B.sc THESIS PAPER

Study on Routing Protocols in Wireless Ad-HOC Networks

The thesis has been submitted to the Department of the Electronics & Communications Engineering at East West University in the partial fulfillment of the requirement for the degree of Bachelor of Science Electronics & Telecommunications Engineering on 31st July 2017.

HON'S Thesis in Electronics and Communications Engineering

STUDY ON ROUTING PROTOCOLS IN WIRELESS AD-HOC NETWORK

Nawshin Rahman Mim

2013-2-55-023

and

Monira Mostafa

2013-2-55-024

East West University, Dhaka

Supervisor: Dr. Anup Kumar Paul

Assistant Professor

Department of Electronics and Communications Engineering

East West University

Dhaka.

Supervisor signature:

ABSTRACT

In computer communications Ad-hoc network is a great concept. A mobile ad-hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links. Mobile ad hoc networks are networks without fixed infrastructure. The mobile nodes perform both as a host and a router forwarding packets to other nodes. Ad-hoc networks has several characteristics which imposes new demands on routing protocols. The most important character is dynamic topology, which is a consequence of node mobility. Nodes can change position quite frequently which means that we need a routing protocol which adapts topology changes quickly. The nodes in ad-hoc networks can consists of laptops and personal digital assistance and other often very limited in resources such as **CPU** capacity, storage capacity ,battery power and bandwidth. This means that routing protocol should try to minimize control traffic, such as periodic updates messages. Instead the routing protocol should be reactive, thus only calculate routes upon a receiving update requests.

Because of the nature of ad hoc networks, there are special demands for ad hoc routing protocols. The performance of MANET is related to the efficiency of the routing protocols in adapting to frequently changing network topology and link status. This thesis paper provides the different categories of routing protocols: Destination-sequenced Distance Vector (DSDV), Ad-hoc On-demand Distance Vector (AODV) and Optimized Link State Routing (OLSR) and the causes of packet losses and their solutions.

TABLE OF CONTENTS

6 PACKET LOSS

LIST OF FIGURES

LIST OF TABLES

B.Sc THESIS PAPER

Study on Routing Protocols in Wireless Ad-HOC Networks

HON'S Thesis in Electrical and Electronics Engineering

STUDY ON ROUTING PROTOCOLS IN WIRELESS AD-HOC NETWORK

Bangladesh 2017

Nawshin Rahman Mim, Monira Mostafa

East West University,Dhaka

Supervisor: Dr. Anup Kumar Paul

Assistant Professor, Department of Electronics and Telecommunication Engineering

East West University

ABSTRACT-

In computer communications Ad-hoc network is a great concept. A mobile ad-hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links. Mobile ad hoc networks are networks without fixed infrastructure. The mobile nodes perform both as a host and a router forwarding packets to other nodes. Ad-hoc networks has several charecterstics which imposes new demands on routing protocols.The most important character is dynamic tropology,which is a consequence of node mobility.Nodes can change position quite frequenty which means that we need a routing protocol which adapts topology changes quickly. The nodes in ad-hoc networks can consists of laptops and personal digital assistance and other often very limited in resources such as **cpu** capacity,storage capacity ,battery power and bandwidth.This means that routing protocol should try to minimize control traffic,such as periodic updates messages.Instead the routing protocol should be reactive,thus only calculate routes upon a receiving update requests.

Because of the nature of ad hoc networks, there are special demands for ad hoc routing protocols. The performance of MANET is related to the efficiency of the routing protocols in adapting to frequently changing network topology and link status.This thesis paper provides the different catagories of routing protocols : Destination-sequenced Distance Vector (DSDV), Ad-hoc On-demand Distance Vector (AODV) and Optimized Link State Routing (OLSR) and the causes of packet losses and their solutions.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER ONE –INTRODUCTION.

1.1 Historical Background

The ability to communicate with people on the move has evolved remarkably since Guglielmo Marconi first demonstrated radio's ability to provide continuous contact with ships sailing the English channel. That was in 1897, and since then new wireless communications methods and services have been enthusiastically adopted by people throughout the world. Particularly during the past ten years, the mobile radio communications industry has grown by orders of magnitude, fueled by digital and RF circuit fabrication improvements, new large-scale circuit integration, and other miniaturization technologies which make portable radio equipment smaller, cheaper, and more reliable. Digital switching techniques have facilitated the large scale deployment of affordable, easy-to-use radio communication networks. These trends will continue at an even greater pace during the next decade.

Wireless communications is enjoying its fastest growth period in history, due to enabling technologies which permit widespread deployment. Historically, growth in the mobile communications field has come slowly, and has been coupled closely to technological improvements. The ability to provide wireless communications to an entire population was not even conceived until Bell Laboratories developed the cellular concept in the 1960s and 1970s. With the development of highly reliable, miniature, solid-state radio frequency hardware in the 1970s, the wireless communications era was born. The recent exponential growth in cellular radio and personal communication systems throughout the world is directly attributable to new technologies of the 1970s, which are mature today. The future growth of consumer-based mobile and portable communication systems will be tied more closely to radio spectrum allocations and regulatory decisions which affect or support new or extended services, as well as to consumer needs and technology advances in the signal processing, access, and network areas.

1.2 Protocol

Protocol means rules.Protocols are used in wireless communication. A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network.

1.3 General

A wireless ad-hoc network is a collection of mobile nodes with no pre-established infrastructure,forming a temporary network.Each of the nodes has a wireless interface and communicate with each other over either radio or infrared. Laptop computers and personal digital assistants that communicate directly with each other and some examples of nodes,such as access points to the internet semi-mobile nodes can be used to deploy relay points in areas where relay points might be needed temporarily.

AN ad-hok network use no centralized administration. This is to be sure that the network wont collaps just because one of the mobile nodes moves out of transmitter range of the others. Nodes should be able to leave the networks they wish. Because of limited transmitter range of the nodes multiple hops may be needed to reach the other nodes.Every node wishing to participate in an ad-hoc network must be willing to forward the packets for other nodes.Thus every nodes acts as both host and as a router. A node can be viewed as an abstract entity consisting of a router and a set of affilimited mobile hosts. A router is an entity which among other things runs a routing protocol protocol.A mobile host is simply an IP – addressable host or entity in the traditional sense.

Ad-hoc networks are also capable of handling tropoloy changes and malfunctions in nodes.It is fixed through network reconfiguration.For instance,if a node leaves the network and causes link breakages, affected nodes can easily request new routers and the problem will be solved. This will slightly increase the delay, but the network will still be operational.

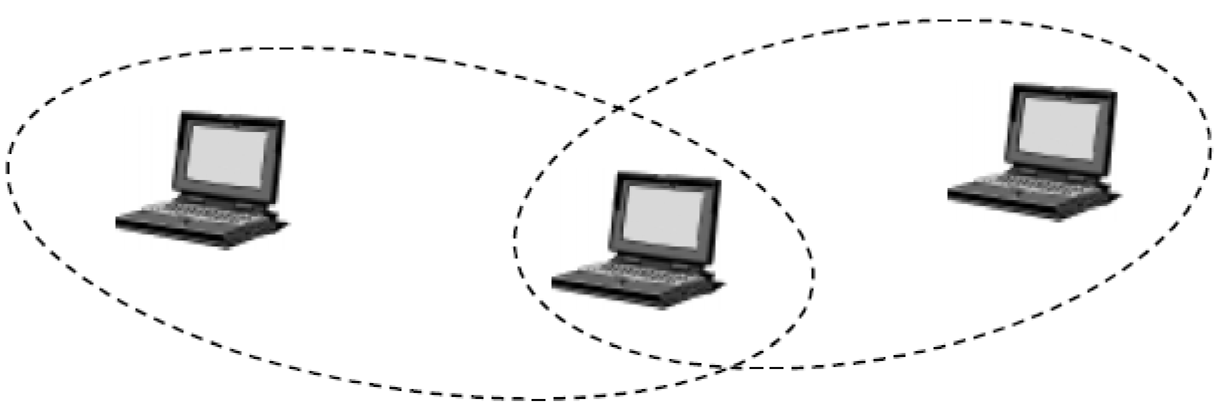


Fig 1.3: A simple Ad-hoc network having three nodes.

1.4 Thesis Outline

The goal is to carry out a systematic performance study of three ad-hoc network routing protocols. The three routing protocols are ad- hoc on demand distance vector protocol(AODV) Destination sequenced Distance-Vector (DSDV) and optimized link state routing protocol(OLSR). Both DSDV and OLSR are regarded as proactive routing protocols and that utilize a table driven technique by recording all routes they find between all source destination pairs regardless of the use or need of such route.the OLSR protocol however is relatively new and the key concept used is that of multipoint relays.The use of MPRs is to minimize routing overhead by reducing duplicate re-transmissions of routing information in the same region.It is an optimization over a pure link state protocol and henceforth expected to perform better in large and dense ad-hoc networks.

CHAPTER TWO- THEORITICAL BACKGROUND.

2.1 Routing

Routers send one another update message advising of changes in in ter network topology and conditions. Each router recalculates its own routing table based on the updated information.

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly.

Hundreds of different network protocols have been created for supporting communication between computers and other types of electronic devices. So-called routing protocols are the family of network protocols that enable computer routers to communicate with each other and in turn to intelligently forward traffic between their respective networks. The protocols described below each enable this critical function of routers and computer networking.

- identify other routers on the network route management - keep track of all the possible destinations (for network messages) along with some data describing the pathway of each path determination - make dynamic decisions for where to send each network message A few routing protocols(called link state protocols) enable a router to build and track a full map of all network links in a region while others (called distance vector protocols) allow routers to work with less information about the network area.

2.2 Classification:

Mobile Ad Hoc Network routing protocols fall into two general categories:

- Proactive Routing Protocols.
- Reactive Routing Protocols.

