it is autonomous in behaviour.

Multi-hop radio relaying- When a source node and 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 with less memory, power and light weight features.

- The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.

- Mobile and spontaneous behaviour 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.

Distributed operation: There is no background network for the central control of the network operations, the control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.

Multi hop routing: When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router.

Dynamic topology: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network.

Light-weight terminals: In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

Shared Physical Medium: The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

Applications of Ad hoc network

- The large number of small size gadgets also as advancement in remote communication, the ad hoc networking is picking up exertion with the large number of far reaching applications.
- Ad hoc networking can be utilized whenever, any place with restricted orthen again no correspondence framework.
- The first framework is extravagant or irritating to utilize. The ad hoc network architecture can be utilized continuous business applications, corporate organizations to expand the efficiency and benefit.

The ad hoc networks can be arranged by their application as :

Mobile Ad hoc Network (MANET) which is a self-organizing infrastructureless system of cell phones communicated through remote connection.
Vehicular Ad hoc Network (VANET) utilizes vehicles as nodes in a networkto make a mobile network.
Wireless Sensor Network (WSN) comprises of independent sensors tocontrol the ecological activities.

Usages of Ad-Hoc network :

Military – An ad hoc networking will give access to the army to maintain an network among all the soldiers, vehicles and headquarters.
Personal area network (PAN) – It is a short range, local network whereeach nodes are usually related with a given range.
Crisis Condition – Because it is fairly easy to create it can be used in timeof crisis to send emergency signals.
Medical Application – It can use to monitor patient.
Environmental Application – It can be used to check weather condition, forest fire, tsunami etc.

Problems : There are several problems that Ad Hoc network faces –

Limited wireless range
Packet losses
– Energy conservation because of limited batteries. – Low-quality communications.

- Hidden-node problem creates collision if two device try to communicate withsame receiver.

- Exposed-node problem.
- Lack of security
- Addressing and service discovery
- Multicasting
- Deployment Considerations

DESIGN ISSUES

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 behaviour 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 partition of the network. This mostly affects the intermediate nodes.

- Limited bandwidth: Wireless link continue to have significantly lower capacity than infra structured networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access,

fading, noise, and interference conditions, etc., is often much less than a radio‘s maximum transmission rate.

- Dynamic topology: Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.

Routing Overhead: In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

Hidden terminal problem: The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

Packet losses due to transmission errors: Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, frequent path breaks due to mobility of nodes.

Mobility-induced route changes: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.

Battery constraints: Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.

Security threats: The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.

Routing In Ad Hoc Networks

- Routing in Ad-hoc networks
- Proactive routing protocols
  - DSDV
- Reactive routing protocols
  - DSR, AODV
- Non-uniform routing protocols
  - ZRP, CEDAR

Routing in Ad Hoc Networks

• Challenges – Dynamic topology – Unreliable links – Limited resources (battery, processing power) – Low link bandwidth – Security – No default router available

• No physical links – Wireless links created and destroyed as nodes move – Frequent disconnections and partitions.

Traditional routing is proactive

• In proactive routing (table-driven routing), the routing tables are created before packets are sent – Link-state (e.g. OSPF) – Distance-vector (e.g. RIP)

• Each node knows the routes to all other nodes in the network

• Problems in Ad-Hoc networks – Maintenance of routing tables requires much bandwidth – Dynamic topology ˇ much of the routing information is never used ˇWasteof capacity – Flat topology ˇNo aggregation

Reactive routing

• In reactive routing the routes are created when needed – Before a packet is sent, a route discovery is performed – The results are stored in a cache – When intermediate nodes move, a route repair is required

• Advantages – Only required routes are maintained

• Disadvantages – Delay before the first packet can be sent – Route discovery usually involves flooding

Routing protocols in Ad Hoc Networks

• Many routing protocols have been proposed – Both proactive and reactive – Some protocols adapted from wired networks, some invented for mobile ad hoc networks

• No single protocol works well in all environment – Attempts to combine different solutions, e.g. adaptive and combinations of proactive and reactive protocols

• Standardization in IETF – MANET (Mobile Ad hoc Network) working group

• Currently considered routing protocols: DSR, AODV, OLSR, TBRPF – MobileIP

ESSENTIAL OF TRADITIONAL ROUTING PROTOCOLS

Link State Routing Protocol

Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table.

Building Routing Tables

In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.

• Creation of the states of the links by each node, called the link state packet (LSP).

• Dissemination of LSPs to every other router, called **flooding,** in an efficient and reliable way.

• Formation of a shortest path tree for each node.

• Calculation of a routing table based on the shortest path tree.

Creation of Link State Packet (LSP)

- A link state packet can carry a large amount of information. For the moment, however, we assume that it carries a minimum amount of data:
- the node identity, the list of links, a sequence number, and age.
- The first two, node identity and the list of links, are needed to make the topology.
- The third, sequence number, facilitates flooding and distinguishes new LSPs from old ones.
- The fourth, age, prevents old LSPs from remaining in the domain for a long time.
- LSPs are generated on two occasions:

• When there is a change in the topology of the domain. Triggering of LSP dissemination is the main way of quickly informing any node in the domain to update its topology.

• On a periodic basis. The period in this case is much longer compared to distance vector routing. As a matter of fact, there is no actual need for this type of LSP dissemination.

Distance Vector Routing Protocol

Routing Information Protocol (RIP) is an implementation of the distance vector protocol. Open Shortest Path First (OSPF) is an implementation of the link state protocol**.**

Border Gateway Protocol (BGP) is an implementation of the path vector protocol.

Distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next- hop routing).

Distance vector routing tables

Initialization

The table for node A shows how we can reach any node from this node. For example, our least cost to reach node E is 6. The route passes through C. Each node knows how to reach any other node and the cost.

Each node can know only the distance between itself and its immediate neighbors, those directly connected to it.

So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors.

Sharing - In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change.

Updating - When a node receives a two-column table from a neighbor, it needs to update its routing table.

