Evaluation of Routing Protocols for Ad Hoc Mobile Wireless Networks

Thesis Submitted in partial fulfilment of the requirements for the award of

degree of

Masters in Engineering

in

Computer science and engineering

Submitted by

S. Gnanendra Reddy

(Roll No: 800832013)

Under the supervision of

Dr. A. K. Verma

Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA-147004

MAY 2010

Certificate

I hereby certify that the work which is being presented in the thesis entitled, "***Evaluation of Routing Protocols for Ad Hoc Mobile Wireless Networks***", in partial fulfillment of the requirements for the award of degree of Master of Engineering in Computer Science and 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 *Dr. A. K. Verma* 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.

(S. Ghanendra Reddy)

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

02/07/10.

(Dr. A. K. Verma)
Assistant Professor
Computer Science & Engineering Department
Thapar University
Patiala.

Countersigned by:

05/07/2010

(Dr.Rajesh Bhatia)
Head
Computer Science & Engineering Department,
Thapar University,
Patiala.

2/7/10

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

Acknowledgement

No volume of words is enough to express my gratitude towards my guide, **Dr. Anil Kumar Verma**, Assistant Professor, Computer Science and Engineering Department, Thapar University, who have been very concerned and have aided for all the material essential for the preparation of this thesis report. He has helped me to explore this vast topic in an organized manner and provided me with all the ideas on how to work towards a research oriented venture.

I am also thankful to **Dr. Rajesh Bhatia**, Head of Department, **Dr. Inderveer Channa**, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.

I would also like to thank the staff members and my friends 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 **Parents** and the **Almighty** 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.

S.G.Reddy
(800832013

Abstract

Mobile ad- hoc networking is a conception in computer communications, which means that users who necessitate communicating with each other form a temporary network, without any form of centralized administration. Mobile ad-hoc network has definite characteristics, which imposes new demands on the routing protocol. The mainly significant characteristic is the dynamic topology, which is a effect of node mobility. Nodes can alter position quite commonly, which means that we require a routing protocol that rapidly adapts to topology changes. The nodes in an ad-hoc network can consist of laptops and individual digital assistants and are habitually very partial in resources such as storage capacity, CPU capacity, battery power and bandwidth. This means that the routing protocol must try to minimize control traffic, such as periodic update messages. Instead the routing protocol should be reactive, thus only calculate routes ahead receiving a particular request.

The presented work evaluates three of the protocols (AODV, DSR and TORA) against the parameters put forth by the Mobile ad-hoc Network's working group. This evaluation is done by way of simulation using Network simulator 2 from Berkeley. These three protocols are DSR, AODV and TORA, Each having its fair of advantages and limitations. Routing protocols utilize numerous metrics to calculate the best path for routing the packets to its destination, comparison between the AODV, DSR and TORA routing protocol by means of the average end to end delay, packet loss and packet delivery fraction performance metrics. A huge network with many mobile nodes and high offered load will increase the overhead for DSR quite drastically. In these situations, a hop-by-hop based routing protocol like AODV is more enviable.

Keywords: MANETs, DSR, AODV, TORA.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ACK	Acknowledgement
MANET	Mobile Ad hoc Network
AODV	Ad-hoc On-demand Distance Vector
DSR	Dynamic Source Routing Protocol
TORA	Temporally Ordered Routing Algorithm Protocol
CBR	Continuous Bit Rate
DARPA	Defence Advanced Research Project Agency
EPPCSIT	Emerging Principles and Practises of Computer Science and Information Technology
FC10	Fedora Core 10
FTP	File Transfer Protocol
GUI	Graphical User Interface I
IETF	Internet Engineering Task Force
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
MAC	Medium Access Control
MH	Mobile Hosts
NAM	Network Animation
NS	Network Simulator
OSI	Open System Interconnect
OTcl	Object Oriented Tool Command Language
PAN	Personal Area Network
Tcl	Tool Command Language
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
VINT	Virtual Inter Network Test-bed
WPAN	Wireless Local Area Network

Chapter 1

Introduction

1.1Motivation:

Wireless communication between mobile users is becoming more popular than ever before. This is due to recent technological advances in laptop computers and wireless data communication devices, such as wireless modems and wireless LANs. This has lead to lower prices and higher data rates, which are the two main reasons why mobile computing continues to enjoy rapid growth.

There are two distinct approaches for enabling wireless communication between two hosts. The first approach is to let the existing cellular network infrastructure carry data as well as voice. The major problems include the problem of handoff, which tries to handle the situation when a connection should be smoothly handed over from one base station to another base station without noticeable delay or packet loss. Another problem is that networks based on the cellular infrastructure are limited to places where there exists such a cellular network infrastructure.

The second approach is to form an ad-hoc network among all users wanting to communicate with each other. This means that all users participating in the ad-hoc network must be willing to forward data packets to make sure that the packets are delivered from source to destination. This form of networking is limited in range by the individual nodes transmission ranges and is typically smaller compared to the range of cellular systems. This does not mean that the cellular approach is better than the ad-hoc approach. Ad-hoc networks have several advantages compared to traditional cellular systems. These advantages include:

- On demand setup
- Fault tolerance
- Unconstrained connectivity

Ad-hoc networks do not rely on any pre-established infrastructure and can therefore be deployed in places with no infrastructure. This is useful in disaster recovery situations and places with no n-existing or damaged communication infrastructure where rapid deployment of a communication network is needed. Ad-hoc networks can also be useful on conferences where people participating in the conference can form a temporary network without engaging the services of any pre-existing network.

Because nodes are forwarding packets for each other, some sort of routing protocol is necessary to make the routing decisions. Currently there does not exist any standard for a routing protocol for ad-hoc networks, instead this is work in progress. Many problems remain to be solved before any standard can be determined. This thesis looks at some of these problems and tries to evaluate some of the currently proposed protocols.

1.2. Thesis Outline

We have organized the thesis into 7 chapters which include Introduction; Background Information; Literature Review; Problem Statement; Installation, Simulation and Design; Results, Performance Evaluation and Analysis and finally Conclusion and Future Scope . Chapter 1 describes Mobile Ad-hoc Network (MANETs) in general in terms of motivation and then follows by the whole thesis outline. Chapter 2, we discuss the background information relating to MANETs and it's routing. Chapter 3, we study the state of the art of various routing protocols in MANETs. DSR, TORA and AODV protocol in detail has been discussed covering the description of protocol modes and working, structure of various packets being transferred; procedures followed by the nodes in the particular modes. Chapter 4 discusses the problem statement and tasks. Chapter 5 discusses the installation of tools and the simulation environment. Chapter 6 describes the results, evaluates the performance, and analysis and finally Chapter 7 summarizes the conclusions drawn in the thesis along with future research directions.

Chapter 2

BACKGROUND AND GENERAL CONCEPTS

2.1 Wireless Networks

Like traditional wired networks, wireless networks are formed by routers and hosts. In a wireless network, the routers are responsible for forwarding packets in the network and hosts may be sources or sinks of data flows. The fundamental difference between wired and wireless networks is the way that the network components communicate. A wired network relies on physical cables to transfer data. In a wireless network, the communication between different network components can be either wired or wireless. Since wireless communication does not have the constraint of physical cables, it allows a certain freedom for the hosts and/or routers in the wireless network to move. This is one of the advantages of a wireless network.

Network components in a wireless network communicate with others using wireless channels. Different radio frequency (RF) spectrum ranges are used in wireless networks, for example, 27.5-29.5 GHz for the Local Multipoint Distribution System (LMDS) [7], 2.5-2.7 GHz for the Multipoint Multichannel Distribution System [12], and 5.15-5.35 GHz and 2.4-2.58 GHz for IEEE 802.11a [16] and 802.11b [20], respectively.

Signal strength in a wireless medium decreases when the signal travels further. When the signal travels beyond a certain distance, the strength reduces to the point where reception is not possible [23]. The distance that the signal travels when it reaches this point is called the radio range for this signal. To simplify the transmission model regarding this property, people assume that the wireless signal is strong enough for the receivers to receive the signal if the receivers are inside of the radio range. Otherwise, the receivers cannot receive the signal at all. The details of wireless communications are not in the scope of this dissertation. Refer to [23] for details.

Several medium access control (MAC) protocols are used in wireless networks to manage the use of the wireless medium. Examples include the Bluetooth MAC layer protocol [23] and IEEE 802.11MAClayer protocol [20]. This research focuses on the network layer. Thus, the details of these MAC protocols are beyond our scope. Refer to [20] and [23] for more details.

Because radio range is usually limited and the network components may have some mobility, the topology of a wireless network can vary with time. According to the relative mobility of hosts and routers, there are three different types of wireless networks.

2.1.1. **Fixed wireless network**: Fixed hosts and routers use wireless channels to communicate with each other and form a fixed wireless network. An example is a wireless network formed by fixed network devices using directed antennas, as shown in Figure2.1.

Figure2.1: An example of a fixed wireless network. [32]

2.1.2. **Wireless network with fixed access points**: Mobile hosts use wireless channels to communicate with fixed access points, which may act as routers for those mobile hosts, to form a mobile network with fixed access points. An example is a number of mobile laptop users in a building that access fixed access points, as illustrated in Figure 2.2.

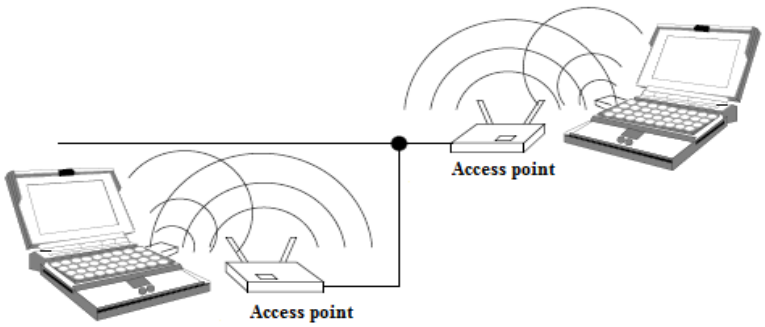


Figure2.2: An example of a wireless network with access points. [32]

2.1.3. Mobile ad hoc network: A mobile ad hoc network is formed by mobile hosts. Some of these mobile hosts are willing to forward packets for neighbours. Examples include vehicle-to-vehicle and ship-to-ship networks that communicate with each other by relying on peer-to-peer routings, as shown in Figure 2.3.

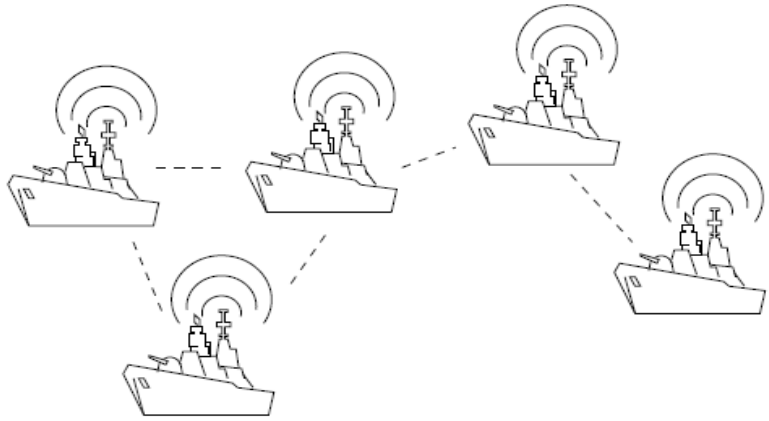


Figure2.3: An example of a mobile ad hoc network [32].

Generally speaking, traditional routing protocols that are used in wired networks can support routing in fixed wireless networks and mobile networks with fixed access points. Only one-hop routing is required over a link in a wireless network with fixed access points and many fixed wireless network. Routing in mobile ad hoc networks and some fixed wireless networks use multiple-hop routing. Routing protocols for this kind of wireless network should be able to maintain paths to other nodes and in most cases, must handle changes in paths due to mobility. Traditional routing cannot properly support routing in a MANET. This thesis focuses on mobile ad hoc routing.

An ad-hoc network uses no centralized administration. This is to be sure that the network won't collapse just because one of the mobile nodes moves out of transmitter range of the others. Nodes should be able to enter/leave the network as they wish. Because of the limited transmitter range of the nodes, multiple hops may be needed to reach other nodes. Every node wishing to participate in an ad-hoc network must be willing to forward packets for other nodes. Thus every node acts both as a host and as a router. A node can be viewed as an abstract entity consisting of a router and a set of affiliated mobile hosts (Figure 2.4). A router is an entity, which, among other things runs a routing protocol. A mobile host is simply an IP-addressable [1] host/entity in the traditional sense.

Ad-hoc networks are also capable of handling topology changes and malfunctions in nodes. It is fixed through network reconfiguration. For instance, if a node leaves the network and causes link breakages, affected no des can easily request new routes and the problem will be solved. This will slightly increase the delay, but the network will still be operational.

Wireless ad-hoc networks take advantage of the nature of the wireless communication medium. In other words, in a wired network the physical cabling is done a priori restricting the connection topology of the nodes. This restriction is not present in the wireless domain and, provided that two nodes are within transmitter range of each other, an instantaneous link between them may form.

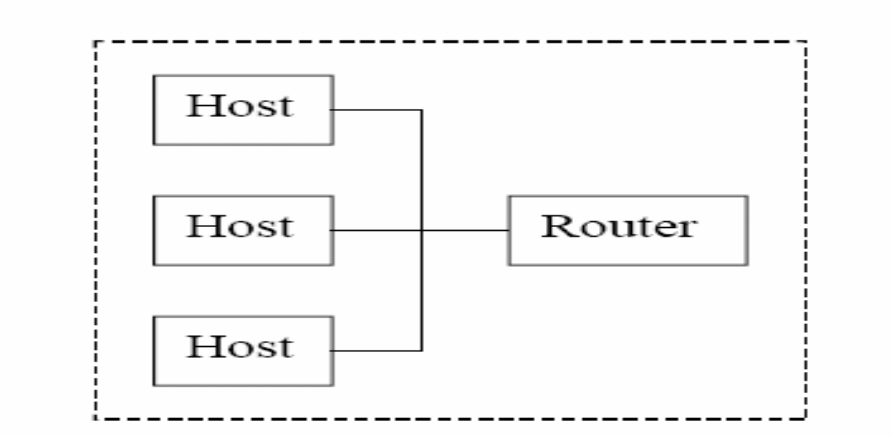


Figure 2.4: Block diagram of a mobile node acting both as hosts and as router.