Different Routing Protocols:

- Flat Routing Protocols.
    - Proactive Routing(table driven) Protocol.
    - ReactiveRouting(on-demand) Protcol.
- Hybrid Routing Protocols.
- Hierarchical Routing Protocols.
- Geographical Routing Protocols.

Routing Protocol Categories:

- Link State Routing Protocol.
- Distance Vector Routing Protocol.

CHAPTER THREE-LINK STATE ROUTING PROTOCOL.

3.1 **Descrption:**

- One of two main classes of routing protocols.
- Every node will have the complete information about the others.
- Pro-active type.

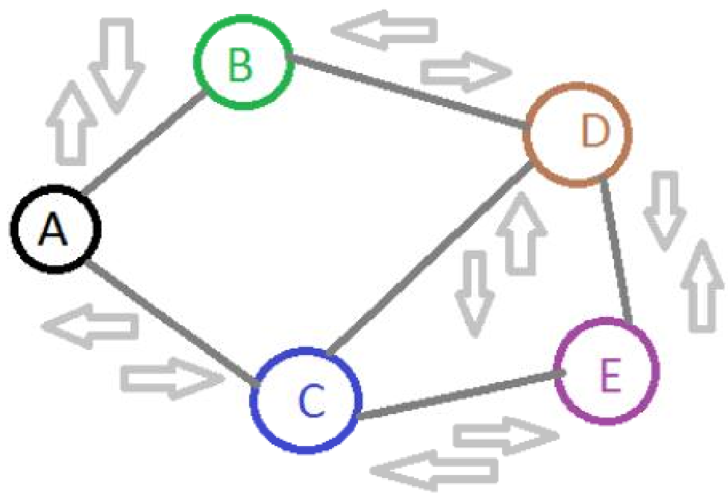


Fig 3.1.1: A network topology of Link State Routing Protocol.

Link-state routing protocols one of the two main classes of routing protocols used in packet switching networks for computer communications, the other being distance-vector routing protocols. Examples of link-state routing protocols include Open Shortest Path First (OSPF) and intermediate system to intermediate system.

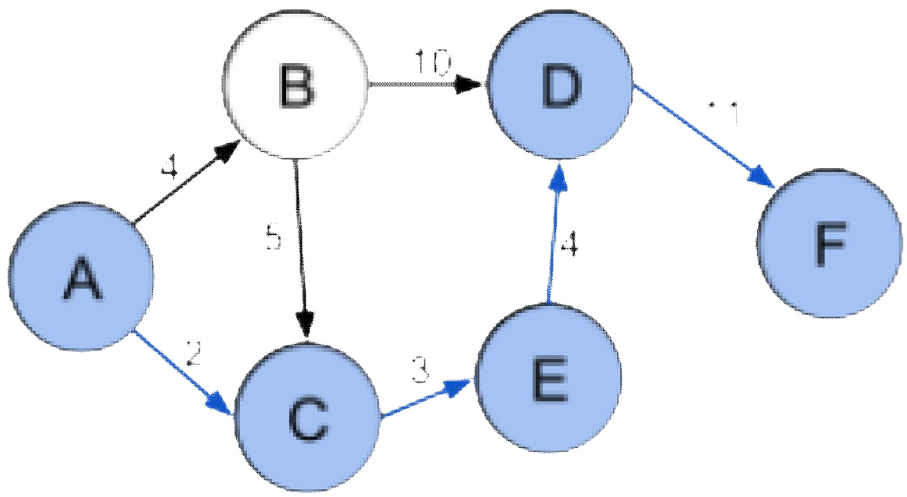


Fig 3.1.2: Process of how Link state Routing Protocol works.

There are two phase:

1) Reliable Flooding:

- Initial State: Each node knows the cost only to its immediate neighbours.
- Final State: Each node knows the entire graph which is called Network Topology.

Each node sends its neighbourhood information which is called link state to all nodes in the network topology reliably.

A will tell the neighbourhood information to B and C at cost 1. If the same thing will done by every other node so finally A will get the entire topology. Suppose this is the original topology and A detects that this is the entire topology. But somehow the link between A and C has failed so A will detect as an entire topology. Now if the packet got lost from A to B so B will think this is the entire topology. Now to reach C, B will send packet to A and again to reach C, a will send the same packet to B. So packet will now get stuck in a loop which we don't want. So this is a problem.

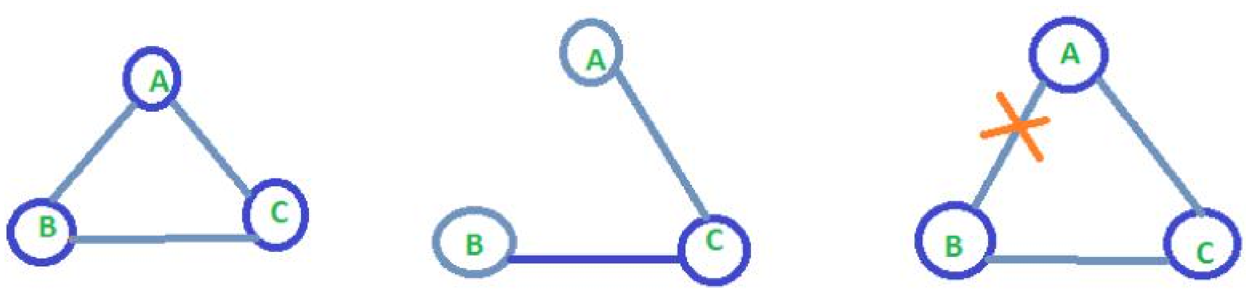


Fig 3.1.3: Network topology of how first state works.

A has some information to send so it will send it to its neighbour nodes B and C. Since C received this information from A so this interference doesn't make any sense to send it back to node A so C will forward it to B. Similarly B will do the same thing and it will forward the information to C. On the other hand if C received information from B so it will again forward this to A and similarly B will do the same thing. Now this process is going to repeat so these packets will be stuck in a loop.

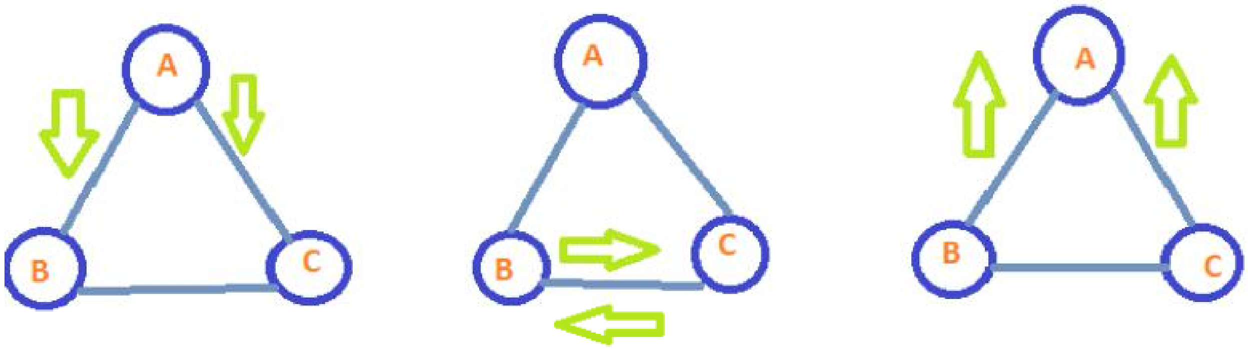


Fig 3.1.4: Network topology of how second state works.

3.2 <u>Drawbacks</u>

- Flooding.
- Unnecessary Transmission.
- Wastage of network Bandwidth.

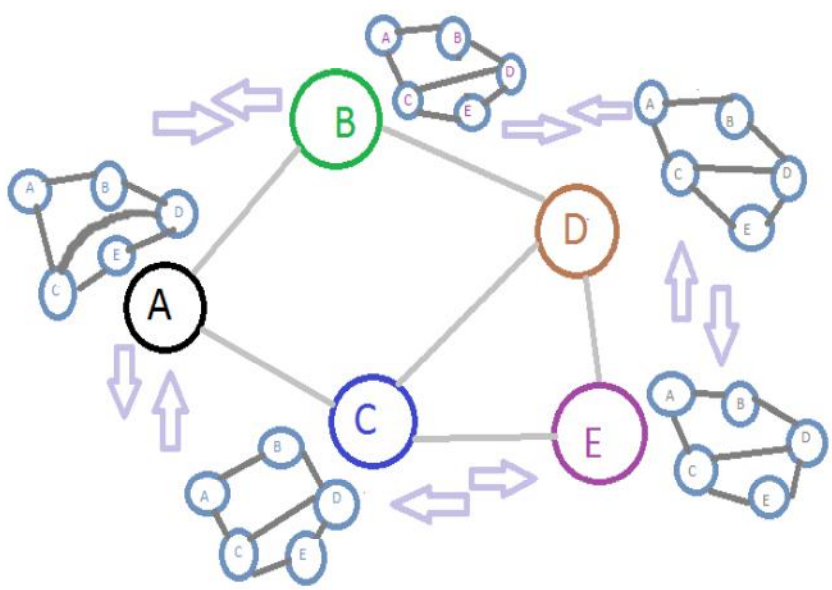


Fig 3.2.1: A network of how drawbacks create.

In flooding process each node will re transmit data to their neighbor nodes. It causes Unnecessary Tranmission which is the wastage of network Bandwidth. So, avoid loops and minimize message exchange by maintaining reliability, at first we need to detects duplicates messages.

- Every packets need unique 'ids'
- For a given id, every node will be sure that this same message with same id (id=x) need not to be send back to the neighbour nodes from where it came.