Updating takes three steps:

- The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is x mi, and the distance between A and C is y mi, then the distance between A and that destination, via C, is x + y mi.
- The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.
- The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

RIP

The Routing Information Protocol (RIP) is an intra-domain routing protocol used inside an autonomous system. It is a very simple protocol based on distance vector routing. RIP implements distance vector routing directly with some considerations:

- In an autonomous system, we are dealing with routers and networks (links). The routers have routing tables; networks do not.
- The destination in a routing table is a network, which means the first column defines a network address.
- The metric used by RIP is very simple; the distance is defined as the number of links (networks) to reach the destination. For this reason, the metric in RIP is called a hop count.
- Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.
- The next-node column defines the address of the router to which the packet is to be sent to reach its destination.

POPULAR ROUTING PROTOCOLS

• Destination Sequenced Distance Vector Routing (DSDV)

- Destination sequenced distance vector routing (DSDV) is adapted from the conventional Routing Information Protocol (RIP) to ad hoc networks routing.
- It adds a new attribute, sequence number, to each route table entry of the conventional RIP.
- Using the newly added sequence number, the mobile nodes can distinguish stale route information from the new and thus prevent the formation of routing loops.

Packet Routing and Routing Table Management

- In DSDV, each mobile node of an ad hoc network maintains a routing table, which lists all available destinations, the metric and next hop to each destination and a sequence number generated by the destination node.
- Using such routing table stored in each mobile node, the packets are transmitted between the nodes of an ad hoc network.
- Each node of the ad hoc network updates the routing table with advertisement periodically or when significant new information is available to maintain the consistency of the routing table with the dynamically changing topology of the ad hoc network.
- Periodically or immediately when network topology changes are detected, each mobile node advertises routing information using broadcasting or multicasting a routing table update packet.
- The update packet starts out with a metric of one to direct connected nodes. This indicates that each receiving neighbor is one metric (hop) away from the node.
- It is different from that of the conventional routing algorithms.

II. Dynamic Source Routing Protocol (DSR)

- **Dynamic Source Routing** (**DSR**) is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting node requests one.
- However, it uses source routing instead of relying on the routing table at each intermediate device.
- Determining source routes requires accumulating the address of each device between the source and destination during route discovery.
- The accumulated path information iscached by nodes processing the route discovery packets.
- The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse.
- This may result in high overhead for long paths or large addresses, like IPv6.

iii. Adhoc On-Demand Distance Vector Routing (AODV)

Reactive protocols seek to set up routes on-demand. If a node wants to initiate communication with a node to which it has no route, the routing protocol will try to establish such a route.

The Ad-Hoc On-Demand Distance Vector routing protocol is described in RFC 3561. The philosophy in AODV, like all reactive protocols, is that topology information is only transmitted by nodes on-demand.

When a node wishes to transmit traffic to a host to which it has no route, it will generate a route request(RREQ) message that will be flooded in a limited way to other nodes.

This causes control traffic overhead to be dynamic and it will result in an initial delay when initiating such communication.

A route is considered found when the RREQ message reaches either the destination itself, or an intermediate node with a valid route entry for the destination.

- For as long as a route exists between two endpoints, AODV remains passive. When the route becomes invalid or lost, AODV will again issue a request.

- AODV avoids the ``counting to infinity'' problem from the classical distance vector algorithm by using sequence numbers for every route. The counting to infinity problem is the situation where nodes update each other in a loop.

Consider nodes A, B, Cand Dmaking up a MANET. Ais not updated on the fact that its route to Dvia Cis broken.

This means that Ahas a registered route, with a metric of 2, to D.

C has registered that the link to D is down, so once node B is updated on the link breakage between C and D, it will calculate the shortest path to D to be via Ausing a metric of 3.

Creceives information that Bcan reach Din 3 hops and updates its metricto 4 hops.

A then registers an update in hop-count for its route to D via C and updates the metric to 5. And so they continue to increment the metric in a loop.

AODV defines three types of control messages for route maintenance:

RREQ - A route request message is transmitted by a node requiring a route to a node. As an optimization AODV uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Data packets waiting to be transmitted(i.e. the packets that initiated the RREQ) should be buffered locally and transmitted by a FIFO principal when a route is set.

RREP - A route reply message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

RERR - Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a ``precursor list'', containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

Vehicular ad hoc network

Vehicular ad hoc networks (**VANETs**) are created by applying the principles of mobile ad hoc networks (MANETs) – the spontaneous creation of a wirelessnetwork of mobile devices – to the domain of vehicles.

VANETs were first mentioned and introduced in 2001 under "car-to-car ad-hocmobile 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 HYPERLINK "https://en.wikipedia.org/wiki/Road_safety" HYPERLINK "https://en.wikipedia.org/wiki/Road_safety"safety HYPERLINK "https://en.wikipedia.org/wiki/Road_safety", navigation, and other roadside services.

VANETs are a key part of the intelligent HYPERLINK "https://en.wikipedia.org/wiki/Intelligent_transportation_systems" HYPERLINK "https://en.wikipedia.org/wiki/Intelligent_transportation_systems"transportation HYPERLINK "https://en.wikipedia.org/wiki/Intelligent_transportation_systems" HYPERLINK "https://en.wikipedia.org/wiki/Intelligent_transportation_systems"systems (ITS) framework. Sometimes, VANETs are referred as Intelligent Transportation Networks.

They are understood as having evolved into a broader "Internet HYPERLINK "https://en.wikipedia.org/wiki/Internet_of_vehicles" HYPERLINK "https://en.wikipedia.org/wiki/Internet_of_vehicles"of vehicles" which itself is expected to ultimately evolve into an "Internet ofautonomous vehicles"

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, 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.

Applications

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 interestto mobile ad hoc networks (MANETs) are of interest in VANETs, but the details
differ. 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 exampleby being constrained to follow a paved highway.

Applications of VANETs are:

Electronic brake lights, which allow a driver (or an autonomous HYPERLINK "https://en.wikipedia.org/wiki/Autonomous_car" HYPERLINK "https://en.wikipedia.org/wiki/Autonomous_car"car or truck) toreact to vehicles braking even though they might be obscured (e.g., by other vehicles).

Platooning, which allows vehicles to closely (down to a few inches) follow a leadingvehicle by wirelessly receiving acceleration and steering information, thus forming electronically coupled "road trains".