2.1.3.1 Mobile Ad hoc Networks Communication Architecture: Protocol Stack

In this section the protocol stack for mobile ad hoc networks is described. This gives a comprehensive picture of, and helps to better understand, mobile ad hoc networks. Figure 2.5, shows the protocol stack which consists of five layers: physical layer, data link layer, network layer, transport layer and application layer. It has similarities to the TCP/IP protocol suite. As can be seen the OSI layers for session, presentation and application are merged into one section, the application layer.

On the left of Fig.2.5, the OSI model is shown. It is a layered framework for the design of network systems that allows for communication across all types of computer systems.

In the middle of the figure, the TCP/IP suite is illustrated. Because it was designed before the OSI model, the layers in the TCP/IP suite do not correspond exactly to the OSI layers. The lower four layers are the same but the fifth layer in the TCP/IP suite (the application layer) is equivalent to the combined session, presentation and application layers of the OSI model.

On the right, the MANET protocol stack -which is similar to the TCP/IP suite -is shown. The main difference between these two protocols stacks lies in the network layer. Mobile nodes (which are both hosts and routers) use an ad hoc routing protocol to route packets. In the physical and data link layer, mobile nodes run protocols that have been designed for wireless channels. Some options are the IEEE standard for wireless LANs, IEEE 802.11, the European ETSI standard for a high-speed wireless LAN, and finally an industry approach toward wireless personal area networks, i.e. wireless LANs at an even smaller range, Bluetooth. In the simulation tool used in this project, the standard IEEE 802.11 is used in these layers. [3]

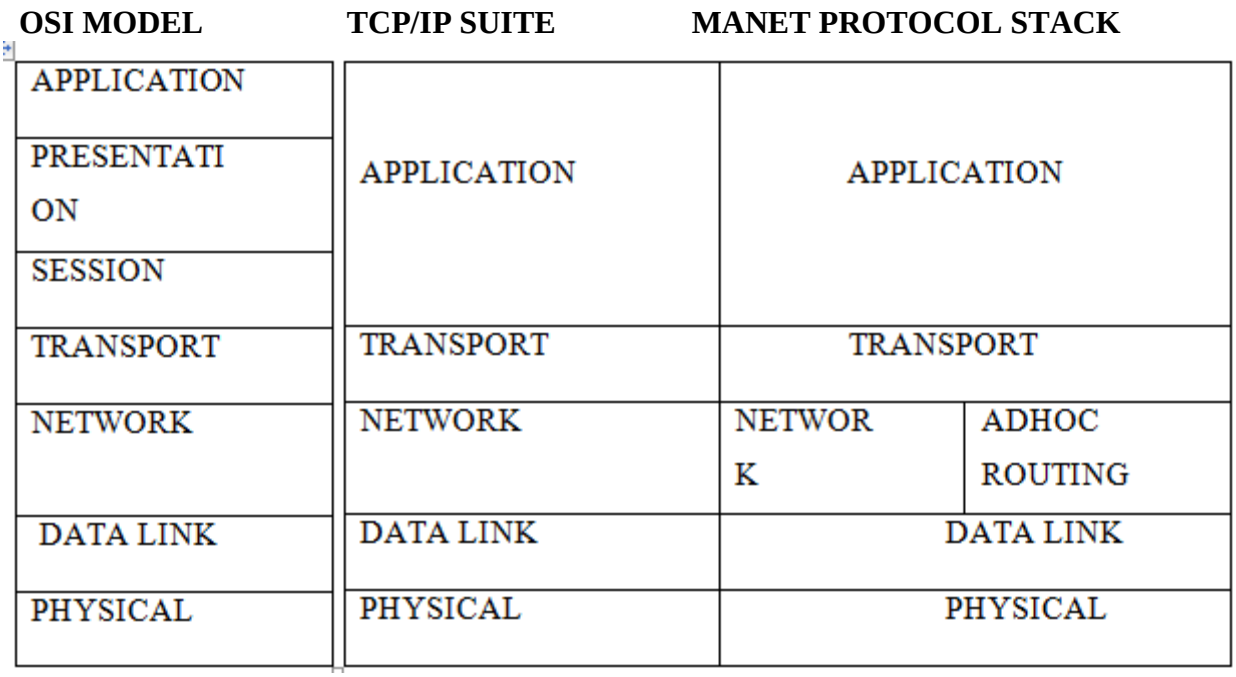


Figure.2.5: Three Models of Protocol Stack

This thesis focuses on ad hoc routing which is handled by the network layer. The network layer is divided into two parts: Network and Ad Hoc Routing. The protocol used in the network part is Internet Protocol (IP) and the protocols which can be used in the ad hoc routing part are AODV, DSR, TORA, etc.

2.1.3.2 Usage of MANETs:

The suggestions vary from document sharing at conferences to infrastructure enhancements and military applications. In areas where no infrastructure such as the Internet is available an ad-hoc network could be used by a group of wireless mobile hosts. This can be the case in areas where a network infrastructure may be undesirable due to reasons such as cost or convenience. Examples of such situations include disaster recovery personnel or military troops in cases where the normal infrastructure is either unavailable or destroyed.

Other examples include business associates wishing to share files in an airport terminal, or a class of students needing to interact during a lecture. If each mobile host wishing to communicate is equipped with a wireless local area network interface, the group of mobile hosts may form an ad-hoc network.

Access to the Internet and access to resources in networks such as printers are features that probably also will be supported.

2.1.3.3 Characteristics of MANETs

An ad hoc network is a collection of mobile nodes forming a temporary network without the aid of any centralized administration or standard support services regularly available on conventional networks.

The MANET working group has defined some unique properties of ad hoc networks in RFC 2501 [27]. The properties does not directly relate to performance. However, they describe the very nature of ad hoc networks and in that sense they formulate the boundary conditions to ad hoc networking. In a manner they impact on performance, since they greatly affect on the design of ad hoc routing protocols.

The following characteristics are defined by the MANET working group in RFC 2501:

1. 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.

2. 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.

3. Energy constrained operation

Mobile nodes are likely to rely on batteries. That is why the primary design criteria may sometimes be energy conservation.

4. 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 to that of centralized networks. Figure 2.6 illustrates a typical wireless mobile ad hoc network composed of seven nodes along with the links between them. Note that links in an ad hoc network can be unidirectional.

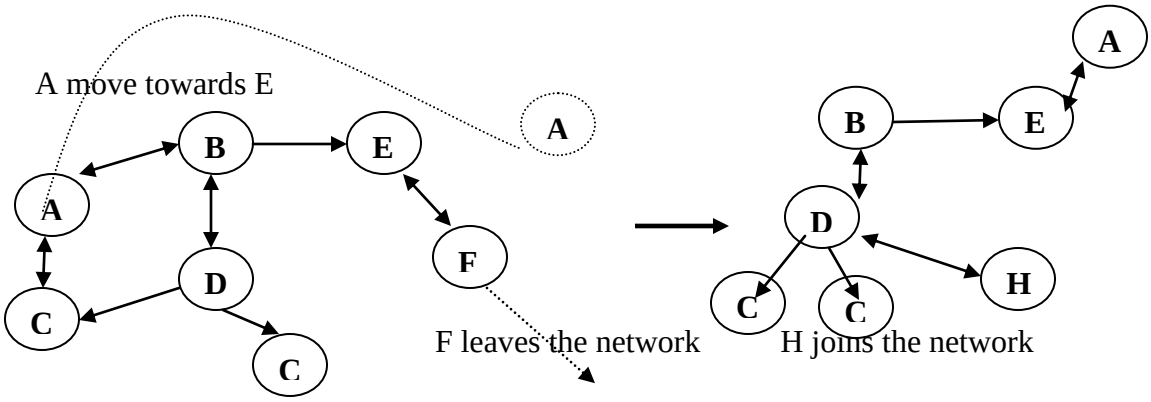


Figure 2.6: A Typical Mobile Ad Hoc Network

The nodes are mobile and can move relative to each other in a random arbitrary manner. As the nodes move, links are broken and new links are established. Existing nodes can leave the network and new nodes may join the network .Thus the network topology can change rapidly and unpredictably over time. In the figure, node A moves away from nodes B, C, D and F leaves the network establishes a new bi-directional link with node E. Node F leaves the network and node H joins the network leading to an arbitrary change in the network topology over time.

2.1.3.4. Applications of MANETs

With the increase of portable devices as well as progress in wireless communication, Ad hoc networking is gaining importance with the increasing number of widespread applications [5]. Ad hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic

networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include:

1. Military battlefield

The modern digital battlefield demands robust and reliable communication in many forms. Most communication devices are installed in mobile vehicles, tanks, trucks etc. Also soldiers could carry telecomm devices that could talk to a wireless base station or 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 soldiers if the called party is not within the radio range. This is the scenario where mobile ad hoc networks come into play. Ad hoc 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.

2. Sensor Networks [40]

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 ad hoc sensor networks could be the key to future homeland security.

3. 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.

4. 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.

5. 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.

2.1.3.5. Challenges Facing MANETs

The ad hoc networks have it's own share of challenges which are listed below:

1. Spectrum allocation [8]

Issues such as interference, limited range, limited data throughput, device mobility and the sharing of the RF spectrum amongst devices all need addressing. Regulation Regarding the use of radio spectrum is currently under the control of FCC. Most experimental Ad hoc networks are based on the ISM band. To prevent interference Ad hoc networks must operate over some form of allowed or specified spectrum range. Most microwave ovens operate in 2.4 GHz band, which can therefore interfere with wireless LAN systems.

2. Energy efficiency

Energy efficiency is a concern. Most existing protocols don't consider power consumption as an issue since they assume the presence of static hosts and routes, which are powered by mains. However mobile devices today mostly operated by batteries .Battery technology are still lagging behind the microprocessor technology. The lifetime

of a Li-on battery today is only 2-3 hours. Such a limitation in operating hours of a device employs a need for power conversion. In particular for mobile ad hoc networks devices will have to perform the role of routers. Hence forwarding packets on the behalf of others will consume power and this can be quite significant for nodes in mobile ad hoc networks.

3. Routing

Routing of data between devices is outside their RF range. The routing protocols used on wired networks do not perform well on networks involving mobility and rapid membership changes. More effective routing protocols are required. In Ad Hoc networks, we need new routing protocols because of the following reasons:

- Nodes in Ad Hoc networks are mobile and topology of interconnections between them may be quite dynamic.
- Existing protocols exhibit least desirable behaviour when presented with a highly dynamic interconnection topology.
- Existing routing protocols place too heavy a computational burden on each mobile computer in terms of the memory-size, processing power and power consumption.
- Existing routing protocols are not designed for dynamic and self-starting behaviour as required by users wishing to utilize Ad-Hoc networks.
- Existing routing protocols like Distance Vector Protocol take a lot of time for convergence upon the failure of a link, which is very frequent in Ad Hoc networks.
- Existing routing protocols suffer from looping problems either short lived or long lived.
- Methods adopted to solve looping problems in traditional routing protocols may not be applicable to Ad Hoc networks.

2.2. Routing Approaches in MANETs: Introduction

Routing is the act of moving information from a source to a destination in an internetwork. During this process, at least one intermediate node within the internetwork is encountered. 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 of 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 concept basically involves, two activities: firstly, determining optimal routing paths and secondly, transferring the information groups (called packets) through an internetwork. The later concept is called as packet switching which is straight forward, and the path determination could be very complex [13].

Routing protocols use several metrics to calculate the best path for routing the packets to its destination. These metrics are a standard measurement that could be number of hops, which is used by the routing algorithm to determine the optimal path for the packet to its destination. The process of path determination is that, routing algorithms initialize and maintain routing tables, which contain the total route information for the packet. This route information varies from one routing algorithm to another.

Routing tables are filled with a variety of information which is generated by the routing algorithms. Most common entries in the routing table are IP-address prefix and the next hop. Routing table's Destination/next hop associations tell the router that a particular destination can be reached optimally by sending the packet to a router representing the "next hop" on its way to the final destination and IP-address prefix specifies a set of destinations for which the routing entry is valid for.

Switching is relatively simple compared with the path determination. The concept of switching is like, a host determines like it should send some packet to another host. By some means it acquires the routers address and sends the packet addressed specifically to the routers MAC address, with the protocol address of the destination host. The router then examines the protocol address and verifies whether it know how to transfer the data

to its destination. If it knows how to transfer the data then it forwards the packet to its destination and if it doesn't then it drops the packet.

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 [21]. 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.

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 [9].

2.2.1 Classification of Dynamic Routing Protocols

Dynamic routing protocols are classified depending on what the routers tell each other and how they use the information to form their routing tables. They are Distance vector protocols and Link state protocols Most of the protocols available in the networks fit into one of the two categories [9].

2.2.1.1 Distance Vector Protocols

By using the distance vector protocols, each router over the internetwork send the neighbouring routers, the information about destination that it knows how to reach. Moreover to say the routers sends two pieces of information first, the router tells, how far it thinks the destination is and secondly, it tells in what direction (vector) to use to get to the destination. When the router receives the information from the others, it could then develop a table of destination addresses, distances and associated neighbouring routers, and from this table then select the shortest route to the destination. Using a distance

vector protocol, the router simply forwards the packet to the neighbouring host (or destination) with the available shortest path in the routing table and assumes that the receiving router will know how to forward the packet beyond that point [25]. The best example for this is the routing information protocol (RIP).

2.2.1.2 Link-State Protocols

In link state protocols, a router doesn't provide the information about the destination instead it provides the information about the topology of the network. This usually consist of the network segments and links that are attached to that particular router along with the state of the link i.e., whether the link is in active state or the inactive state. This information is flooded throughout the network and then every router in the network then builds its own picture of the current state of all the links in the network.