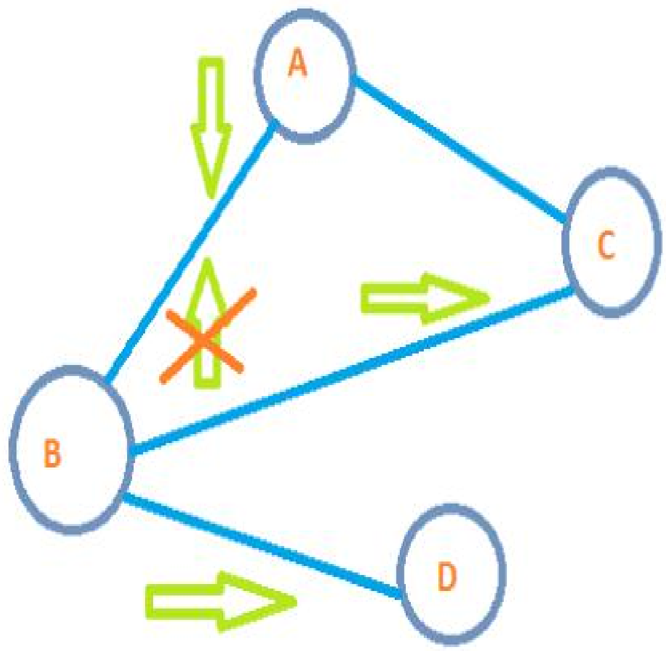


Fig 3.2.2: A network of how drawbacks can be removed.

New information should precede older information.

- Uniquily identifies a packet we need to use sequence number which can do the same work like an unique id.
- At a node, increment sequence number for each new message flooded.

3.3 <u>Route Calculation:</u> Once you have the entire graph, that time very well known Dijkstra's algorithm is used on the graph to calculate Optimal paths to all the nodes. Later we will describe about the steps or process of this algorithm which is very useful process for the Route calculation.

3.4 **Advantages**

- Smaller routing tables. Only a single optimal route for each network ID is stored in the routing table.
- Low network overhead. Link state–based routers do not exchange any routing information when the internetwork has converged.
- Ability to scale.
- Lower convergence time.
- Uses metrics (costs) to calculate path.

3.5 **Disadvantages:**

- They require more memory and processor power than distance vector protocols. This makes it expensive to use for organizations with small budgets and legacy hardware.
- They require strict hierarchical network design, so that a network can be broken into smaller areas to reduce the size of the topology tables.
- They require an administrator who understands the protocols well.
- They flood the network with LSAs during the initial discovery process. This process can significantly decrease the capability of the network to transport data. It can noticeably degrade the network performance.
- Increased complexity in designing networks.

CHAPTER FOUR- OPTIMIZED LINK STATE ROUTING PROTOCOL.

4.1 Description

OLSR is the extension of Link State Routing Protocol. It is Proactive type. Initially the nodes are not aware of each other. In this figure, A is sending an information to it's neighbor nodes so during this process after some time every node they will be having an idea about it's neighbours. And these nodes will re-transmit the information to their neighbours.

- Multi Point Relay(MPR): Every node can selects it's neighbour node who can re-tranmit or re-broadcast packets. So, those nodes are known as MPR. In this figure, C and E is the MPR. Only MPR can re-transmit, other node don't transmit.
- MPR Selector: Node which is selected byt it's one hop neighbour to re-transmit all broadcast information received by it, is the MPR selector. In this figure, A is the MPR selector.

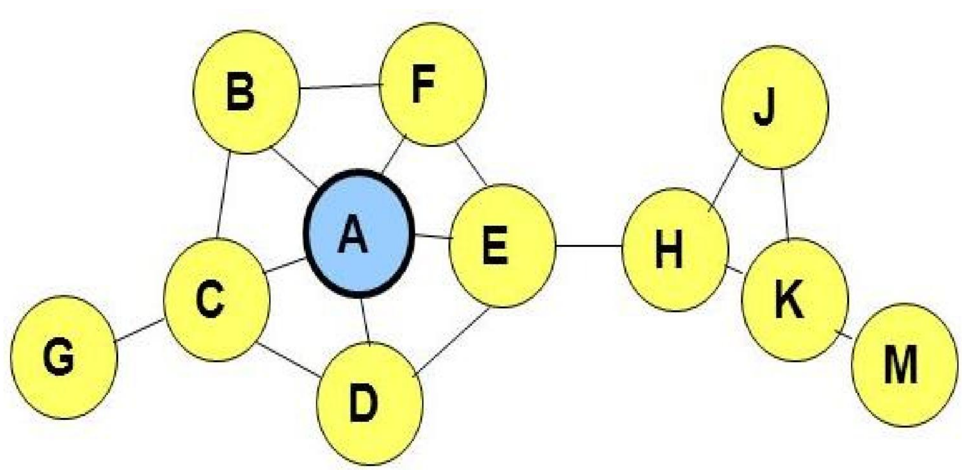


Fig 4.1: How OLSR works in Wireless Network Communications.

4.2 OLSR Terminology:

- Neighbour Node: Node A is neighbour node of B if B can hear A. Similarly H, F, G, C, B are the neighbour nodes of A.
- Two Hop neighbor: A node which can be heard by it's neighbour node. If a neighbour and the node having a distance of two hop that node is a Two Hop neighbour of another node. In this figure I can be heard by H so, I is the two hop neighbour of H. Similarly, J,

D, E are the two hop neighbour of F, C, and B. According to deffination C also can be two hop neighbour of B. Similarly, B is the two hop neighbour of C. And A itself a two hop neighbour of I, J, D, E, B and C.

- Strict two hop neighbor: Node which can be heard by neighbour excluding node itself and it’s neighbour. So, in this figure I, J, D and E are the Strict two hop neighbour.
- MPR: A node which is selected by it’s one hop neighbour to re-transmit all broadcast information received by it. So, in this figure, A is selecting H, F, C, B as the MPR.

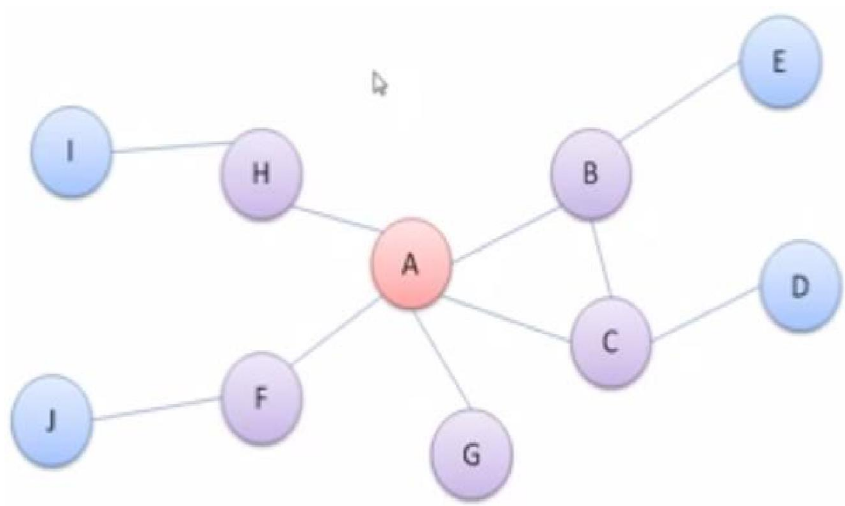


Fig 4.2: How terminology works in a network.

4.3 <u>Links:</u>

4.3.1 Symmetric Link(Bidirectional): A can send any data to B and againg B can resend any data to A so A and B has a Symmetric Link to each other which is called Bidirectional.

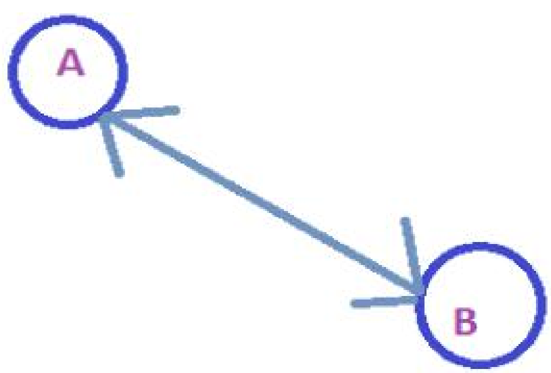


Fig 4.3.1: A structure of Symmetric Link.

4.3.2 Asymmetric Link(Unidirectional): B can send any data to A but A can't send any data to B so B has an Asymmetric Link with A which is called Unidirectional.

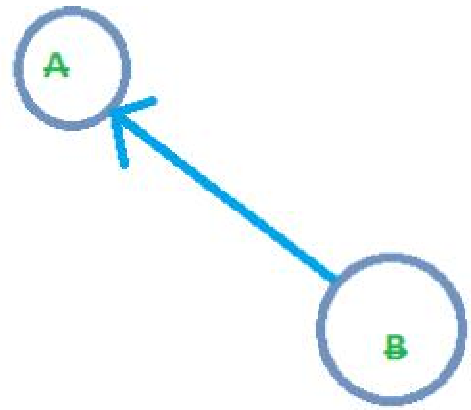


Fig 4.3.2: A structure of Asymmetric Link.

4.4 <u>Symmetric Link:</u>

- Symmetric One Hop Neighbour: Symmetric one hop neighbourhood of any node X is set of neighbours which has at least one Symmetric Link to X. In this figure, X is considering as A. Any neighbours node of A which are having Symmetric Link with A. So, F, G, C and E are called Symmetric One Hop Neighbour Neighbour.(as like One Hop Neighbour)
- Symmetric Two Hop Neighbour: Symmetric two hop neighbourhood of any node X is set of neighbours excluding X itself, which have a Symmetric Link to the Symmetric one hop neighbourhood of X. In this figure, J is having a Symmetric Link with F which is the neighbour of A. Similarly, G also having a Symmetric Link with C and C also having a Symmetric Link with C and both C and G are neighbour of A. So, excluding A itself J, G and C are the Symmetric Two Hop Neighbour.
- Symmetric Strict Two Hop Neighbour: Strict Symmetric Two Hop Neighbourhood of any node X is set of neighbours excluding X itself and it's neighbours which have a Symmetric Link to the Symmetric one hop neighbourhood of X. In this figure, J, G and C are the Symmetric Two Hop Neighbour but G and C are the neighbour of A. So, J is known as Symmetric Strict Two Hop Neighbour excluding G and C.

