ANALYSIS OF REACTIVE ROUTING PROTOCOLS BASED ON SIMULATION TIME FOR MANETs

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Software Engineering

By:
Deepak Chaudhary
(800831001)

Under the supervision of:
Mr. Sumit Miglani
Assistant Professor, CSED

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

JUNE-2010

Certificate

I hereby certify that the work which is being presented in the thesis entitled, **"Analysis of Reactive Routing Protocols Based on Simulation Time for MANETs"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in Software Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Mr.Sumit Miglani and refers other researcher's works which are duly listed in the reference section.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

Deepak Chaudhary

(Deepak Chaudhary)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Sumit Miglani

(Mr. Sumit Miglani)
Assistant Professor
Computer Science and Engineering Department
Thapar University, Patiala

Countersigned by

24/07/10

(Dr. RAJESH BHATIA)
Head, Computer Science & Engineering, Department,
Thapar University,
Patiala.

R.K. Sharma 24/7/10

(Dr. R.K.SHARMA)
Dean (Academic Affairs)
Thapar University,
Patiala.

Acknowledgement

I am highly thankful to my guide, **Mr.Sumit Miglani**, Assistant Professor Computer Science and Engineering Department, Thapar University, Patiala for his advice, motivation, guidance, moral support, efforts and the attitude with which he solved my queries in making this thesis possible. It has been great honor to work under him.

I am also thankful to **Dr. Rajesh Bhatia**, Head of Department, CSED, **Dr.Inderveer Chana**, P.G. Coordinator and **Dr. Anil Kumar Verma,** Assistant Professor, for the motivation and inspiration that triggered me for the thesis work.

I would also like to thank the staff members and my colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis.

Most importantly, I would like to thank my **Mother,** my Brothers and my Friends for showing me the right direction out of the blue, to help me stay calm in the oddest of the times and keep moving even at times when there was no hope.

Deepak Chaudhary

Deepak Chaudhary

(800831001)

Abstract

The recent advancements in the field of the wireless networks lead to the development of the short-lived networks formally known as Mobile Adhoc Networks. Mobile Adhoc Networks are the networks that basically consist of mobile nodes connected to each other through the wireless links. In this each mobile node plays the dual role of acting both as a router and the host in order to forward, send and receive packets to the other node. The mobile nodes are free to move anywhere and organize themselves into the network when they come in the range of each other. To forward the packets in the mobile adhoc network the routing protocol is needed.

The routing protocol in Mobile Adhoc Networks is classified into two classes: the table driven routing protocols and on demand driven protocols.

In this thesis work an attempt has been made to study, understand the behavior of the existing protocols and to analyze the difference between the two frequent used reactive protocols DSR and AODV in terms of packet losses and packets received by varying the simulation time and finding out with the help of simulation analysis carried out in the ns-2 simulator that which one out of two performs better when the mobile adhoc network has to be formed.

The results presented in this thesis work help us to choose one protocol out of two when the mobile adhoc network has to be set up for the small amount of time.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ABR	Associativity-Based Routing
AODV	Ad-hoc On-demand Distance Vector
CBR	Continuous Bit Rate
DSDV	Destination Sequenced Distance Vector Routing
DSR	Dynamic Source Routing
GPS	Global Positioning System
GUI	Graphical User Interface
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
MAC	Message Authentication Code
MANET	Mobile Ad hoc Network
MANETs	Mobile Ad hoc Networks
NAM	Animator
NS	Network Simulator
OLSR	Optimized Link State Routing
OTcl	Object Oriented Tool Command Language
RERR	Route RERRor
RREP	Route REPly
RREQ	Route REQuest
RWPMM	Random Waypoint Mobility Model
TCL	Tool Command Language
TCP	Transmission Control Protocol
TORA	Temporally Ordered Routing Algorithm
URL	Uniform Resource Locator
VINT	Virtual Internetwork Test-bed
WRP	Wireless Routing Protocol
ZHLS	Zone-Based Hierarchical Link State Protocol
ZRP	Zone Routing Protocol

Chapter 1
Introduction

1.1. Introduction

Wireless networks refer to those networks that make use of radio waves or microwaves in order to establish communication between the devices. The wireless network offers certain advantages over the wired networks that are as follows:

- Setting up a wireless system is easy and fast and it eliminates the need for pulling out the cables through walls and ceilings.
- Wireless networks can be extended to the places that cannot be wired.
- Wireless networks offer more flexibility and adapt easily to changes in the configuration of the network.

Wireless networks can be classified in two types: Infrastructure network and Infrastructure less (ad hoc) networks. These are defined as follows:

1.1.1. Infrastructure networks

In the infrastructure-based network, communication typically takes place only between the wireless nodes and the access point, but not directly between the wireless nodes. The access point does not just control medium access, but also acts as a bridge to other to wireless or wired networks. The base stations are fixed as the node goes out of the range of a base station; it gets into the range of another base station. The cellular networks are infrastructure-based network.

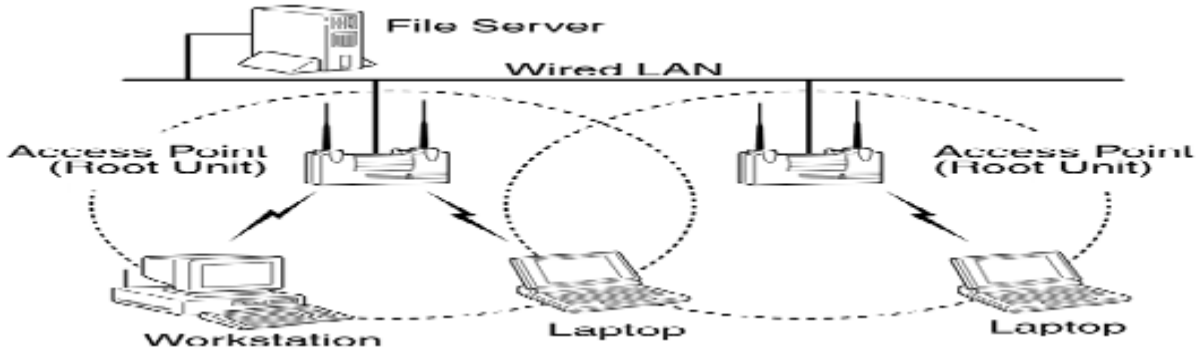


Figure 1.1: An Infrastructure Network [1]

1.1.2. Infrastructure less networks

Ad-hoc wireless network do not need any infrastructure to work .Each node can communicate directly with other node so no access point controlling medium access is necessary. Infrastructure less networks, do not have fixed routers all the nodes in the network need to act as routers and all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Mobile Ad hoc Networks (MANET) are example of infrastructure less network. In the ad hoc network shown in Figure 1.2, node A can communicate with node D via nodes B and C, and vice versa.

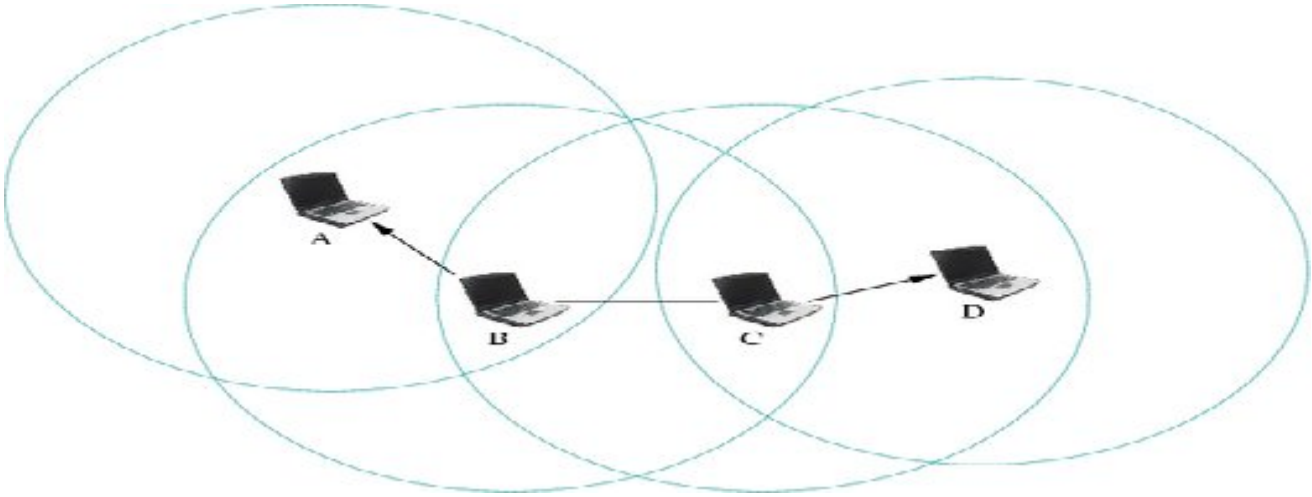


Figure 1.2: An Infrastructure less Network [2]

1.2. Mobile Adhoc Network

Mobile Adhoc Network (MANET) refers to a form of infrastructure less network connecting mobile devices with wireless communication capability. Each node behaves as a router as well as an end host, so that the connection between any two nodes is a multi-hop path supported by other nodes [3]. MANET represents a system of wireless mobile nodes that can freely and dynamically self-organize in to arbitrary and temporary network topologies, allowing people and devices to communicate without any pre-existing communication architecture. Each node in the network also acts as a router, forwarding data packets for other nodes. They communicate directly with devices inside their radio range in a peer-to-peer nature. If they wish to communicate with a device outside their range, they can use an intermediate device or devices within their radio

range to relay or forward communications to the device outside their range. An ad hoc network is self-organizing and adaptive [4].

We quote the definition of a mobile ad hoc network from the charter of the corresponding Internet Engineering Task Force (IETF) "A 'mobile ad hoc network' (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links-the union of which forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet"[5].

The presence of wireless communication and mobility make an adhoc network unlike a traditional wired network, and requires the routing protocols used in ad hoc network based on new and different principles. Routing in ad hoc environment is one of the important issues of the most challenging and interesting research areas in MANET. Since mobile ad hoc network change their topology frequently, routing in such network is a challenging task. Generally, the main function of routing in a network is to detect and maintain the optimal route to send data packets between source and destination via intermediate nodes. A MANET is a peer-to-peer network that allows direct communication between any two nodes, when adequate radio propagation conditions exist between these two nodes. If there is no direct link between the source and the destination nodes, multi-hop routing is used. In multi-hop routing, a packet is forwarded from one node to another, until it reaches the destination.

1.2.1. MANET Characteristics [5]

- **Autonomous and infrastructure less**-MANET is self-organized and independent of any established infrastructure and centralized network administration. Each node runs as a router and operates in distributed manner.

- **Multihop routing-** As there is no dedicated router, every node functions as a router and aids in forwarding each others' packets to intended destination. Hence, information sharing among mobile nodes is made available.

- **Dynamic network topology-** Since MANET nodes move randomly in the network, the topology of MANET changes frequently, leading to regular route changes, network partitions, and possibly packet losses.

- **Variation on link and node capabilities-** Each participating node may be equipped with different type of radio devices that have varying transmission and receiving capabilities, and possibly operate on multiple frequency bands Asymmetric links might be resulted due to this heterogeneity in the radio capabilities. Additionally, different software or hardware configuration might result in variability in processing capabilities. Thus, designing and standardization of MANET protocols and algorithms for this heterogeneous network are complicated as dynamic adaptation is required.

- **Energy-constrained operation-** The processing power of node is restricted because the batteries carried by portable mobile devices have limited power supply. As a result, the services and applications that can be supported by each node are limited. Network protocols must be developed to be power-aware since each node is functioning as both an end system and a router.

- **Network scalability-** Many MANET applications may involve large networks with tens of thousands of nodes especially that can be found in tactical networks. Scalability is crucial to the successful deployment of MANET.

1.2.2 MANET Applications [5]

There are many applications of MANET:

- **Military battlefield-**The modern digital battlefield demands robust and reliable communication in many forms. Most communication devices are installed in mobile vehicles, tank, trucks etc. Also soldiers could carry telecomm devices that could talk to a wireless base stationer directly to other telecom devices if they are within the radio range. However these forms of communication are considered to be primitive. At times when wireless base station is destroyed by enemy, a soldier will be prohibited from communicating with other soldier if the called party is not within the radio range. This is the scenario where mobile ad hoc networks come into play. Adhoc networks are well known as self organizing networks since they are robust when nodes disappear due to

destruction or mobility. Through multi-hop communication, soldiers can communicate to remote soldiers via data hoping and data forwarding from one radio device to another.

- **Sensor Networks-**Another application of MANETs is sensor networks. This technology is a network composed of a very large number of small sensors. These can be used to detect any number of properties of an area. Examples include temperature, pressure, toxins, pollutions, etc. Applications are the measurement of ground humidity for agriculture, forecast of earthquakes. The capabilities of each sensor are very limited, and each must rely on others in order to forward data to a central computer. Individual sensors are limited in their computing capability and are prone to failure and loss. Mobile adhoc sensor networks could be the key to future homeland security.

- **Automotive Applications-**Automotive networks are widely discussed currently. Cars should be enabled to talk to the road, to traffic lights, and to each other, forming ad-hoc networks of various sizes. The network will provide the drivers with information about road conditions, congestions, and accident-ahead warnings, helping to optimize traffic flow.

- **Commercial sector-**Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small handheld. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

- **Personal Area Network**-Personal Area Networks (PANs) are formed between various mobile (and immobile) devices mainly in an ad-hoc manner, e.g. for creating a home network. They can remain an autonomous network, interconnecting various devices, at home, for example, but PANs will become more meaningful when connected to a larger network. In this case PANs can be seen as an extension of the telecom network or Internet. Closely related to this is the concept of ubiquitous / pervasive computing where people, noticeable or transparently will be in close and dynamic interaction with devices in their surroundings.

1.3. Motivation

A wireless network is a growing new technology that will allow users to access services and information electronically, irrespective of their geographic position. Wireless Networks are classified in two classes - infrastructure network and infrastructure less (ad hoc) networks. On the other hand the adhoc networks work without any pre-existing infrastructure. They are easy to deploy and set up at any place and time, hence it decreased the dependence of the infrastructure. Routing is the integral part of any kind of the network as it not only exchanges the data but also the control information in the form of packets with its respective connected nodes in its range. There are varieties of routing protocols available in the area of the mobile adhoc networks. Witnessing and simulating their behavior by varying different parameters for improving the performance of the adhoc network is the motivation for the chosen of the topic.