Traffic HYPERLINK "https://en.wikipedia.org/wiki/Traffic_information" HYPERLINK "https://en.wikipedia.org/wiki/Traffic_information"information systems, which use VANET communication to provide up-to-the minute obstacle reports to a vehicle's satellite navigation system

Road Transportation Emergency Services – where VANET communications, VANET networks, and road safety warning and status information dissemination areused to reduce delays and speed up emergency rescue operations to save the livesof those injured.

On-The-Road Service – it is also envisioned that the future transportation highwaywould 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.

Electronic Toll Collection– The tolling application performed with the C-ITS equipment. These latter use the ITS-G5 technology, the Roadside Unit (RSU) and the on-board unit (OBU) with features specified by the standardization Institute ETSI. To perform this service, we highlight two mains requirements: how to have a reliable geolocation of the vehicle when it crosses the tollgate and how to secure thecommunication during the transaction process.

Technology

VANETs can use any wireless networking technology as their basis. The most prominent are short-range radio technologies are WLAN and DSRC. In addition, cellulartechnologies or LTE and 5G can be used for VANETs.

Simulations

Prior to the implementation of VANETs on the roads, realistic computer simulations of VANETs using a combination of Urban Mobility simulation and Network HYPERLINK "https://en.wikipedia.org/wiki/Network_simulation" HYPERLINK "https://en.wikipedia.org/wiki/Network_simulation"simulation are necessary. Typically open source simulator like SUMO(which handles road traffic simulation) is combined with a network simulator like TETCOS NetSim, or NS-2 to study the performance of VANETs. Further simulations are also done for communication channel modeling that captures the complexities of wireless network for VANETs.

Standards

Major standardization of VANET protocol stacks is taking place in the U.S., in Europe,and in Japan, corresponding to their dominance in the automotive industry HYPERLINK "https://en.wikipedia.org/wiki/Automotive_industry".

In the U.S., the IEEE 1609 WAVE Wireless Access in Vehicular Environments protocolstack builds on IEEE 802.11p WLAN operating on seven reserved channels in the
5.9 GHz frequency band.

The WAVE protocol stack is designed to provide multi-channel operation (even for vehicles equipped with only a single radio), security, and lightweight application layer protocols. Within the IEEE HYPERLINK "https://en.wikipedia.org/wiki/IEEE_Communications_Society" HYPERLINK "https://en.wikipedia.org/wiki/IEEE_Communications_Society"Communications HYPERLINK "https://en.wikipedia.org/wiki/IEEE_Communications_Society" HYPERLINK "https://en.wikipedia.org/wiki/IEEE_Communications_Society"Society, there is a Technical Subcommittee on Vehicular Networks & Telematics Applications (VNTA).

The charter of this committee is to actively promote technical activities in the field of vehicular networks, V2V, V2R and V2I communications, standards, communications- enabled road and vehicle safety, real-time traffic monitoring HYPERLINK "https://en.wikipedia.org/wiki/Traffic_monitoring", intersection managementtechnologies, future telematics applications, and ITS-based services.

MANET Vs VANET :

S.No.	MANET	VANET
1	Production cost of MANET is cheap as compared to VANET	Much Expensive
2	Mobility of MANET is low as it make bit difficult for network enables the serving networks to locate a mobile subscriber's point.	High Mobility, as serving networks to locate a mobile subscriber's point is easy.

3	Change in network topology orientation is slow.	Frequent and very fast change of network topology,
4	Sparse node density.	Node density is frequent variables.
5	MANET HAVE 100 Kps bandwidth available.	VANET bandwidth is 1000 Kps.

S.No.	MANET	VANET
6	It ranges Upto 100 m.	500 m range available in VANET.
7	MANET node lifetime depends on power resources.	Depend on lifetime vehicle.
8	MANET have medium reliability.	High reliability of VANET.
9	Movement of the nodes affects the operation of a MANET as node movement MANETs need to rely on robust routing protocols.And this MANET have random node movement.	Regular, moving pattern of nodes.
10	Attribute Based addressing scheme.	Location Bases addressing scheme.
11	Position acquisition is obtained using Ultrasonic.	VANET maintain position acquisition by using GPS, RADAR.
12	Availability of Multi-hop Routing	Weakly available Multi-hop Routing.

1. Availability

The main goal of availability is to node will be available to its users when expected, i.e. survivability of network services despite denial of service attack. For example, on the physical and media access control layers, an adversary could employjamming to interfere with communication on physical channel while on network layer it could disrupt the routing protocol and continuity of services of the network.

Again, in higher levels, an adversary could bring down high-level services such as key management service, authentication service .

- **Confidentiality**

The goal of confidentiality is to keeping information secret from unauthorized user or nodes. In other words, ensures payload data and header information is never disclosed to unauthorized nodes. The standard approach for keeping information confidential is to

encrypt the data with a secret key that only intended receivers posses, hence achieving confidentiality.

- **Integrity**

The goal of integrity is to guarantee the message being transmitted is never corrupted. Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways .

Malicious altering:–

A message can be removed, replayed or revised by an adversarywith malicious goal.

Accidental altering:-

if the message is lost or its content is changed due to some benign failures, whichmay be transmission errors in communication or hardware errors such as hard disk failure.

- **Authentication**

The goal of authentication is too able to identify a node with which it is communicating and to prevent impersonation. In infrastructure-based wireless network, it is possible to implement a central authority at a point such as base station or access point. But in MANETs, no central administration so it is difficult to authenticate an entity.

- **Non repudiation**

The main goal of non repudiation is sender of a message cannot deny having sent the message. This is useful when for detection and isolation of compromised nodes. When node P receives an erroneous message from Q, non repudiation allows P to access Q using this message and to convince other nodes that Q is compromised.

- **Authorization**

Authorization is a process.

********** UNIT -IV**********

UNIT-5

Mobile Platforms and Application

Mobile Platforms

- A mobile operating system (mobile OS) is the operating system that controls a smartphone, tablet, PDA, or other mobile device.
- Modern mobile operating systems combine the features of a personal computer operating system with touchscreen, cellular, Bluetooth, WiFi, GPS mobile navigation, camera, video camera, speech recognition, voice recorder, music player, Near field communication, personal digital assistant (PDA), and other features.
- Mobile Internet Devices (MIDs) , Netbooks, Internet Tablets, Smart phones and Ultra-Mobile PCs (UMPCs) maybe just buzzwords today, but they are without doubt the devices of the future.