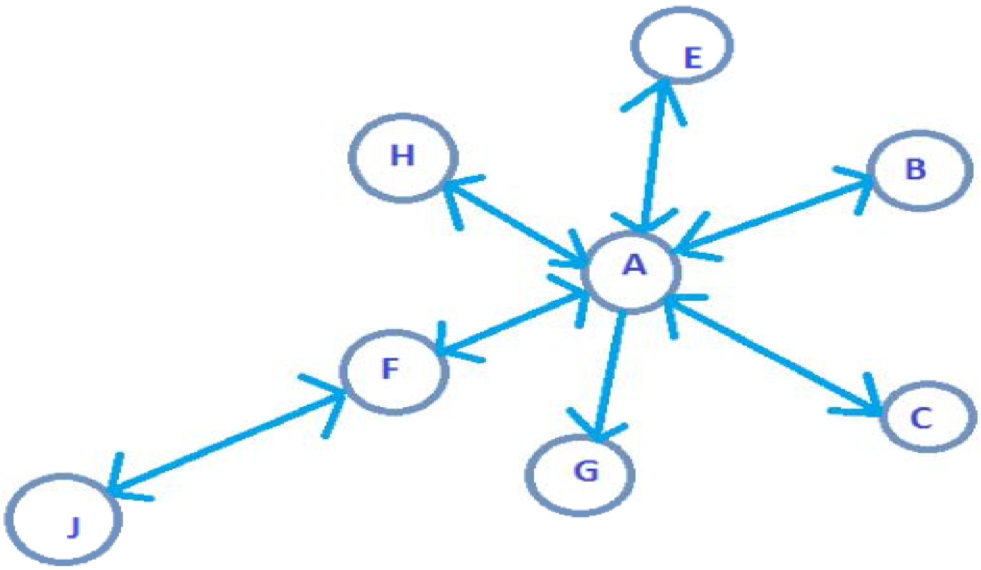


Fig 4.4: How Symmetric links works in a network topology.

4.5 <u>Types of Packets in OLSR:</u>

- Hello Packets: These packets are used to sense link to know the state of link. Every node transmit their neighbour information about state of their link to their neighbours. For those purpose Hello Packets are used.
- Topology Control Packets: These packets are used to tell another node what are the MPR.
- MID Packets: These packets used to inform about multiple interface. If a node is having multiple interface so those interface information is send by MID.

In this figure, D will send a message to it's neighbour nodes C and B. As Hello packets only can be received by One Hop Neighbour. So, C and B will find out D as their One Hop Neighbour. Now C will send this information D and A. So, C is the One Hop Neighbour of D and A. Similarly B will send this packets to it's neighbour D and A. So, D and A will find out B as their One Hop Neighbour. Again A will send this message to C and B. So, A is the One Hop Neighbour of C and B. After a time every node wil have their neighbours information.

Now these node also send this information to their neighbours. So, every node will send their neighbours information in Hello packet. So, when C, B will received these packets from D, C would know that B is a neighbour of D. It means B is far from C with two hop. So, B is the Two Hop Neighbour of C. Similarly, D is the Two Hop Neighbour of A. C is the Two Hop Neighbour of B and A is the Two Hop Neighbour of D.

And in the same process after receiving packets every node will insert an entry for two hop neighbours. Once every node will create their one hop and two hop neighbour information on the basis of Hello packets then they select MPR.

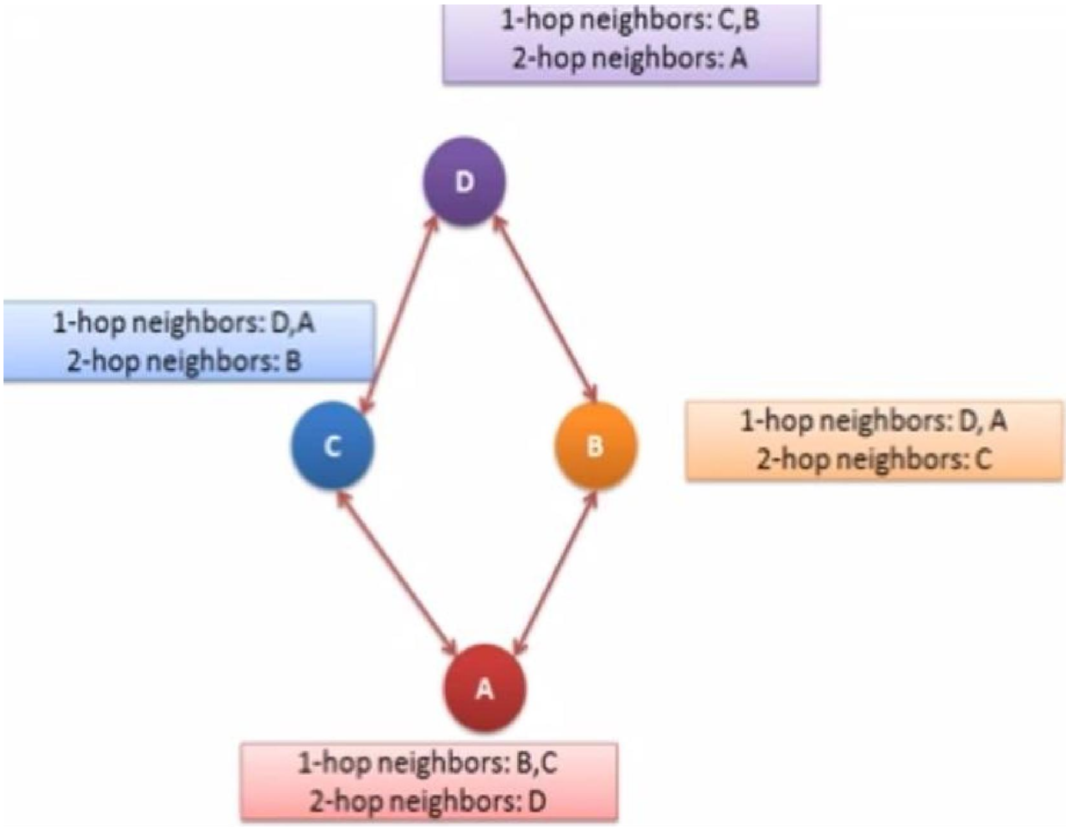


Fig 4.5: How three types of packets works in OLSR network.

4.6 <u>Hello Packets:</u>

- Each node periodically transmit it's Hello packets: These packets actually provide that the node is active and these packets also used to send their existence even their neighbour information.
  - Containing the information about it's neighbours and their link status.
  - Hello messages are received by all one hop neighbour.
- Hello message contains:
  - List of address of the neighbours to which there exits a valid Bidirectional link.
  - List of address of the neighbours which are heard by node (a message has been received).
  - But link is not yet validated as Bidirectional.
- On the reception of Hello message:
  - Each node constructs it's MPR selector table.

4.7 **MPR Selection Algorithm:**

- Each point will be selcted by its MPR's set.
- One neighbourhood of U is represented by N1(u) and two neighbourhood of U is represented by N2(u)

  Steps:
- Select nodes of N1(u) which cover isolated points of N2(u)
  - **Isolated Point:** Some two hop neighbours of N2(u) which are only connected with some nodes of one hop neighbours N1(u)
- How many nodes in two hop neighbours of N2(u) are left. Then from N1(u) we will select those nodes which can cover maximum number of nodes in N2(u).

In this figure, Let's consider u as a MPR selector. u selects the yellow colour nodes for MPR. Red colour are two hop neighbour nodes which are covered by the MPRs. First step complited.

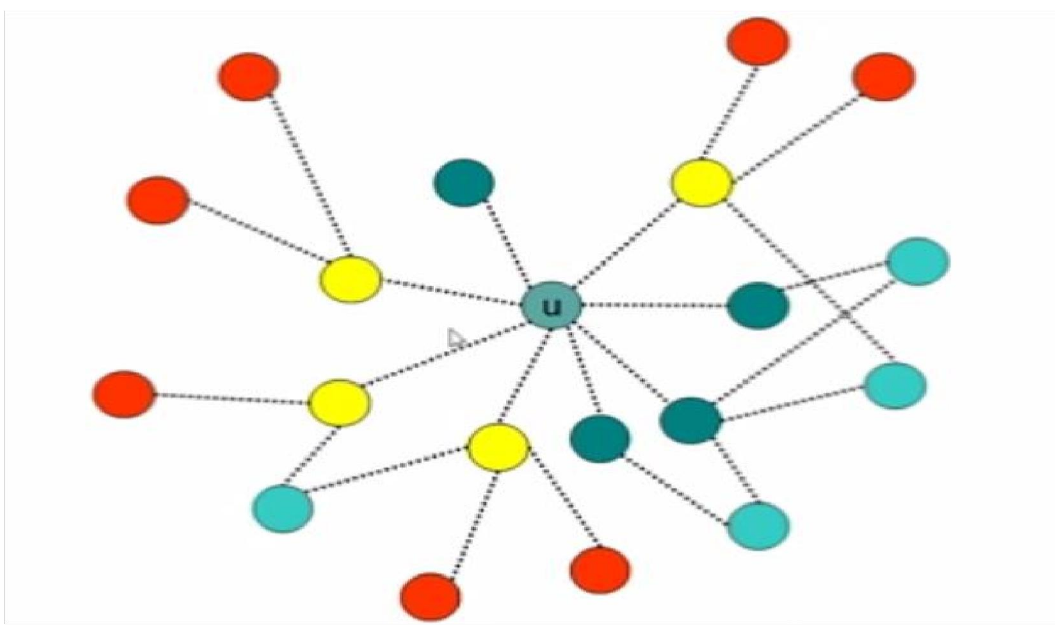


Fig 4.7.1: How MPR selection algorithm works.

