Institute of Engineering and Technology

Devi Ahilya Vishwavidyalaya, Indore (M.P.)

Academic Session Jan-April 2020

Department: Computer Engineering

Assignment 3

Subject: Wireless Communication and Technologies

Submitted By :	**Submitted To :**
Deepam Gupta	**Mr. Aditya Makwe**
Class : CS-A	**Roll No. : 17C6013**

Date of Submission : 25/04/2020

Assignment 5

1. Explain different routing protocols of fixed networks. What are the consequences of and problems of using IP together with routing protocols of fixed networks for mobile communication? What could be quick solutions?
Ans.

1. Transmission Control Protocol (TCP):
   TCP is a popular communication protocol which is used for communicating over a network. It divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination.

2. Internet Protocol (IP):
   IP is designed explicitly as addressing protocol. It is mostly used with TCP. The IP addresses in packets help in routing them through different nodes in a network until it reaches the destination system. TCP/IP is the most popular protocol connecting the networks.

3. User Datagram Protocol (UDP):
   UDP is a substitute communication protocol to Transmission Control Protocol implemented primarily for creating loss-tolerating and low-latency linking between different applications. Post office Protocol (POP): POP3 is designed for receiving incoming E-mails.

4. Simple mail transport Protocol (SMTP):
   SMTP is designed to send and distribute outgoing E-Mail.

5. File Transfer Protocol (FTP):
   FTP allows users to transfer files from one machine to another. Types of files may include program files, multimedia files, text files, and documents, etc.

6. Hyper Text Transfer Protocol (HTTP):
   HTTP is designed for transferring a hypertext among two or more systems. HTML tags are used for creating links. These links may be in any form like text or images. HTTP is designed on Client-server principles which allow a client system for establishing a connection with the server machine for making a request. The server acknowledges the request initiated by the client and responds accordingly.

7. Hyper Text Transfer Protocol Secure (HTTPS):
   HTTPS is abbreviated as Hyper Text Transfer Protocol Secure is a standard protocol to secure the communication among two computers one using the browser and other fetching data from web server. HTTP is used for transferring data between the client

browser (request) and the web server (response) in the hypertext format, same in case of HTTPS except that the transferring of data is done in an encrypted format. So it can be said that https thwart hackers from interpretation or modification of data throughout the transfer of packets.

Problems with Mobile IP

Although growing rapidly, Mobile IP still has the following problems:

(1) "Triangle routing" Problem

The Communication Host (CH) has to send packets to the Mobile Host (MH) via the Home Agent (HA), while the MH sends packets directly to the CH. As the communication in the two directions follows different routes, the problem of "triangle routing" arises, which leads to low efficiency especially when the MH is far away from the HA and the CH is near to the MH.

(2) Handoff Problem

Handoff problem means that the HA sends the IP packets of the MH to the original foreign network via the tunnel because it doesn't know the latest Care of Address (CoA) of the MH during the period starting when the MH leaves the original foreign network and ending when the HA receives the new registration address of the MH. As a result, these dropped IP packets have an influence on the communication between the MH and the CH especially when handoff occurs frequently or the MH is far away from the HA.

(3) Problem of Intra-Domain Movement

The frequent intra-domain movement of the MH within a small area will lead to frequent handoff. Consequently, a great amount of registered messages are generated in the network and the network performance is greatly affected.

(4) QoS Problem

In the mobile environment, it is hard to provide QoS over Mobile IP due to dynamically varying wireless network topologies, limited network resources, unpredictable effective bandwidth and high error rate.

Solutions to problems with IP

2.1 Solution to "Triangle Routing" Problem

For Mobile IP, routing optimization is necessary because all packets sent to the MH shall pass through the HA but the route may not be the best. After receiving the packets sent by the CH to the MH, the HA notifies the CH of the binding information about the MH, i.e., the current Foreign Agent (FA) address of the MH, and the CH encapsulates the packets and establishes the tunnel to the FA for transparent transmission. The binding information is transferred via a definite port number. If the MH moves again, the new FA will transfer the updated binding information to the old FA to ensure that the packets are transferred to the new FA. And meanwhile the HA gets the updated binding information so the subsequent packets will be transferred directly from the CH to the new FA. The mobile IP with route optimization sets high requirements on the CH. The CH shall have the ability to obtain the binding information, encapsulate the packets and establish the tunnel. Therefore the CH protocol stack needs lots of modifications.

2.2 Solution to Handoff Problem

The handoff process falls into two stages:

(1) Mobile Test Stage

In this stage, a mobile test is conducted for the MH to determine whether it has changed the sub-network for access.

(2) Re-Registration Stage

The re-registration stage refers to the period starting when the MH sends a registration request to the HA and ending when the HA receives the request, after the MH confirms the move. The length of the period depends on the distance from the MH to the HA.

After the above two stages are completed, the MH continues to communicate with the CH. But any dropped packets caused in this period may interact with high-layer protocols, and consequently worsen the communication performance. The interaction with TCP is a typical example. In the mobile IP environment, the dropped packets caused by the handoff will make the interruption duration for TCP connection longer, and thus degrade the TCP performance. The most serious interruption is up to 12 s or so, and meanwhile there are several overtime retransmissions. In a word, the communication performance during the MH handoff depends on three factors: mobile test, re-registration and interaction with the high-layer protocol.

In view of these problems, the concept of achieving local registration through the layered Mobile IP is put forward in the reference document, i.e., only when moving out of the area does the MH need re-registration to the HA. This method helps reduce the time delay for re-registration and improve the handoff performance of Mobile IP.

In the reference document, a solution of "original FA notification" is proposed. It can effectively reduce the dropped data packets through the buffer memory. However, how to set the capacity of the buffer memory in the FA is a knotty problem. Also, it is necessary to define a new protocol to support the communication between the old FA and the new one.