- In a nutshell, these are portable, small form-factor devices capable of browsing the Internet and having their own set of applications which can be executed in limited memory and processing power.
- Traditionally OSes like Windows CE and Symbian's S60 were the popular smart-phone OSes a few years ago. Today Linux as an embedded or a Netbook OS takes the top slot.

- As a result of this a number of SIGs (Special Interest Groups) were formed by bigger companies who decided to start investing seriously in Open Source Mobile platforms.

Apple iOS

- OS (formerly iPhone OS) is a mobile operating system developed and distributed by Apple Inc.
- Originally released in 2007 for the iPhone and iPod Touch, it has since been extended to support other Apple devices such as the iPad and Apple TV
- iOS, an operating system from Apple, was originally developed for the iPhone. Later it was extended to support iPod Touch, iPad and Apple TV. Apple's App Store contains more than 500,000 applications and boasts more than 25 billion downloads collectively.
- It holds the reputation of intelligent UI creator which is based on the concept of direct manipulation, using multi-touch gestures.

Android

- With an amazingly fast browser, cloud sync, multi-tasking, easy connect & share, and the latest Google apps (and thousands of other apps available on Google Play) your Android powered device is beyond smart.
- Android is a Linux based mobile operating system developed by the Open Handset Alliance led by Google.
- Android boasts large community of developers writing applications extending the functionality of the devices.
- It has 450,000 apps in its Android Market and download exceeds 10 billion count.

BlackBerry OS

- BlackBerry OS is developed by Research In Motion (RIM) for its line of smartphones.
- This operating system is known for its native support for corporate e- mail through MIDP allowing complete wireless activation and synchronization with Microsoft Exchange and Lotus Domino.
- Accordingly to one research approximately 45% of mobile developers were using the platform at the time of publication.
- It provides BlackBerry API classes for developers to write applications.

Windows Phone

- A successor to Windows Mobile platform, Windows Phone, is a mobile operating system launched by Microsoft in late 2010.
- This mobile OS is targeted at consumer market. With this new operating system Microsoft offered a new user interface, Metro, integrating the operating system with third party and other Microsoft services, and controls the hardware on which it runs.

    - Windows Phone is a mobile operating system developed by Microsoft, and is the successor to its Windows Mobile platform.
    - Unlike its predecessor, it is primarily aimed at the consumer market rather than the enterprise market.

Unity

- With Unity, game developers can more rapidly create compelling and complex 3D worlds and do better device testing, without having to know all of the ins and outs of Xcode.

Appcelerator

- What makes Appcelerator and other cross-platform toolkits important in the world of mobile application development is that they help break down some of the barriers to getting software created in the first place

Symbian

- The Symbian platform is the successor to Symbian OS and Nokia Series 60;
- unlike Symbian OS, which needed an additional user interface system, Symbian includes a user interface component based on S60

Mobile Application

- A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer.
- Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited function.

- This use of app software was originally popularized by Apple Inc. and its App Store, which offers thousands of applications for the iPhone, iPad and iPod Touch.

There are three basic types of mobile apps if we categorize them by the technology used to code them:

- Native app
- Hybrid app
- Web app

Native App

- Native apps are created for one specific platform or operating system.

- Native apps are built for specific operating systems on mobile devices. That means the app can run on Android devices or Apple iOS devices but not both. This is why many businesses hire software developers who specialize in particular operating systems. Native apps can be developed with a wide variety of programming languages, from Java to Python to C++.
- There are a number of advantages to native apps. The chief benefit is performance. These apps are faster than hybrid apps, as well as more consistent. Additionally, the user experience (UX) tends to be superior, because they use the device's user interface (UI). These apps can also access different features that come with the device itself, such as bluetooth and GPS.
- But native apps aren't without their downsides. One reason why some businesses shy away from building them over hybrid apps is that if they want

to reach a wide audience, including both iOS and Android users, they will need to fully duplicate their development and maintenance efforts.

- There are some tools to help streamline these efforts, such as the popular Facebook framework React Native, but the process will still require significantly more time and effort than hybrid development, and you can't completely repurpose your code. This means that Native app development can get very pricey.
- Native apps also require more storage space on user's devices, particularly when they download developer-released updates.

Web apps are responsive versions of websites that can work on any mobile device or OS because they're delivered using a mobile browser.

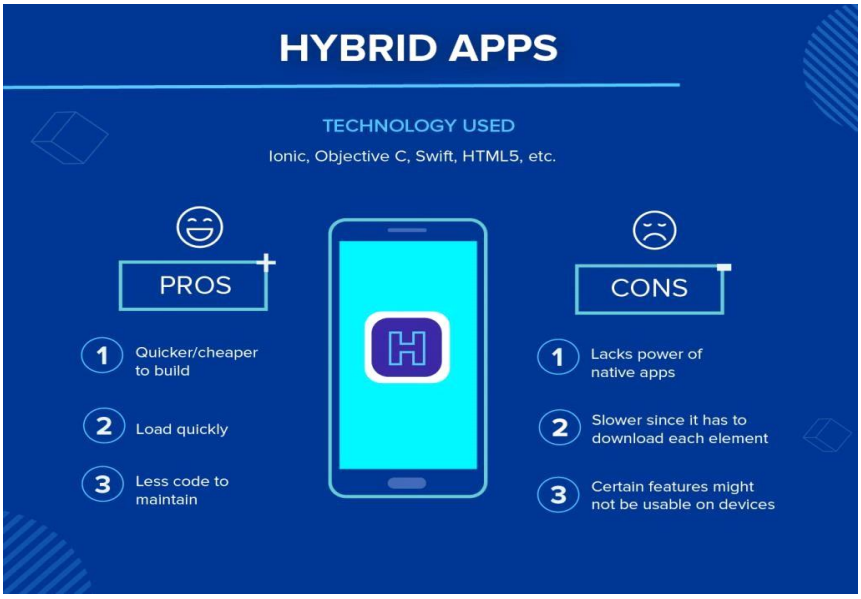
Hybrid App

- Instagram and Gmail are 2 extremely popular examples of hybrid apps. These are technically web apps, but they behave and act like native apps.
- They run within an app-embedded web browser. Unlike native apps,

however, operating systems.