1.4. Thesis Outline

The thesis consists of 6 chapters which are organized as follows:
In Chapter 1 describes the introduction of wireless networks and mobile ad hoc network characteristics and its application, motivation and thesis outline, Chapter 2 explains the concept of routing protocols of MANET including the detailed description of AODV and DSR protocols, Chapter 3 covers the problem statement, Chapter 4 describes the simulation model, Chapter 5 discusses the results of DSR and AODV protocols on varying simulation time and Chapter 6 describes conclusion with fixed parameters and feature scope.

Chapter 2
Literature Review

2.1. Routing

Routing is a process of determining a path between source and destination upon request of data transmission during this process, at least one intermediate node within the internetwork is encounter. This concept is not new to computer science since routing was used in the networks in early 1970's. But this concept has achieved popularity from the mid- 1980's. The major reason for this is because the earlier networks were very simple and homogeneous environments; but, now high end and large scale internetworking has become popular with the latest advancements in the networks and telecommunication technology. The routing protocol has two main functions, selection of routes for various source-destination pairs and the delivery of messages to their correct destination. The second function is conceptually straightforward using a variety of protocols and data structures.

Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement; such as path bandwidth, reliability, delay, current load on that path etc; that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which contain route information. Route information varies depending on the routing algorithm used.

Routing algorithms fill routing tables with a variety of information. Mainly Destination/Next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular node representing the "next hop" on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop. Some of the routing algorithm allows a router to have multiple "next hop" for a single destination depending upon best with regard to different metrics. For example, let's say router R2 is be best next hop for destination "D", if path length is considered as the metric; while Router R3 is the best for the same destination if delay is considered as the metric for making the routing decision[6].

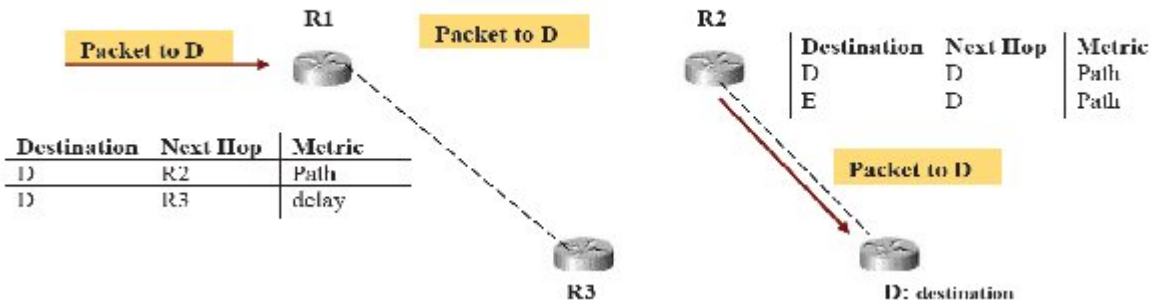


Figure 2.1: Routing in a Network [6]

Figure 2.1 shows a small part of a network where packet destined for node "D", arrives at router R1, and based on the path metric i.e. the shortest path to destination is forwarded to router R2 which forward it to the final destination. Routing tables also can contain other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes, and these metrics differ depending on the design of the routing algorithm used. Routers communicate with one another and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analyzing routing updates from all other routers, a router can build a detailed picture of network topology.

Routing is mainly classified into static routing and dynamic routing. Static routing refers to the routing strategy being stated manually or statically, in the router. Static routing maintains a routing table usually written by a networks administrator. The routing table doesn't depend on the state of the network status, i.e., whether the destination is active or not. Dynamic routing refers to the routing strategy that is being learnt by an interior or exterior routing protocol. This routing mainly depends on the state of the network i.e., the routing table is affected by the activeness of the destination [7]. The major disadvantage with static routing is that if a new router is added or removed in the network then it is the responsibility of the administrator to make the necessary changes in the routing tables. But this is not the case with dynamic routing as each router announces its presence by flooding the information packet in the network so that every router within the network learn about the newly added or removed router and its entries. Similarly this is the same with the network segments in the dynamic routing [8].

2.1.1. Conventional protocols

If a routing protocol is needed, why not use a conventional routing protocol like link state or distance vector? They are well tested and most computer communications people are familiar with them. The main problem with link-state and distance vector is that they are designed for a static topology, which means that they would have problems to converge to a steady state in an ad-hoc network with a very frequently changing topology.

Link state and distance vector would probably work very well in an ad-hoc network with low mobility, i.e. a network where the topology is not changing very often. The problem that still remains is that link-state and distance-vector are highly dependent on periodic control messages. As the number of network nodes can be large, the potential number of destinations is also large. This requires large and frequent exchange of data among the network nodes. This is in contradiction with the fact that all updates in a wireless interconnected ad hoc network are transmitted over the air and thus are costly in resources such as bandwidth, battery power and CPU. Because both link-state and distance vector tries to maintain routes to all reachable destinations, it is necessary to maintain these routes and this also wastes resources for the same reason as above. Another characteristic for conventional protocols are that they assume bi-directional links, e.g. that the transmission between two hosts works equally well in both directions. In the wireless radio environment this is not always the case. Because many of the proposed ad-hoc routing protocols have a traditional routing protocol as underlying algorithm, it is necessary to understand the basic operation for conventional protocols like distance vector, link state and source routing.

2.1.2. Link State

In link-state routing [9], each node maintains a view of the complete topology with a cost for each link. To keep these costs consistent; each node periodically broadcasts the link costs of its outgoing links to all other nodes using flooding. As each node receives this information, it updates its view of the network and applies a shortest path algorithm to choose the next-hop for each destination. Some link costs in a node view can be incorrect because of long propagation delays, partitioned networks, etc. Such inconsistent network topology views can lead to

formation of routing-loops. These loops are however short-lived, because they disappear in the time it takes a message to traverse the diameter of the network.

2.1.3. Distance Vector

In distance vector [9] each node only monitors the cost of its outgoing links, but instead of broadcasting this information to all nodes; it periodically broadcasts to each of its neighbors an estimate of the shortest distance to every other node in the network. The receiving nodes then use this information to recalculate the routing tables, by using a shortest path algorithm. Compared to link-state, distance vector is more computation efficient, easier to implement and requires much less storage space. However, it is well known that distance vector can cause the formation of both short-lived and long-lived routing loops. The primary cause for this is that the nodes choose their next-hops in a completely distributed manner based on information that can be stale.

2.1.4. Source Routing

Source routing [9] means that each packet must carry the complete path that the packet should take through the network. The routing decision is therefore made at the source. The advantage with this approach is that it is very easy to avoid routing loops. The disadvantage is that each packet requires a slight overhead.

2.1.5. Flooding

Many routing protocols uses broadcast to distribute control information, that is, send the control information from an origin node to all other nodes. A widely used form of broadcasting is flooding [9] and operates as follows. The origin node sends its information to its neighbors (in the wireless case, this means all nodes that are within transmitter range). The neighbors relay it to their neighbors and so on, until the packet has reached all nodes in the network. A node will only relay a packet once and to ensure this some sort of sequence number can be used. This sequence number is increased for each new packet a node sends.

2.2. Routing in Mobile Ad hoc Networks

Routing in MANETs is difficult since mobility causes frequent network topology changes and requires more robust and flexible mechanisms to search for and maintain routes. When the

network nodes move, the established paths may break and the routing protocols must dynamically search for other feasible routes. With a changing topology, even maintaining connectivity is very difficult. In addition, keeping the routes loop free is more difficult when the hosts move. Besides handling the topology changes, routing protocols in MANETs must deal with other constraints, such as low bandwidth, limited energy consumption, and high error rates, all of which may be inherent in the wireless environment. Furthermore, the possibility of asymmetric links, caused by different power levels among mobile hosts and other factors such as terrain conditions, make routing protocols more complicated.

2.3. Problems with routing in Mobile Ad-hoc Networks

- **Asymmetric links:** Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad-hoc networks as the nodes are mobile and constantly changing their position within network. For example consider a MANET where node B sends a signal to node A but this does not tell anything about the quality of the connection in the reverse direction [10].

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

- **Interference:** This is the major problem with mobile ad-hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other nodes and can corrupt the total transmission.

- **Dynamic Topology:** This is also the major problem with ad-hoc routing since the topology is not constant. The mobile node might move or medium characteristics might change. In ad-hoc networks, routing tables must somehow reflect these changes in topology and routing algorithms have to be adapted. For example in a fixed network routing table updating takes place for every 30sec [10]. This updating frequency might be very low for ad-hoc networks.

2.4. Classification of routing Protocols in MANET

These protocols can be divided into three categories proactive, reactive and hybrid. Proactive protocols maintain routes to all nodes, including nodes to which no packets are sent. In reactive protocols, routes between hosts are determined only when they are explicitly needed to forward packets. Hybrid methods combine proactive and reactive methods to find efficient routes, without much control overhead.

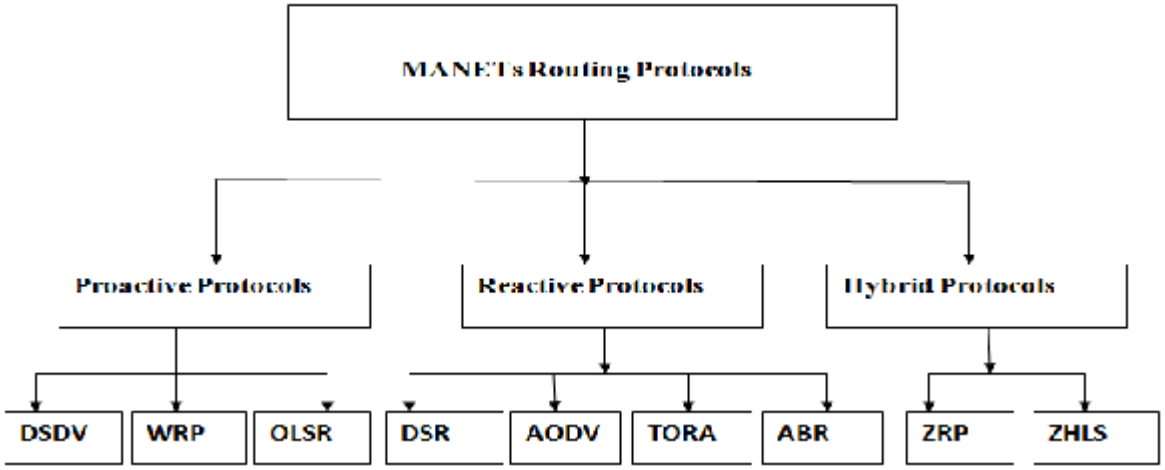


Figure 2.2: Classification of Routing Protocols in MANET

2.5. Proactive Protocols (Table Driven Routing protocols)

The proactive protocols are maintained the routing information even before it is needed [11]. Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. Many of these routing protocols come from the link-state routing [12]. There exist some differences between the protocols that come under this category depending on the routing information being updated in each routing table. The different types of Table driven protocols are:

2.5.1. DSDV

The Destination-Sequenced Distance-Vector (DSDV) Routing Algorithm is based on Bellman-Ford Routing Algorithm [13] with certain improvements. This protocol adds a new attribute,

sequence number, to each route table entry at each node. Routing table is maintained at each node and with this table; node transmits the packets to other nodes in the network.

The routing table updates can be sent in two ways: a full dump [14] or an incremental update. A full dump sends the full routing table to the neighbors and could span many packets whereas in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet. If there is space in the incremental update packet then those entries may be included whose sequence number has changed. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent. In a fast changing network, incremental packets can grow big so full dumps will be more frequent.

2.5.2. WRP

The Wireless Routing Protocol (WRP) is based on Distributed Bellman-Ford algorithm [15]. It substantially reduces the number of cases in which routing loop can occur. It utilizes information regarding the length and second-to-last hop of the shortest path to each destination. WRP requires each node to maintain four routing tables.

- Distance table
- Routing table
- Link cost table
- Message retransmission list (MRL) table

Each entry of the MRL contains the sequence number of the update message, a retransmission counter, an acknowledgment-required flag vector with one entry per neighbor, and a list of updates sent in the update message. The MRL records which updates in an update message need to be retransmitted and which neighbors should acknowledge the retransmission.

Nodes learn of the existence of their neighbors from the receipt of acknowledgments and other messages. If a node is not sending messages, it must send a hello message within a specified time period to ensure connectivity. Otherwise, the lack of messages from the node indicates the failure of that link; this may cause a false alarm. When a mobile receives a hello message from a new

node, that new node is added to the mobile's routing table, and the mobile sends the new node a copy of its routing table information.

2.5.3 OLSR

The Optimized link state routing (OLSR) protocol [16] is a proactive routing protocol and based on periodic exchange of topology information. The key concept of OLSR is the use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required. In OLSR, each node selects its own MPR from its neighbors. Each MPR node maintains the list of nodes that were selected as an MPR; this list is called an MPR selector list. Only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs. Generally, two types of routing messages are used in the OLSR protocol, namely, a HELLO message and a topology control (TC) message. A HELLO message is the message that is used for neighbor sensing and MPR selection.

In OLSR, each node generates a HELLO message periodically. A node's HELLO message contains its own address and the list of its one-hop neighbors. By exchanging HELLO messages, each node can learn a complete topology up to two hops. HELLO messages are exchanged locally by neighbor nodes and are not forwarded further to other nodes. A TC message is the message that is used for route calculation. A TC message contains the list of the sender's MPR selector. In OLSR, only MPR nodes are responsible for forwarding TC messages. For MPR selection, each node selects a set of its MPR nodes that can forward its routing messages.