In the second step we get four green colour nodes which are called remaining nodes. Now in order to cover these nodes we have to selected nodes in such a way which can covered maximum number of nodes. In the figure-2, if we select two green nodes as MPR so both can cover only one node to their neighbour nodes but if we select the yellow node as MPR so it can cover two red nodes.

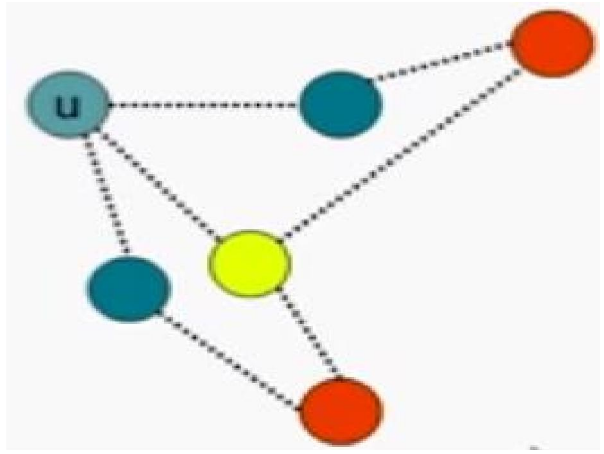


Fig 4.7.2: How Isolated point works.

By the same process, in figure-3 we are getting three MPR that means u node is having five yellow MPR nodes. Each MPR node is covering more than one node.

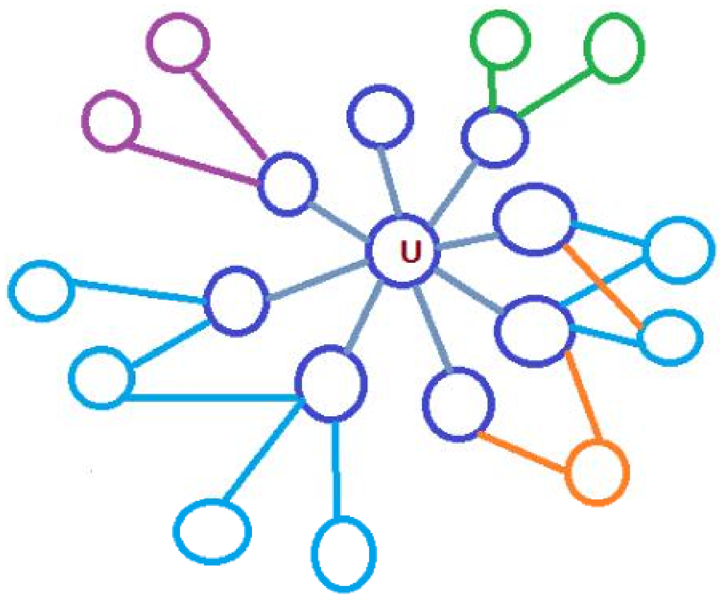


Fig 4.7.3: How the second step of MPR selection algorithm works.

Example: Now these steps we are using in our Network Topology. If we select A is the MPR selector and B, C are the MPR so D will cover both B and C. So, at first A wil follow the first step which tell try to follow the Isolated two hop node which are having connection only single neighbour but node D is connected with two neighbours of B and C. So, there is no first step. In the second step we have to select the node as MPR which can cover maximum node. We can select either C or B. So, whatever message is sending by A it will go to the C and B but as B is the selecting MPR so it will re-transmit the message to D and one copy will be there. **And this is the advantage of Link State Routing Protocol**

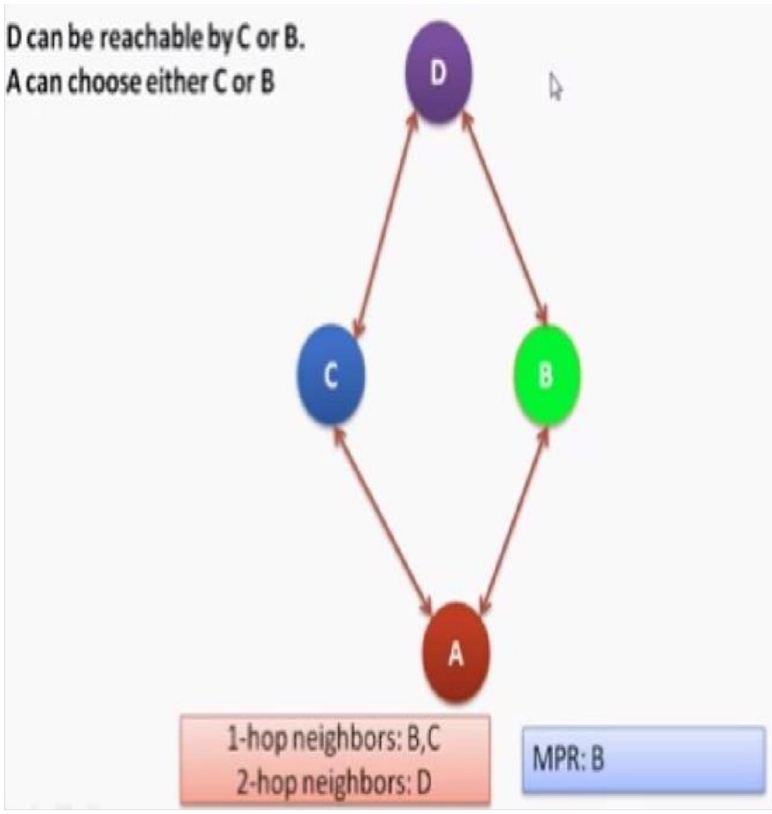


Fig 4.7.4: An example of MPR selection algorithm.

4.8 <u>Advantages</u>

4.9 Disadvantages

4.10 Dijkstra's Algorithm for OLSR

Steps:

- Construct the network or graph.
- Label the starting node with 0_A and put a square box around it which means that this path is visited.
- Look at each of the node connecting to the starting node and choose the one of least value.
- Temporarily label all nodes connecting to the permanent labelled nodes with their distance from the straight point.
- Choose the temporary label of least value and box it.
- Repeat steps 4 and 5 until the node you are trying to reach has a permanent label.
- Retrace the shortest route backwards through the network back to your start node.

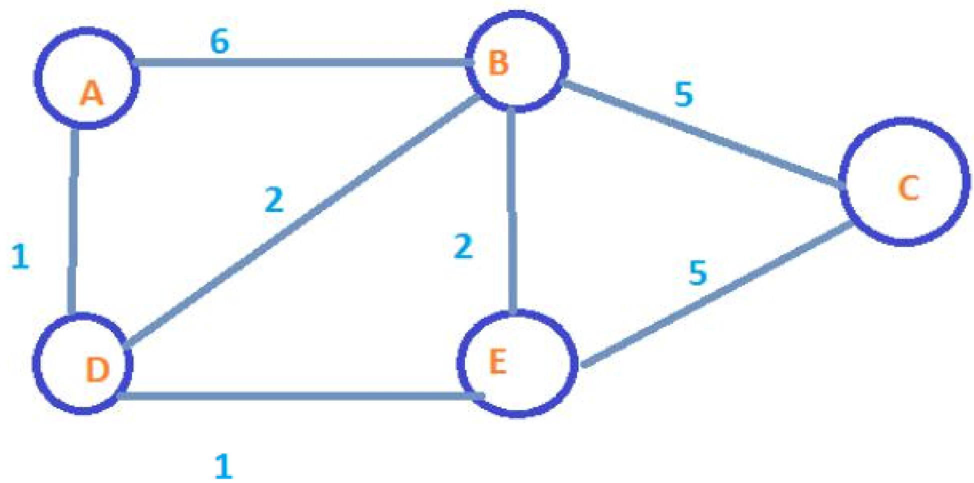


Fig 4.7: An example of Dijkstra's Algorithm.

V	A	B	C	D	E
A	**0_A**	6_A	∞	1_A	∞
B		3_D	∞	**1_A**	2_D
C		3_D	7_E		**2_D**
D		**3_D**	7_E		
E			**7_E**		

- The shortest path is, A-D-E-C = 1+1+5 = 7.

CHAPTER FIVE-Distance Vector Routing Protocol.

- **Description**

Every node transmit information distance with every other node. These distance count in the no. of hops. Initially every node are not aware of other nodes in the network all they know is about their neighbours. So, they exchange information in the network and after some time every node will be having distance cost for every other nodes. If a link is broken in that case, the cost will be infinity.

  - Distance: How Far.
  - Vector: In which Direction

In Distance vector when we are sending the message to neighbour nodes the node will again sends the same information to it's neighbour nodes. After some time all nodes will have the same information. To solve this problem we will use a sequence number when we will send information to it's neighbour.

This is an extension of Distance Vector Routing Protocol. Every node share their routing table to the neighbours. After receiving these tables other nodes update a new table and again re-transmit those tables.

In this figure we are not using Next Hop field, we are only using Destination and Distance cost here. A has idea about B and C. B is in 1 at distance cost and C is in 1 at distance cost. As A has no idea about D so D is in infinity (∞) at distance cost. In the same manner every node initialize their routing table. Every node broadcast their routing table to it's neighbours. This is the Initial Routing.