2.2.1.3 Source Routing

Source routing [29] 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.

2.2.1.4 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 [29] 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.

2.2.2. Routing Challenges and Design Issues

- **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 MANETs (Mobile Ad-hoc Network) 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 [17].

- **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 [17]. This updating frequency might be very low for ad-hoc networks.

2.2.3. Desirable Characteristics of Routing Protocol

The MANET working group also defines some desirable qualitative properties of ad hoc routing protocols in RFC 2501 [27]. They are useful when assessing performance or suitability of an ad hoc routing protocol thus they are worth to mention in the context of this paper. The following properties are defined in RFC 2501:

- **Distributed operation:** This property is essential to ad hoc networks. It is self-evident that ad hoc networks operate in distributed manner because of their very nature. Therefore, the routing protocols should be distributed, not dependent on a centralized controlling node.
- **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, sequence numbers 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 operations are unacceptable, proactive approach can be used especially when energy and bandwidth capacities support the use of proactive operation.
- **Security:** Ad hoc routing protocols are exposed to several kinds 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 disruption or modification of protocol operation. Probably emerge rarely.
- **Power Conservation:** The nodes in ad hoc network can be laptops and thin clients such as Personal Digital Assistance (PDAs) that are very limited in battery power and therefore uses some sort of stand-by mode to save power. It is therefore important that the routing protocols have support for these sleep-modes.
- **Unidirectional support:** The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing performance.

Chapter 3

LITERATURE REVIEW

3.1. An Overview of Routing Protocols for MANETs:

Routing is a difficult problem in a MANET. A lot of solutions have been proposed trying to address a sub-space of the problem domain. Because of complexity and diversity, Internet Engineering Task Force (IETF) has not determined a standard of routing. A number of routing protocols have been suggested for ad-hoc networks [2], [6], [10], [14], [18]. These protocols can be classified into Flat, Hierarchical, Geographical Routing, Flat routing can be classified into three main categories: proactive (table driven), reactive (source-initiated or demand-driven) and Hybrid (taking both proactive and reactive).

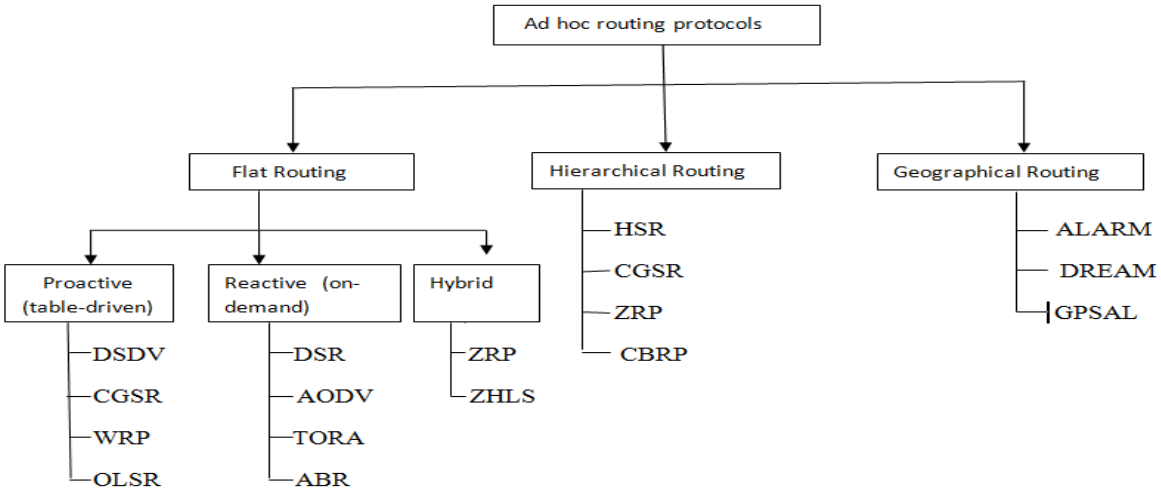


Figure3.1: Classification of Routing Protocols.

3.1.1 Table-driven or Proactive Protocols [2]

Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed intervals. As the resulting information is usually maintained in tables, the protocols are sometimes referred to as table-driven protocols. Representative

proactive protocols include: Destination-Sequenced Distance- Vector (DSDV) routing [6], Clustered Gateway Switch Routing (CGSR) [24], Wireless Routing Protocol (WRP) [26], and Optimized Link State Routing (OLSR) [18].

3.1.2 On-demand or Reactive Protocols [2]

A different approach from table-driven routing is reactive or on-demand routing. These protocols depart from the legacy Internet approach. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Once a route has been established, it is maintained by the node until either the destination becomes inaccessible or until the route is no longer used or has expired. Representative reactive routing protocols include: Dynamic Source Routing (DSR) [2], Ad hoc On Demand Distance Vector (AODV) routing [10, 41], Temporally Ordered Routing Algorithm (TORA) [14] and Associativity Based Routing (ABR) [30].

3.1.3 Hybrid Routing Protocols

Purely proactive or purely reactive protocols perform well in a limited region of network setting. However, the diverse applications of ad hoc networks across a wide range of operational conditions and network configuration pose a challenge for a single protocol to operate efficiently [11]. For example, reactive routing protocols are well suited for networks where the call-to-mobility ratio is relatively low. Proactive routing protocols, on the other hand, are well suited for networks where this ratio is relatively high. The performance of either class of protocols degrades when the protocols are applied to regions of ad hoc networks space between the two extremes.

Researchers advocate that the issue of efficient operation over a wide range of conditions can be addressed by a *hybrid* routing approach, where the proactive and the reactive behaviour is mixed in the amounts that best match these operational conditions. Representative hybrid routing protocols include: Zone Routing Protocol (ZRP) [22] and Zone-based Hierarchal Link state routing protocol (ZHLS) [31].

Of these proposed protocols, I have chosen to analyze and compare (simulation based) the following routing protocols. These are:

• Ad-hoc On-demand Distance Vector (AODV) [10] reactive approach

• Dynamic Source Routing (DSR) [2] reactive approach

• Temporal Ordered Routing Algorithm (TORA) [14] also reactive

3.2. Description and Properties of Routing Protocols

3.2.1. Ad-hoc On-demand Distance Vector (AODV) Protocol

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The operation of AODV is loopfree, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link. One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number.

Route Discovery

Whenever there exists a valid route between two communication peers, AODV Route Discovery is not used. As soon as a route is missing between the two communications

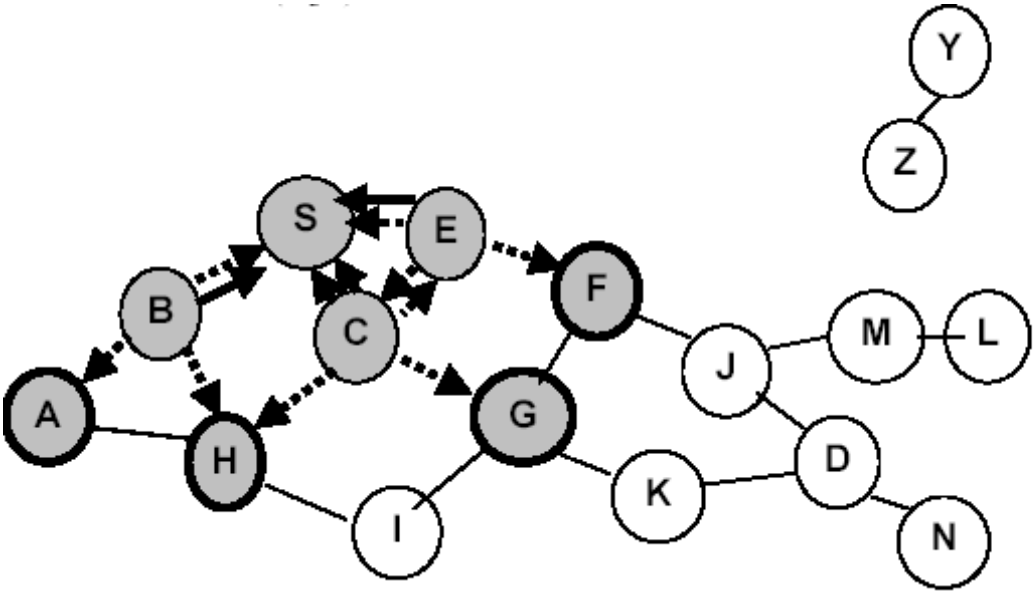
partners, e.g. when a new route to a destination is needed, a link is broken, or the route has expired, the source node **S** broadcasts a ROUTE REQUEST message in order to find a route to the destination **D**.(in figure3.2)

Type	Reserved	Hop Count
Broadcast ID		
Destination IP Address		
Destination Sequence Number		
Source IP Address		
Source Sequence Number		
Request Time		

Figure.3.2.AODV: Structure of an RREQ packet [31]

• Route Requests (RREQ) are forwarded in a manner similar to DSR described below

• When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source (Figure 3.3).



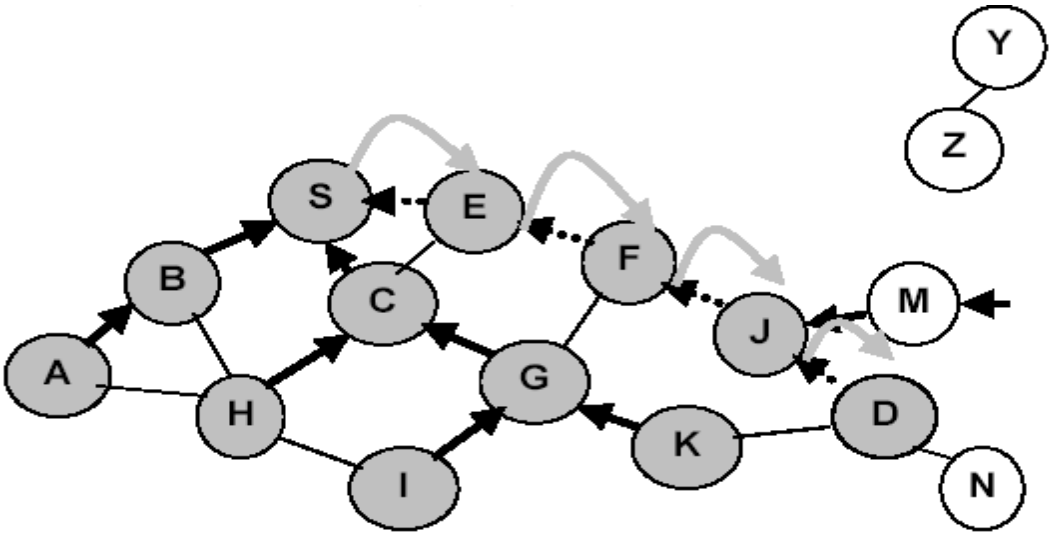
Represents links on the reverse path (in Figure 3.3).

Figure 3.3.AODV: Route Discovery [10]

• Here again nodes do not forward RREQ if they have already forwarded it once.

• When the intended destination receives a Route Request, it replies by sending a Route Reply message. The destination does not forward the Route Request message as it is intended for itself.

• The Route Reply message travels along the reverse path set-up when Route Request was forwarded (in Figure 3.4).



Represents links on path taken by RREP (in Figure 3.4).
Represents link on the forward path (in Figure 3.4).
Figure 3.4.AODV: Route Reply [10]

• Forward links are set up when RREP travels along the reverse path. This information is stored in the routing table.

• These routing table entries are used to forward the data packets and is not included in the packet header.

Timeouts

A routing table entry maintaining a reverse path is purged after a timeout interval. In this case timeout should be long enough to allow RREP to come back. A routing table entry maintaining a forward path is purged if not used for an active_route_timeout interval.

That if no data is being sent using a particular routing table entry, that entry will get deleted from the routing table (even if the route may actually still be valid).

The Business of Sequence Numbers

An intermediate node (not the destination) may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender S. To determine whether the path known to an intermediate node is more recent, destination sequence numbers are used.

Route Maintenance

To maintain routes the nodes survey the link status of their next hop neighbors in active routes. The node detecting a link break sends a ROUTE ERROR message to each of its upstream neighbors to invalidate this route and these propagate the ROUTE ERROR to their upstream neighbors. This continues until the source node is reached. Normally the nodes in AODV sends periodic HELLO messages and the failure of reception of three consecutive HELLO messages from a neighbor are handled as link error. (in figure3.5)

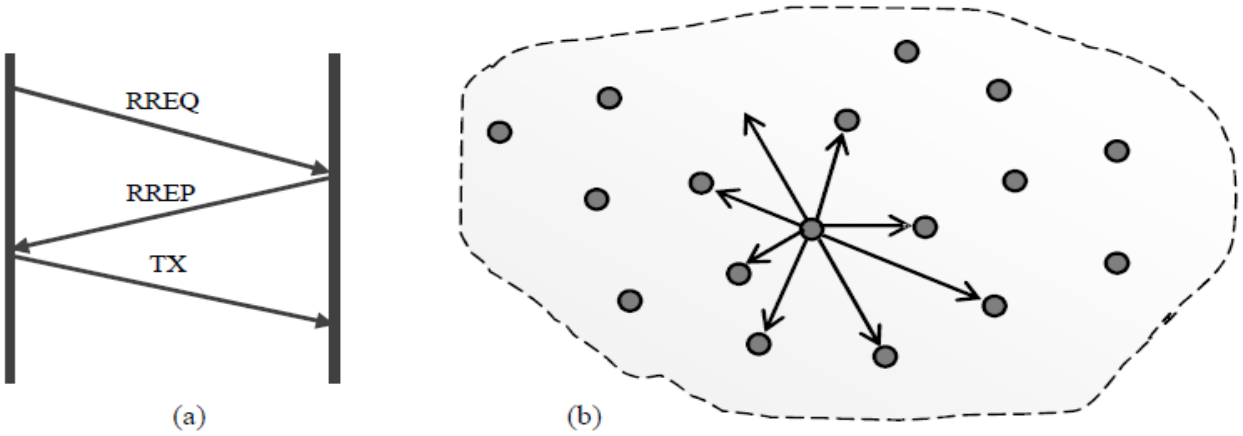


Figure.3.5. AODV; (a) Timing diagram, (b) Broadcasts a HELLO packet to the neighbours [10]

Another possibility of link breakage detection uses link layer notification. This alternative results in a pure on-demand nature of the link breakage detection. A broken link cannot be identified until packets should be sent over the link. By contrast the HELLO messages in standard AODV allows the detection of broken links before a packet must be

forwarded, but this has the disadvantage of use of bandwidth for the periodic transmission of HELLO messages. The ROUTE ERROR message contains a infinite metric for the destination and causes the receiver to invalidate the route. Now the node must start a new Route Discovery for a connection to this destination.