can function on multiple platforms and

- The main advantage of choosing hybrid apps is that development is streamlined since businesses only need to build one version of the product.
- This also means that the development process is typically quicker than that of native apps, as well as less costly.
- Apps can also function offline, and updates are easier to facilitate.
- Hybrid apps can also serve as a minimum viable product (MVP) to demonstrate the app's capabilities before building a native app. Additionally, they are helpful for users in countries with slow internet connections.
- However, there are some major downsides to building hybrid apps. For one, they tend to suffer performance-wise compared with their native counterparts.
- They're typically slower and less reliable than native apps.
- Moreover, the app may look and behave differently in terms of UX and appearance from one operating system to the next.
- Additionally, and depending on the developers' skill set and experience, they may build an app that functions better on Android



- They are accessed on a mobile device and don't require downloading on the part of the user. Commonly, developers use traditional web development languages like HTML5, JavaScript, CSS, and others to create web apps.
- As with hybrid apps, a major advantage of web apps is that they don't require multiple codebases or customization to unique operating systems.
- Therefore, development time can be fairly quick, and the app won't be expensive to create.
- They also behave responsively, adapting to the UI of the specific device on which it is functioning.
- web apps don't require downloading, so they won't take up any storage space on their device, both in terms of the app itself and any maintenance updates.
- Still, as it happens with the other app types, there are some downsides to web apps.
- The biggest drawback is that the app solely depends on the web browser to function.
- That means if the browser's capabilities are limited, then the app's will be, too. In addition, browsers often have different capabilities, so the UX can vary across them.
- Web apps can't completely function offline, either. They may have an offline mode, but their capabilities will still be limited. For example, you won't be able to back up data without an internet connection.

MOBILE DEVICE OPERATING SYSTEMS

- A mobile operating system (or mobile OS) is an operating system for smart phones, tablets, PDAs, or other mobile devices.

- While computers such as the typical laptop are mobile, the operating systems usually used on them are not considered mobile ones as they were originally designed for bigger stationary desktop computers that historically did not have or need specific "mobile" features.
- This distinction is getting blurred in some newer operating systems that are hybrids made for both uses.
- Mobile operating systems combine features of a personal computer operating system with other features useful for mobile or handheld use; usually including, and most of the following considered essential in modern mobile systems; a touch screen, cellular, Bluetooth, Wi-Fi, GPS mobile navigation, camera, video camera, speech recognition, voice recorder,music player, near field communication and infrared blaster.

- Mobile devices with mobile communications capabilities (e.g. smartphones) contain two mobile operating systems .

- the main user-facing software platform is supplemented by a second low-level proprietary real-time operating system which operates the radio and other hardware.

- Research has shown that these low-level systems may contain a range of security vulnerabilities permitting malicious base stations to gain high levels of control over the mobile device

- A mobile operating system, also called a mobile OS, is an operating system that is specifically designed to run on mobile devices such as mobile phones, smartphones, PDAs, tablet computers and other handheld devices.

- The mobile operating system is the software platform on top of which other programs, called application programs, can run on mobile devices.

SPECIAL CONSTRAINTS AND REQUIREMENTS

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

Physically Constrained

- Battery-powered device
- Small screens of varying shapes, sizes, and resolutions
- Memory
- Storage space

Working in Uncertainty

- Networks come and go
- Other devices appear and disappear

- OS need to provide robust methods for handling connections and coping with service interruptions and ad hoc attempts to communicate
- Today's mobile devices are multifunctional devices capable of hosting a broad range of applications for both business and consumer use.
- Smartphones and tablets enable people to use their mobile device to access the Internet for email, instant messaging, text messaging and Web browsing, as well as work documents, contact lists and more.
- Mobile devices are often seen as an extension to your own PC or laptop, and in some cases newer, more powerful mobile devices can even completely replace PCs.
- And when the devices are used together, work done remotely on a mobile device can be synchronized with PCs to reflect changes and new information while away from the computer.
- 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.
- A mobile operating system, also called a mobile OS, is an operating system that is specifically designed to run on mobile devices such as mobile phones, smartphones, PDAs, tablet computers and other handheld devices.

COMMERCIAL MOBILE OPERATING SYSTEM

Many people have ample knowledge about different mobile phones and their companies, but a very few of them know something about operating systems. It is vital to learn about different **mobile OS** used by many companies so that you can know that what is behind your smartphone‘s smooth and colorful touchscreen.

Above is the popularity graph, which represents last 12 months trends. It is apparent that Android is beating up all other operating systems, even the IOS. Symbian, which was once an industry leader, is also observing a diminishing slope. IOS might continue to compete Android, and with the release of Windows Phone 8, we might see some healthy competition in future.

Comparison Of Top Mobile OS

Symbian

Symbian OS is officially the property of Nokia. It means that any other company will have to take permission from Nokia before using this operating system. Nokia has remained a giant in the low-end mobile market, so after Java Symbian was the most used in the mobile phones till a couple of years ago. Still Symbian is widely used in low-end phones but the demand rate has ben continuously decreasing. By upgrading Symbian mobile OS, Nokia has made it capable to run smartphones efficiently. Symbian ANNA and BELLE are the two latest updates that are currently used in Nokia‘s smartphones. Overall, the Symbian OS is excellently designed and is very user-friendly.

Unfortunately, Symbian OS graph is going downwards nowadays due to the immense popularity of Android and iOS. Some of the phones currently running on Symbian OS are Nokia C6-01, Nokia 603, Nokia 700, Nokia 808 Pure View, Nokia E6 (ANNA) and Nokia 701 (BELLE). Symbian is a popular choice among Nokia dual sim mobile phones as well.

Android

September 20th, 2008 was the date when Google released the first Android OS by the name of _**Astro**‘. After sometime next upgraded versions _Bender‘ and _Cupcake‘ were also released. Google then adopted the trend of naming Android versions after

The other releases are Donut, Éclair, Froyo, Gingerbread, Honeycomb, Ice Cream Sandwich and Jelly Bean.Marshmallow (Android 6.0) is so far the latest Android version from Google.