2.3 Solution to Problem of Intra-Domain Movement

For the intra-domain micro-movement, improved protocols such as Cellular IP, HAWAII and TeleMIP can be adopted to solve the problem of frequent handoffs, and reduce handoff delay, packet loss ratio and registration information to the HA. For details please refer to reference document.

2.4 Solution to QoS Problem

Resource Reservation Protocol (RSVP) and Differentiate Service (DiffServ) have their respective strengths and weaknesses in providing QoS over Mobile IP. But they can be combined to solve the end-to-end QoS problem as shown in Figure 1. The Diffserv is employed in the backbone router, and the RSVP in the access part. When the host originates RSVP requests to the border router of the backbone access point, the border router will divide the requests into certain QoS levels and map them onto the DS field based on the content such as bandwidth and time delay carried by the RSVP requests and the preliminary definition. In the backbone DiffServ domain, the DS field can guarantee the QoS of transmission, and the border router at the backbone output restores the original RSVP requests and sends them to the destination

2. How does the symmetry of wireless links influence the routing algorithms?
Ans.

Most algorithms fail if the links are asymmetric up to the extreme case of unidirectional links. Think of DSR – the algorithm states that the receiver simply sends the packet collecting routers on the way between source and destination back to the source by choosing the routers in the reverse order. But what if some reverse links do not exist? Then DSR has to find a way or the other way round, too. Now source and destination both got a way – but in the wrong direction! Somehow this information must reach the other side – without a route quite difficult broadcast is always a solution.

3. What is DHCP? What is its basic purpose? Name the entities of DHCP. How can DHCP be used for mobility and support of mobile IP?
Ans.

DHCP at a glance

DHCP (Dynamic Host Configuration Protocol) is a protocol that provides quick, automatic, and central management for the distribution of IP addresses within a network. DHCP is also used to configure the subnet mask, default gateway, and DNS server information on the device.

Purpose of DHCP

Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses for new computers or computers that are moved from one subnet to another must be configured manually; IP addresses for computers that are removed from the network must be manually reclaimed.

Because these devices can get an IP address automatically, devices can move freely from one network to another (given that each device is set up with DHCP) and receive an IP address automatically, which is helpful with mobile devices.

DHCP Entities

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

Dynamic Host Configuration Protocol (DHCP) involves two main entities; DHCP Server and DHCP Client. When a computer is added to a network, it goes through a four-step process in order to get an IP address. The computer acts as DHCP Client in this process and gets an IP address from the DHCP Server.

IP mobility using DHCP:

Requirements for IP Mobility:

- If a host wants to become nomadic (move around across multiple IP networks), then one of the routers in its home network must become a home agent
- In the DHCP solution, the mobile host itself will become its own foreign agent.

Preparing to become mobile:

- Similar to the foreign host approach, before the nomadic host leaves its home network, the nomadic host listens for agent advertising messages on its home network
- It must record the IP address of the agent on its home network.
  This agent is the home agent for the nomadic host

Arriving at the foreign network:

i. When the nomadic host enters a foreign network, it acquires a new IP address using the DHCP protocol. This new IP address given by the DHCP server on the foreign network will have a foreign IP network ID. When the mobile host receives the new IP address, it records the IP address as its foreign address.

ii. The mobile host then sends a CareOf message to its home agent containing:

- The mobile host's IP address
- The foreign IP address

iii. When the home agent receive the CareOf message, the home agent creates (just like before) an IP tunnel to the foreign agent. This is achieved by adding the following entry into its routing table:

Destination	Tunnel	Next
IP address of nomadic host	1	IP address of foreign agent

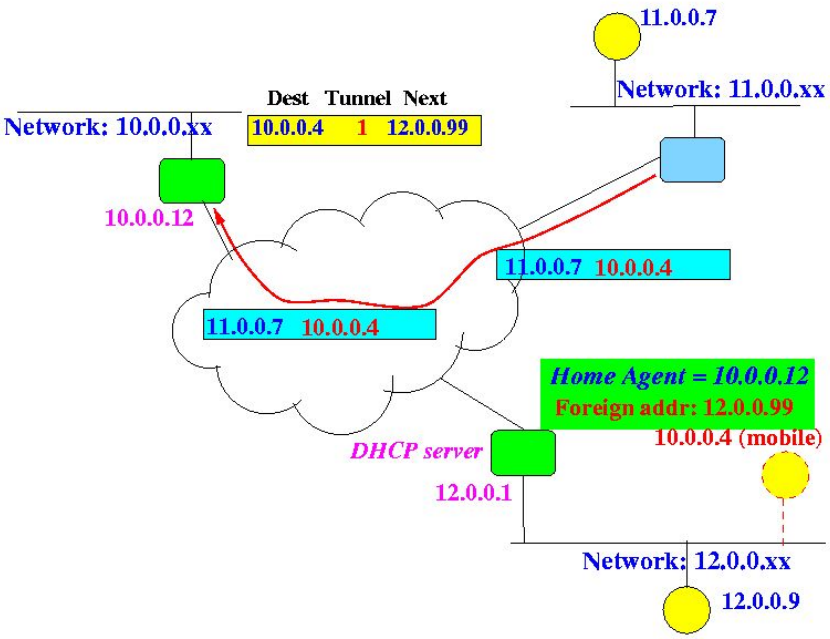
Result of the registeringCareOf operation:

When the home agent (a router) receives a message destined for the nomadic host, it will tunnel the message directly