Use of Sequence numbers

The sequence numbers are mainly used for the following purposes:

a) To avoid using old/broken routes.

b) To prevent formation of loops (counting to infinity problem).

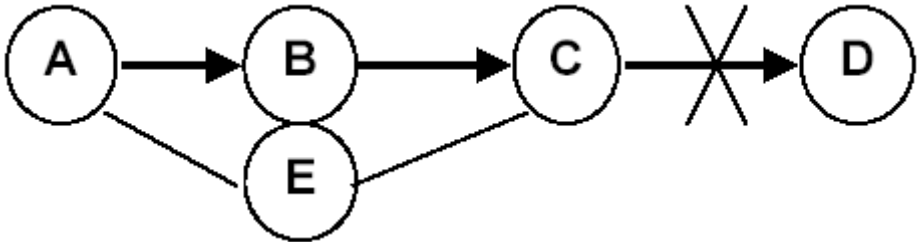


Figure 3.6.AODV: Uses of Sequence Numbers [10]

• Let us assume that A does not know about failure of link C-D because RERR sent by C is lost.

• Now C performs a route discovery for D. Node A receives the RREQ (say, via path CE-A).

• Node A will reply since A knows a route to D via node B.

• Results in a loop (for instance, C-E-A-B-C).

Resource Usage

The routing table maintained at each node contains the following information: destination, next hop, sequence number, and status of the link. However, because AODV is an on-demand protocol, the actual size of the route table is much smaller on average compared to the table maintained by DSDV. The size of the routing table at each node is directly proportional to the number of active destination nodes. Thus even though some memory is required to maintain these routing tables, it is less than the amount required to maintain the routing tables for DSDV.

The CPU is used to route packets and discover the routes to the destination, so this approach does not impose any additional load on the CPU compared to DSDV.

Scalability

As the number of nodes in a network increases, the number of routing packets sent is likely to increase as well. Increasing network size most likely translates to an increase in number of destinations to which each node must maintain working routes. Also the incremental cost for nodes added to the network decreases, because the new nodes use the information learned from one route discovery to fill their tables with information from previous route discoveries already captured at other nodes.

Advantage: Routes need not be included in packet headers.

Disadvantage: Unused routes expire even if topology does not change.

3.2.2. Dynamic Source Routing (DSR) Protocol

The dynamic Source Routing (DSR) is an on-demand routing protocol that is based on the concept of source routing. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned. The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multihop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring, requiring no existing network infrastructure or administration.

Mode of Operation

DSR operate on demand, which means that no data, such as route advertisement messages, is send periodically and therefore routing traffic caused by DSR can scale down and overhead packages can be avoided. DSR is a source routing protocol, which means the entire route is known before a packet transmission is begun. DSR stores discovered routes in a Route Cache.

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

Route Discovery

When a node S sends a packet to the destination D, it first searches its Route Cache for a suitable route to D. If no route from S to D exists in S's route cache, S initiates Route

Discovery and sends out a ROUTE REQUEST message to find a route. The fields of the ROUTE REQUEST message are explained in Table 3.1.

The initiator initializes the Address List to an empty list and set the Initiator ID, the Target Id and the Unique Request Id in the ROUTE REQUEST message and then broadcasts the message.

Table 3.1.DSR: Fields of the ROUTE REQUEST Message. [2]

Fields	**Explanation**
Initiator ID	The address of the initiator
Target ID	The address of the target
Unique Request	ID A unique ID that can identify the message
Address List	A list of all addresses of intermediate nodes that the message passes before its destination. This is empty when the message is first send.
Hop Limit	The hop limit can be used to limit the number of nodes that the message is allowed to pass.
Network Interface List	If nodes have several network interfaces this information can be stored in this list.
Acknowledgment bit	There is an option of setting a bit so that the receiver returns an acknowledgment when a packet is received.

This causes the packet to be received by nodes within the wireless transmission range. The initiator keeps a copy of the packet in a buffer, referred to as the send buffer. It timestamp's the message so it can be examined later to determine if it should be send again. If no route is discovered within a specified time frame, the packet is dropped from the send buffer. Packets are also dropped from the send buffer if the buffer overruns.

When a node receives a ROUTE REQUEST message it examines the Target ID to determine if it is the target of the message. If the node is not the target it searches its own route cache for a route to the target. If a route is found it is returned. If not, the nodes own id is appended to the Address List and the ROUTE REQUEST is broadcasted. If a node subsequently receives two ROUTE REQUESTs with the same Request id, it is possible to specify that only the first should be handled and the subsequent discarded. If the node

is the target it returns a ROUTE REPLY message to the initiator. This ROUTE REPLY message includes the accumulated route from the ROUTE REQUEST message. The target searches its own Route Cache for a route to the initiator. The reason that the target node doesn't just reverse the found route and use it is that that would require bidirectional links. If a route is not found in the targets Route Cache, it performs a route discovery of its own and sends out a ROUTE REQUEST where it piggybacks the ROUTE REPLY for the initiator.

Route Maintenance

Since nodes move in and out of transmission range of other nodes and thereby creates and breaks routes, it is necessary to maintain the routes that are stored in the Route Cache. When a node receives a packet it is responsible for confirming that the packet reaches the next node on the route. Figure 3.7 that the mechanism works like a chain where each link has to make sure that the link in front of it is not broken. The figure also illustrates that node C might use another route to communicate to node A.

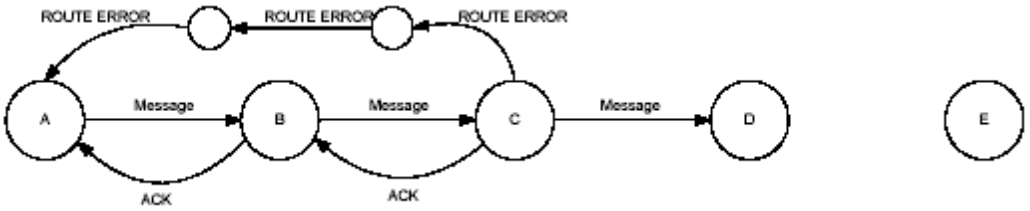


Figure 3.7.DSR: The Acknowledgement Mechanism Works like a Chain [28]

Acknowledgment can be performed either by using mechanisms in the underlying protocol such as link-level acknowledgment or passive acknowledgment. If none of these mechanisms are available, the transmitting node can set a bit in the packets header to request a specific DSR acknowledgment. If a node transmits a packet and does not receive an acknowledgment it tries to retransmit a fixed number of times. If no acknowledgement is received after the retransmissions, it returns a ROUTE ERROR message to the initiator of the packet. In this message the link that was broken is included. The initiator removes the route from its Route Cache and tries to transmit using

another route from its Route Cache. If no route is available in the Route Cache a ROUTE REQUEST is transmitted in order to establish a new route.

Advantages

Routes are maintained only between nodes that need to communicate. This reduces the overhead of route maintenance. Route caching can further reduce route discovery overhead. A single route discovery may yield many routes to the destination, due to intermediate nodes replying from their local caches.

Disadvantages

Packet header size keeps on growing with the route length. Flooding problems can take place every now and then. Care needs to be taken to avoid collisions between route requests propagated by neighboring nodes. Insertion of random delays before forwarding RREQ may be a measure to minimize this collision.

Resource usage

Typical routing protocols such as distance-vector store just the next hop for any route, but DSR requires each node to maintain a full topology for all hosts with which it wants to communicate. Hence this adds a load on memory resources. DSR uses more CPU time than other routing protocols like AODV and DSDV. One reason for this could be that DSR requires each host to monitor all of the network traffic going on within its receiving range.

Scalability

DSR uses an optimized form of flooding to reduce network overhead. On route discovery it sends one broadcast packet to all its neighbors. If it does not receive information from them on how to reach the destination node, then it sends a network-wide broadcast. Due to the use of such optimizing techniques, DSR produces a significantly lower amount of network overhead; However, DSR may still not be a very scalable protocol because each node is required to maintain full knowledge of the paths over which it needs to communicate. The more destinations, the more memory is required, a likely condition as the network gets busier.

3.2.3. Temporally Ordered Routing Algorithm (TORA) Protocol

TORA [14] is a distributed routing algorithm based on the concept of link reversal. The protocol consists of three basic functions: Route Creation, Route Maintenance and Route Erasure [28]. For route creation and maintenance, nodes use a height and reference metric to establish a directed acyclic graph (DAG) rooted at the destination. Route creation is accomplished using QRY and UPD packets. The route creation process is initiated by broadcasting a QRY packet with the destination ID in it. The height of the destination is set to 0 and the height of all other nodes is set to null. A node with a non-null height responds to a QRY packet with a UPD packet. A node receiving an UPD packet sets its height to one more than the node that generated the packet. Thus, a node with higher height is considered upstream and a node with lower height is considered downstream. This technique permits the source to construct a DAG rooted at the destination. Each node discards a QRY packet if it has already seen the packet. A node always uses the least height offered by an UPD packet. The route creation process is illustrated below.(in figure 3.8).

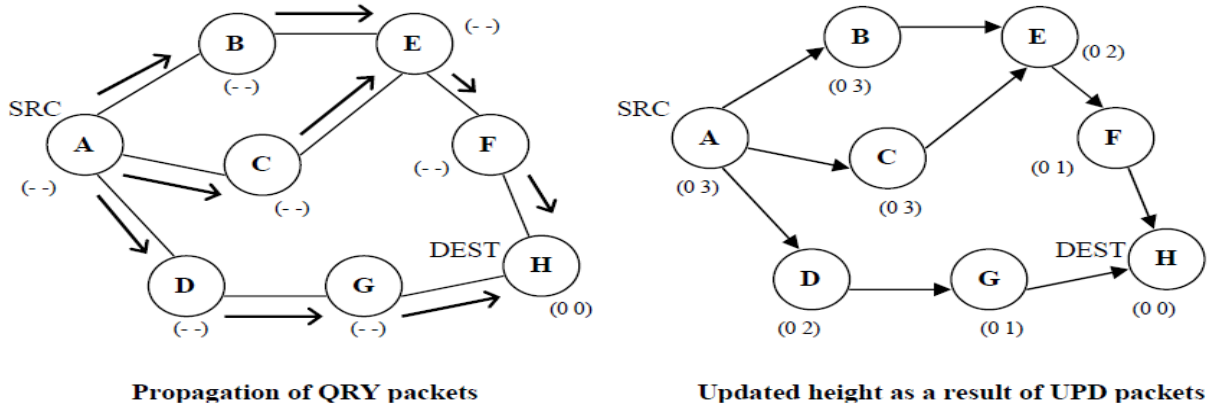


Figure 3.8.TORA: Propagation of QRY and Update of UPD packets

When a node moves, the DAG is broken and route maintenance is necessary to re-establish a DAG for the destination. When an upstream neighbor observes a link failure, it generates a new reference level. The neighboring nodes propagate the reference level and each node reverses its link to reflect the change in adapting to the new reference

level. Each link reversal message is time stamped and this mechanism provides a network partition detection capability to TORA. The route maintenance mechanism is illustrated below. (in figure 3.9).

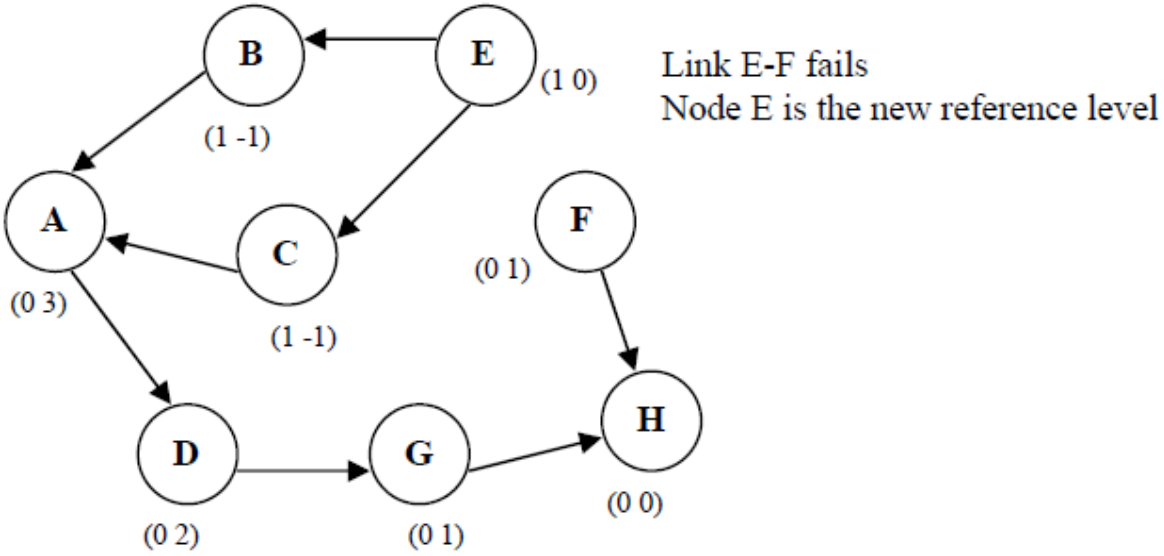


Figure 3.9 Route maintenance mechanism of TORA

In the route erasure phase, TORA floods a broadcast CLR packet throughout the network to erase invalid routes. TORA assumes that all the nodes have synchronized clocks and cannot function properly if the timing is unreliable. In addition, it suffers from temporary instability problems similar to the “count to infinity” problem in distance vector routing protocols.