Since the platform is not closed like iOS, there are too many great Android apps built by developers. Just after stepping into the smartphone and tablets market Android gained immense popularity due to its beautiful appearance and efficient working. Many new features were introduced which played a significant role in Android‘s success. Google Play is an official app market that contains millions of different apps for Android devices. Samsung, HTC, Motorola and many other top manufacturers are using Android in their devices. Currently, Android is one of the top operating systems and is considered serious threat for iPhone.

Some of the smartphones operating on Android are HTC Desire, Samsung Galaxy Gio, Motorola Droid Razr, Samsung Galaxy S3 and HTC Wildfire.

Apple iOS

iOS was introduced in **29th June 2007** when the first iPhone was developed. Since then iOS has been under gone many upgrades and currently the latest one is the iOS 9. Apple has still not allowed any other manufacturer to lay hands on its operating system. Unlike Android, Apple has more concentrated on the performance along with appearance. This is the reason that the basic appearance of iOS is almost the same as it was in
2007. Overall it is very user-friendly and is one of the mobile best operating systems in the world. So far iOS has been used in all iPhones, iPod & iPad.

Blackberry OS

Blackberry OS is the property of RIM (Research In Motion) and was first released in 1999. RIM has developed this operating system for its Blackberry line of smartphones. Blackberry is much different from other operating systems. The interface style, as well as the Smartphone design, is also different having a trackball for moving on the menu and a qwerty keyboard.

Like Apple, Blackberry OS is a close source OS and is not available for any other manufacturer. Currently, the latest release of this operating system isBlackberry OS

7.1 which was introduced in May 2011 and is used inBlackberry Bold 9930. It is a very reliable OS and is immune to almost all the viruses.

Some of the smartphones operating on Blackberry OS are Blackberry Bold, Blackberry Curve, Blackberry Torch and Blackberry 8520.

Windows OS

All of you will be familiar with Windows OS because it is used in computers all over the world. Windows OS has also been used in mobile phones, but normal mobile phone users find it a bit difficult to operate it but at the same time it was very popular among people who were used to it.

This was the case until Nokia and Microsoft joined hands to work together. The latest Windows release by Microsoft is known as Windows 7 which has gained immense popularity among all kind of users. With its colorful and user-friendly interface, it has given Windows OS a new life and is currently in demand all over the world. Another reason behind its success is that this latest OS is used in very powerful devices made by Nokia. The computer like look has totally vanished from the windows phones with the release of Windows 7. Samsung and HTC also released some Windows-based phones, but they could not many places in the market.

Nokia Lumia series is completely windows based. Some of the latest Windows Phones are Nokia Lumia 800, Nokia Lumia 900, Samsung Focus and HTC Titan 2.

BADA

Like others, Samsung also owns an operating system that is known as BADA. It is designed for mid-range and high-end smartphones. Bada is a quiet user-friendly and efficient operating system, much like Android, but unfortunately Samsung did not use Bada on a large scale for unknown reasons.

The latest version Bada 2.0.5 was released on March 15th, 2012. There are only three phones that are operating on Bada. These three smartphones are Samsung Wave, Samsung Wave 2 and Samsung Wave

3. I believe that Bada would have achieved much greater success if Samsung had promoted it properly.

Palm OS (Garnet OS)

Palm OS was developed by Palm Inc in 1996 especially for PDAs (Personal Digital Assistance). Palm OS was designed to work on touchscreen GUI. Some Years later it was upgraded and was able to support smartphones. Unfortunately, it could not make a mark on the market and currently is not being used in any of the latest top devices.

It has been 5 and half years since we saw the latest update of Palm OS in 2007. Palm OS was used by many companies including Lenovo, Legend Group, Janam, Kyocera and IBM.

SOFTWARE DEVELOPMENT KIT:
iOS, ANDROID,BLACKBERRY,WINDOWS PHONE

iOS:

iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware. It is the operating system that presently powers many of the company's mobile devices, including the iPhone, iPad, and iPod touch. In October 2015, it was the most commonly used mobile operating system, in a few countries, such as in Canada, the United States, the United Kingdom, Norway, Sweden, Denmark, Japan, and Australia, while iOS is far behind Google's Android globally; iOS had a 19.7% share of the smartphone mobile operating system units shipped in the fourth quarter of 2014, behind

Android with 76.6%.However, on tablets, iOS is the most commonly used tablet operating system in the world, while it has lost majority in many countries (e.g. the Africa continent and briefly lost Asia).

Originally unveiled in 2007, for the iPhone, it has been extended to support other Apple devices such as the iPod Touch (September 2007), iPad(January 2010), iPad Mini (November 2012) and second-generation Apple TV onward (September 2010). As of January 2015, Apple's App Store contained more than 1.4 million iOS applications, 725,000 of which are native for iPads. These mobile apps have collectively been downloaded more than 100 billion times.

The iOS user interface is based on the concept of direct manipulation, using multi-touch gestures. Interface control elements consist of sliders, switches, and buttons. Interaction with the OS includes gestures such as swipe, tap,pinch, and reverse pinch, all of which have specific definitions within the context of the iOS operating system and its multi-touch interface. Internal accelerometers are used by some applications to respond to shaking the device (one common result is the undo command) or rotating it in three dimensions (one common result is switching from portrait to landscape mode).

iOS shares with OS X some frameworks such as Core Foundation and Foundation Kit; however, its UI toolkit is Cocoa Touch rather than OS X's Cocoa, so that it provides the UIKit framework rather than the AppKit framework. It is therefore not compatible with OS X for applications. Also while iOS also shares the Darwin foundation with OS X, Unix-like shell access is not available for users and restricted for apps, making iOS not fully Unix-compatible either.

Major versions of iOS are released annually. The current release, iOS 9.1, was released on October 21, 2015. In iOS, there are four abstraction layers: the Core OS layer, the Core Services layer, the Media layer, and the Cocoa Touch layer. The current

version of the operating system (iOS 9), dedicates around 1.3 GB of the device's flash memory for iOS itself. It

runs on theiPhone 4S and later, iPad 2 and later, iPad Pro, all models of the iPad Mini, and the 5th-generation iPod Touch and later.