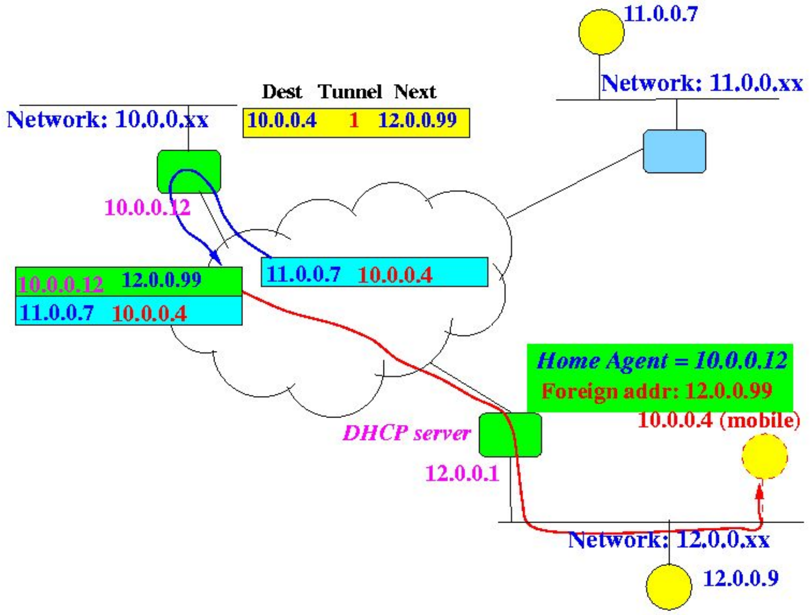
- NOTE: The tunnel is again unidirectional (only from home agent to foreign agent).
- You have seen that the reverse direction of the tunnel is not necessary --- because message from the mobile host can reach their destination normally !

Example: Mobile IP routing using DHCP

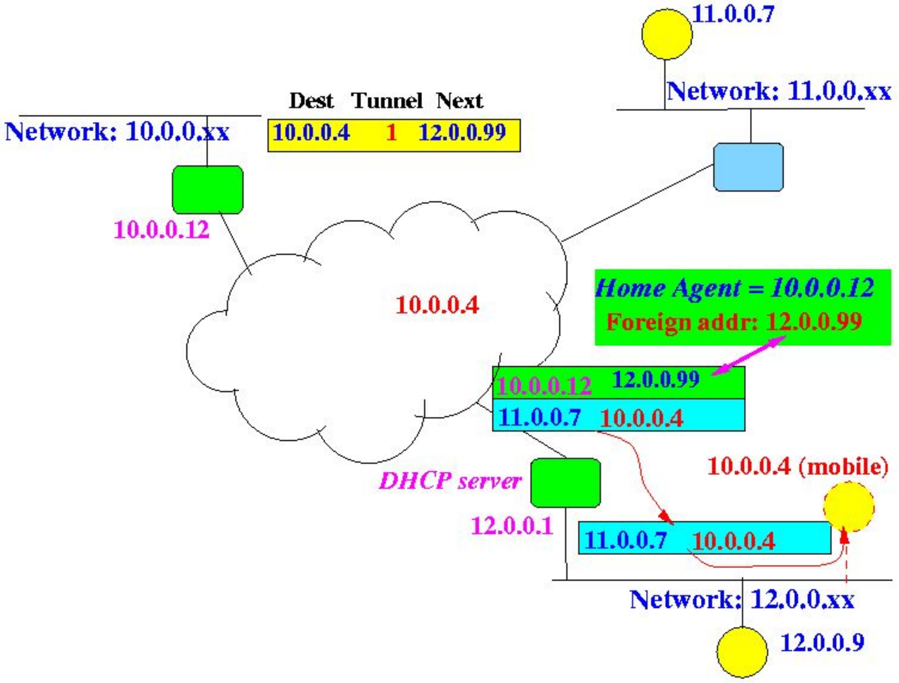
i. Host (11.0.0.7) sends an IP message to the mobile host (10.0.0.4). The message is routed (as usual) using the destination network ID towards the home network (10.0.0.xx):



ii. When the home agent receives the IP packet, the routing table entry (10.0.0.4, Tunnel, 12.0.0.99) will cause the home agent to tunnel the IP packet to the mobile host at 12.0.0.99. The receive IP message will be encapsulated inside a new IP message and then sent towards the mobile host (12.0.0.99):



iii. When the mobile IP module in the mobile host received the tunneled message, it will detect that the packet is destined for its foreign address. The IP module will extract the inner IP packet and delivers it to the mobile host:



Note:

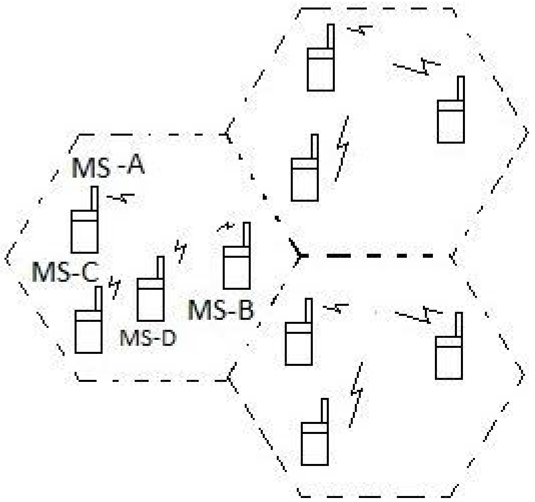
- The mobile host will receive an encapsulated IP message addressed to its foreign address
- Thus: the IP module in the nomadic host must be able to handle such strange IP packet - i.e., the IP module in the nomadic host must have been updated with IP mobility support !

4. Name the main differences between multi-hop ad-hoc networks and other networks. What advantages do these ad-hoc networks offer? Why is routing in multi-hop ad-hoc networks complicated, what are the special challenges?

Ans.