Tables 3.2 and 3.3 outline the basic characteristics and complexity of the three routing protocols discussed in this section.

Table3.2. Basic Characteristics of DSR, AODV and TORA [40]

Protocol	**Multiple Routes**	**Route Metric Method**	**Route Maintained In**	**Route Reconfiguration Strategy**
DSR	Yes	Shortest Path or next path available	Route Cache	Erase Route then Source Notification.
AODV	No	Freshest and Shortest Path	Route Table	Erase Route then Source Notification or Local Route repair
TORA	Yes	Shortest Path or next path available	Route Table	Link reversal and Route repair

Table3.3. Complexity Comparison of DSR, AODV and TORA [40].

Protocol	**Time Complexity for Route Discovery**	**Time Complexity for Route Maintenance**	**Advantage**	**Disadvantage**
DSR	O(2*Diameter of Network)	O(2*Diameter of Network)	Multiple Routes, Promiscuous overhearing	Scalability problem due to source routing and flooding.
AODV	O(2*Diameter of Network)	O(2*Diameter of Network)	Adaptable to highly dynamic topologies.	Scalability Problems and large Delays.
TORA	O(2*Diameter of Network)	O(2*Diameter of Network)	Multiple routes	Temporary routing loops.

Chapter 4

PROBLEM STATEMENT & OBJECTIVE

4.1. Problem Statement

Mobile ad hoc networks (MANETs) are rapidly evolving as an important area of wireless mobility. MANETs are infrastructure less and wireless in which there are several routers which are free to move arbitrarily and perform management of routes. Network topology changes very rapidly and unpredictably in which many mobile nodes moves to and from a wireless network without any fixed access point where routers and hosts move, so topology is dynamic. Most current Mobile Ad hoc routing protocols assume that the wireless network in benign and every node in the network strictly follow the routing behavior and is willing to forward packets to other nodes. Most of these protocols cope well with the dynamically changing topology. However, they do not address the problems when misbehavior nodes are present in the network.

A commonly observed misbehaviour is packet dropping. Practically, in a MANETs, most devices have limited computing and battery power while packet forwarding consumes a lot of such resources. The design of routing protocols for MANETs must consider the power and resource limitation of the network nodes, the time varying quality of wireless channels and possibility of packet loss and delay. To address these design requirements several design strategies for MANETs have been proposed. AODV, DSR and TORA are some of the common protocols. Each one having it's fair share of advantages and limitations. Routing protocols use several metrics to calculate the best path for routing the packets to its destination. The process of path determination is that, routing algorithms initialize and maintain routing tables, which contain the total route information for the packet. This route information varies from one routing algorithm to another.

These protocols are also called reactive protocols since they 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. The route discovery usually occurs by flooding the route request packets throughout the network

AODV expects/requires that the nodes in the broadcast medium can detect each other's broadcasts. AODV is a reactive routing protocol. This means that AODV does not discover a route until a flow is initiated. This route discovery latency result can be high in large-scale mesh networks.

4.2. Objective and Sub-tasks

Routing in these networks is highly complex due to moving nodes and hence many protocols have been developed. This Master thesis concentrate mainly on routing protocols and their functionality in Ad-hoc networks with a discussion being made on three selected protocols AODV,DSR and TORA, ending with their comparison.

- To analyze the three protocols - AODV, DSR and TORA.
- To simulate the three protocols - AODV, DSR and TORA in a simulation environment.
- To evaluate the three protocols - AODV, DSR and TORA in a simulation environment.

Chapter 5

INSTALLATION, SIMULATION & DESIGN

5.1. Fedora Core

The Fedora Project builds open source software communities and produces a Linux distribution called "Fedora." The Fedora Core [33] Project's mission is to lead the advancement of free and open source software and content as a collaborative community, is a flavor of Linux. Red Hat being developed by the open source community and the Red Hat engineers sponsor the development of Fedora. Fedora Core 10(FC10) and FC11 are the release of the Fedora Project. Some primary features of FC10 are extensive performance improvements, support for Intel-based Macs and a new Graphical User Interface (GUI) virtualization manager. Basic simple architecture of Linux shown bellow.(in figure 5.1)

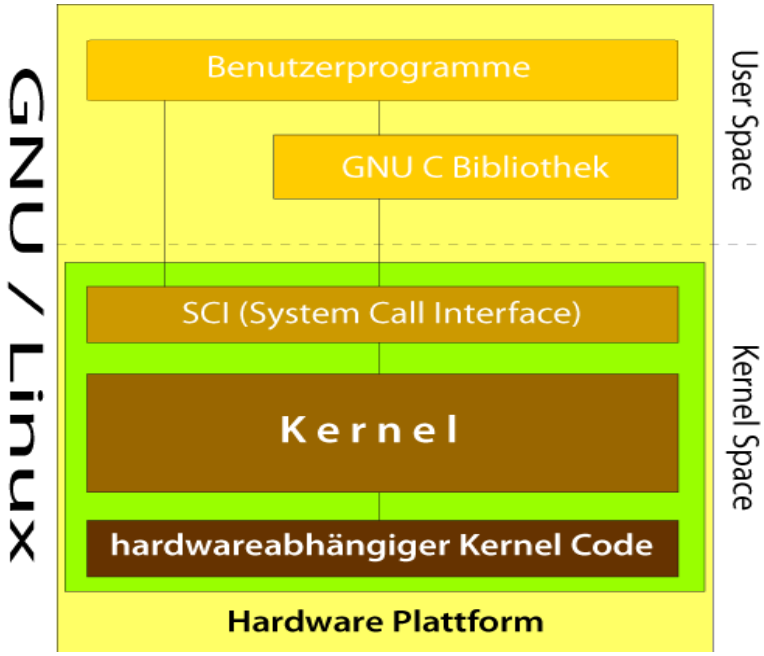


Figure5.1 Decomposition of Linux System into Major Subsystems

5.2. The Network Simulator (ns-2)[34]

Simulation can be defined as “Imitating or estimating how events might occur in a real situation”. It can involve complex mathematical modeling, role playing without the aid of

technology, or combinations. The value lies in the pacing you under realistic conditions that change as a result of behaviour of others involved, so you cannot anticipate the sequence of events or the final outcome.

5.2.1. Software structure and mechanism of ns-2

The key to get to know ns-2 is it is a discrete event network simulator. In ns-2 network physical activities are translated to events, events are queued and processed in the order of their scheduled occurrences. And the simulation time progresses with the events processed. And also the simulation "time" may not be the real life time as we "inputted".

But, why is ns-2 that useful, what kind of work can be done by ns-2, it can model essential network components, traffic models and applications. Typically, it can configure transport layer protocols, routing protocols, interface queues, and also link layer mechanisms. We can easily see that this software tool in fact could provide us a whole view of the network construction, meanwhile, it also maintain the flexibility for us to decide. Thus, just this one software can help us simulate nearly all parts of the network [34-39]. This definitely will save us great amount of cost invested on net work constructing. The following Figure 5.2 shows a layered structure which ns-2 can simulate for us.

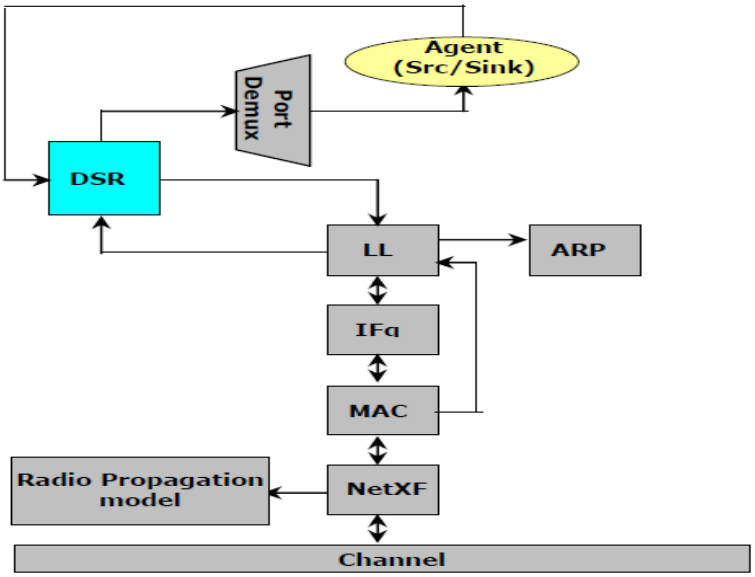


Figure 5.2 ns-2 simulate layered structure of network

After the simulation finish, the way ns-2 used to present the most details information on that much network layer is that it provides us a huge trace file recording all the events line by line in it. So, now we see why event driven mechanism is used in ns-2, since it really could maintain the things ever happened as records. And we can trace these records to evaluate the performance of special stuffs in our network, such as routing protocol, Mac layer load, and so on.

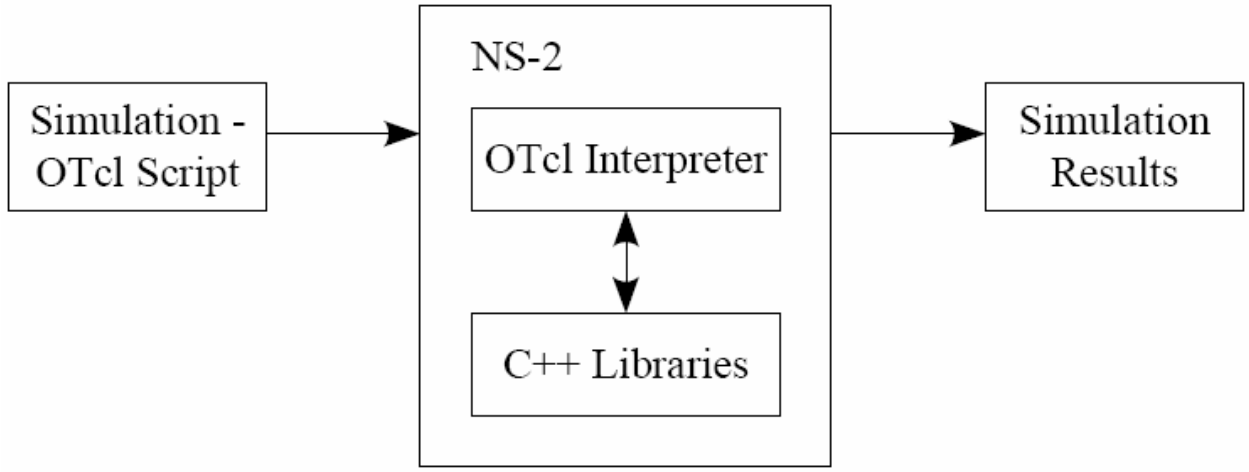


Figure 5.3 data flow for one time simulation

As Figure 5.3 shows, for the data flow of one time simulation in ns-2, the user input an OTcl source file, the OTcl script do the work of initiates an event scheduler, sets up the network topology using the network objects and the plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through the event scheduler. And then, this OTcl script file will be passed to ns-2, in this view, we can treat ns-2 as Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries, and network setup module libraries. And then the detail network construction and traffic simulation will be actually done in ns-2. After a simulation is finished, NS produces one or more text-based output files that contain detailed simulation data, and the data can be used for simulation analysis [37, 39].

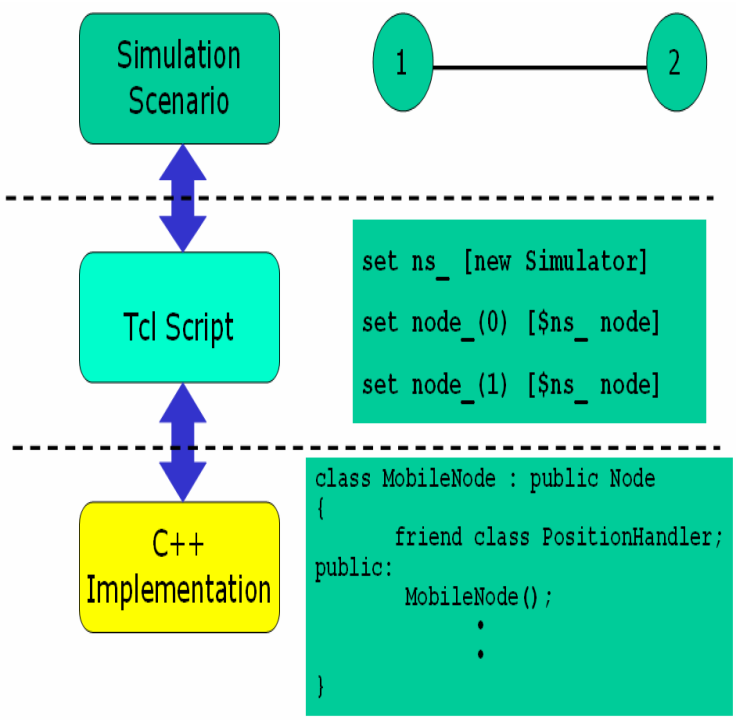


Figure 5.4 Layered structure from the ns-2 developer view [39]

From the ns-2 developer view, Figure 5.4 shows the layered architecture of ns. The event schedulers and most of the network components are implemented in C++ and available to Tcl Script, thus the lowest level of ns-2 is implemented by C++, and the Tcl script level is on top of it to make simulation stuffs much easier to be conducted. Then, upon the Tcl level, we see the overview of the network. That is the simulation scenario. These all things combined as so called ns-2 software.

5.2.2. Parts needed by one simulation in ns-2

To successfully carry out one simulation, we must first tell ns-2 things it may need from us for one simulation. Following three necessary items are necessary:

1) Appearance of the network: the whole topology view of sensor network or mobile network, this includes the position of nodes with (x, y, z) coordinate, the node movement parameters, the movement starting time, the movement is to what direction, and the node movement speed with pausing time between two supposed movement.

2) Internal of the network: Since the simulation is on the network traffic, so it is important we tel the ns2 about which nodes are the sources, how about the connections, what kind of connection we want to use.