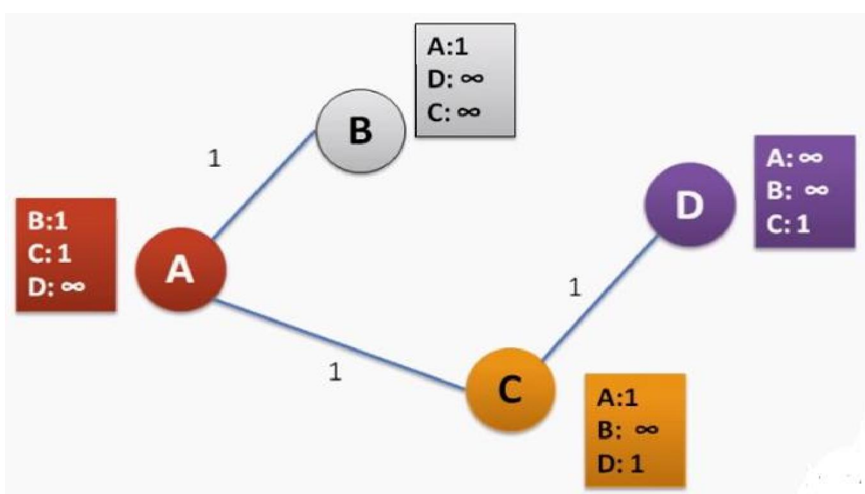


Fig 5.1: How Distance Vector Routing Protocol works.

A will broadcast information table to it's neighbours B and C. On the basis of these received tables B and C B and C will update their table. Here, B will find out that it won't be able to go C and D. As, C is reachable from A so B will re-transmit the table to A. So, B will set C cost = 2 = 1+1 (B to A = 1 + A to C = 1). B would know that there is a path to C from A because this table has been received from node A.

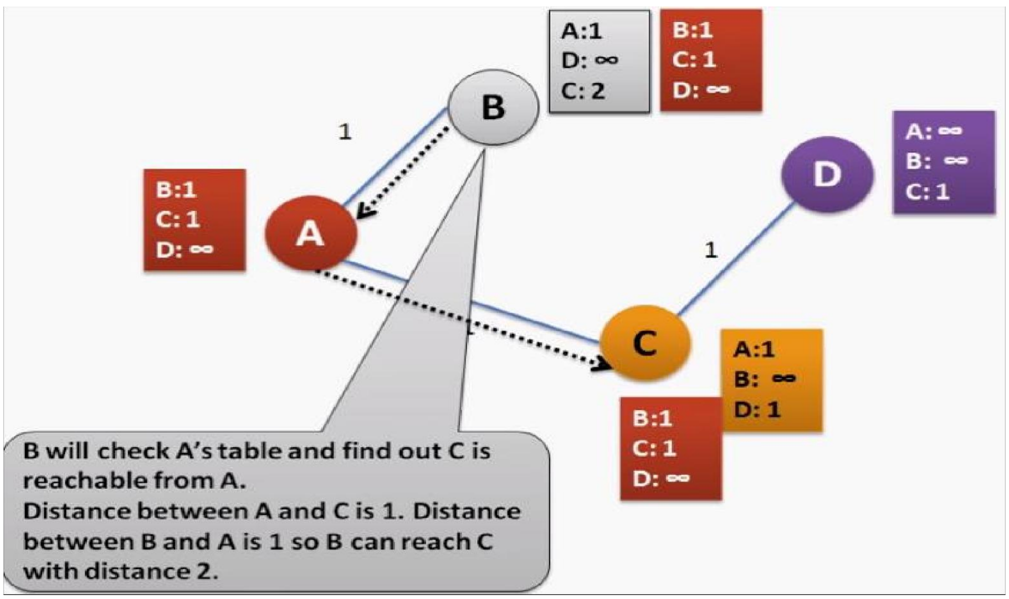


Fig 5.2: How Distance Vector Routing Protocol works by using updated table.

Now, for node C, B is unreachable. But the table received from A saying B is reachable at cost 1 so from C the total cost is 2. C will update it's table and make it 2. That means this is a path to B from A.

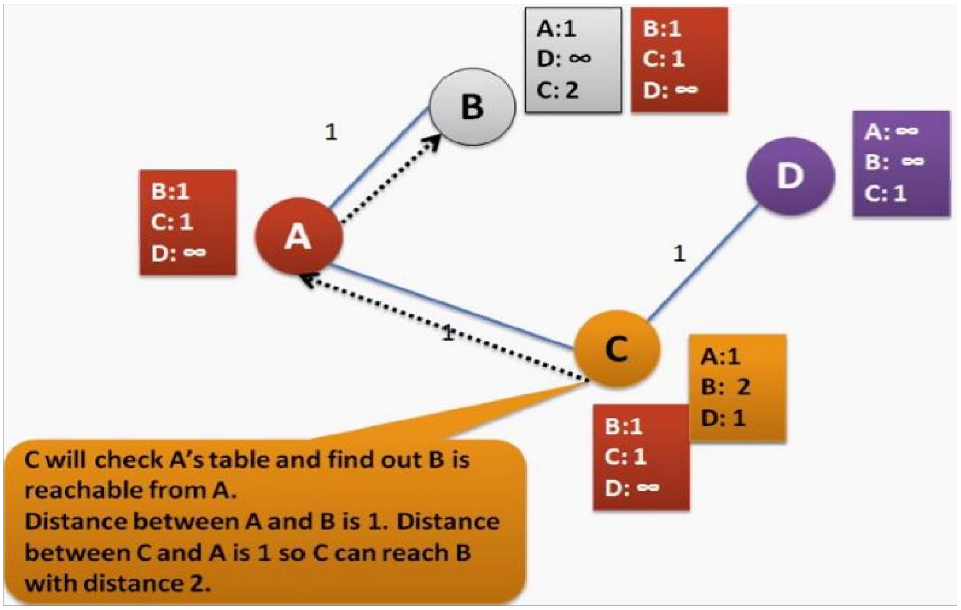


Fig 5,3: How Distance Vector Routing Protocol works by using updated table.

Now, C is transmitting routing table to it's neighbour A and D. C is reachable to B with distance cost= 2 = 1+1(C to A + A to B). D will check C's table a to A + A to B). D also find out that it can reach A via C with Distance cost = 2 = 1+1(D to C + C to A)

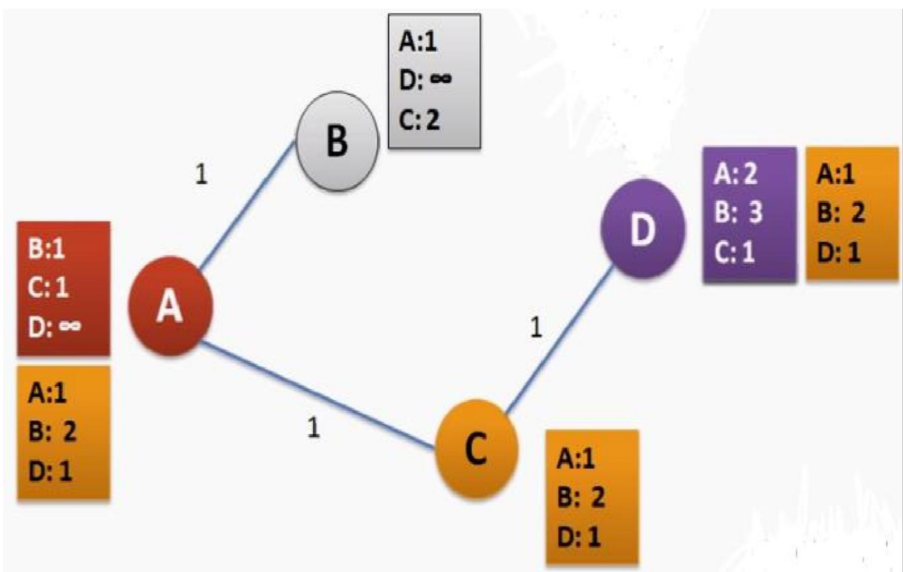


Fig 5.4: How Distance Vector Routing Protocol works with distance cost.

Each node also need to store direction. Node B can reach node D via A. Node B has to store this information. Similar as for A node.

- **Advantages:**
  - Distance Vector is a relatively simple approach and easy to use, implement and maintain and does not require High-level knowledge to deploy.
  - It does not demand high bandwidth level to send their periodic updates as the size of the packets are relatively small.
  - Distance vector protocols do not require a large amount of CPU resources or memory to store the routing data.

- **Disadvantages:**
  - The main drawbacks of Distance Vector are limited scalability due to slow convergence time, bandwidth consumption and routing loops.
  - It is not suitable for large networks that require very small propagation delay.
  - Another problem is bandwidth consumption, which is caused by the unsolicited periodic update, which takes place every 30 seconds if the network has not changed.
  - One final problem is the routing loops, which has a severe impact on the overall network performance.

- **Bellmen Ford Algorithm:**

Steps:

- It is based on Bellmen Ford Algorithm.
- Initial state at a node: Distance cost to neighbours.
- Final state at a nod: Distance cost to all nodes are known and also the next hop.
- Need to handle:
  - ➢ What information to exchange.
  - ➢ How to act on an information.
  - ➢ When to send an information.
- Each node maintains a routing table(distance vector):
  - ➢ Destination.
  - ➢ Estimate Cost.
  - ➢ Next hop via which to reach destinations.
- Each node exchanges with all it's neighbours routing info called "Routing Table". It can share only:
  - ➢ Destination and estimated cost to destination.

➢ Next hop information is not shared.

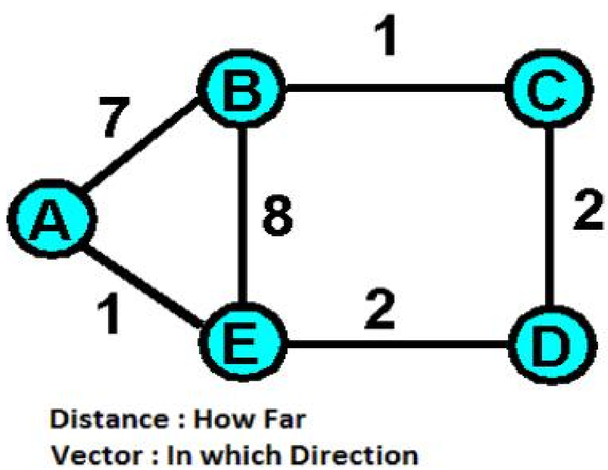


Fig 5.4: How Bellmen Ford Algorithm works.