Differences between multi-hop ad-hoc networks and other networks:

Ad Hoc network



Ad Hoc Network

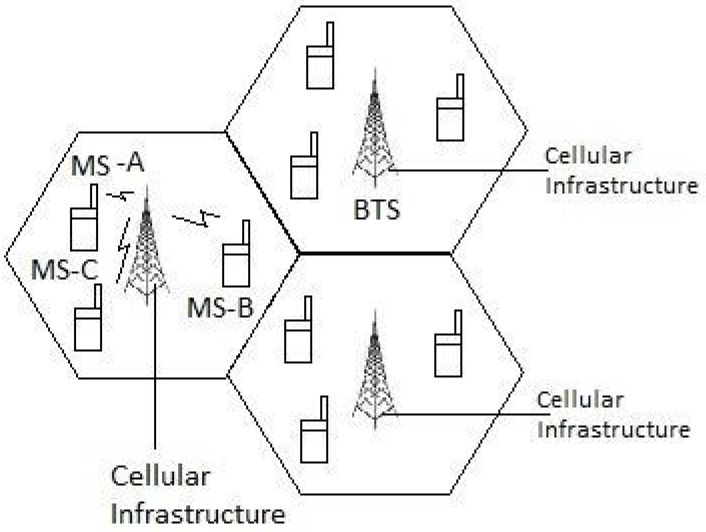
The ad hoc networks operate of its own without the need of any infrastructure. They are called self organizing networks. It utilizes multi-hop radio relay concept and hence are known as multi-hopped networks. As there is no central entity such as base station, routing and resource management (i.e frequency) are complex compare to cellular network.

The cell boundary has no significance, it is just mentioned for representative purpose only. The communication between MS-A to MS-C goes through MS-D.

<u>Examples: Mesh networks and WSN networks.</u>

The nodes in ad hoc networks are very complex as they need to house transmitter, receiver and routing functionalities.

Cellular network:



Cellular Network

Currently deployed cellular wireless networks such as GSM/CDMA/LTE are infrastructure type. Cellular network consists of central entity known as base station and mobile devices as MSs (Mobile Subscribers). If MS-B wants to communicate with MS-C, communication happens via base station(BTS).

Before development of Cellular network users are served using very high power transmitter which used to cover range in Kms but at the cost of high power. Later on cellular networks consisting of many low power transmitters covering more subscribers within its coverage reach have been designed and developed. The main function of Cellular network is to increase more and more subscriber capacity. Due to low power transmitters, the area is divided into small cells, each served by one base station(i.e. BTS in GSM) each. All the base stations are connected in different topology configurations. These BTSs are connected with MSCs and other cellular infrastructure systems.

There are two types cells viz. Macrocell and microcell. Macrocell covers 1 to 20Km while Microcell covers 0.1 to 1 Km. Macrocell uses high power transmitters while microcell uses low power transmitters. Access techniques such as TDMA, FDMA and CDMA are mainly employed in order to enhance the supported capacity of subscribers in a cellular network. It is referred as single hopped system.

Advantages these ad-hoc networks offer -

Ad hoc networks are wireless connections between two or more computers and/or wireless devices (such as a Wi-Fi enabled smart phone or tablet computer). A typical wireless network is based on a wireless router or access point that connects to the wired network and/or Internet. An ad hoc network bypasses the need for a router by connecting the computers directly to each other using their wireless network adapters.

Router Free

Connecting to files on other computers and/or the Internet without the need for a wireless router is the main advantage of using an ad hoc network. Because of this, running an ad hoc network can be more affordable than a traditional network---you don't have the added cost of a router. However, if you only have one computer an ad hoc network won't be possible.

Mobility

Ad hoc networks can be created on the fly in nearly any situation where there are multiple wireless devices. For example: emergency situations in remote locations make a traditional network nearly impossible, but "The medical team can utilize 802.11 radio NICs in their laptops and PDAs and enable broadband wireless data communications as soon as they arrive on the scene."

Speed

Creating an ad hoc network from scratch requires a few settings changes and no additional hardware or software. If you need to connect multiple computers quickly and easily, then an ad hoc network is an ideal solution.

Challenges in multi-hop ad hoc networks -

- Medium access scheme;
- Routing and multicasting
- Transport layer protocol
- Pricing scheme;
- Quality of service provisioning;
- Security;
- Energy management;
- Addressing and service discovery;
- Scalability;
- Deployment considerations

5. Why one cannot use distance vector and link state routing algorithm of fixed networks in multi Hop Adhoc networks?

Ans.

One of the drawbacks in these routing protocols is that they do not consider the transition of link quality in their process of computing forwarding paths; they use hop counts as their basic criteria to compute forwarding paths of packets. However, the transition of link quality including link failure is not avoidable in MANET because its basic requirements include node mobility and wireless links. To take this important characteristic into account, many routing metrics have been proposed that quantifies link quality from various points of view [6]-[11]. For MANETs in which mobility is included in general, the event that affects the most on communication performance is link failure due to mobility. Thus, most of the proposed link metrics tries to quantify the probability of link failure by way of measuring node speed, RSSI (Received Signal Strength Indication), and so on [6]-[11]. For Wireless Mesh Networks (WMN) [5] in which nodes are stationary, because the risk of link failure is far smaller than MANET, the link quality that should be quantified is the quality of communications such as communication speed, delay, and stability of links [12]-[16]. For example, ETX (Expected Transmission Count) [12], which is one of the most commonly used link metrics, quantifies the average transmission count in 802.11 MAC computed from success ratio of MAC transmission, and ETT (Expected Transmission Time) [13] extends ETX to quantify the average transmission time of a MAC frame in the link.

As far as proactive link-state routing such as OLSR is concerned, it is well understood that introducing dynamic link metrics make networks far robust and resilient, and consequently improve performance of networks in practical situations. However, simultaneously, such dynamic metrics cause communication paths to be changed frequently. Note that the paths flapping behavior is not always bad, because it is the result of continuous effort of routing protocols to find better quality paths. Nevertheless, it certainly increases the risk of several inconvenient phenomena such as packet looping.

Packet looping is one of the very harmful problems because looping packets travel along the same link repeatedly and consume significant capacity of the network. In general, larger number of looping packets appears when the network topology changes including link metrics more frequently. In other words, dynamic metrics by nature involves the risk of this kind of instability in exchange for the flexibility against wireless instability. Therefore, it is one of the goals for us to reduce the harmful influence of packet loops, while simultaneously holding the flexibility brought from dynamic metrics.