2.6. Reactive Protocols (On-Demand Routing Protocols)

The reactive protocols don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet [17]. These protocols were designed to reduce the overhead encountered in proactive protocols by maintaining information for active routes only. This means that the routes are determined and maintained for the nodes that are required to send data to a particular destination. The route discovery usually occurs by flooding the route request packets throughout the network. The different types of Table driven protocols are:

2.6.1. DSR

The Dynamic Source Routing is use of source routing. That is, the sender knows the complete hop-by-hop route to the destination. These routes are stored in a route cache [18]. The data packets carry the source route in the packet header. When a node in the ad hoc network attempts to send a data packet to a destination for which it does not already know the route, it uses a route discovery process to dynamically determine such a route. Route discovery works by flooding the network with route request (RREQ) packets. Each node receiving an RREQ rebroadcasts it, unless it is the destination or it has a route to the destination in its route cache. Such a node replies to the RREQ with a route reply (RREP) packet that is routed back to the original source. RREQ and RREP packets are also source routed. The RREQ builds up the path traversed across the network. The RREP routes itself back to the source by traversing this path backward. If any link on a source route is broken, the source node is notified using a route error (RERR) packet. The source removes any route using this link from its cache. A new route discovery process must be initiated by the source if this route is still needed. DSR makes very aggressive use of source routing and route caching.

2.6.2. AODV

The Ad hoc On-demand Distance Vector (AODV) routing protocol is based on DSDV and DSR algorithm [19]. It uses the periodic beaconing and sequence numbering procedure of DSDV and a similar route discovery procedure as in DSR. However, there are two major differences between DSR and AODV. The most distinguishing difference is that in DSR each packet carries full routing information, whereas in AODV the packets carry the destination address. This means that AODV has potentially less routing overheads than DSR. The other difference is that the route replies in DSR carry the address of every node along the route, whereas in AODV the route replies only carry the destination IP address and the sequence number. An important feature of AODV is the maintenance of timer-based states in each node, regarding utilization of individual routing table entries. A routing table entry is expired if not used recently.

2.6.3. TORA

The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive loop-free distributed routing algorithm based on the concept of link reversal [20]. TORA is proposed to operate in a

highly dynamic mobile networking environment. It is source initiated and provides multiple routes for any desired source/destination pair. The key design concept of TORA is the localization of control messages to a very small set of nodes near the occurrence of a topological change. To accomplish this, nodes need to maintain routing information about adjacent (one-hop) nodes. The protocol performs three basic functions: route creation, route maintenance, and route removal.

2.6.4. ABR

The Associatively Based Routing (ABR) protocol checks the association between nodes and transfer the messages from sources to destinations. Association [21] is a concept that verifies the wireless connection between two nodes that actually involve in the procedure of transferring the packets. In ABR, a route is selected based on the degree of association stability of mobile nodes. Each node periodically generates an inspiration to signify its existence. When received by neighboring nodes, this inspiration causes their Associativity tables to be updated. Association stability is defined by connection stability of one node with respect to another node over time and space. A high degree of association stability may indicate a low state of node mobility, while a low degree may indicate a high state of node mobility. The three phases of ABR are: Route discovery, Route reconstruction and Route deletion.

2.7. Hybrid Protocols

Hybrid routing protocols are combination of reactive and proactive protocol. The hybrid protocols are:

2.7.1. ZRP

Zone Routing Protocol (ZRP) [22], the nodes have a routing zone, which defines a range that each node is required to maintain network connectivity proactively. Therefore, for nodes within the routing zone, routes are immediately available. For nodes that lie outside the routing zone, routes are determined on-demand and it can use any on-demand routing protocol to determine a route to the required destination.ZRP divides its network in different zones. That's the nodes local neighborhood. Each node may be within multiple overlapping zones, and each zone may be of a different size. The size of a zone is not determined by geographical measurement. It is given

by a radius of length, where the number of hops is the perimeter of the zone. Each node has its own zone. The advantage of this protocol is that it has significantly reduced the amount of communication overhead when compared to pure proactive protocols.

2.7.2. ZHLS

The Zone-Based Hierarchical Link State Protocol [23] is based on the GPS (Global Positioning System). ZHLS is similar to the Zone Routing Protocol. It is a hybrid routing protocol acting similar like ZRP. The protocol is proactive when the destination node is in the same zone as the node which sent the request. On the other hand, the protocol is reactive when the destination node isn't within the zone from the source node. But in ZHLS the network is divided in non overlapping zones. Unlike other hierarchical protocol, there is no zone head. The zone size depend on node mobility, network density, transmission power and propagation characteristics. Each node only knows the connectivity within its zone and the zone connectivity of the whole network. The node knows its position and zone ID because of the Global positioning system. It can determine its zone ID by mapping its physical location to a zone map. This zone map has to be worked out at the design stage.

2.8. Comparison of Proactive and Reactive routing protocols

The following Table 2.1 briefly compares the Proactive (Table ‐Driven) routing protocol
With Reactive (On-Demand) routing protocols.

Table 2.1: Comparison of Proactive and Reactive Routing Protocols

Proactive (Table Driven) **Routing protocols**	**Reactive (On Demand)** **Routing protocols**
Proactive routing protocols are tried to maintain routes to all possible destination.	In Reactive routing protocols, a route is built only when demand.
It maintain multiple routes that might never needed and adding un necessary routing overhead.	Does not maintain unnecessary routes and minimize to control overhead.
First packet latency is less when compare with reactive routing protocols.	First packet latency is more when compare with proactive routing protocols because routes

	need to be built.
Acquire large traffic and power consumption.	Does not acquire large traffic and power consumption compare to proactive routing protocols.
Higher overhead in maintaining rout To all destinations.	Lower overhead of message and Storage.

2.9. Detail Description of Adhoc on Demand Distance Vector Routing (AODV)

AODV is an on-demand dynamic routing protocol (AODV) [24] that maintains routing tables with one entry per destination. This is in difference to DSR, which can maintain multiple routes cache entries for each destination. It is an on-demand and distance-vector routing protocol, meaning that a route is established by AODV from a destination only on demand. Used for both uncast and multicasts using the 'J' (Join multicast group) flag in the packets [25]. AODV defines three types of control messages for route maintenance:

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

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

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

To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the (RREQ) packet to their neighbors till it reaches an intermediate node that has recent route information about the destination or till it reaches the destination in Figure 2.3. A node rejects a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only.

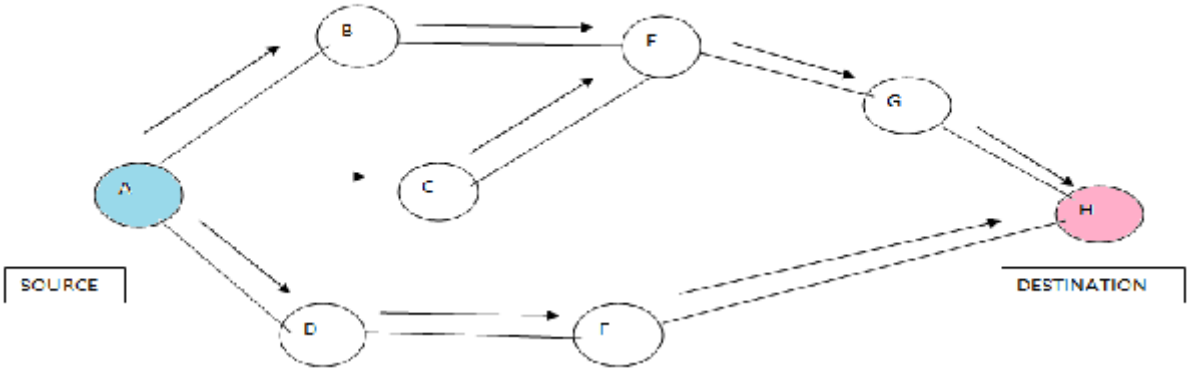


Figure 2.3: Propagation of Route Request (RREQ) Packet

When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply (RREP) packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. A Route Reply Packet traverses back to the source in Figure 2.4; nodes along the path enter the forward route into their tables.

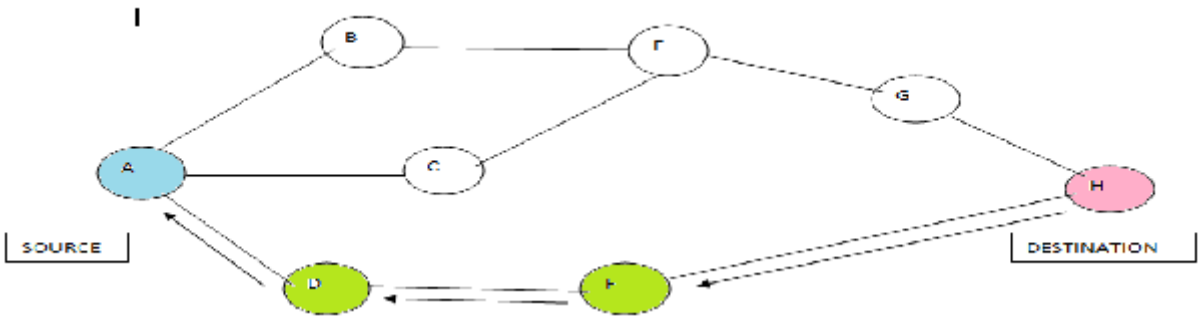


Figure 2.4: Path Taken by Route Reply (RREP) Packet

Link failures are propagated by a route error (RRER) message from the link failure point to the source node of that route. When the next hop link breaks, RRER packets are sent to a set of neighboring nodes that communicate over the broken link with the destination. This process is recursive and thus removes all routing entries containing these broken links in the routing tables. A node also checks connectivity by broadcasting local Hello messages. Since nodes reply to the first arriving RREQ, AODV favors least crowded route than shortest one.

2.9.1. Interesting Concepts of AODV

The concepts of AODV that make it desirable for MANETs with limited band width include the following [25]:

- **Minimal space complexity:** The algorithm makes sure that the nodes that are not in the active path do not maintain information about this route. After a node receives the RREQ and sets a reverse path in its routing table and propagates the RREQ to its neighbors, if it does not receive any RREP from its neighbors for this request, it deletes the routing info that it has recorded.

- **Maximum utilization of the bandwidth:** This can be considered the major achievement of the algorithm. As the protocol does not require periodic global advertisements, the demand on the available bandwidth is less. And a monotonically increased sequence number counter is maintained by each node in order to supersede any stale cached routes. All the intermediate nodes in an active path updating their routing tables also make sure of maximum utilization of the bandwidth. Since, these routing tables will be used repeatedly if that intermediate node receives any RREQ from another source for same destination. Also, any RREPs that are received by the nodes are compared with the RREP that was propagated last using the destination sequence numbers and are discarded if they are not better than the already propagated RREPs.

- **Simple:** It is simple with each node behaving as a router, maintaining a simple routing table, and the source node initiating path discovery request, making the network self-starting.

- **Most effective routing info:** After propagating an RREP, if a node finds receives an RREP with smaller hop-count, it updates its routing info with this better path and propagates it.
- **Most current routing info:** The route info is obtained on demand. Also, after propagating an RREP, if a node finds receives an RREP with greater destination sequence number, it updates its routing info with this latest path and propagates it.
- **Loop-free routes:** The algorithm maintains loop free routes by using the simple logic of nodes discarding non better packets for same broadcast-id.
- **Coping up with dynamic topology and broken links:** When the nodes in the network move from their places and the topology is changed or the links in the active path are broken, the intermediate node that discovers this link breakage propagates an RERR packet. And the source node re-initializes the path discovery if it still desires the route. This ensures quick response to broken links.

2.9.2. Advantages and Disadvantages of AODV

The main advantage of 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 [26].

One of the disadvantages of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries and also multiple Route Reply packets in response to a single Route Request packet can lead to heavy control overhead [26]. Another disadvantage of AODV is that the periodic beaconing leads to unnecessary bandwidth consumption.

2.10. Detail Description of Dynamic Source Routing (DSR) Protocol

Dynamic Source Routing (DSR) is an on demand, source based routing protocol. The sender knows the complete hop by hop route to the destination [27]. In the route discovery process, the

network is flooded by the route request (RREQ) packets where each node receiving it rebroadcasts it, unless it is the destination. The addresses of intermediate nodes are enlisted on DSR RREQ and RREP control packets.

Every node in the network uses these addresses to learn about the routes to other nodes in the network and store them in their route caches. Once a RREP message is received, the sender node knows the entire route to the destination. The sender stores this route in its cache for future use. Data packets in DSR are routed by intermediate nodes using the complete route to destination enlisted in the packet header. If the link breaks and the next node on the source route is not its neighbor, it sends an error message to the source using a route error RRER packet, and leaves it to the source to establish a new route. Else the node may try an alternate path. DSR stores multiple paths per destination and does not use any expiry timers on route cache entries.

The two major phases of the protocol are route discovery and route maintenance. When the source node wants to send a packet to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the packet. But if the node does not have such a route, then it initiates the route discovery process by broadcasting a route request packet. The route request packet contains the address of the source and the destination, and a unique identification number. Each intermediate node checks whether it knows of a route to the destination. If it does not, it appends its address to the route record of the packet and forwards the packet to its neighbors. A route reply is generated when either the destination or an intermediate node with current information about the destination receives the route request packet.

The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network:

2.10.1. DSR Route Discovery In route discovery source node is wishing to send a packet to a destination node obtains a source route to destination**.** Route Discovery is used only when source node attempts to send a packet to destination node and does not already know a route to destination when any host receives a route request packet (RREQ). It processes the request according to the following steps [27].

- If (initiator address, request id) is found in this host than discard the route request packet (RREQ).
- If this host's address is already listed in the route record than discard the route request packet (RREQ).
- If the target of the request matches this host's address than return a copy of this route in a route reply packet (RREP) to the initiator.
- Otherwise, append this host's address to the route record, and re-broadcast the request.

In Figure 2.5, a node **A** is trying to discover a route to node **G**. To initiate the Route Discovery, **A** transmits a RREQ message as a single local broadcast packet, which is received by all nodes currently within wireless transmission range of **A**. Each RREQ message identifies the initiator and target of the route discovery, and also contains a unique request id, determined by the initiator of the RREQ. Each RREQ also contains a record listing the address of each intermediate node through which this particular copy of the RREQ message has been forwarded. When another node receives a RREQ, if it is the target of the route discovery, it returns a RREP message to the initiator of the route discovery, giving a copy of the buildup route record from the RREQ; when the initiator receives this RREP, it caches this route in its route cache for use in sending subsequent packets to this destination.