3) Configuration of the layered structure of each node in the network, this includes the detail configuration of network components on sensor node, and also we need to drive the simulation, so we need to give out where to give out the simulation results which is the trace file, and how to organize a simulation process.

5.2.3. Writing tcl to run simple wireless simulations

In this section, we then will present step by step of how to do all the things as needed by one simulation in ns-2 with one tcl scripts sequence [34-39]:

Step 1. Create an instance of the simulator:

set ns_ [new Simulator]

Step.2. Setup trace support by opening file ”trace_bbtr.tr” and call the procedure trace-all

set tracefd [open trace_bbtr.tr w]

$ns_ trace-all $tracefd

Step 3. Create a topology object that keeps track # of all the nodes within boundary

set topo [new Topography]

Step 4. The topography is broken up into grids and the default value of grid resolution is 1. A different value can be passed as a third parameter to load_flatgrid {}.

$topo load_flatgrid $val(x) $val(y)

Step 5. Create the object God, "God (General Operations Director) is the object that is used to store global information about the state of the environment, network or nodes. The procedure create-god is defined in $NS2_HOME/tcl/mobility/com.tcl, which allows only a single global instance of the God object to be created during a simulation. God object is called internally by MAC objects in nodes, so we must create god in every cases.

set god_ [create-god $val(nn)]

Step 6. Before we can create node, we first needs to configure them. Node configuration API may consist of defining the type of addressing (flat/hierarchical etc), for example, the type of adhoc routing protocol, Link Layer, MAC layer, IfQ etc.

```
$ns_ node-config -adhocRouting $val(rp) \
-llType $val(ll) \
-macType $val(mac) \
-ifqType $val(ifq) \
-ifqLen $val(ifqlen) \
-antType $val(ant) \
-propType $val(prop) \
-phyType $val(netif) \
-channe
-channel [new $val(chan)] \
-topoInstance $topo \
-agentTrace ON \
-routerTrace ON \
-macTrace OFF \
-movementTrace OFF
```

Step 7. Create nodes and the random-motion for nodes is disabled here, as we are going to provide node position and movement (speed & direction) directives next

```
for {set i 0} {$i < $val(nn) } {incr i} {
set node_($i) [$ns_ node]
$node_($i) random-motion 0
# Disable random motion
}
```

Step 8. Give nodes positions to start with, Provide initial (X,Y, for now Z=0) co-ordinates for node_(0) and node_(1). Node0 has a starting position of (5,2) while Node1 starts off at location (390,385).

```
$node_(0) set X_ 5.0
$node_(0) set Y_ 2.0
```

$node_(0) set Z_ 0.0

$node_(1) set X_ 390.0

$node_(1) set Y_ 385.0

$node_(1) set Z_ 0.0

Step 9. Setup node movement as the following example, at time 50.0s, node 1 starts to move towards the destination (x=25, y=20) at a speed of 15m/s. This API is used to change direction and speed of movement of nodes.

$ns_ at 50.0 "$node_(1) setdest 25.0 20.0 15.0"

Step 10. Setup traffic flow between the two nodes as follows: TCP connections between node_(0) and node_(1)

set tcp [new Agent/TCP]

$tcp set class_ 2

set sink [new Agent/TCPSink]

$ns_ attach-agent $node_(0) $tcp

$ns_ attach-agent $node_(1) $sink

$ns_ connect $tcp $sink

set ftp [new Application/FTP]

$ftp attach-agent $tcp

$ns_ at 10.0 "$ftp start"

Step 11. Define stop time when the simulation ends and tell nodes to reset which actually resets their internal network components. In the following case, at time 150.0s, the simulation shall stop. The nodes are reset at that time and the "$ns_ halt" is called at 150.0002s, a little later after resetting the nodes. The procedure stop{} is called to flush out traces and close the trace file.

for {set i 0} {$i < $val(nn) } {incr i} {

$ns_ at 150.0 "$node_($i) reset";

}

$ns_ at 150.0001 "stop"

$ns_ at 150.0002 "puts \"NS EXITING...\" ; $ns_ halt"

proc stop {} {

global ns_ tracefd nf

$ns_ flush-trace

close $tracefd

close $nf }

Step 12. Finally the command to start the simulation

puts "Starting Simulation...\n" $ns_ run

So, these 12 steps could finish one time simulation, and we can pack these 12 steps into one tcl file and do the simulation. However, there exist some problems on such kind of use on typical network performance test situations. Performance testing usually needs to be scalable in the number of nodes and network transmitting packets. Suppose for one network there are hundreds of nodes, we need to set all of the nodes' positions and their movement, this a huge amount of workload, also, suppose we need to setup all the possible sources and destinations and even connections, also is a huge workload, Furthermore, even if we can set them, we cannot guarantee our input is randomly select, which is necessary for a fair comparison.

5.2.4. Tool Command Language (tcl)

Short for Tool Command Language, tcl [39] 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.

5.2.5. The Network Animation (nam)[39]

The network animator began in 1990 as a simple tool for animating packet trace data. his trace data is typically derived as output from a network simulator like ns or from real network measurements, e.g., using tcpdump. Steven McCanne wrote the original version as a member of the Network Research Group at the Lawrence Berkeley National

Laboratory, and has occasionally improved the design, as he's needed it in his research. Marylou Orayani improved it further and used it for her Master's research over summer 1995 and into spring 1996. The nam development effort was an ongoing collaboration with the VINT project.

5.2.6. The Trace File

The trace file is an ASCII code files and the trace is organized in 12 fields as in Figure 5.5. shown below.

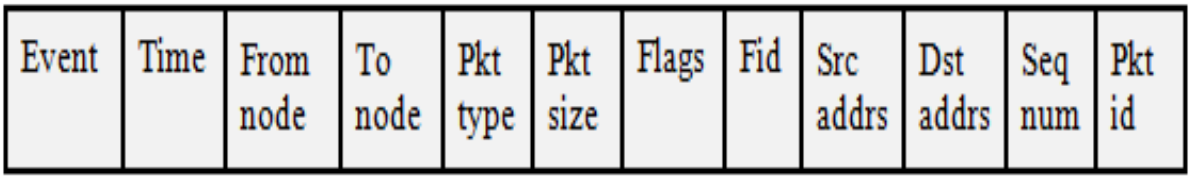


Figure.5.5. Fields of Trace File

The first field is the event type and given by one of four available symbols r, +, - and d which correspond respectively to receive, enqueued, dequequed and dropped. The second field is telling the time which the event occurs. The third and fourth fields are the input and output node of the link at which the events takes place. The fifth is the packet type such as continuous bit rate (cbr) or transmission control protocol (tcp). The sixth is the size of the packet and the next field is some kind of flags. The eighth field is the flow identity of IPv6, which can specify stream color of the NAM display and can be use for further analyze purposes. The ninth and tenth fields are the source and destination address in the form of "node.port". The eleventh is the network layer protocol's packet sequence number. ns-2 keeps track of UDP packet sequence number for the analysis purposes. The twelfth, which is 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.

5.2.7. The Tracegraph

It is a data presentation system for Network Simulator ns-2. The simulator doesn't have any options implemented to analyze simulations results so it's hard to use it. Trace graph [40] system provides many options for analysis, including 250 graphs and statistical

reports. It is implemented in MATLAB 6.0 and can be compiled to run without MATLAB. Compiled versions for Linux and Windows systems are available for download at http://www.geocities.com/tracegraph/. Trace graph supports the following ns-2 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.

5.3. Simulation of Routing Protocols

For this thesis, we create a square flat platform of finite dimensions for simulation. Various parameters are kept permanent while others are varied to help us analyze the performance of the three protocols. The simulation is done in the random waypoint model in a rectangular field. The field configurations used is: 1000 m x 1000 m field with 15 nodes and 25 nodes. Here, each packet starts its journey from a random location to a random destination with a randomly chosen speed (uniformly distributed between 0–20 m/s). Once the destination is reached, another random destination is targeted after a pause. The pause time, which affects the relative speeds of the mobiles, is varied. Simulations are run for 150simulated seconds. Identical mobility and traffic scenarios are used across protocols to gather fair results. Various parameters that are considered for simulation are listed in table 5.1.

Table 5.1 Network Simulation Parameters

Parameter Name	**AODV**	**DSR**	**TORA**
channel type	Channel/Wireless Channel	Channel/Wireless Channel	Channel/Wireless Channel
netif	Phy/WirelessPhy	Phy/WirelessPhy	Phy/WirelessPhy/802_15_4
mac protocol	Mac/802_11	Mac/802_11	Mac/802_15_4
ifq	Queue/DropTail/PriQueue	CMUPriQueue	Queue/DropTail/PriQueue
ifqlen	50	50	50
number of nodes	15 and 20	15 and 20	15 and 20
routing protocol	AODV	DSR	TORA
grid size	1000×1000	1000×1000	1000×1000
Data payload	Bytes/packet	Bytes/packet	Bytes/packet
simulation time	150	150	150
Topology	Random	Random	Random
Traffic type	CBR(UDP)	CBR(UDP)	CBR(UDP)
Source Node	12	12	12
Destination node	4	4	4

5.4 Performance Metrics

This work was focus on 3 performance metrics which are quantitatively measured. The performance metrics are important to measure the performance and activities that are running in ns-2 simulation. The performance metrics are:

Packet Delivery Ratio: The ratio of the data packets delivered to the destinations to those generated by the CBR sources. The PDR shows how successful a protocol performs delivering packets from source to destination. The higher for the value give use the better results. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness.

$$\textbf{Packet delivery ratio} = \frac{\sum \textbf{CBR packets received by CBR sinks}}{\sum \textbf{CBR packets sent by CBR sources}}$$

Packets Lost: It is a measure of the number of packets dropped by the routers due to various reasons. The reasons we have considered for evaluation are Collisions, time outs, looping, errors.

$$\textbf{Packet loss} = \sum \textbf{Data packets Drop}$$

Average end-to-end delay of data packets: There are possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times. The thesis use Average end-to-end delay. Average end-to-end delay is an average end-to-end delay of data packets. It also caused by queuing for transmission at the node and buffering data for detouring. Once the time difference between every CBR packet sent and received was recorded, dividing the total time difference over the total number of CBR packets received gave the average end-to-end delay for the received packets. This metric describes the packet delivery time: the lower the end-to-end delay the better the application performance.

$$\textbf{Average end-to-end delay} - \frac{\sum(\textbf{CBRsent Time} - \textbf{CBRecv Time}}{\sum \textbf{CBRrec}}$$

Chapter 6

RESULTS, PERFORMANCE EVALUATION &ANALYSIS

This section described simulation of thee routing protocols and the analysis is being done by using results of *.nam file and *.tr file of each protocol, comparison between the AODV, DSR and TORA routing protocol using the average end to end delay, packet loss and packet delivery fraction performance metrics [15]. The value of simulation in studies of protocols is that it allows near perfect experimental control: experiments can be designed at will and then rerun while varying an experimental variable and holding all other variables constant [19]. The nam is a built-in program in ns2-allinone package. It helps us to see the flow of packets between various nodes. With this, we are also able to know whether the packets have reached to their destination properly or dropped in between. NAM is invoked within the Tcl file. We are able to analyze the simulation of AODV, DSR and TORA with different number of nodes, with the help of 2D and 3D graphs. These graphs are generated with a program called tracegraph. The NAM scripts are stored in *.nam file and scripts for tracegraph are stored in *.tr file.

The simulation is divided in to two Scenarios (With 15nodes and 25 nodes) that have been created, basis on the number of nodes that vary, in each scenario the simulation is done in the following:

- Simulation of AODV routing protocol
- Simulation of DSR routing protocol
- Simulation of TORA routing protocol

6.1 Scenario 1:

In the first simulation scen_15node_1s_10mps_150sim_1000x1000 and cbr_15node_15con_3rate scenario files have been used as movement scenario and traffic scenario respectively. It can easily be inferred from the name of the scenario files, it have 15 mobile nodes with a 1 seconds of pause time and with a maximum speed of 10m/s in a

1000x1000 region. After the simulation and analyzing the trace files, it has been obtained the graphs as presented;

6.1.1. Simulation of AODV routing protocol: My aim here was to simulate AODV routing protocol for 15 nodes sending cbr packets with random speed. First the cbr files and scenario files are generated and then using AODV protocol simulation is done which gives the nam file and trace file.

The following figures are the execution of the nam files instances created. We can view the output on the network simulator. The figure 6.1, shows that the source is broadcasting its data to all its neighboring nodes. The source (node 12) is broadcasting RREQ message to all its neighbors and Node 4, which is the destination node, is sending RREP (route reply) back to the source. RREP in red color has been shown in figure 6.2. As the energy of the nodes decreases, packet dropping starts. Packet dropping has been shown with the 3D graph. As the packet dropping starts, again broadcast will happen and different route will be followed.