Note that, in wireless multi-hop routing, there are several causes of reducing communication performance other than packet looping, and they are deeply related with one another. Not only packet loops, but also congestions due to interference, and further link failures due to wireless instability or mobility are also regarded as the essential elements that should be considered in MANET routing schemes. Especially, interference would be the most focused element in the current state of the art. However, in wireless networks, packet looping and interference are deeply related with each other so that improving performance from the viewpoint of looping would also be an important part of the contribution.

6. What are the benefits of location information for routing in ad-hoc networks?
Ans.
LAR is an on-demand routing protocol where location information is used to reduce the search space for a desired route. The source uses the last known destination location in order to estimate the zone in which the destination is expected to be found.

7. What are the differences between AODV and the standard distance vector algorithm?

Ans.

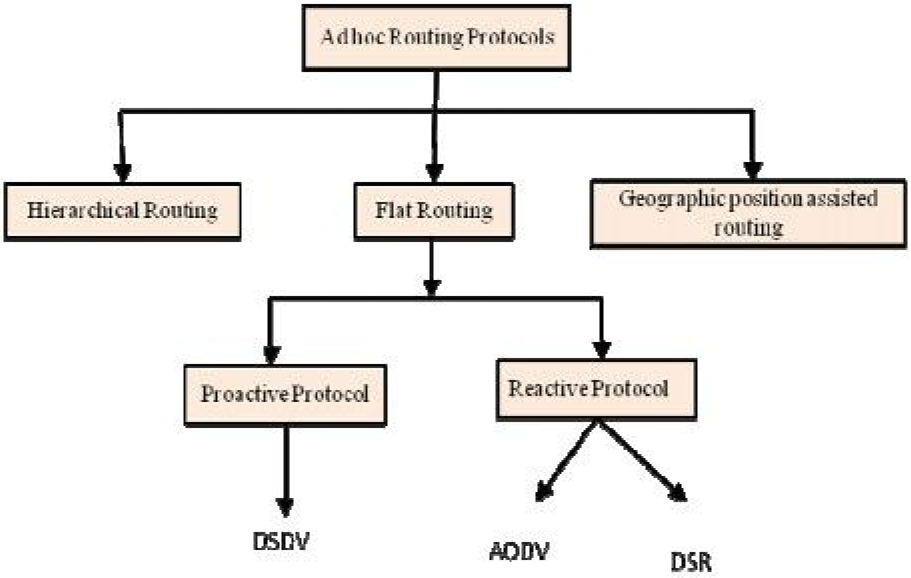
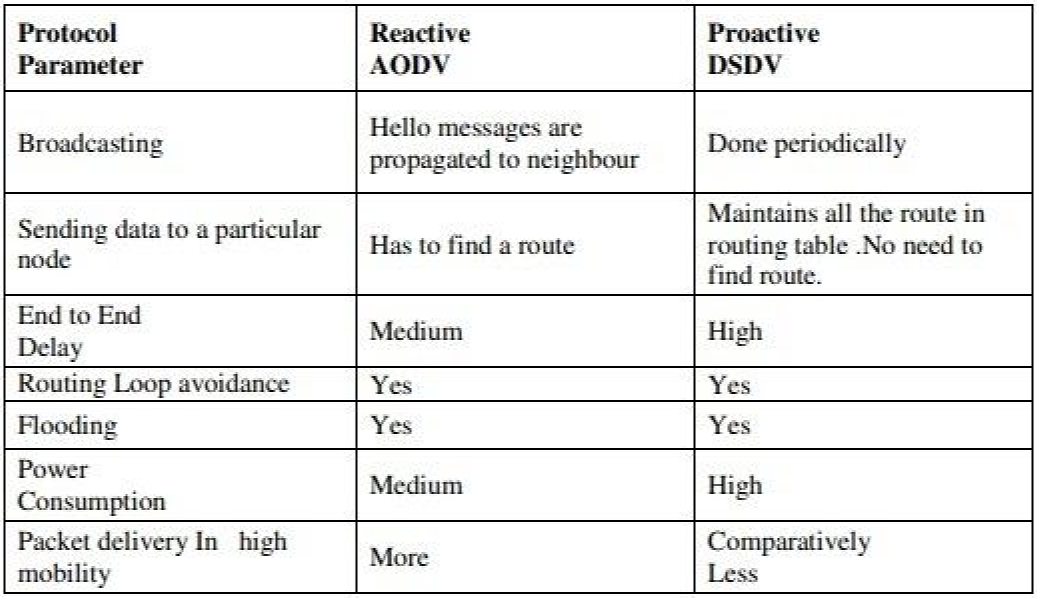


Figure 1. Classification of Routing Protocols In Mobile Ad-hoc Networks

Dynamic Source Routing (DSR) and AdHoc On Demand Distance Vector Routing (AODV) are both routing protocols for wireless mesh/ad hoc networks. Both the protocols employ different mechanisms that result in varied performance levels.

Table 5. Comparison between AODV and DSDV



Protocol Parameter	**Reactive AODV**	**Proactive DSDV**
Broadcasting	Hello messages are propagated to neighbour	Done periodically
Sending data to a particular node	Has to find a route	Maintains all the route in routing table .No need to find route.
End to End Delay	Medium	High
Routing Loop avoidance	Yes	Yes
Flooding	Yes	Yes
Power Consumption	Medium	High
Packet delivery In high mobility	More	Comparatively Less

DSR and AODV can be compared and evaluated based on the packet delivery ratio, normalized MAC load, normalized routing load, and average end-to-end delay by altering the number of sources.