Android

Android is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touch screen mobile devices such as smart phones and tablets. Android's user interface is mainly based on direct manipulation, using touch gestures that loosely correspond to real-world actions, such as swiping, tapping and pinching, to manipulate on-screen objects, along with a virtual keyboard for text input.

In addition to touch screen devices, Google has further developed Android TV for televisions, Android Auto for cars, and Android Wear for wrist watches, each with a specialized user interface. Variants of Android are also used on notebooks, game consoles, digital cameras, and other electronics. As of 2015, Android has the largest installed base of all operating systems.

Initially developed by Android, Inc., which Google bought in 2005, Android was unveiled in 2007, along with the founding of the Open Handset Alliance – a consortium of hardware, software, and telecommunication companies devoted to advancing open standardsfor mobile devices. As of July 2013, the Google Play store has had over one million Android applications ("apps") published, and over 50 billion applications downloaded. An April–May 2013 survey of mobile application developers found that 71% of developers create applications for Android, and a 2015 survey found that 40% of full-time professional developers see Android as their priority target platform, which is comparable to Apple's iOS on 37% with both platforms far above others.

At Google I/O 2014, the company revealed that there were over one billion active monthly Android users, up from 538 million in June 2013. Android's source code is released by Google under open source licenses, although most Android devices ultimately ship with a combination of open source

and proprietary software, including proprietary software required for accessing Google services. Android is popular with technology companies that require a ready-made, low-cost and customizable operating system for high-tech devices.

Its open nature has encouraged a large community of developers and enthusiasts to use the open-source code as a foundation for community- driven projects, which add new features for advanced users or bring Android to devices originally shipped with other operating systems. At the same time, as Android has no centralised update system most Android devices fail to receive security updates: research in 2015 concluded that almost 90% of Android phones in use had known but unpatched security vulnerabilities due to lack of updates and support.

The success of Android has made it a target for patent litigation as part of the so-called "smartphone wars" between technology companies.

BlackBerry

BlackBerry OS is a proprietary mobile operating system developed by BlackBerry Ltd for its BlackBerry line of smart phone handheld devices. The operating system provides multitasking and supports specialized input devices that have been adopted by BlackBerry Ltd. for use in its handhelds, particularly the track wheel, trackball, and most recently, the trackpad and touch screen.

The BlackBerry platform is perhaps best known for its native support for corporate email, through MIDP 1.0 and, more recently, a subset of MIDP 2.0, which allows complete wireless activation and synchronization with Microsoft Exchange, Lotus Domino, or Novell

GroupWise email, calendar, tasks, notes, and contacts, when used with BlackBerry Enterprise Server. The operating system also supports WAP
1.2. Updates to the operating system may be automatically available from wireless carriers that support the BlackBerry over the air software loading (OTASL) service.

Third-party developers can write software using the available BlackBerry APIclasses, although applications that make use of certain functionality must be digitally signed. Research from June 2011 indicated that approximately 45% of mobile developers were using the platform at the time of publication. BlackBerry OS was discontinued after the release of BlackBerry 10, but BlackBerry will continue support for the BlackBerry OS.

Windows Phone

Windows Phone (WP) is a family of mobile operating systems developed by Microsoft for smart phones as the replacement successor to Windows Mobile and Zune. Windows Phone features a new user interface derived from Metro design language. Unlike Windows Mobile, it is primarily aimed at the consumer market rather than the enterprise market. It was first launched in October 2010 with Windows Phone 7. Windows Phone 8.1 was the last public release of the operating system, released to manufacturing on April 14, 2014

Work on a major Windows Mobile update may have begun as early as 2004 under the codename "Photon", but work moved slowly and the project was ultimately cancelled. In 2008, Microsoft reorganized the Windows Mobile group and started work on a new mobile operating system. The product was to be released in 2009 as Windows Phone, but several delays prompted Microsoft to develop Windows Mobile 6.5 as an interim release.

Windows Phone was developed quickly. One result was that the new OS would not be compatible with Windows Mobile applications. Larry Lieberman, senior product manager for Microsoft's Mobile Developer Experience, told eWeek: "If we'd had

more time and resources, we may have been able to do something in terms of backward compatibility." Lieberman said that Microsoft was attempting to look at the mobile phone market in a new way, with the end user in mind as well as the enterprise network. Terry Myerson, corporate VP of Windows Phone engineering, said, "With the move to capacitive touch screens, away from the stylus, and the moves to some of the hardware choices we made for the Windows

Phone 7 experience, we had to break application compatibility with Windows Mobile 6.5.

Mobile Commerce

Mobile commerce, also known as m-commerce, involves using wireless handheld devices like cell phones and tablets to conduct commercial transactions online, including the purchase and sale of products, online banking, and paying bills.

- Mobile commerce refers to business or purchases that are conducted over mobile devices like cell phones or tablets.

- M-commerce lets users transact anywhere, provided that there's a wireless Internet provider available in that area.
- Mobile commerce has increased rapidly as security issues have been resolved.
- Companies like Apple and Google have introduced their own mobile commerce services.

Mobile Commerce

Mobile commerce is a large subset of electronic commerce, a model where firms or individuals conduct business over the Internet. Nearly 97% of Americans owned a cell phone by 2021, and 85% of them owned a smartphone. This is up from 35% in 2011, according to the Pew Research Center.

Many products and services can be transacted via m-commerce, including banking, investing, and purchases of books, plane tickets, and digital music. The rapid growth of mobile commerce has been driven by several factors, including increased wireless handheld device computing power, a proliferation of m-commerce applications, and the resolution of security issues.

Benefits of Mobile Commerce

The range of devices capable of mobile commerce has grown. Digital wallets like Apple Pay and Google Pay let customers make in-store

purchases without the inconvenience of swiping cards. Social media platforms such as Facebook,Twitter, Pinterest,and Instagram

M-commerce apps allow for location tracking via GPS to offer customers help finding items in stores. Personalized shopping experiences can also connect retailers with their clients. Digital commerce transactions are likely to continue climbing as content delivery over wireless devices becomes more streamlined, secure, and scalable.