Initally E is the given table and second table is the message from B.

Routing Table Of **E**

Source	Cost	Next Hop
A	1	A
B	8	B
D	2	D

Message from **B**

Source	Cost
B	0
A	7
E	8
C	1

Using Bellmen Ford Algorithm,

DX (Y) = min {Current-Estimate , Cost (X , V) + DV(Y)}

Here,

X = source;
Y = Destination;
V = Intermediate Node

DE(A) = min {1, Cost(E,B) +DB(A)} = min (1, 8+7) = 1
DE(B) = min {8, Cost(E,B) +DB(B)} = min (8, 8+0) = 8

DE(D) = min {2, Cost(E,B) +DB(D)} = min (2, 8+∞) = 2
DE(C) = min {∞ , Cost(E,B) +DB(C)} = min (∞, 8+1) = 9

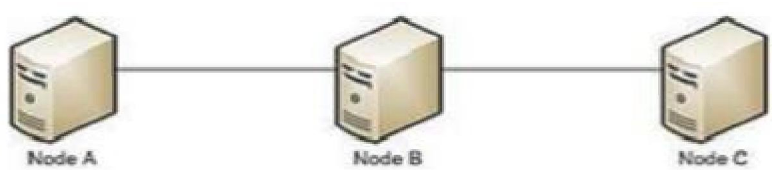
Updated Routing Table of E

Source	Cost	Next Hop
A	1	B
B	8	B
D	2	D
C	9	B

5.5 <u>Destinationa Sequenced Distance Vector Routing Protocol(DSDV)</u>

5.5.1 <u>Description</u>

Destination Sequenced Distance Vector Routing Protocols are Proactive type.



For example the routing table of Node A in this network is

Destination	Next Hop	Number of Hops	Sequence Number
A	A	0	A 46
B	B	1	B 36
C	B	2	C 28

Fig 5.5.1: How Destination Sequenced Distance Vector works.

5.5.2 Advantages:

- DSDV was one of the early algorithms available. It is quite suitable for creating ad hoc networks with small number of nodes. Since no formal specification of this algorithm is present there is no commercial implementation of this algorithm.
- DSDV guarantees for loop free path.

5.5.3 Disadvantages:

- DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle.
- Whenever the topology of the network changes, a new sequence number is necessary before the network re-converges; thus, DSDV is not suitable for highly dynamic networks.

5.6 AD-HOC on Demand Distance Vector(AODV)

5.6.1 Description:

Ad Hoc On-Demand Distance Vector (AODV) is Reactive or on Demand. uIt ses bi-directional links. Route discovery cycle used for route finding. It maintance active routes. Sequence numbers used for loop prevention and as route freshness criteria. Provides unicast and multicast communication.

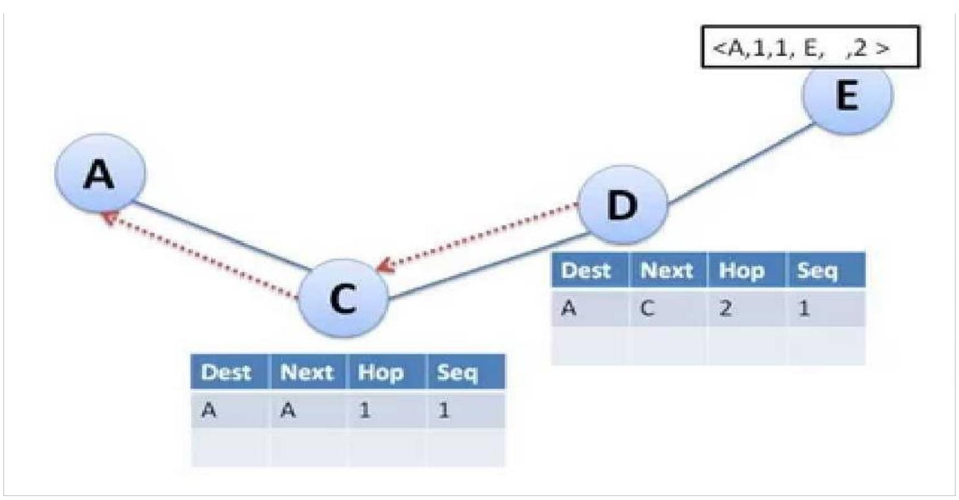


Fig 5.6.1: How Ad-Hoc on demand Routing Protocol works.

5.6.1 **Advantages**

- AODV protocol is that routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The connection setup delay is less.
- The HELLO messages supporting the routes maintenance are range-limited, so they do not cause unnecessary overhead in the network.

5.6.2 **Disadvantages:**

- Here intermediate nodes can lead to inconsistent routes if the source number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having staleentries.
- Multiple Route Reply packets in responseto a single Route Request packet can lead to heavy control overhead.
- AODV is that the periodic beacoming leads to unnecessary bandwidth consumption.

5.7 Dynamic Source Routing(DSR)

5.7.1 Description:

Dynamic Source Routing (DSR) is Reactive type. It 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.

Any data to another node at that time they will go for route searching, they will not maintain any information. So, we are considering this network node S is representing source node and D is representing destination node. And the other node work as an intermediate node. Node S wants to send data to node D. But S don’t know the route to reach D. At first it will search a neighbour route.

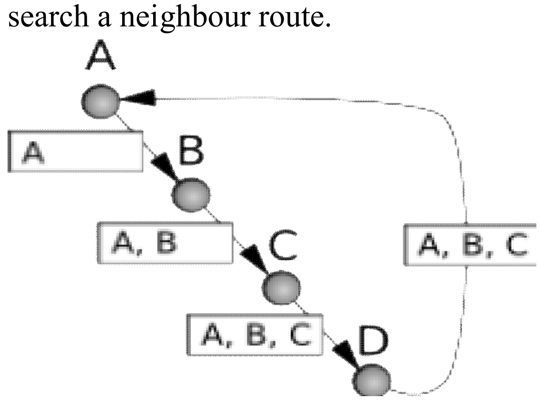


Fig 5.7.1: How Dynamic Source Routing Protocol works.

5.8 Advantages:

- This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach.

5.9 Disadvantages:

- The route maintenance mechanism does not locally repair a broken link.
- The connection setup delay is higher than in table-driven protocols.
- Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility.

CHAPTER SIX-PACKET LOSS.

When one user is sending data to an another user, that time data transmits in a packet. Packets of data are sent over the network at specific time intervals. If a packet does not reach to its end destination, that time the original user will receive a ping which alerts user that a packet was unsuccessful to reach.

Fig: Process of Packet Loss.

6.1 **Packet Loss Defination**

First, let's break down the term.

The first part, 'packet', is technical shorthand for 'data packet'.Regardless of what you're doing on the internet, consistent online connectivity is reliant on your home network's ability to send and receive data packets.

The second part of the term, 'loss', is more straightforward.

It refers to an instance where one or more data packets fail to reach its or their intended destination.

Certain applications tend to be built with packet loss in mind, which means you may never notice if a low number of packets are dropped, as they're seamlessly re-requested and retransmitted.

In other online scenarios, packet loss can result in a reduced experience.

For instance, online gaming and file transfers are dependent on zero packet loss for a smooth (gaming) or complete (file transfer) experience.

Packet loss occurs when one or more packets of data travelling across a computernetwork fail to reach their destination. Packet loss is typically caused by networkcongestion. Packet loss is measured as a percentage of packets lost with respect topackets sent.

6.2 <u>Cause of Packet Loss</u>

REASONS BEHIND PACKET LOSS AND THEIR REMEDI:

1. Link Congestion

Your data must travel through multiple devices and links during its trip across your network. If one of these links is at full capacity when your data arrives, then it must wait its turn before being sent across the wire (this is known as queuing).

If a network device is falling very far behind, it won’t have room for the new data to wait (queue), so it does the only thing it can, which is to discard the information.

Hearing that data is “discarded” may sound harsh, but most applications are able to gracefully handle this, and the user probably won't ever notice it. The user’s application realizes that a packet was lost, slows down its transfer speed, and re-transmits the data. If this was a file download, an email, or another non real-time application, the effect will be minimal as long as the packet loss doesn’t continue to happen.

Some applications do not handle this very well at all, and the effect is very noticeable to the users. If you are on a phone call and the network loses some data, there is no time to resend the packets since it is a real-time conversation. The user will typically hear breaks in the audio during small packet loss, and potentially lose the phone call if the packet loss is severe. Another critical application that has a low threshold for packet loss is video conferencing. If data is lost between the two end points, the video will show artifacts and the audio will be distorted.

Remediation

There are two main ways to help reduce the effect of packet loss due to network congestion:

- Increase the bandwidth of the congested link(s).
- Implement Quality of Service (<u>QoS</u>) to give priority to real-time traffic. This will not help the congestion of the link, but it can give priority to applications like voice or video which lowers the likelihood of a drop.

2. Device (Router/Switch/Firewall/etc.) Performance

If your bandwidth is adequate, you can still face an issue if your router/switch/firewall is not able to keep up with the traffic.

Let's take a scenario where you recently upgraded a link from 1Gb to 10Gb because traffic reports show that you were at full capacity during peak hours of the day. After the upgrade, your charts show the bandwidth going up to 1.5Gb, but you are still experiencing network performance issues. The issue could be that the device is not able to keep up with the traffic, and you have hit the maximum throughput your hardware can provide.

The traffic is reaching the device, but the device's CPU or memory is maxed out and not able to handle extra traffic.

This results in packet loss for all traffic that is beyond the capacity of the box.

Remediation

You must replace the hardware with a new appliance that can handle your maximum throughput, or potentially cluster additional hardware to increase your throughput.

3. Software issues (bugs) on a network device

While we can hope that the software written for our network devices is perfect, I can assure you that it is not. These network devices are extremely complex, and it is a matter of time before you stumble upon a bug.