- The DSR is based on source routing in which all the routing information such as is maintained at the mobile nodes. The DSR computes the routes and also updates them. The source routing is a technique in which the packet sender identifies the entire sequence of the node into which the packet has to pass through. The packet sender lists the route in the packet's header so that the next node to which the packet has to be transmitted can be identified by the address on the way to the destination host.
- Both DSR and AODV are demand-driven protocols which form a route on demand when a transmitting computer desires a route. The main difference between DSR and AODV is the source routing feature.
- The AODV uses a combination of a DSR and DSDV mechanism. It uses the route discovery and route maintenance from a DSR and hop-by-hop routing, periodic advertisements, sequence numbers from DSDV. The AODV easily overcomes the counting to infinity and Bellman Ford problems, and it also provides quick convergence whenever the ad hoc network topology is altered.
- When DSR and AODV are analyzed using a packet delivery ratio parameter by varying the paused time in the intervals of 0, 10, 20, 40, 100, the results obtained for both on demand routing protocols look similar.
- The normalized routing load is analyzed for both protocols by varying paused times. The values for the DSR protocol were less as compared to the AODV which show fairly stable results even after increasing the number of sources. If normalized routing load is stable, the protocol is considered to be scalable.
- The routing overhead for AODV is mainly from the route requests. DSR finds the route in the cache as a result of aggressive caching. This helps to avoid a frequent route discovery process in DSR thereby decreasing the routing overhead for DSR when compared to AODV.
- The normalized MAC load is analyzed by varying different paused times. The values for AODV is less when compared to DSR when analyzed for lower paused times.
- The performance of DSR is better than AODV as the route is always found quickly in cache avoiding the route discovery process.

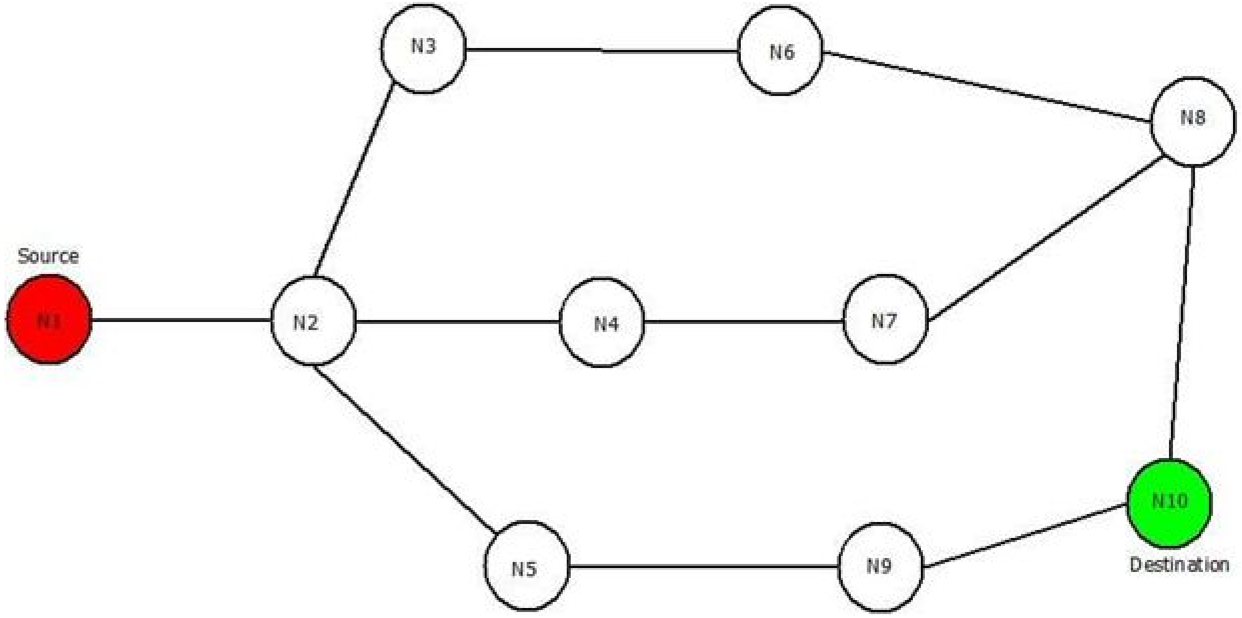
8. How does dynamic source routing handle routing? What is the motivation behind dynamic source routing compared to other routing algorithms from fixed networks? How does the symmetry of wireless links influence the routing algorithms proposed
Ans.

- Dynamic Source Routing (DSR) comes under the reactive routing protocol category, as it is capable of discovering the route from source to destination only when required and needed.
- Dynamic Source Routing protocol uses a process called "Route Discovery Mechanism" that is capable of discovering the route for data packets from source node to destination nodes using intermediate nodes.
- As like proactive routing protocols such as Global State Routing an Dynamic Sequence Distance Vector Routing no separate table is maintained.

- The major change in DSR as compare to GSR and DSDV is, in DSDV after asking a requirement of route from source to destination, path via intermediate nodes is checked for its length. Then a "Re-Request" packet is sent back from destination to source via the smallest route possible in the whole network. The "Re-Request" packet does contains its unique ID also.
- This process of separately sending a "Re-Request" packet from destination to source makes it easier for the sender to send the data packets on fixed path rather than sending it on multiple paths to check for total distance.