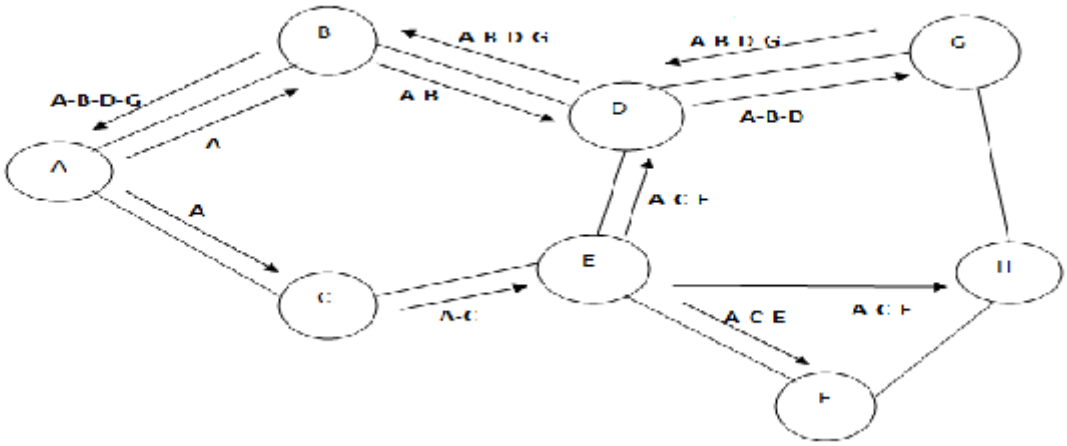


Figure 2.5: Route Discovery in DSR Routing Protocols

2.10.2. DSR Route Maintenance In route maintenance source node is able to detect, while using a source route to destination**,** if the network topology has changed such that it can no longer use

its route to destination because a link along the route no longer works. When Route Maintenance indicates a source route is broken, source can attempt to use any other route it happens to know to destination, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when source node is actually sending packets to destination node.
Basic Operations of Route Maintenance are [27]:

- Conventional routing protocols integrate route discovery with route maintenance by continuously sending periodic routing updates.
- There are no periodic messages of any kind from any of the mobile hosts.
- It monitors the operation of the route and in form the sender of any routing errors. The host sends a route error packet to the original sender.

In Figure 2.6, Node **A** has originated a packet for **G** using a source route through intermediate nodes **B** and **D**. In this case, node **A** is responsible for receipt of the packet at **B**, node **B** is responsible for receipt at **D** and node **D** is responsible for receipt finally at the destination **G.** If the packet is retransmitted by some hop the maximum number of times and no receipt confirmation is received, this node returns a RERR message to the original sender of the packet, identifying the link over which the packet could not be forwarded. For example, in Figure 2.6, if **D** is unable to deliver the packet to the next hop **G**, then **D** returns a RERR to **A**, stating that the link from **D** to **G** is currently broken. Node **A** then removes this broken link from its cache any retransmission of the original packet is a function for upper layer protocols such as TCP and for sending such a retransmission or other packets to this same destination **G**.

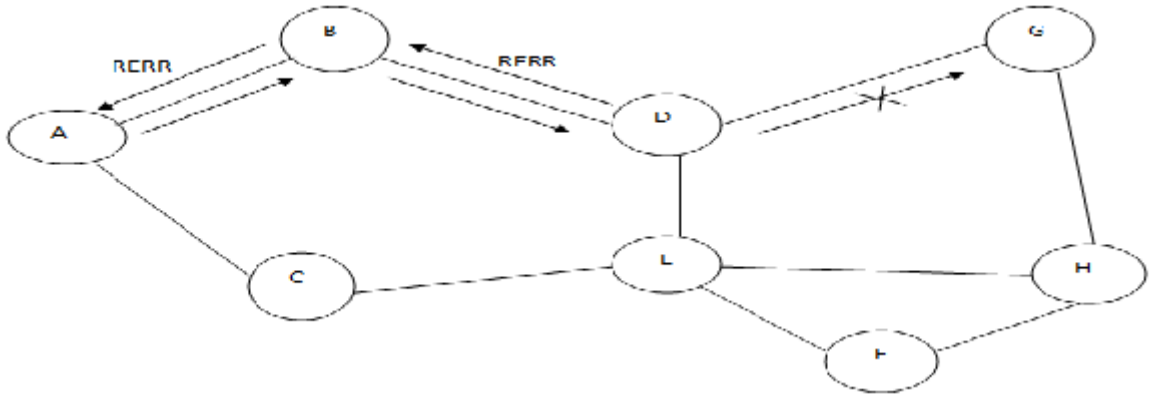


Figure 2.6: Route Maintenance in DSR routing protocol

2.10.3. Advantages and Disadvantages of DSR

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

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

2.11. Comparison between AODV and DSR

The AODV and DSR protocols have been analyzed theoretically. Table 2.2 summarizes and compares the result from these theoretical, qualitative analyses and shows what properties the protocols have and do not have. There are comparison between DSR and AODV on the base of their characteristics are defined as

Table 2.2: Comparison of AODV and DSR

	AODV	**DSR**
Loop free	Yes	Yes
Multiple routes	No	Yes
Distributed	Yes	Yes
Reactive routing protocols	Yes	Yes
Unidirectional link support	No	Yes
Multicast	Yes	No
Periodic broadcasts	Yes	No

Chapter 3

3.1. Problem Statement

The objective of the thesis is to select one out of a AODV and DSR reactive protocol when the mobile ad hoc network has to be created for the small duration .In order to fulfill the objective a comparative analysis between these two reactive protocols has to be carried out in the simulated environment created in the ns-2 simulator comprising of 15 mobile nodes based on the two basic parameters – packet received and packet loss and examining their values based on the different simulation time scenarios.

3.2. Objectives

The various tasks carried out in achieving the objective can be outlined as follows:

- Get a general understanding of ad -hoc networks.
- Literature review of the existing routing protocols including DSR and AODV.
- Learning of the OTCL script and its use in the NS-2.
- Creating the simulated environment comprising of 15 mobile nodes in a boundary of 640 by 640.
- Implementing DSR and AODV protocol on 15 mobile nodes by the use of OTCL script in NS-2
- Analyzing the behavior of both the protocols with the help of X graph in NS2 simulator
- Discussing the results based on the study of X graph.

Chapter 4
Simulation Model

4.1. Simulation

Simulation can be defined as "Imitating or estimation how events might occur in a real situation." It can involve complex mathematical modeling, role playing without the aid of technology, or combinations. These assumption from a model of the system .The value lies in the placing you under realistic conditions, that change as a result of behavior of others involved so you cannot predict the sequence of events or the final outcome[28].

- **Simulation can be used:**
  To study complex systems, compare design alternatives for a system that doesn't exist and study the effect of alternations to an exit system.

- **Simulations should not be used:**
  If model assumptions are simple such that mathematical methods, those can be used to obtain exact answers.

There are different simulators such as ns2, GloMoSim, OPNET etc., are being used by researchers in order to evaluate the routing protocols. We have used ns2 for the evaluation of the proposed routing protocol as the same is an open source, freely available and the programming languages used are C++, Tcl and OTcl.

4.2. NS2 Overview

The network simulator (NS) [28], which is a discrete event simulator for networks, is a simulated program developed by VINT (Virtual Internetwork Test-bed) project group. It supports simulations of TCP and UDP, some of MAC layer protocols, various routing and multicast protocols over both wired and wireless network etc. As shown in the figure 4.1, it is necessary to trace the output in some of the output files for post-simulation analysis.

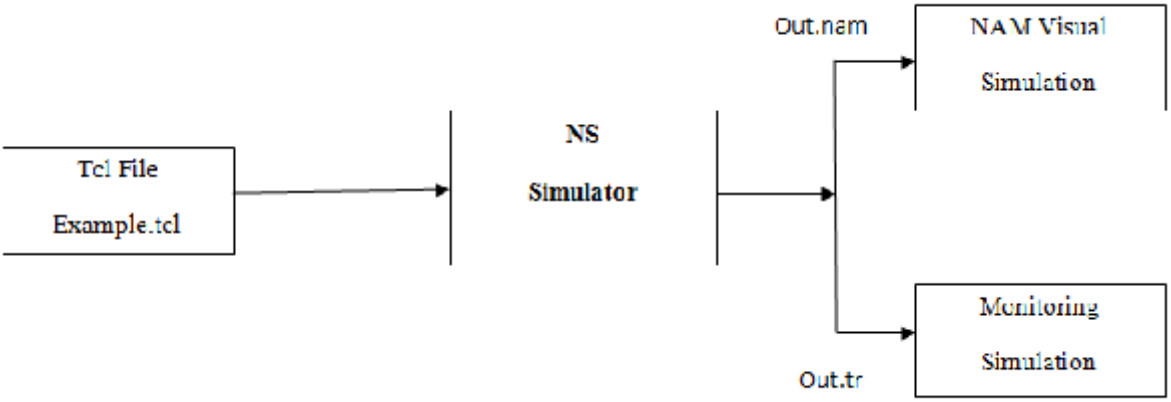


Figure 4.1: Network Simulator

Depending on user's requirement the simulation are stored in trace files, which can be fed as input for analysis by different component:

- A NAM trace file (.nam) is used for the ns animator to produce the simulated environment.
- A trace file (.tr) is used to generate the graphical results with the help of a component called X Graph [29].

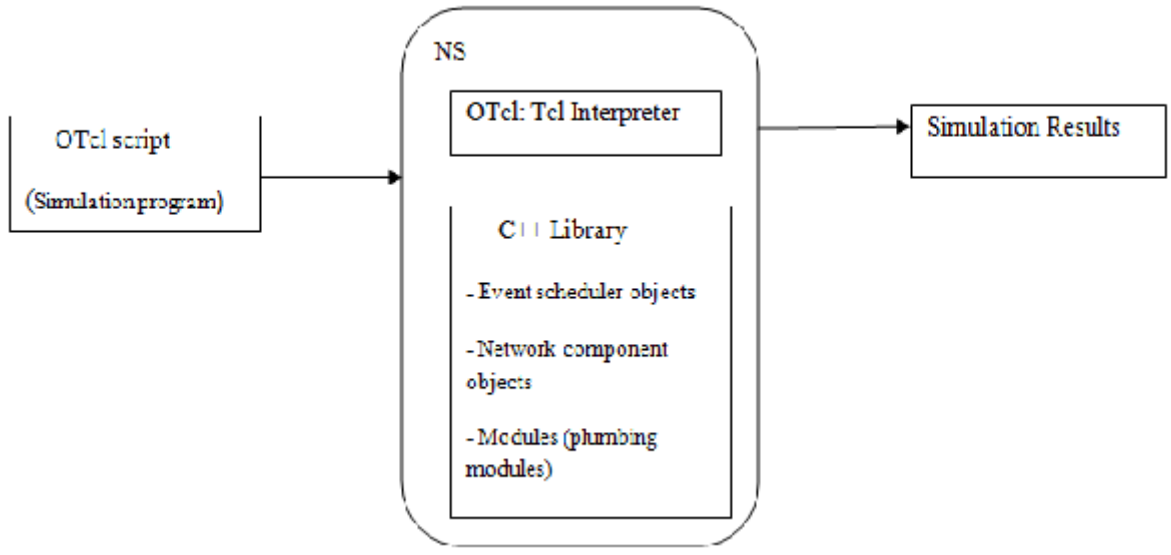


Figure 4.2: Simplified User's View of NS

Figure 4.2, shows a simplified user's view,ns is object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries, and network setup (plumbing) module libraries(actually, plumbing modules are implemented as member functions of the base simulator object). In the other words, to use ns, you program in OTcl script language.
To setup and run a simulation network, a user should write an OTcl script that initiates an event scheduler, set up the network topology using the network objects and plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through event scheduler. The simulator uses this script during simulation .the term "plumbing " is used for a network setup, because setting up a network is plumbing possible data paths among network objects by setting the neighbor pointer of an object to the address of an appropriate object. The power of ns comes from this plumbing.

When the simulation is finished, the simulation results are produced in one or more text-based output files that contain detailed simulation data, which can be used to analyze directly or can be used in the graphical user interface Network Animator (NAM) [30]. This graphical user interface shows the simulation result in an easy way.

The language that is written in NS-2 is not only OTcl but also C++. The event scheduler and the basic network component objects in the data path are written and compiled using C++ to reduce packet and event processing time. These compiled objects need the OTcl linkage to create a matching OTcl object for each of the C++ objects to be able to work with OTcl interpreter.

4.2.1. Architectural of NS

The NS-2 architecture is composed of five parts:

- Event scheduler
- Network components
- Tclcl
- OTcl library
- Tcl 8.0 script language

These five components together make up NS, which is an object-oriented extended Tcl interpreter with network simulator libraries Figure 4.3 shows the general architecture of ns. In

this figure, a general user (not an ns developer) can be thought of standing at the left bottom corner, designing and running simulations in Tcl using the simulator objects in the OTcl library. The event schedulers and most of the network components are implemented in C++ and available to OTcl through the OTcl linkage that is implemented using Tclcl. The whole thing together makes the ns, which is a OO extended Tcl interpreter with network simulator libraries.