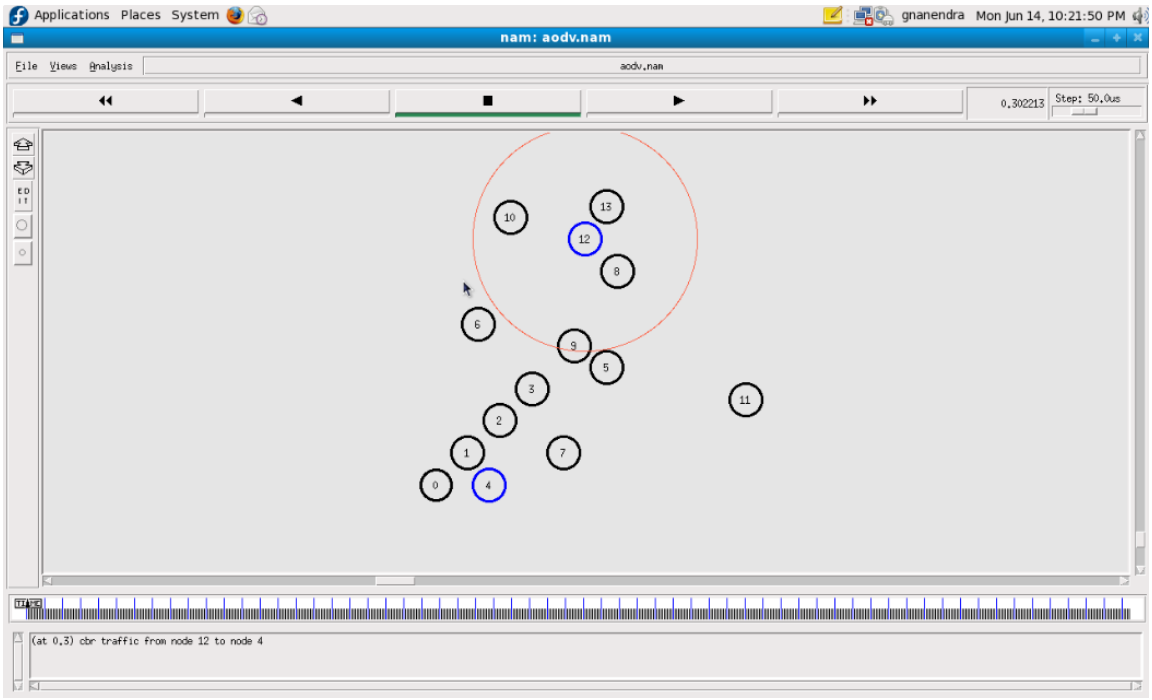


Figure.6.1 AODV (Random Topology): Source Node broadcasts RREQ

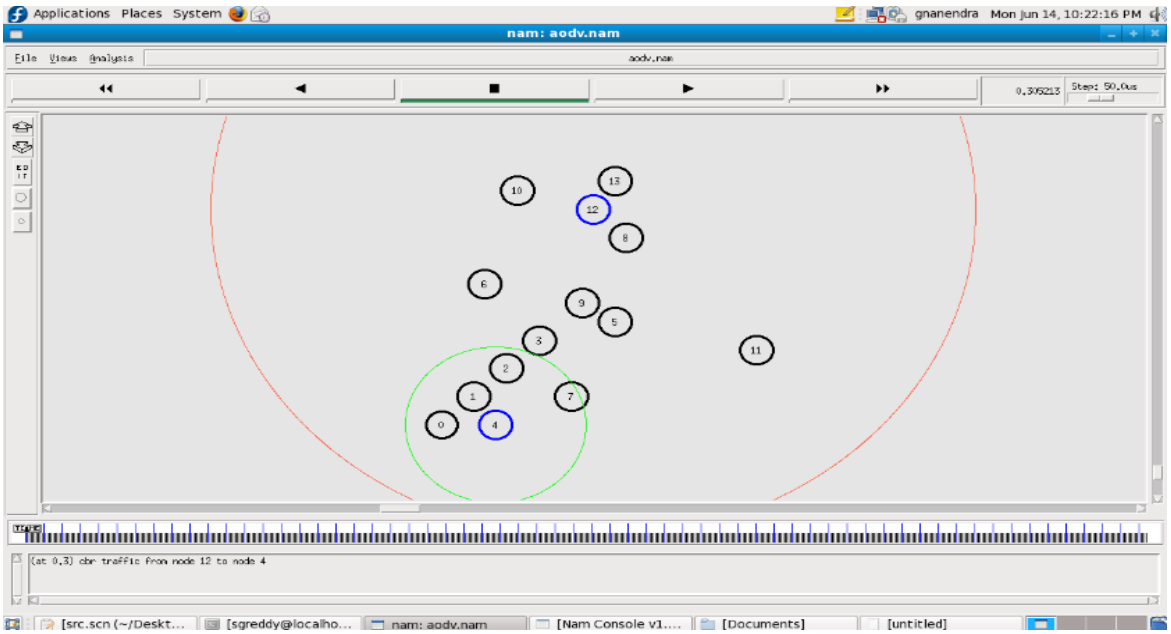


Figure.6.2 AODV: Destination Node sends back RREP

The tracegraph snapshots have been taken with the simulation time of 150 seconds. In figure 6.3, the entire simulation scenario has been displayed along with the end-to-end delay. The throughput of sending and receiving protocols has been displayed in figure 6.4 and 6.5.

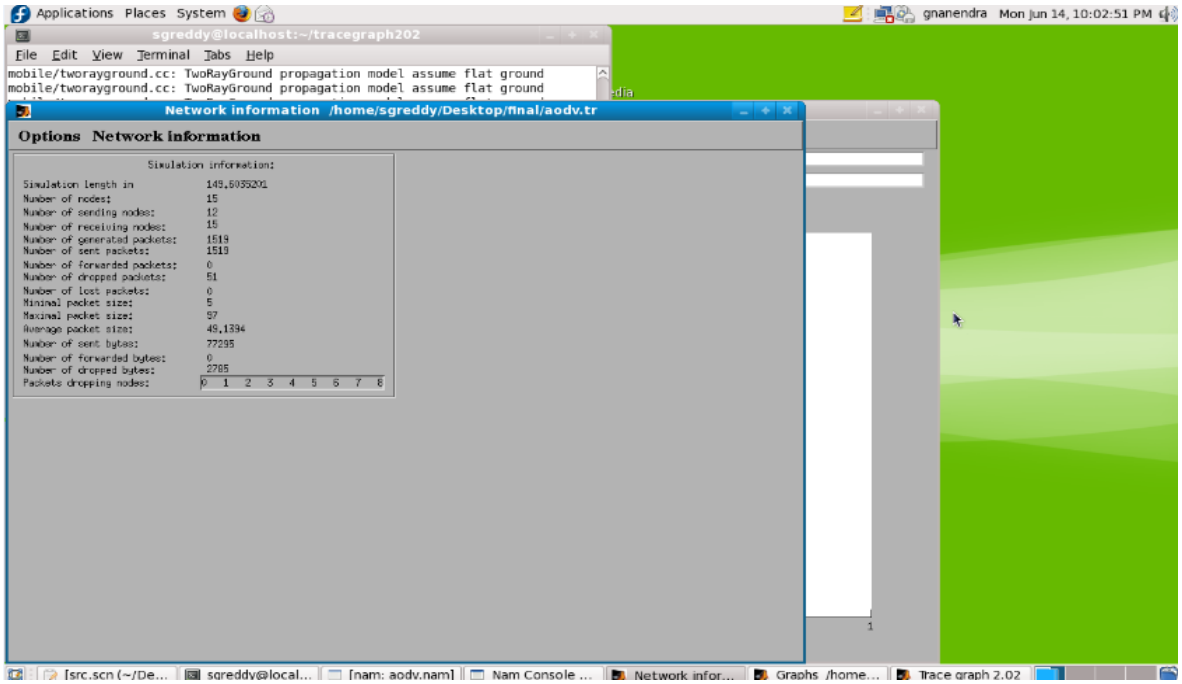


Figure 6.3 AODV (Random Topology): Simulation Details

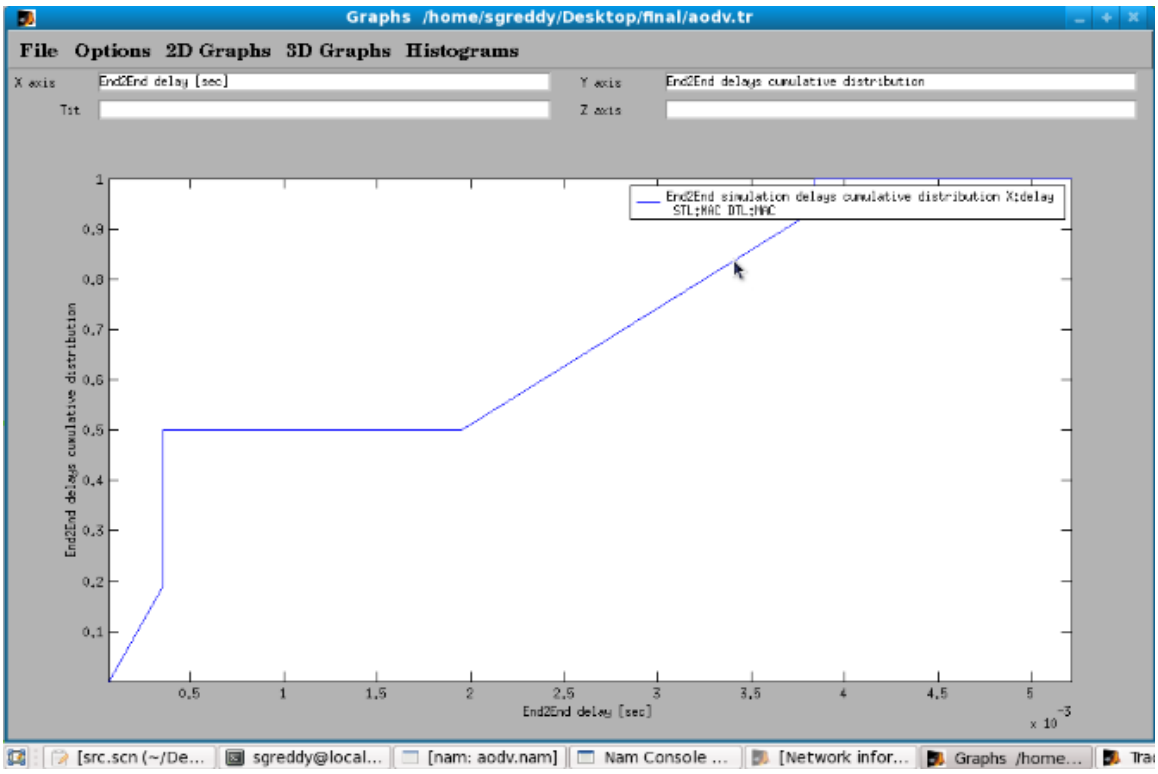


Figure6.4. AODV (Random Topology): End-to-end Simulation Delay Cumulative Distribution

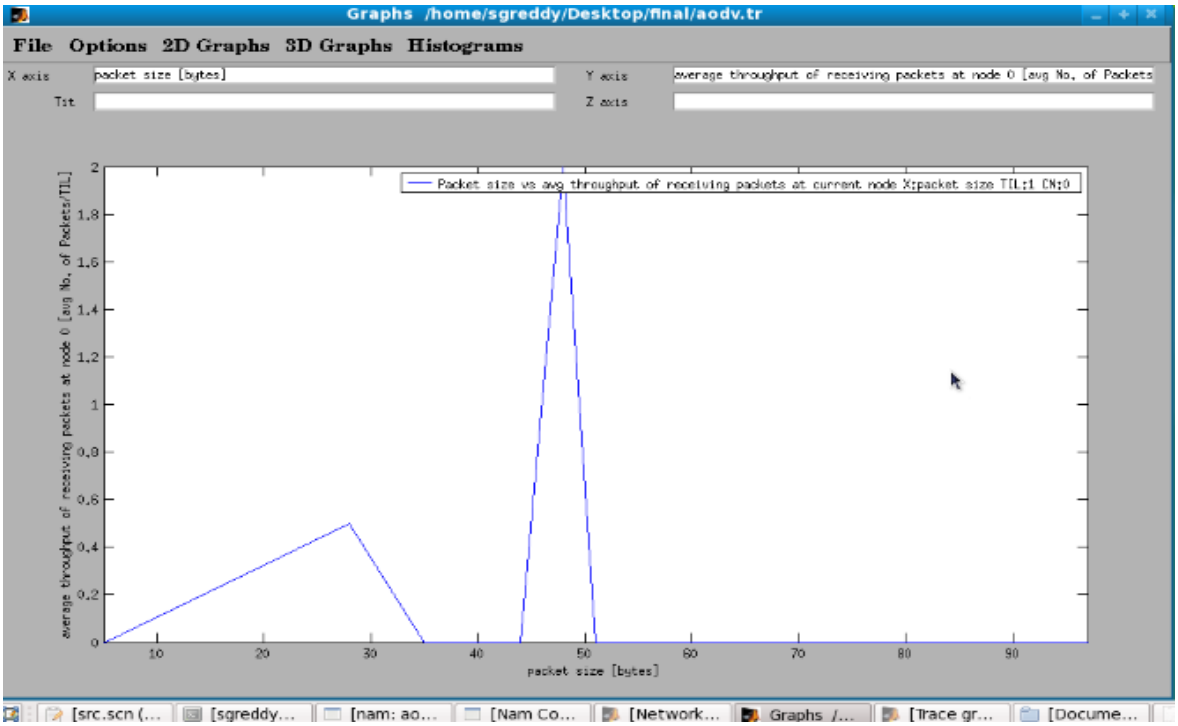


Figure6.5 (AODV): Average throughput of receiving packet at node verses packet size (bytes)