Dynamic Source Routing Protocol : Working

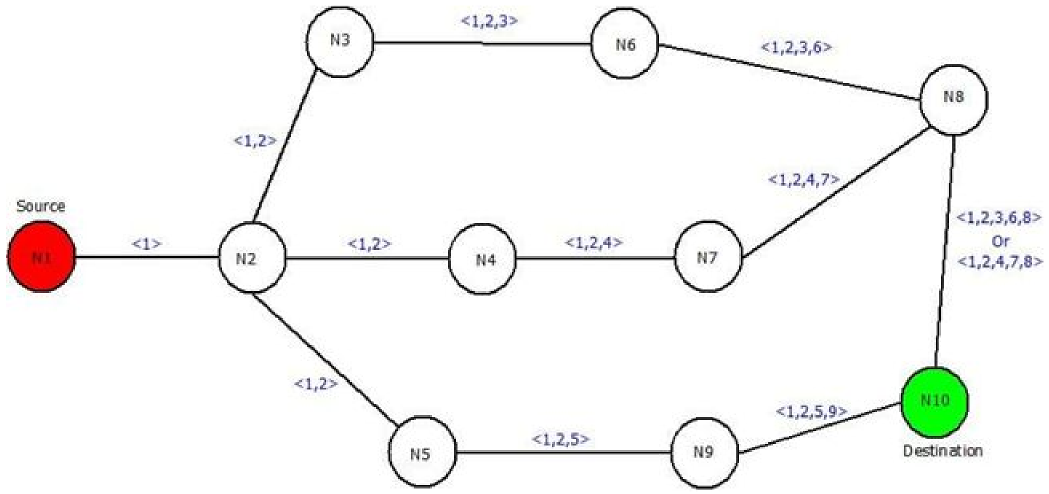
- Dynamic Source Routing does broadcast the route to its neighbors but does not floods the information. It only trace the route by calculating the total distance or by calculating the number of nodes present in between source and destination nodes.
- Consider a network containing 10 nodes where node N1 being the source and node N10 being the destination nodes. Below mentioned steps will let you know how DSR protocol works and how Re-Request packet is transmitted through the network.



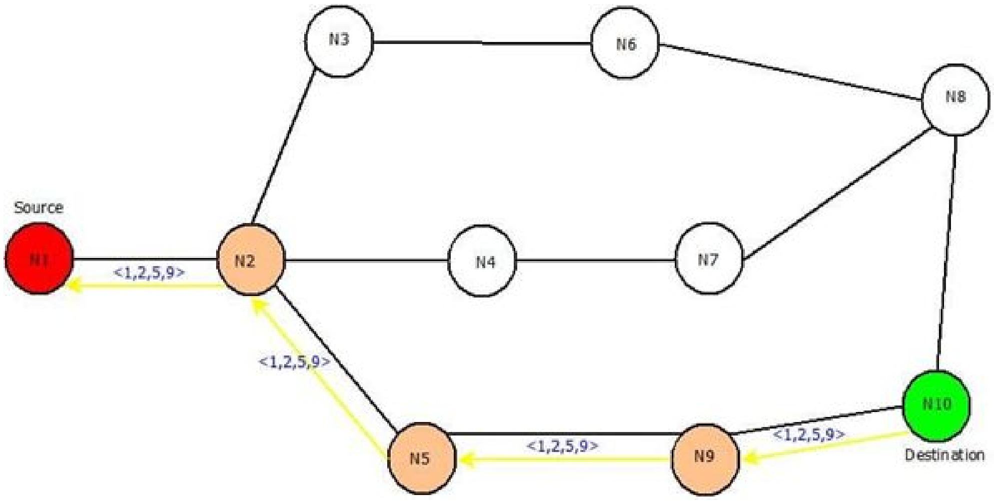
- Step 1: Start from source node N1 and broadcast the information about it to its neighbors i.e. in this case the route information is "<1>", because of its one-to-one link between node N1 and N2.
- Step 2: Broadcast previous route information to neighbors of node N2 i.e. to node N3, N4, N5. The new route will remain same "<1,2>" in all the cases.

- Step 3: Take node N3 and broadcast previous route(<1,2>) to next neighboring nodes i.e. node N6. New route till node N6 will be “<1,2,3>” and same process can be done for other nodes i.e. Node N4 and N5.
- Step 4 : Further, broadcast the new routes i.e. <1,2,3,6> , <1,2,4> , <1,2,5> to nodes N8, N7 & N9 respectively.
- Step 5: Repeat the above steps until destination node is reached via all the routes.

The updated routes will be as:



- After this, “Re-Request” packet will be sent in backward direction i.e. from destination node “N10” to source node “N1”. It will trace the shortest route by counting the number of nodes from route discovered in previous steps.
- The three possible routes are :
  - Route 1: <1,2,3,6,8>
  - Route 2: <1,2,4,7,8>
  - Route 3: <1,2,5,9>
- Route 3 i.e. "<1,2,5,9>” will be chosen as it contains the least number of nodes and hence it will definitely be the shortest path and then data can be transferred accordingly.
- The Re-Request Packet route can be located as:



Most algorithms fail if the links are asymmetric up to the extreme case of unidirectional links. Think of DSR – the algorithm states that the receiver simply sends the packet collecting routers on the way between source and destination back to the source by choosing the routers in the reverse order. But what if some reverse links do not exist? Then DSR has to find a way or the other way round, too. Now source and destination both got a way – but in the wrong direction! Somehow this information must reach the other side – without a route quite difficult broadcast is always a solution.

9. What are Wireless sensor networks? Explain.
Ans.

Wireless sensor networks have evolved from the idea that small wireless sensors can be used to collect information from the physical environment in a large number of situations ranging from wild fire tracking and animal observation to agriculture management and industrial monitoring. Each sensor wirelessly transmits information toward a base station. Sensors help each other to relay the information to the base station, as illustrated in Figure 1.5. The research field of wireless sensor networks has been very active since the early 2000s with several annual conferences, many journals, and a large number of annual workshops. Wireless sensor networks are sometimes called ubiquitous sensor networks to highlight the ubiquity of the sensors.

Wireless sensor networks (WSNs) are interconnected sensor nodes that communicate wirelessly to collect data about the surrounding environment. Nodes are generally low power and distributed in an ad hoc, decentralized fashion. Although WSNs have gained a lot of popularity, there are some serious limitations when implementing security imposed by resource limitations in memory, computing, battery life, and bandwidth. A range of attacks can target privacy, control, or availability. This chapter presents an overview of requirements for encryption, authentication, lightweight public key infrastructure proposals, and key management in WSNs.

10. Explain IoT and IoE.
Ans.

“The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.”