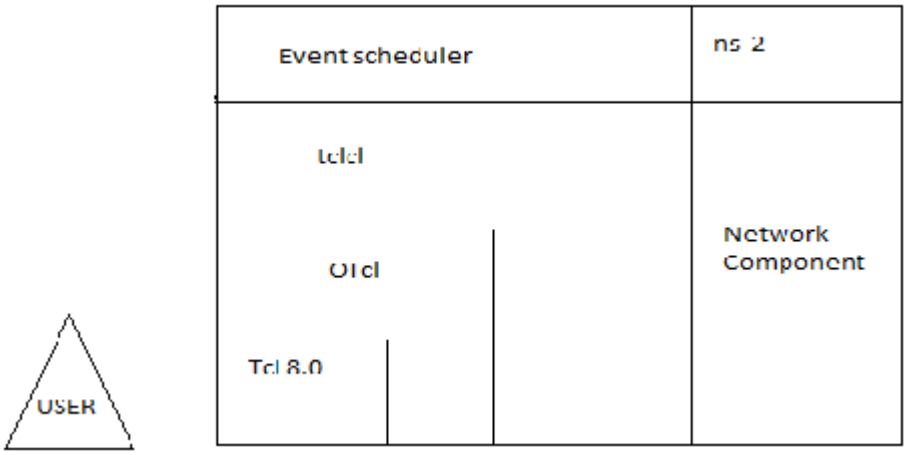


Figure 4.3: Architectural views of ns

4.2.2. Tool Command Language (Tcl)

Tool Command Language, Tcl [31] is a powerful interpreted programming language developed by John Ouster out at the University of California, Berkeley. Tcl is a very powerful and dynamic programming language. It has a wide range of usage, including web and desktop applications, networking, administration, testing etc. Tcl is a truly cross platform, easily deployed and highly extensible. The most significant advantage of Tcl language is that it is fully compatible with the C programming language and Tcl libraries can be interoperated directly into C programs.

4.2.3. The Network Animator (NAM)

The biggest advantage of network animator (NAM) is that it provides a graphical user interface (GUI) for the different simulation environment according to the parameters specified by the user. The Xgraph utility generates the graphical output of the input data (or trace files).

To animate network traffic in several ways, nam interprets a trace file containing time-indexed network events, as Figure 4.4 shows. Typically, an ns simulation generates this trace, but nam can also use processing data from a live network to produce a trace. Nam usually runs offline using traces stored on disk, but it can also play traces from a running program. The nam trace file contains all information needed for the animation—both on static network layout and on dynamic events such as packet arrivals, departures, and drops and link failures [30]. The input file for wireless networking simulations also includes information on node location and movement.

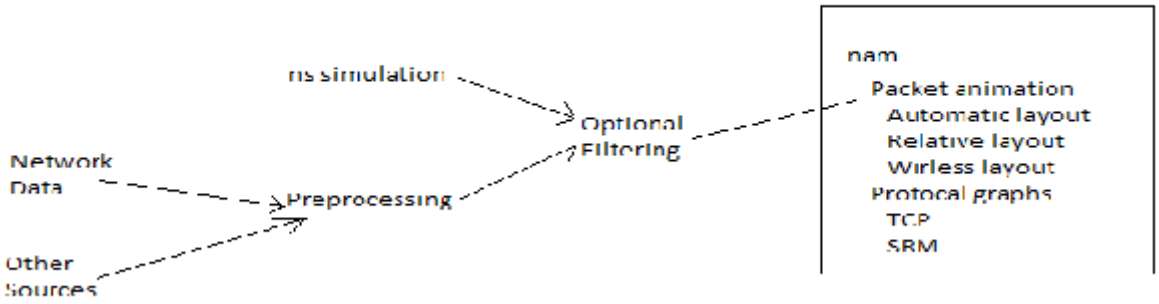


Figure 4.4: Block diagram of NAM

NAM is GUI for replaying the simulation and auto-layout or defines node positions in script. Nam is a visual aid showing how packets flow along the network .It is a Tcl based animation tool for viewing network simulation traces and real world packet trace data. The first step to use NAM is to produce the trace file. The trace file should contain topology information, e.g., nodes, links, as well as packet traces. Usually, the trace file is generated by ns2. When the trace file is generated, it is ready to be animated by NAM. Upon startup, NAM will read the trace file, create topology, pop up a window, do layout if necessary and then pause at the time of the first packet in the trace file, through its user interface, NAM provides control over many aspects of animation [30] The main window of NAM is shown below:

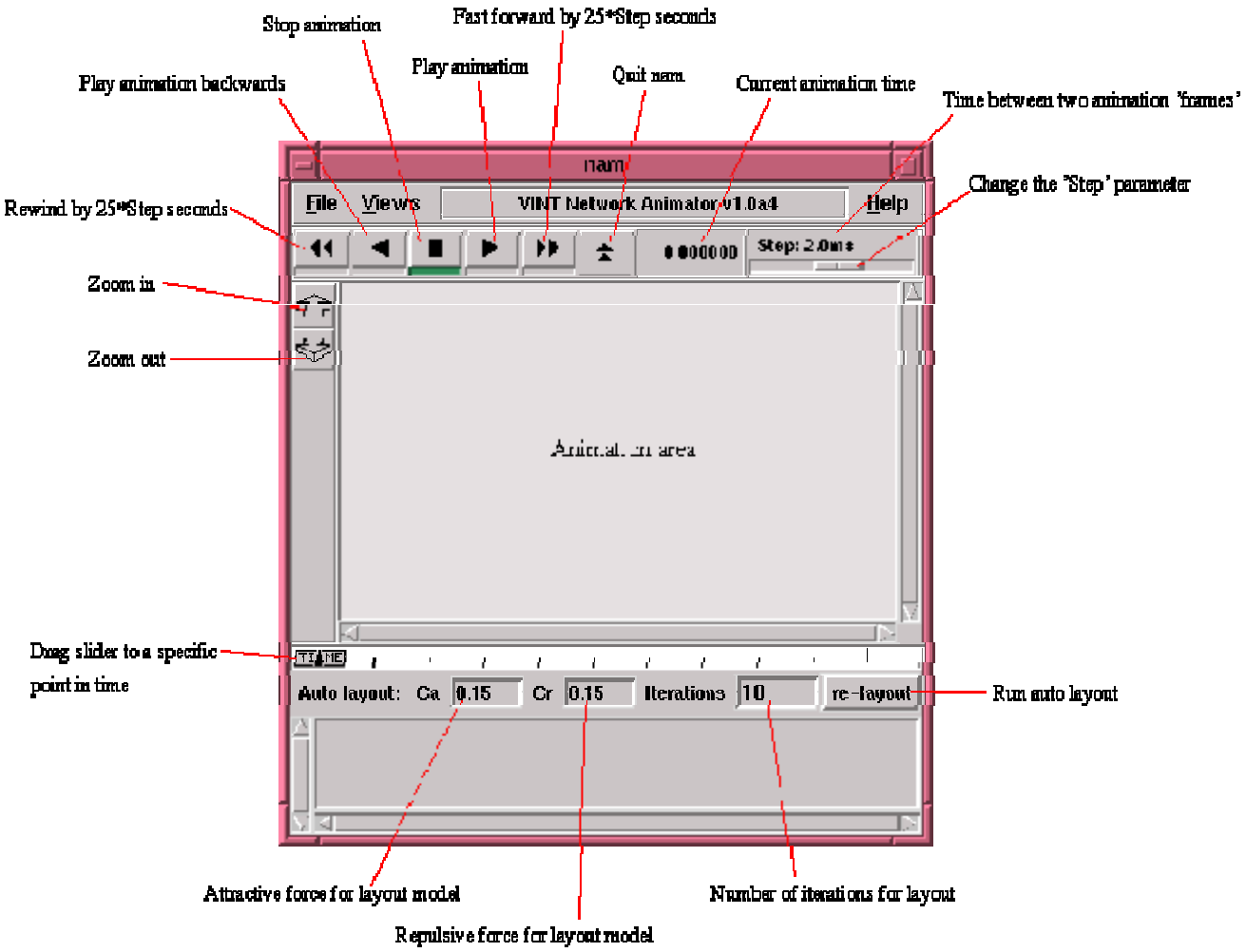


Figure 4.5: Screenshot of NAM Window [32]

4.2.4 Structure of Trace File

When tracing in to an output ASCII file, the trace is organized in 12 fields as in Figure 4.6, the meaning of fields is:

Event	Time	From Node	To Node	Pkt Type	Pkt Size	Flags	Fid	Src Addrs	Dst Addrs	Seq Num	Pkt id

Figure 4.6: Fields of Trace File

1) The first field is the event type and given by one of four available symbols r, +, - and d which correspond respectively to receive, enqueued, dequeued and dropped.
2) The second field is telling the time which the event occurs.
3) Gives the input node of the link at which the events occurs.
4) Gives the output node of the link at which the events occurs.
5) Gives the packet type such as continuous bit rate (CBR) or transmission control protocol (TCP).
6) Gives the size of the packet.
7) The field is some kind of flags.
8) This is the flow identity of IPv6, which can specify stream color of the NAM display and can be use for further analyze purposes.
9) This is the source address in the form of "node. Port".
10) This is the destination in the form of "node. Port".
11) This is the network layer protocol's packet sequence number. NS keeps track of UDP packet sequence number for the analysis purposes.
12) The last field is the unique identity of the packet.

Results of simulation are stored into trace file (*.tr). Trace Graph was used to analyze the trace file.

4.2.5. The Trace Graph

It is a data presentation system for Network Simulator NS2. The simulator doesn't have any options implemented to analyze simulations results so it's hard to use it. Trace graph [33] system provides many options for analysis, including 250 graphs and statistical reports. Trace graph supports the following NS2 trace file formats; wired, satellite, wireless (old and new trace), wired-cum-wireless. Trace file loading stage is divided into 4 stages; automatic trace file format recognition, trace file parsing to extract necessary simulation data which is saved to a temporary file, trace files can contain much more data than is needed by the system, so unnecessary information is omitted to speed up trace file loading, temporary file loading, constants calculations (packets types, packets sizes, flows IDs, trace levels, number of nodes, simulation time) – in order to speed up data processing. Wireless and wired-cum-wireless trace files are parsed and saved in Trace graph format.

4.3 Mobility Models

The mobility model is designed to describe the movement pattern of mobile users, and how their location, velocity and acceleration change over time. Since mobility patterns may play a significant role in determining the protocol performance, it is desirable for mobility models to follow the movement pattern of targeted real life applications in a reasonable way. One frequently used mobility model in MANET simulations is the Random Waypoint model [34], in which nodes move independently to a randomly chosen destination with a randomly selected velocity. The Random Waypoint model is extensively used in simulation studies of MANET so that Random Waypoint Mobility Model is used in our work.

4.3.1. Random Waypoint Mobility Model

The Random Waypoint Mobility Model [34] is extensively used in simulation studies of MANET. In this mobility model a node selects its destination and its speed. The node keeps moving until it reaches its destination at that speed. In the RWP model the nodes, i.e.; mobile users, moves along a zigzag path consisting of straight legs from one waypoint to the next. the movement of the nodes is in a straight-line and we assume that is way point is drawn from the uniform distribution over the given convex domain. The nodes choose their destination either randomly or get their coordinates from the tcl script that is provided by the user. This is very clearly shown in the figure 4.6 given below. In RWPMM node begins the simulation by waiting a specified pause-time. After this time it selects a random destination in the area and a random speed distributed uniformly between 0 m/s and Vmax. After reaching its destination point, the mobile node waits again pause for time seconds before choosing a new waypoint and speed.

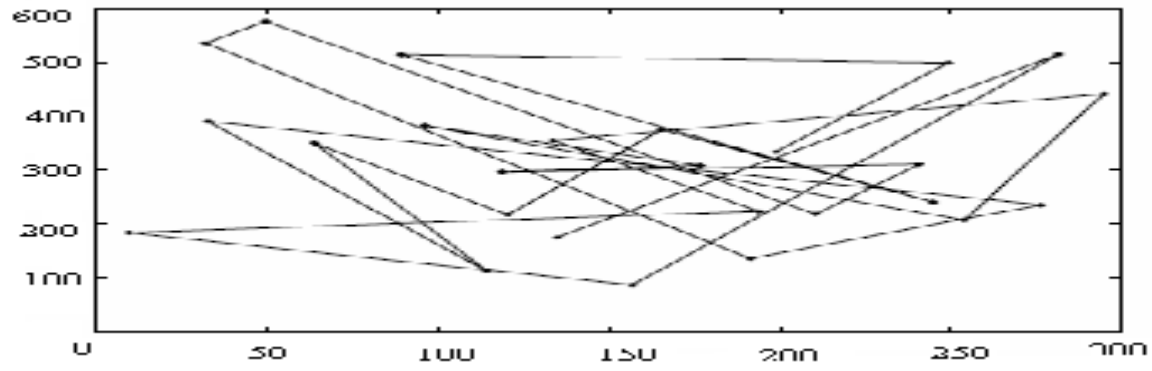


Figure 4.7: Traveling Pattern of Different Mobile Nodes using the RWPMM

4.4. Traffic Model

Continuous bit rate (CBR) traffic sources are used. The source-destination pairs are spread randomly over the network. The number of source-destination pairs and the packet-sending rate in each pair is varied to change the offered load in the network.

The mobility model uses the random waypoint model in a rectangular field. The field configurations used is: 670 m x 670 m field with 15 nodes. Here, each packet goes from its location to a destination with a randomly. When they are reached at its destination than another random destination is targeted after a pause time. Here,simulations are run for 10 and 20 simulated seconds.

Chapter 5
Implementation & Results

5.1. Simulation Parameters

As already outlined, we have to select one out of DSR and AODV reactive protocol when the mobile adhoc network has to be created for the small duration. The whole scenario comprises of 15 mobile nodes using both DSR and AODV is simulated in NS-2 simulator with the assumption that all the mobile nodes receives packets as well as forward them to all the neighboring nodes without filtering them on the basis of the destination address.

The needed Parameters to carry out the simulation and their corresponding values for both protocols are specified below:

Table 5.1: Simulation Parameters

Parameter	Value
Number of Nodes	15
Topography Dimension	670 m x 670 m
Traffic Type	CBR
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.11.Mac Layer
Packet Size	512 bytes
Mobility Model	Random Way Point
Antenna Type	Omni directional

All the above mentioned parameters in the table remains same for both DSR and AODV protocols but only one parameter – Simulation Time is varied for 10 seconds and 20 seconds and the behavior of both DSR and AODV is examined by studying the X Graph.

5.1.1. Simulation Scenario of 15 mobile nodes

The mobile adhoc network comprising of 15 mobile nodes is constructed in the NS-2 simulator with the use of OTCL script in the topological boundary area of 670 m x 670 m. The position of the mobile nodes is defined in terms of X and Y coordinates values and it is written in the movement scenario file.