Ways to Improve Mobile Commerce

Quick-loading web pages are likely to win more sales because consumers can be impatient and demand instant gratification. Mobile checkouts must let buyers easily enter payment information, preferably with mobile wallets that eliminate the use of manual entry, thereby reducing human error and facilitating a smoother checkout experience.

Mobile Commerce Videos and Marketing

Mobile applications that use video to demonstrate a product's key features are likely to generate more revenue. An online foreign exchange broker who sends video links illustrating its new mobile trading application will likely win more clients.

PROS AND CONS

Pros:

- Increased access to user data (e.g. by requesting Facebook login).
- Better use of the screen (not inside the browser window).
- Better use of smartphone features / tools (e.g. camera, GPS).
- Can access without an internet connection, using 3G for example.
- More control on how it is being shown.

Cons:

- Apps need to be downloaded.
- Apps need to be upgraded.
- There is a low repeated usage of apps.
- Needs to be built for each platform (iOS, Android, Windows).
- Needs to be right the first time – reviews stay ―forever‖.

MOBILE PAYMENT SYSTEM AND SECURITY ISSUES

The development of smartphones has gone and replaced a few things we grew up with: the watch, the alarm clock, the tape recorder, music players, and it seems that very soon, we can add cash and wallets to that list. It‘s hardly a surprise. Payment methods have been morphing through various channels: from cash to cheques, to credit cards and debit cards, and now to online banking and mobile commerce.

Close to 10 million mobile subscribers in Japan are already paying for purchases with their smartphones by the end of 2010, and reports are saying that the more than $200 billion dollar mobile payment industry willl be worth a trillion by 2015.

There are 6 billion mobile phone subscriptions in the world, and more than a billion smartphones already in the market. Perhaps it‘s just a matter of time before we embrace the idea of losing that wallet and opting for a digital one to buy flight tickets, lunch, coffee or even to pay the rent.

Digital Wallets

The verdict is still out on what to call these cashless wallets: digital wallet, electronic wallet, e-wallet, virtual wallet etc but they all work the same way. By downloading an app onto your phone, you can link the service or app account to your bank account or payment card. With that done, you can start paying for your wares with your digital wallet.

Paying is a Breeze

If your digital wallet is an NFC enabled Android phone, you can tap your smartphone at the card terminal at the checkout counter, like you would your debit card. But let‘s face it, not all Android phones carry NFC technology and it‘s hardly a strong reason for you to consider when it comes to picking your next smartphone. But fret not, other e-wallets, like Square Wallet, let you pay just by saying your name to the cashier. Systems like ERPLY allow you to check in at a store, and let the cashier identify you by facial recognition; your purchases are then auto-deducted from your PayPal account.

Restaurants and pubs would love platforms like Tabbedout, which lets their diners check in when they arrive, and pay for their meal anytime without needing to wait for the bill or to bring their wallets along. All of this is made possible with smartphones and the right apps.

Digital Wallets not only carry payment details to allow their owners to make purchases, they also help them to better manage their loyalty cards. If your really want to go full digital (wallet) then it only makes sense that you need not carry around your loyalty cards either.

To cater for this, there are also apps that let users scan the information on the barcodes of their loyalty cards, then store them up in the phone. At the checkout counter, they can let the cashier scan the barcode displayed on their mobile screen to ensure that they don‘t miss out on any rewards.

Loyalty Apps and Programs

But then other apps take it up a notch and become the reward platform itself. Loyalty platforms like LevelUp, Perka and rewardjunkie! give business owners the flexibility to customize reward programs for their loyal, paying customers, and to engage new customers for their booming business.

For the rest of us, this means that we don‘t have to carry around stacks of brand-specific loyalty cards that are used probably once every couple of months. Everything is in our smartphone, including new offers, discounts and deals offered by participating merchants.

Alternative Payment Methods

If however you are cautious with your spending and prefer to not put all your chicken eggs in the same basket (i.e. what if you lose your smartphone?), then there are other online payment methods to use.

Carrier or Mobile Billing

The idea is to charge all your online purchases to your phone bill and clear that at the end of the month. The good thing with this method is that you need not even own a smartphone to start making online purchases. Having a mobile phone is enough as you can pay via sms. There are confirmation codes or authorization pins or text to punch in they are intended for security purposes.

Is it Secure?

Ultimately, the security of these mobile payment systems is always at the back of our heads. What happens if I transfer all my payment card details into the smartphone and the unthinkable happens: someone else gets hold of my lost or stolen smartphone?. Well, it‘s a good thing that most of these accounts, as well as your smartphone, can be remotely deactivated or wiped out. It is a good idea to have a passcode lock, at least to give your phone an extra layer of protection. Also, before you start linking your sensitive data to any mobile payment platform, do take a look at customer reviews or coverage of the platform from reliable sources first.

Resources for accepting mobile payment

To wrap up, here is a small list of resources developers can adapt to their online business to start accepting mobile payments from their online customers.

Card io

Tired of having to punch in line after line of credit card details? You can skip through all that with Card.io by taking a photo of your credit card, then punching in the CVV code manually. This help reduce fraud and developers can easily join the program by grabbing the SDK for card.io at the site.

Jumio

Here is another app that lets you take photos of your credit card as a payment method via Netswipe. It also has a similar online ID verification tool calledNetverify, which lets your customer‘s computer work in your favor as an ID scanning tool.

BancBox

BancBox is an all-in, one-stop solution for businesses that cater to the online marketplace. With the payment portal in place, the business owner can receive credit card payments, wire transfers and checks, among others. It also has a relatively low fee of 0.5% + 30 cents per transaction for its services.

Stripe

Stripe helps developers take care of credit card payments online with a simple JS script. It lets you build your own payment forms, and avoid PCI requirements. Embedding the codes in the site lets Stripe to handle all your online payment needs at 2.9% + 30 cents per successful charge.

Zooz

ZooZ gives developers 3 lines of code, which they can integrate into their mobile applications. There is also a sandbox environment to let developers test out transactions at no charge. Prices are locked in at 2.8%
+ 19 cents per transaction.