The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data. Thanks to the arrival of super-cheap computer chips and the ubiquity of wireless networks, it's possible to turn anything, from something as small as a pill to something as big as an aeroplane, into a part of the IoT. Connecting up all these different objects and adding sensors to them adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate real-time data without involving a human being. The Internet of Things is making the fabric of the world around us more smarter and more responsive, merging the digital and physical universes.

How does it work?

Devices and objects with built in sensors are connected to an Internet of Things platform, which integrates data from the different devices and applies analytics to share the most valuable information with applications built to address specific needs.
These powerful IoT platforms can pinpoint exactly what information is useful and what can safely be ignored. This information can be used to detect patterns, make recommendations, and detect possible problems before they occur.

What are the main components to IoT?

1. Communication: An IoT device should collect and communicate information. For example, an IoT-enabled HVAC system can report if its air filter is clean and functioning properly. Or, Maersk, a shipping company, could use sensors to track the location of a refrigerated shipping container and its current temperature. Or, you, a consumer, could look to your Nest thermostat for data about your home's temperature.
2. Control: You should be able to remotely or automatically control an IoT device. For example, a business can remotely turn on or shut down a specific piece of equipment or adjust the temperature in a climate-controlled environment. Or, you can use IoT to unlock your car or start the washing machine via an app. Or, you can use Amazon's Alexa platform to control your smart devices. Imagine saying, "Alexa, good night", which will trigger a scene that automatically causes your smart door lock to lock, your smart blinds to close, and your smart lights to turn off.
3. Cost savings: This last one is a bit more loosely defined. While many companies will adopt IoT to save money, consumers will adopt IoT just to automate processes, like in their home, as well as to save money. For instance, you can use IoT-enabled sensors to,

say, measure items, such as driving behavior and speed, in order to reduce fuel expense, or heating meters in homes to better understand energy consumption.

How big is the Internet of Things?

Big and getting bigger -- there are already more connected things than people in the world.
Tech analyst company IDC predicts that in total there will be 41.6 billion connected IoT devices by 2025, or "things." It also suggests industrial and automotive equipment represent the largest opportunity of connected "things,", but it also sees strong adoption of smart home and wearable devices in the near term.

Examples:-
Pretty much any physical object can be transformed into an IoT device if it can be connected to the internet to be controlled or communicate information.
A lightbulb that can be switched on using a smartphone app is an IoT device, as is a motion sensor or a smart thermostat in your office or a connected streetlight. An IoT device could be as fluffy as a child's toy or as serious as a driverless truck.

Internet Of Everything:-

The internet of everything (IoE) is a broad term that refers to devices and consumer products connected to the internet and outfitted with expanded digital features. It is a philosophy in which technology's future is comprised of many different types of appliances, devices and items connected to the global internet.
The term is somewhat synonymous with the internet of things (IoT).
IoE is based on the idea that in the future, internet connections will not be restricted to laptop or desktop computers and a handful of tablets, as in previous decades. Instead, machines will generally become smarter by having more access to data and expanded networking opportunities.
Actual IoE applications range from digital sensor tools/interfaces used for remote appliances to smarter and more well-connected mobile devices, industrial machine learning systems and other types of distributed hardware that have recently become more intelligent and automated.
IoE features fall under two main categories:

- Input: Allows analog or external data to be put into a piece of hardware
- Output: Allows a piece of hardware to be put back into the internet

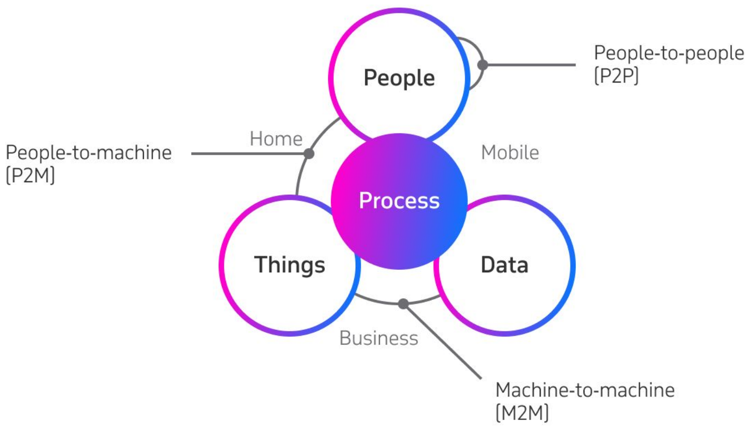
IoE Features

- Decentralization and moving to the edge — data is processed not in a single center, but in numerous distributed nodes
- Data input and output — external data can be put into devices and given back to other components of the network
- Relation to every technology in the process of digital transformation — cloud computing, fog computing, AI, ML, IoT, Big Data, etc. Actually, a rise in Big Data and the IoE technology development are interconnected.

The IoE term is driving much discussion about IT's future. For example, organizations like Cisco use the term in its branding to refer to the potential of modern and future technology.

Pillars of The Internet of Everything (IoE) :-

- People: Connecting people in more relevant, valuable ways.
- Data: Converting data into intelligence to make better decisions.
- Process: Delivering the right information to the right person (or machine) at the right time.



Internet of everything

Data source: cisco.com—The internet of everything. How more relevant and valuable connections will change the world

Things: Physical devices and objects connected to the Internet and each other for intelligent decision making; often called Internet of Things (IoT).

The difference between IoE and IoT :-

The Internet of Everything (IoE) with four pillars: people, process, data, and things builds on top of The Internet of Things (IoT) with one pillar: things. In addition, IoE further advances the power of the Internet to improve business and industry outcomes, and ultimately make people’s lives better by adding to the progress of IoT. (Dave Evans, Chief Futurist Cisco Consulting Services).

The Future :-

The Internet of Everything will re-invent industries at three levels: business process, business model, and business moment.

“At the first level, digital technology is improving our products, services and processes, our customer and constituent experiences, and the way we work in our organizations and within our partnerships,” said Hung Le Hong, research vice president and Gartner Fellow.