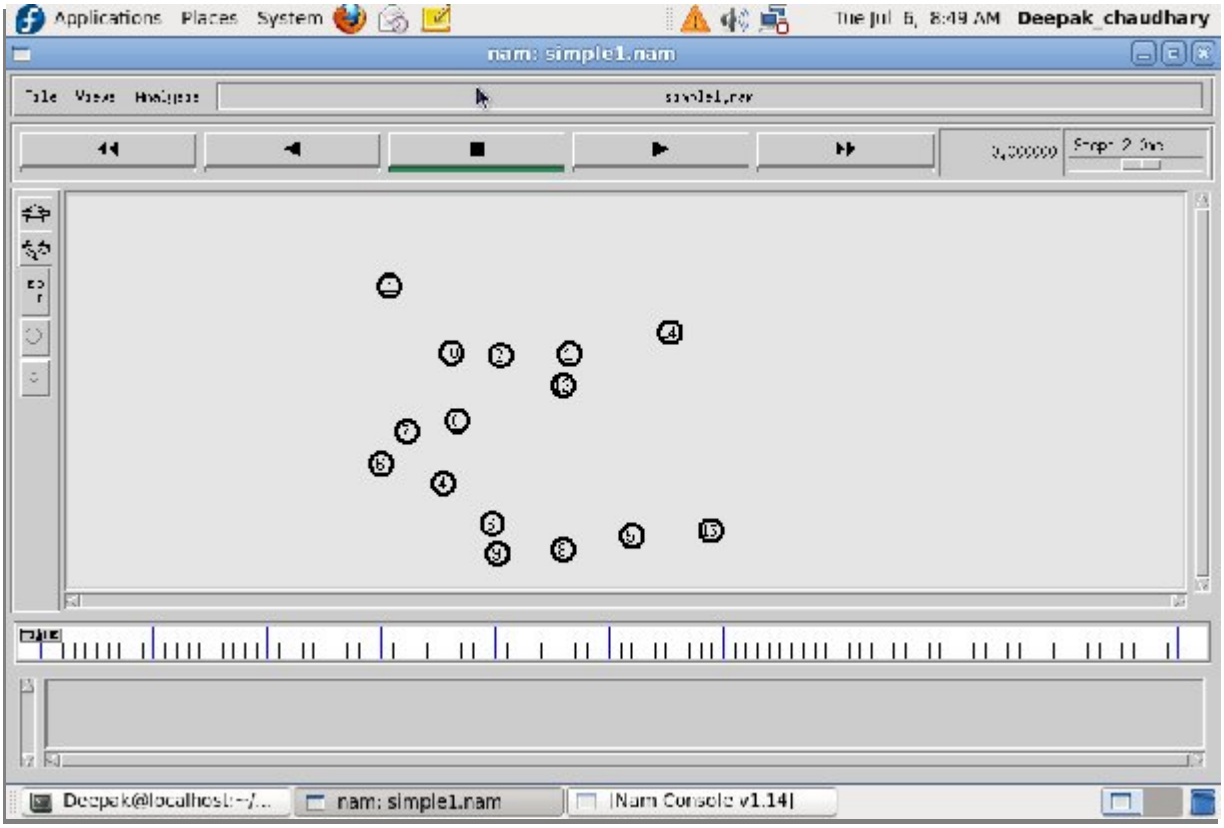


Figure 5.1: A Screenshot of 15 Mobile Nodes Implementing DSR and AODV

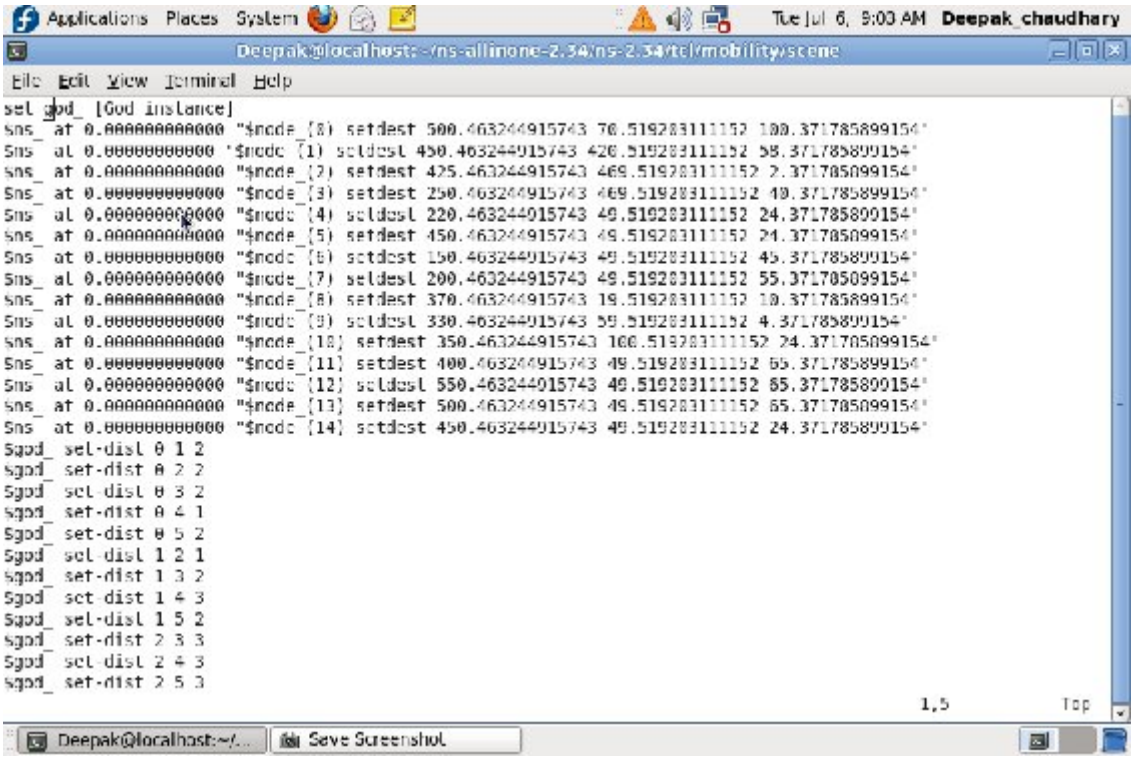


Figure 5.2 (a): A Screenshot of Movement Scenario file showing Nodes Movements

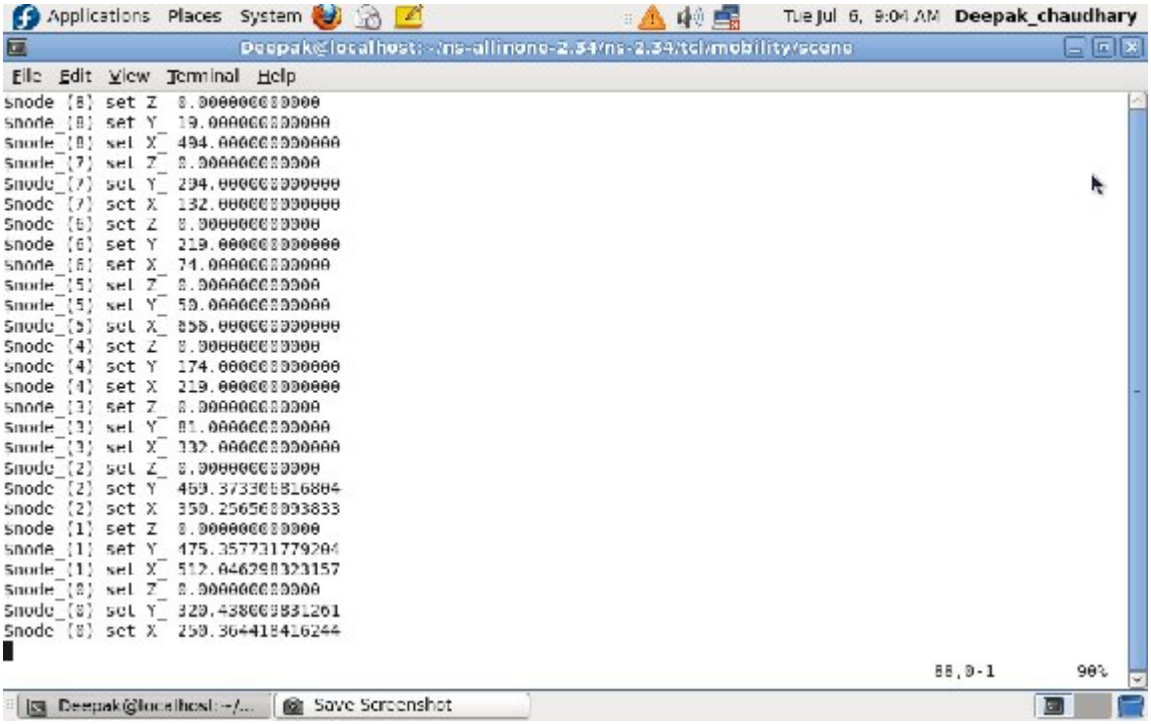
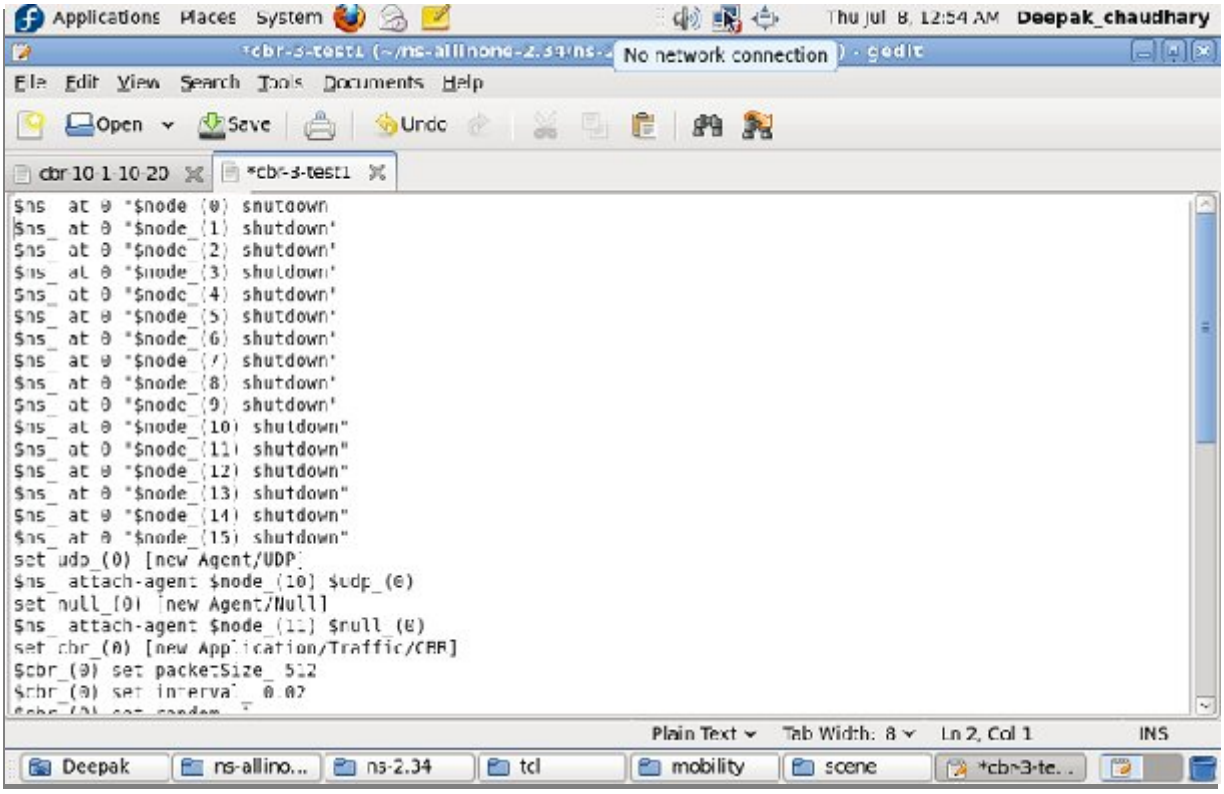


Figure 5.2 (b): A Screenshot of Movement Scenario file showing Nodes Position

5.1.2. Traffic set up between the Mobile Nodes

The traffic flow in terms of the exchange of packets between the mobile nodes is read from the following traffic generator script.



. **Figure 5.3:** A Screenshot of Traffic Generator Script

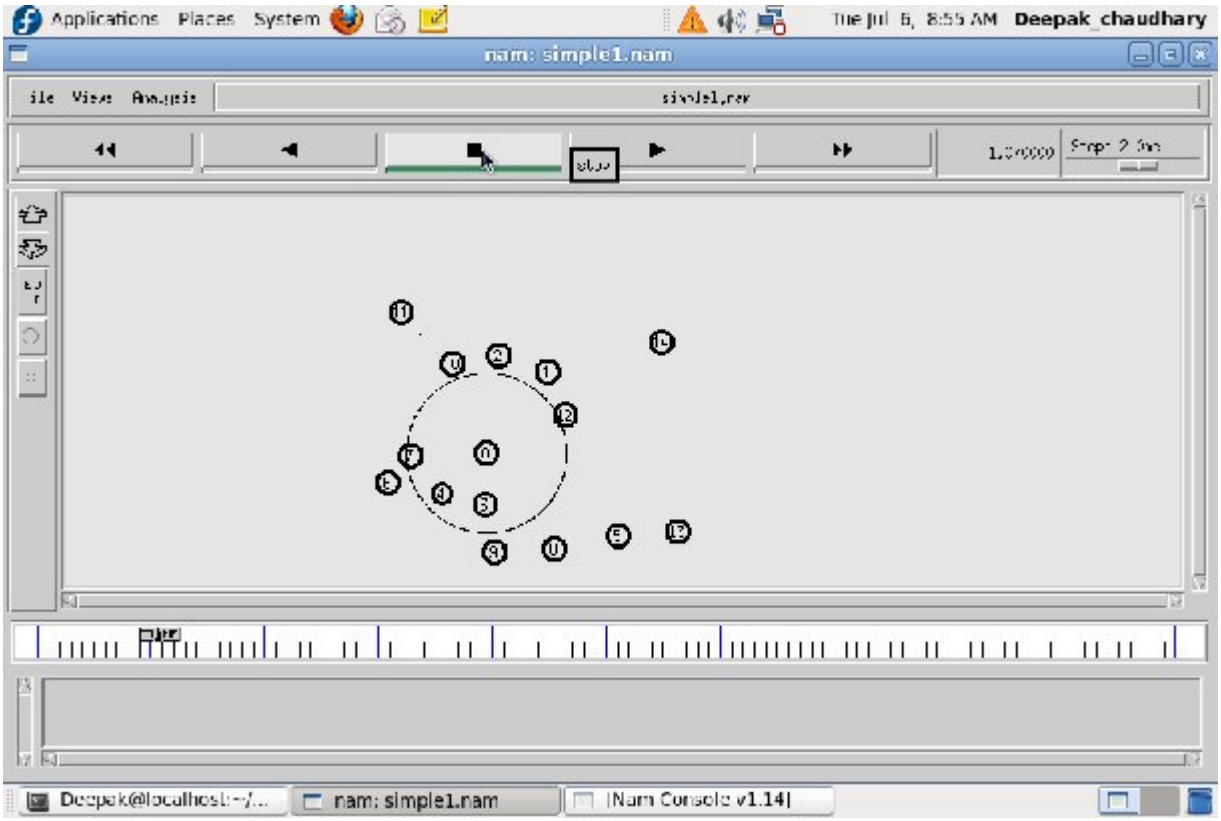


Figure 5.4: Flow of Traffic between the Mobile Nodes

5.1.3. Generation of Trace File

The trace file is generated after running the simulation for the specified simulation time. The trace file provides the following information about the action that happens with the respect of packets-send(s), received(r), dropped (d), the time when the action happens, the node where the action takes place, the layer of the node where the action takes place, the sequence number of packet, packet type etc.