These bugs can cause new features to not work at all when you deploy them, or can go undetected for awhile before you may notice performance issues.

Once the performance issue is detected and troubleshooting has started, these types of issues are usually found using system logs and packet captures.

Remediation

You must upgrade the software on the affected device(s).

4. Faulty Hardware or Cabling

Your traffic report shows that your links are not over-utilized, and the hardware utilization is within specification. The next common issue that can lead to drops would be a physical component that is malfunctioning.

If hardware is not working properly, it will usually lead to error messages being seen on the console of the device or within system logs.

If there is a link issue, it can usually be seen as errors on an interface. This can be seen on both copper cabling and fiber optic.

Remediation

The faulty hardware must be replaced, or the fault link must be repaired.

These are the most common reasons for packet loss on a network, but there are many other reasons that can contribute to packet drops. The best way to determine the root cause is through a network assessment and detailed troubleshooting.

A partner who is specialized in uncovering various network pitfalls can help you plan a remediation strategy so that you don't have to live with a degraded network.

CHAPTER SEVEN-FIELDS OF AD-HOC ROUTING PROTOCOL

7.1 Characteristics

- No fixed Infrustructure.
- Multi-hoping: Obstacles, Spectrum, Reuse, Energy conservation.
- Dynamic topologies The topic refers to the most essential property of an ad hoc network: Nodes can move arbitrarily with respect to other nodes in the network.
- Bandwidth-constrained Nodes in an ad hoc network are mobile. Thus, they are using radio links that have far lower capacity than hardwired links could use. In practice the realized throughput of a wireless network is less than a radio's theoretical maximum transmission rate.
- Energy constrained operation.
- Mobile nodes are likely to rely on batteries. That is why the primary design criteria may sometimes be energy conservation.
- Security: limited.
- Limited physical security In general, radio networks are vulnerable to physical security threats compared to fixed networks. The possibility of eavesdropping, spoofing and DoS attacks is higher. Existing link security techniques can be applied. However, a single point failure in an ad hoc network is not as crucial as in more centralized networks.
- Scalability: thousands of nodes.

7.2 Properties:

- Distributed operation: This property is essential to ad hoc networks. It is selfevident that ad hoc networks operate in distributed manner because of their very nature.
- Loop-freedom: This property is generally desirable. It refers to avoiding packets spinning around in the network for arbitrary time. Solutions such as TTL values can be used to limit performance effects of the problem. However, a more structured or a sophisticated solution will probably lead to better overall performance.
- Demand based operation: Ad hoc routing does not have to assume uniform traffic load in a network but it can adapt to traffic patterns on need basis. This will increase route discovery delay but when implemented intelligently bandwidth and energy resources can be more efficiently utilized.
- Proactive operation: This is opposite to demand based operation. If additional delays that occur in demand based operation are unacceptable, proactive approach can be used specially when energy and bandwidth capacities support the use of proactive operation.
- Security: Because of the vulnerabilities in the physical security mentioned in section 2.1, ad hoc routing protocols are exposed to many kind of attacks. Maintaining link layer security is in

practice harder with ad hoc networks than with fixed networks. Sufficient routing protocols security is desirable. Sufficient within this context covers prohibiting.

7.3 Applications:

- Mobile Ad Hoc Networks include establishing survivable, efficient and dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks.
- MANETs are not solely intended for disconnected autonomous operations or scaled scenarios.
- Wearable Computing.
- It provides extended service and allows low-cost, low complexity dynamic adjustments to provide coverage regions and range extensions away from the more fixed infrastructure backbone networks.
- Sensor Networks.
- Wireless Mesh Networks.
- A hybrid infrastructure extension is a dynamic enhancement to a home or campus wireless networking environment.
- Butterfield: Unmanned ground/air-borne/Under water vehicles.

7.4 Advantages and Challenges of Ad-Hoc Networks:

- Lower getting-started costs.
- Well suited to free unlicensed spectrum.
- Inherent scalability.
- Hidden terminal problem.
- Power control necessarily more coarse than on full-duplex IS-95 or HDR channel.

7.5 Disadvantages and Limitations of Ad-Hoc Networks:

- Higher error rate.
- Lower data rate.
- Dynamic topology and scalability.
- Security:
  - Eavesdropping,Traffic analysis,Masquerading,Replay (active).
  - Message modification (active), Denial-of-service or interruption.
- Energy Limitation.

Characteristics and Properties:
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.443.4992&rep=rep1&type=pdf

Different types of Protocols: https://krazytech.com/technical-papers/mobile-ad-hoc-network

Applications: https://krazytech.com/technical-papers/mobile-ad-hoc-network

Advantage and Disadvantage of Link State Routing Protocol:
http://www.cisco.com/networkers/nw03/presos/docs/RST-1001.pdf

Advantage and Disadvantage of Distance Vector Routing Protocol:
http://expertitgurus.blogspot.com/2011/02/advantages-and-disadvantages-of.html

Description of Packet Loss: http://www.nbnco.com.au/blog/education/packet-loss-what-it-is-and-what-causes-it.html

Causes of Packet Loss: http://www.annese.com/blog/what-causes-packet-loss

Advantage and Diadvantage of Destination sequenced Direct Vector Routing Protocol:
http://www.readorrefer.in/article/Destination-Sequenced-Distance-Vector--DSDV---Algorithm--Illustration--Advantages--Disadvantages_9940/

Description of Ad-Hoc on Demand Routing Protocol: https://www.cs.jhu.edu/~cs647/aodv.pdf

Advantage and Disadvantage of Ad-Hoc on Demand Routing Protocol:
http://www.academia.edu/15442120/Performance_Comparison_of_AODV_DSR_On-Demand_Routing_Protocols_for_Ad_Hoc_Networks

Protocol:
https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.google.com%2Furl%3Fsa%3Dt%26source%3Dweb%26rct%3Dj%26url%3Dhttps%253A%252F%252Fwww.lifewire.com%252Ftop-network-routing-protocols-explained-817965%26ved%3D0ahUKEwje8L6ypabVAhXKnJQKHTSjC64QFgh0MA0%26usg%3DAFQjCNH3AL6rZsfsgzWphVt63SDIdYya2w&h=ATN4I4GbH7VWsMbmgwPHhygYVp4nZHBAX4oQW7DLneB_BS8btRhpCFiAKO_dvhjqWYnbYKe0UgsaPYBrOVb6hTdM5Pt4Mc_fIddbdt_PqZ2XLdfuvIrG6FKPsPOv1BWOw5_XUCi-biP7mQ

[1] History: Graduate School of Information and Communication, Ajou University **School of Information and Computer Engineering, Ajou University Suwon, Republic of Korea jmc@crhc.uiuc.edu, youngko@ajou.ac.kr

[2] Protocol: Djamel,Abdelouahid Derhab,and Nadjib Badache Basic software Laboratory,CERIST research center,Algeria.Computer science Department,USTHB university,Algeria.
A PERFORMANCE ANALYSIS OF ROUTING PROTOCOLS FOR AD-HOC NETWORKS by Ghee Lye Pore March 2006 Thesis Advisor: John C. McEachen Second Reader: Weilian Su.

[3] Characteristics and Properties: Sampo Naski Helsinki University of Technology Telecommunications Software and Multimedia Laboratory.

[4] Applications: Mobile Ad Hoc Network Routing Protocols and Applications By Ravi Bandakkanavar | September 24, 2016

[5] Advantage and Disadvantage f Ad-Hoc Networks: PERFORMANCE COMPARISON OF AODV/DSR ON-DEMAND ROUTINGPROTOCOLS FOR AD HOC NETWORKS. Jethva Harikrishna, Department of Computer Engineering L. D. College of Engineering, Ahmedabad (Gujarat-India)

[6] Classification: Mobile Ad Hoc Network Routing Protocols and Applications By Ravi Bandakkanavar | September 24, 2016

[7] Advantage and Disadvantage of Link State Routing Protocol: C.Jeyalakshmi, Assistant Professor, Department of CSE, SIT, Dr.R.Sukumar, Professor, Department of CSE, SIT

[8] Advantage and Disadvantage of Optimized Link State Routing Protocol: International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 6, June 2015

[9] Advantage and Disadvantage of Distance Vector Routing Protocol: Introduction to Link State Protocols Session RST-1001 Scott Sturgess

[10] Description of Destination Sequenced Direct Vector Routing Protocol: Routing Protocols in Wireless Ad-Hoc Networks-A Simulation Study. Stockholm. 1998. Tony Larsson and Nicklas Hedman, LuleaUniversity of Technology.

[11] Advantage and Disadvantage of Destination Sequenced Direct Vector Routing Protocol: Destination-Sequenced Distance Vector (DSDV) Protocol Guoyou He Networking Laboratory Helsinki University of Technology

[12] Description of Ad-Hoc on Demand Routing Protocol: Routing Protocols in Wireless Ad-Hoc Networks-A Simulation Study. Stockholm. 1998. Tony Larsson and Nicklas Hedman, LuleaUniversity of Technology.

[13] Advantage and Disadvantage of Ad-Hoc on Demand Routing Protocol: PERFORMANCE COMPARISON OF AODV/DSR ON-DEMAND ROUTINGPROTOCOLS FOR AD HOC NETWORKS. Jethva Harikrishna, Department of Computer Engineering L. D. College of Engineering, Ahmedabad (Gujarat-India)

[14] Advantage and Disadvantage of Dynamic State Routing Protocol: PERFORMANCE COMPARISON OF AODV/DSR ON-DEMAND ROUTINGPROTOCOLS FOR AD HOC NETWORKS. Jethva Harikrishna, Department of Computer Engineering L. D. College of Engineering, Ahmedabad (Gujarat-India)

[15] Description of Packet Loss: Introduction to Link State Protocols Session RST-1001 Scott Sturgess scsturge@cisco.com

[16] Causes of Packet Loss: http://www.annese.com/blog/what-causes-packet-loss