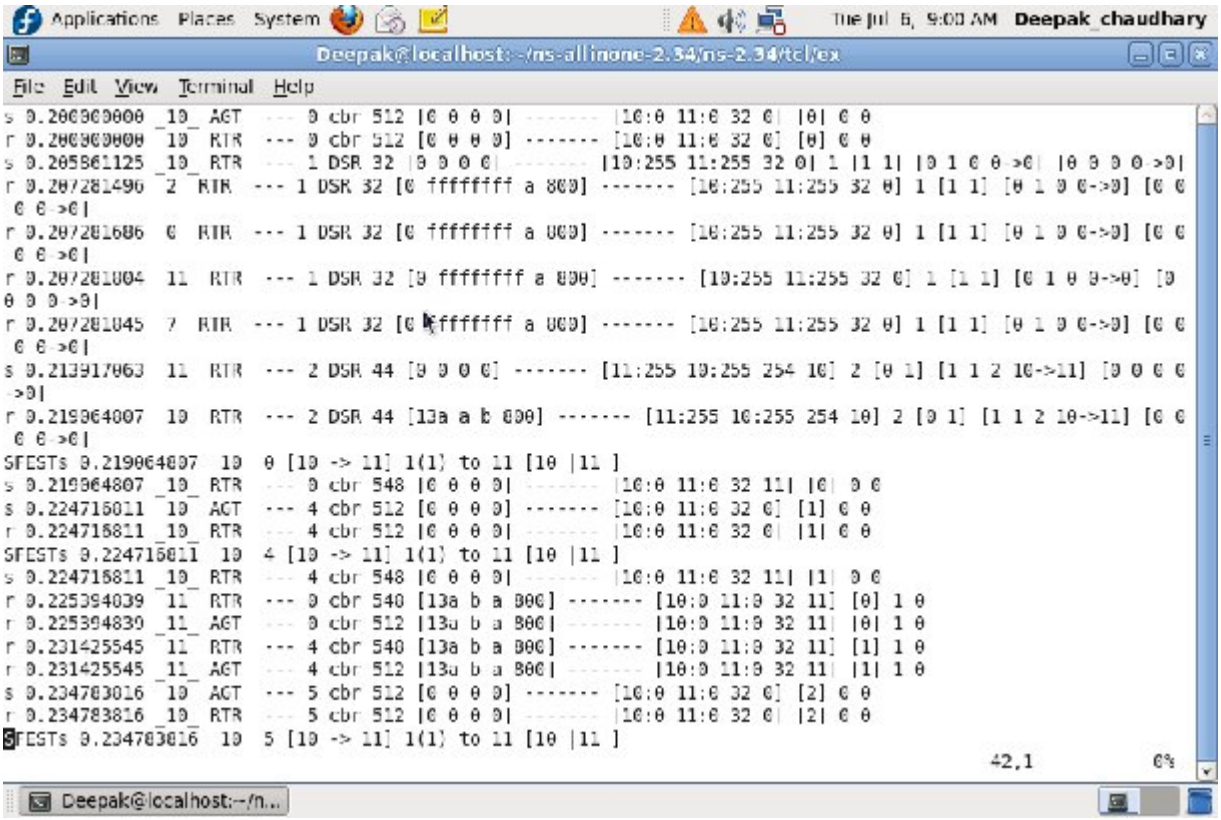


Figure 5.5: A Screenshot of Generated Trace File

The trace file output is then converted into X Graph to show the results in graphical format by the following command: exec X Graph dsr.tr aodv.tr –geometry 800 m x 600 m.

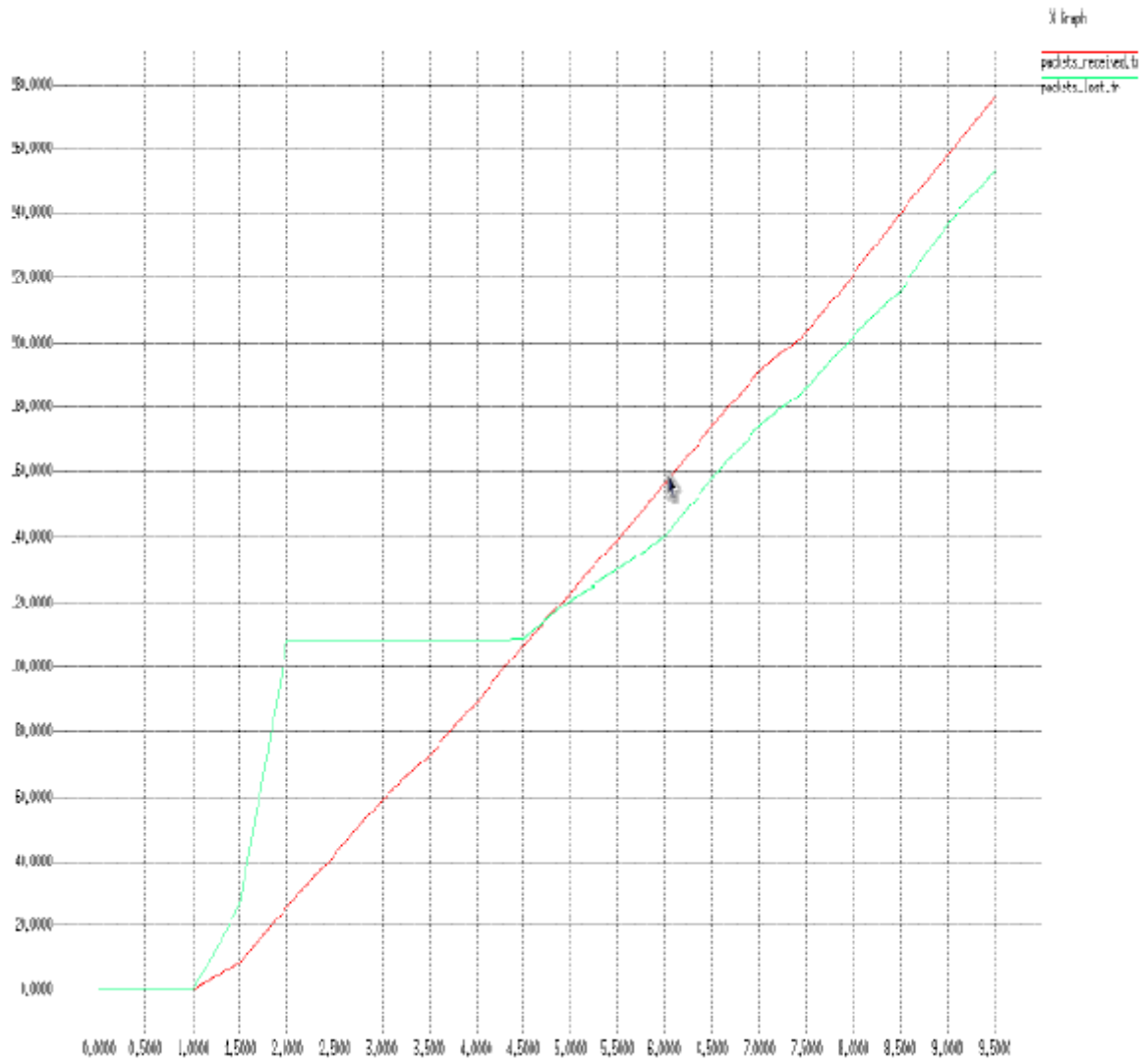


Figure 5.6: X Graph of 10 Seconds Simulation time for DSR

Figure 5.6 shows the X graph of DSR when the simulation is carried only for 10 seconds . the packet received and packet loss is initially zero at the time of start because initially there is no CBR connection. As the CBR connections establish the number of packet that lost increases as compare to packet received but as simulation time increases substantially the number of packet received increases.

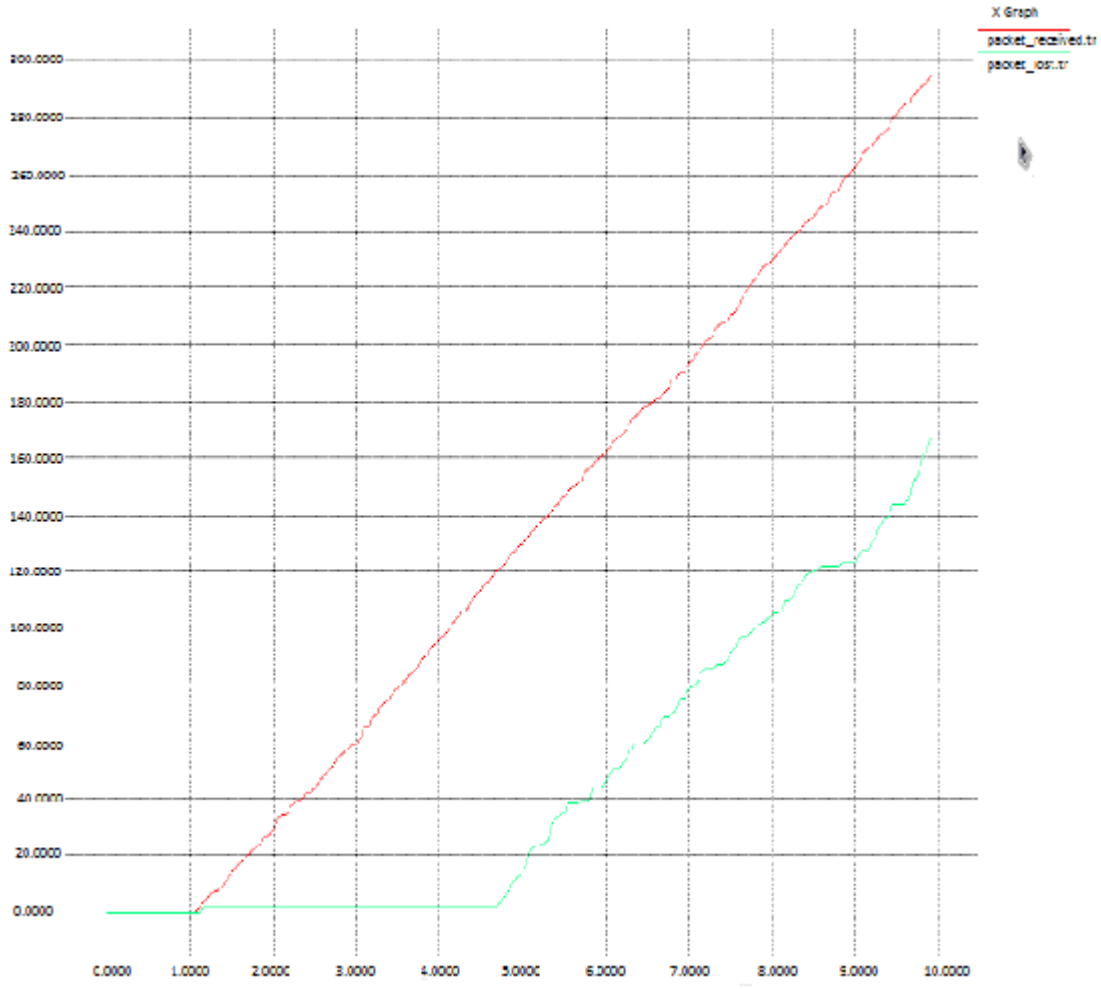


Figure 5.7: X Graph of 10 Seconds Simulation time for AODV

Figure 5.7 shows the X graph of AODV when the simulation is carried only for 10 seconds the packet received and packet loss is initially zero at the time of start because initially there is no CBR connection. As the CBR connections establish between the nodes the number of packet received in comparison to packet loss increases. Later on, the packet loss increases substantially as simulation time increases.

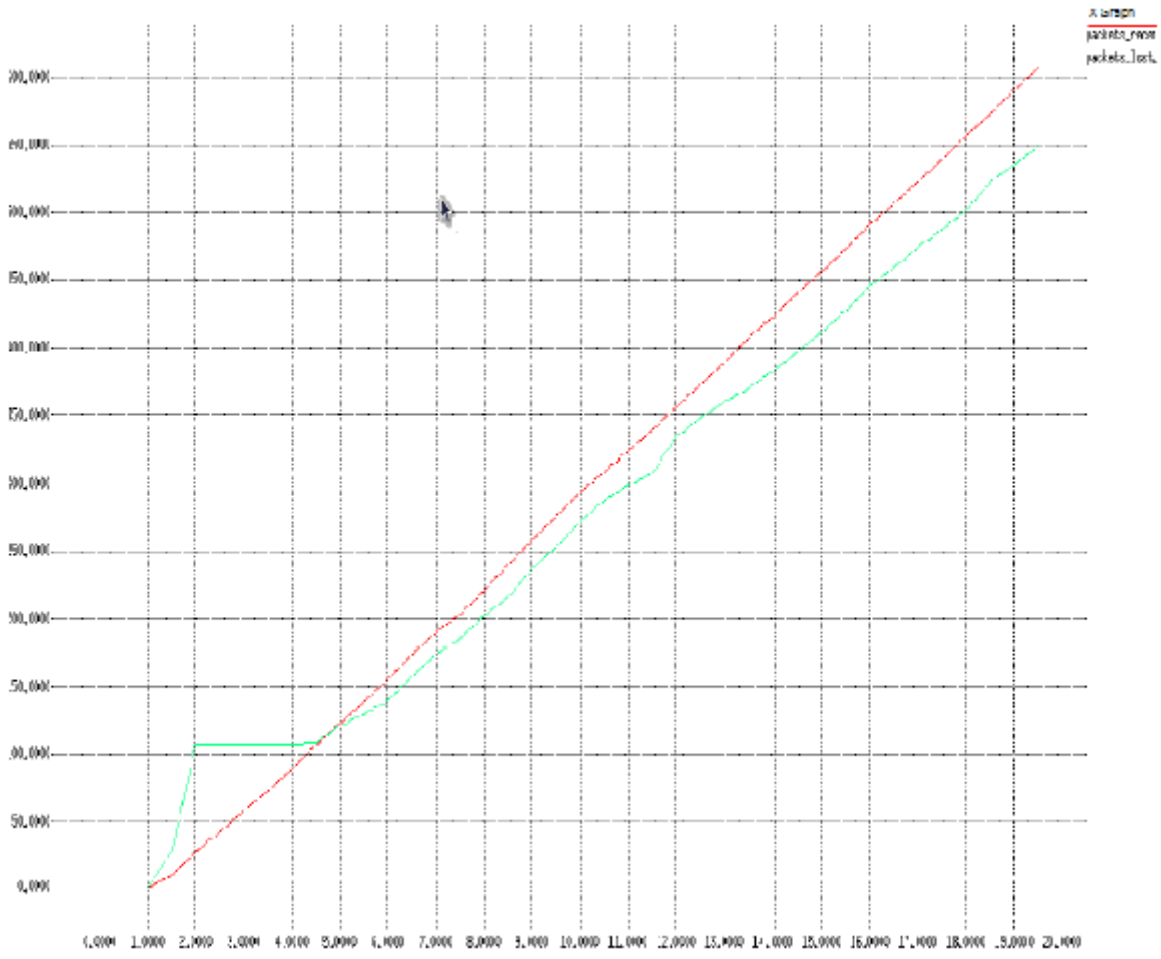


Figure 5.8: X Graph of 20 Seconds Simulation time for DSR

Figure 5.8 shows that initially in the case of DSR the packet losses are higher as compared to the packet received but as the simulation precedes further the packet loss rate decreases in case of DSR.

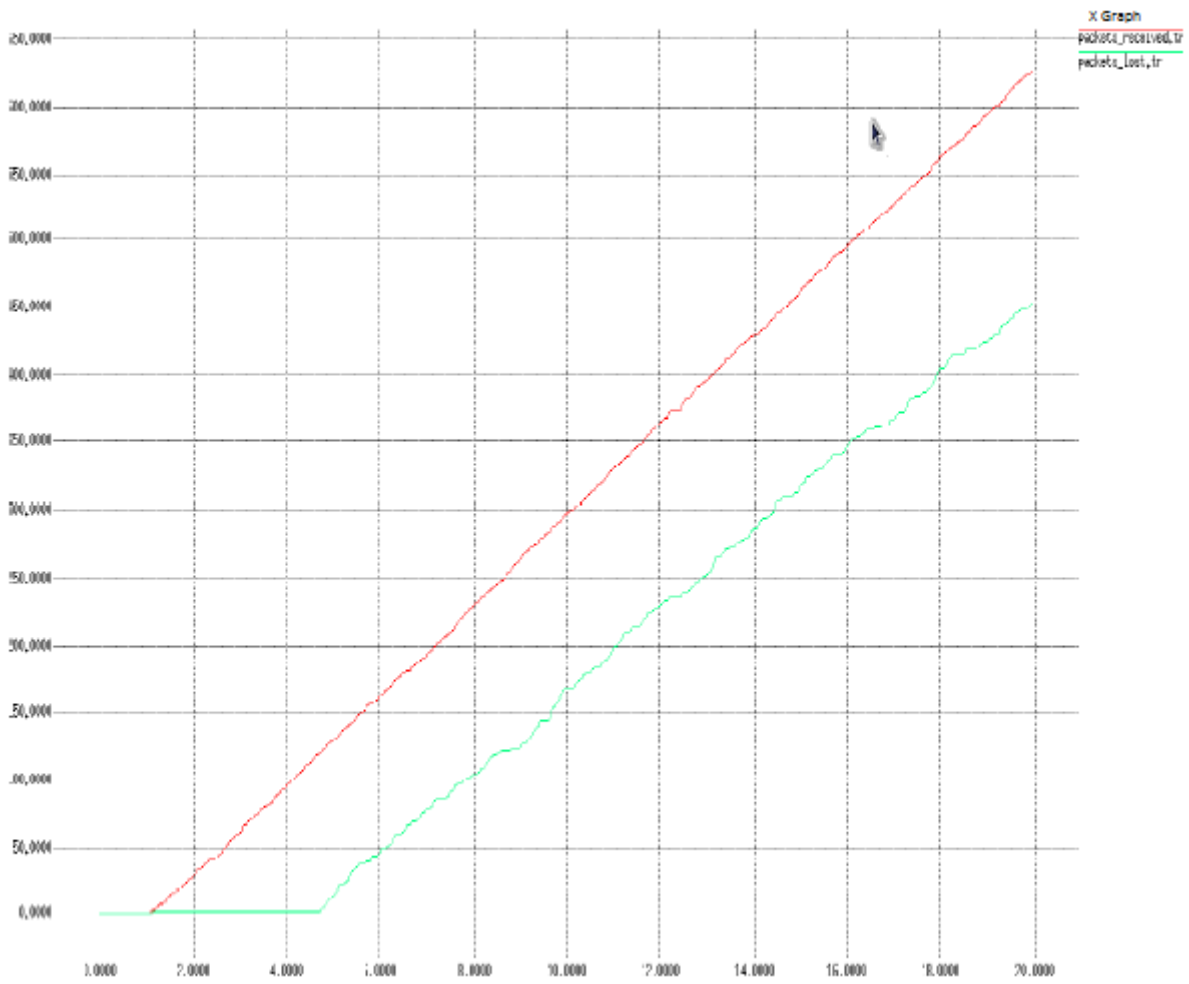


Figure 5.9: X Graph of 20 Seconds Simulation time for AODV

Figure 5.9 shows that initially the packet losses in the case of AODV approximate equal tozero. As simulation time increases the packet loss goes down and packet receiving increases.

Chapter 6
Conclusions

6.1. Conclusions

- We have simulated and compared the two frequent used reactive protocols DSR and AODV in two different simulation time scenarios 10 seconds and 20 seconds and observing their behavior in terms of two significant parameters Packet Loss and Packet Received in order to find out which one should be preferred when the mobile ad hoc network has to be set up for the small amount of time.
- The whole simulation scenario consisting of 15 nodes is created by writing the OTCL script in NS-2 and analyzing the parameters Packet Loss and Packet Received with the help of generated X Graph.
- By studying and analyzing the outputs appeared in Xgraph we come to this conclusion that AODV must be preferred over DSR when the MANET has to be set up for the small amount of time.

6.2. Future Scope

- In the future, the work can be extended on the other categories of the routing protocols such as proactive and hybrid routing protocols in order to find the appropriate protocol in their category on the basis of the varied simulation time.
- It can be further extended by implementing the scenario with the different mobility models such as Random Walk, Random Point Group Mobility Models and observing the behavior of protocols by varying the simulated time.
- Also the behavior of the protocols can be studied further by carrying the simulations on different parameters like varying the number of mobile nodes, the topology area choice of the traffic type between the mobile nodes other than the simulation time.

References

[1] An infrastructure network, URL: http://support.dell.com/support/edocs/network/79pcf/wiredlan.gif.

[2] An infrastructure less network, URL: http://perso.crans.org/raffo/papers/phdthesis/adhoc.png.

[3] M. Gerla, J.T. Tsai, "Multicluster Mobile, Multimedia Radio Network," ACM-Blatzer Wireless Networks, vol. 1, pp. 255-65, 1995.

[4] C.K.Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Englewood Cliff, Press: Prentice Hall, 2002.

[5] IETF MANET Working Group. Mobile Ad Hoc Networks (MANET). Working Group charter, available: http://www.ietf.org/html.charters/manet-charter.html.

[6] Routing and congestion control-basic of Routing URL: http://www.scribd.com/doc/7042140/Routing-and-Congestion-Control-Bsaics-of- Routing.

[7] Bassam Halabi, "Internet Routing Architectures", Press: Cisco, 2000

[8] Scott M. Ballew, "Managing IP Networks with Cisci Routers". Orilley, vol. 1, 1997.

[9] Larry L. Peterson and Bruce S. Davie, "Computer Networks - A Systems Approach". San Francisco, Morgan Kaufmann Publishers Inc. ISBN 1-55860-368-9.

[10] Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic (Eds.),"Mobile Ad Hoc Networking," *IEEE Press,* Wiley Interscience. 2004.

[11] Xiaoyan Hong, Kaixin Xu, Mario Gerla, "Scalable Routing Protocols for Mobil ad hoc Networks", 2002.

[12] Martha Steenstrup, "Routing in Communication Networks", New Jersey, Press: Prentice Hall, ISBN 0-13-010752-2.

[13] C.E. Perkins, P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance- Vector Routing for Mobile Computers", Computer Communication Review, pp. 234-244, 1994.

[14] Larry L. Peterson, Bruce S. Davie, "Computer Networks -A Systems Approach". San Francisco, Morgan Kaufmann Publishers, ISBN 1-55860-368-9.

[15] S. Murthy, J. J. Garcia-Luna-Aceves, “An Efficient Routing Protocol for WirelessNetworks,” Special Issue ACM Mobile Networks Application and Mobile Communication Networks, pp. 183–97, 1996.

[16] L. Lamont Y. Ge, T. Kunz, “Quality of service routing in ad-hoc networks using OLSR,” The 36th.Hawaii International Conference on System Sciences (HICSS-36), 2003.

[17] Y.C. Tseng, C.C. Shen, “Chen W.T. Mobile ip and ad hoc networks: An integration and implementation experience”, A Technical Report in Department of Computer Science and Information Engineering, Nat. Chiao , Hsinchu,, Taiwan, 2003.

[18] Josh Broch, David B. Johnsson, David A. Maltz, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks”, Internet Draft, draft-ietf-manet-dsr, 1998.

[19] C. E. Perkins, E. M. Royer, “The Ad Hoc On-Demand Distance-Vector Protocol (AODV),” In Ad Hoc Networking, C. E. Perkins (Ed.), pp. 173–219, Addison-Wesley, 2001.

[20] V. Park and S. Corson, Temporally Ordered Routing Algorithm(TORA) Version 1, Functional specification IETF Internet draft (1998), http://www.ietf.org/internet-drafts/draft-ietf-manet-tora-spec-01.txt.

[21] C.-K. Toh, "Associativity-Based Routing For Ad Hoc Mobile Networks," Special Issue on Mobile Networking and Computing Systems, vol. 4, no. 2, pp. 103-39, 1997.

[22] Zygmunt J. Haas and Marc R. Pearlman, “The Performance of QueryControl Schemes for the Zone Routing Protocol,” *In Proc. of the ACM SIGCOMM ’98 Conference*, pages 167–177, September 1998.

[23] M. Joa-Ng and I.-T. Lu, “A peer-to-peer zone-based two level link state routing for mobile ad hoc networks,”IEEE Journal on selected Areas in Communication,vol. 17, pp. 1415–1425, Aug. 1999.

[24] Mobile Ad Hoc Networking Working Group, Charles E. Perkins Nokia Research Center, 22 October 1999, Elizabeth M.Royer University of California, Santa Barbara Samir R.Ds University of Texas, San Antonio Ad Hoc On-Demand Distance Vector (AODV) Routing.

[25] Krishna Ramachandran. Aodv. Technical report, University of California, Santa Barbara, USA URL: http://moment.cs.ucsb.edu/AODV/aodv.

[26] Luke Klein-Bernd, ―A Quick Guide to AODV Routing‖, National Institute of Standards and Technology, US.

[27] David B. Johnson and David A.Maltz, "Dynamic source routing in ad hoc wireless networks". In *Mobile* Computing, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153-181. Kluwer Academic Publishers,1996

[28] A. Law and W. Kelton, "Simulation Modeling and Analysis," *McGraw-Hill*, 2000

[29] XGraph homepage, URL: http:/www.isi.edu/nsnam/xgraph.

[30] NAM: Network Animator, URL: http://www.isi.edu/nsnam/ns/ns-documentation.html

[31] TCL Tutorial,URL:http://www.tcl.tk/man/tcl8.5/tutorial/tcltutorial.html

[32] Tutorial for the network simulator ns URL: http://www.isi.edu/nsnam/ns/tutorial/

[33] Trace graph URL: http://www.tracegraph.com/download.html

[34] J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva. "Multi-Hop Wireless Ad Hoc Network Routing Protocols." ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM'98), pages 85-97, 1998.

List of Publications

[1] Deepak Chaudhary and Sumit Miglani," Performance Analysis of Routing Protocols for MANET Using NS2 Simulator", National Conference on Emerging Trends in IT and Computing (ETIC-2010), March 27-28, 2010, GITM -Gurgaon (Haryana).

[2] Deepak Chaudhary and Sumit Miglani, "Performance Comparison of Reactive Routing Protocols for MANET" National conference on computing, communication and information technology (CCIT-2010), May 28-29, 2010, SLIT -Longowal (Punjab).