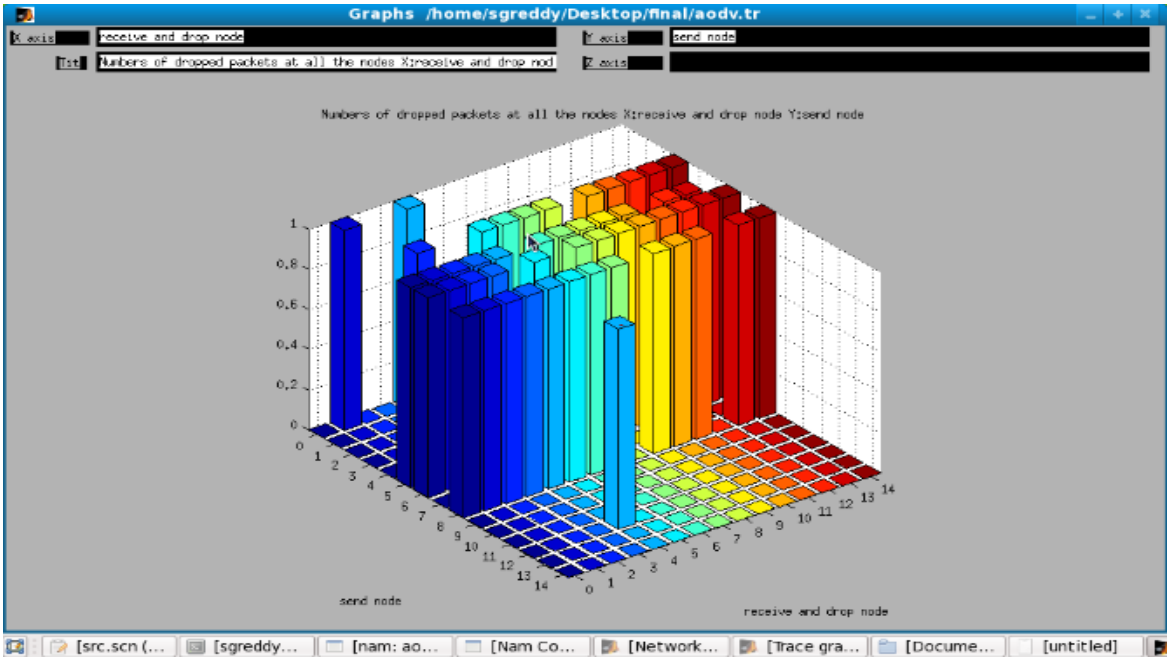


Figure.6.6. AODV (Random Topology): Dropped Packets

6.1.2. Simulation of DSR routing protocol: The simulation of DSR routing protocol for 15 nodes sending cbr packets with random speed. First the cbr files and scenario files are generated and then using DSR protocol simulation is done which gives the nam file and trace file. [2]. The following figures are the execution of the nam files instances created. We can view the output on the network simulator and the analysis is being done by using results of *.tr file of protocol with the 2D and 3D graphs which were created by using tracegraph. as shown below:

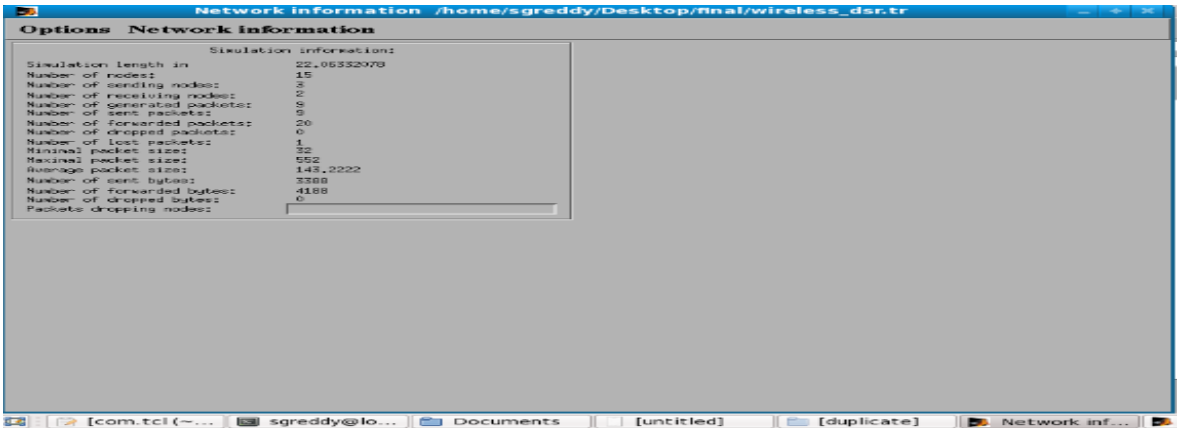


Figure.6.7. DSR (Random Topology): Simulation Details

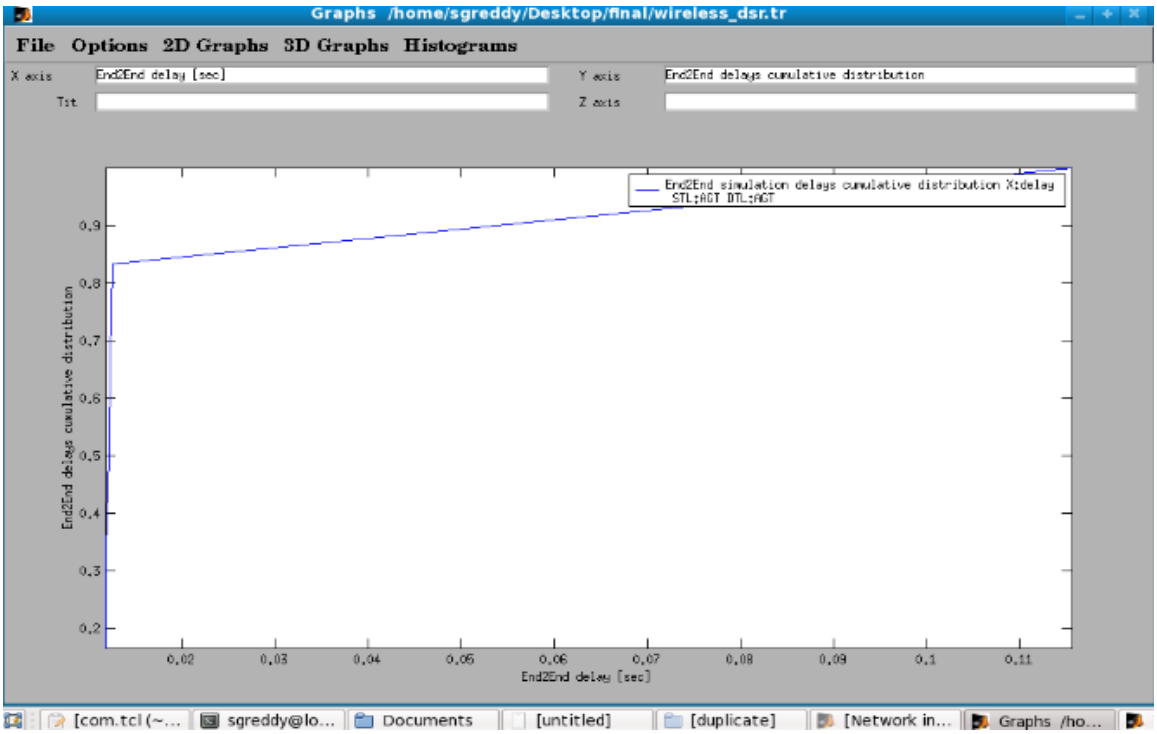


Figure.6.8. DSR (Random Topology): End-to-end Simulation Delay Cumulative Distribution

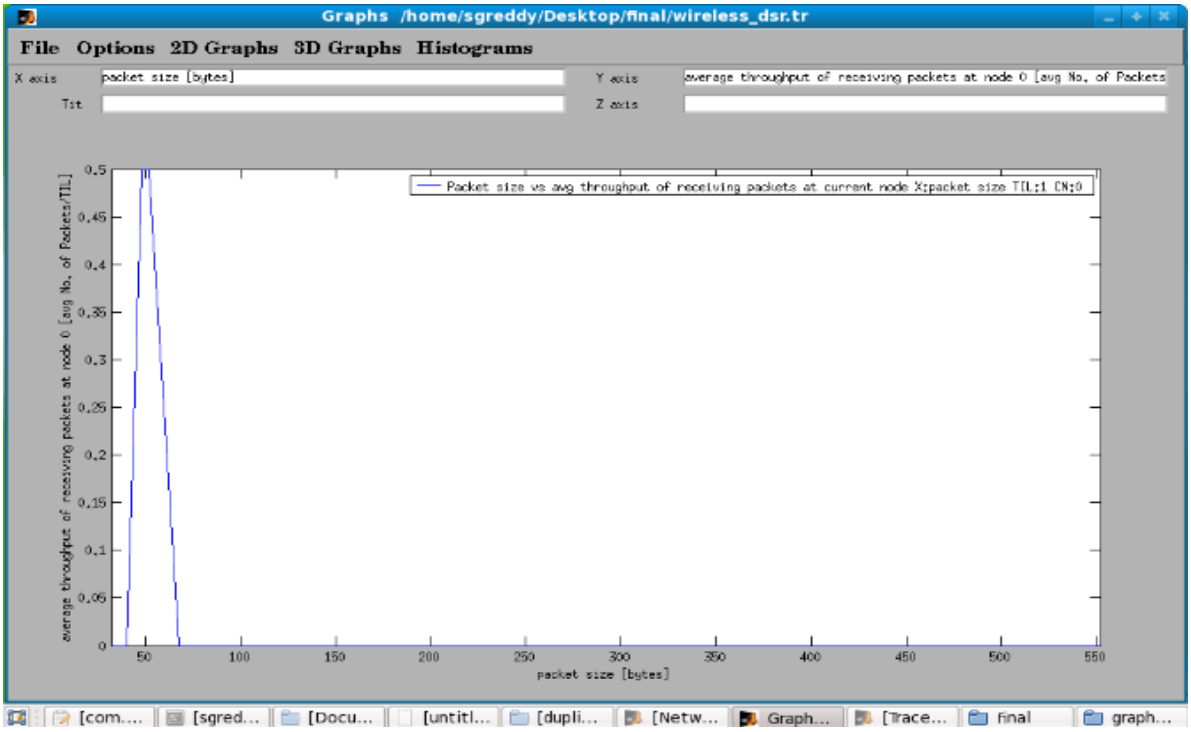


Figure.6.9. (DSR): Average throughput of receiving packet at node verses packet size(bytes)

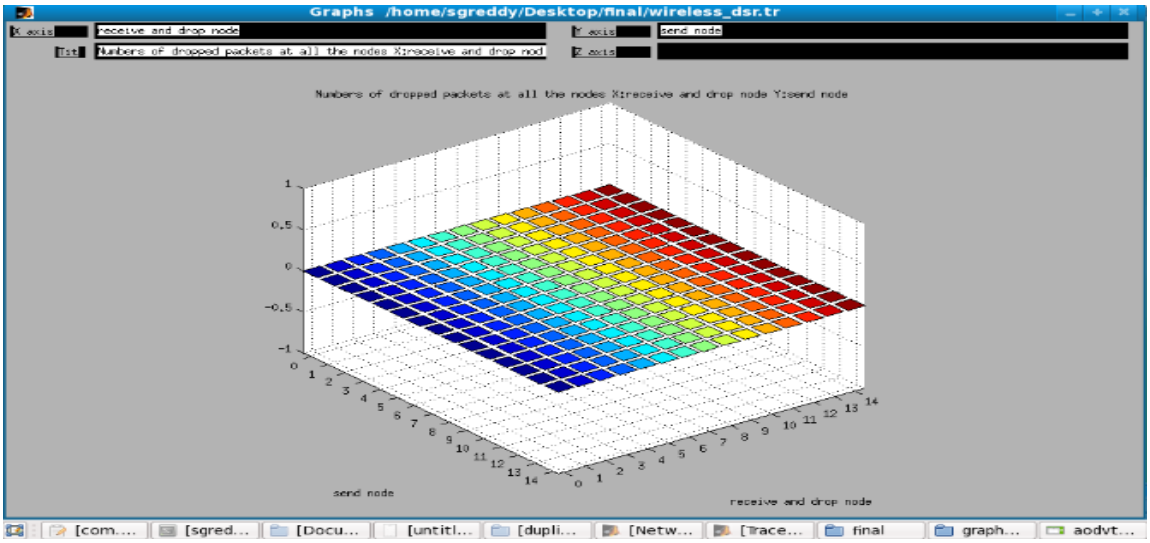


Figure.6.10. DSR (Random Topology): Dropped Packets

6.1.3. Simulation of TORA routing protocol: The simulation of TORA routing protocol for 15 nodes sending cbr packets with random speed. First the cbr files and scenario files are generated and then using TORA protocol simulation is done which gives the nam file and trace file. [2]. The following figures are the execution of the nam files instances created. We can view the output on the network simulator and the analysis is being done by using results of *.tr file of protocol with the 2D and 3D graphs which were created by using tracegraph. as shown below:

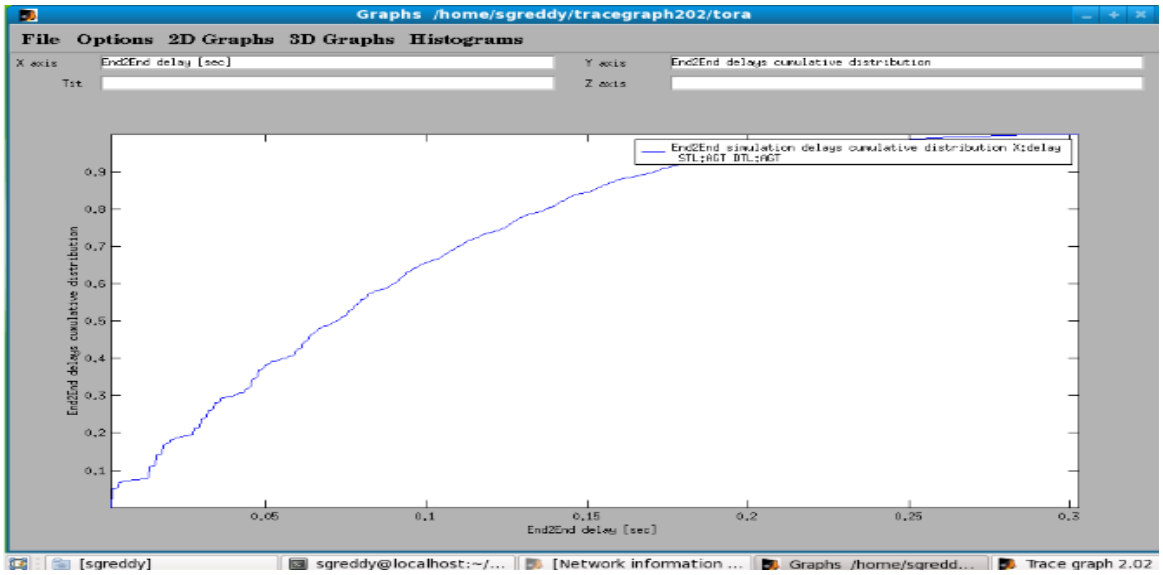


Figure.6.11. TORA (Random Topology): End-to-end Simulation Delay Cumulative Distribution

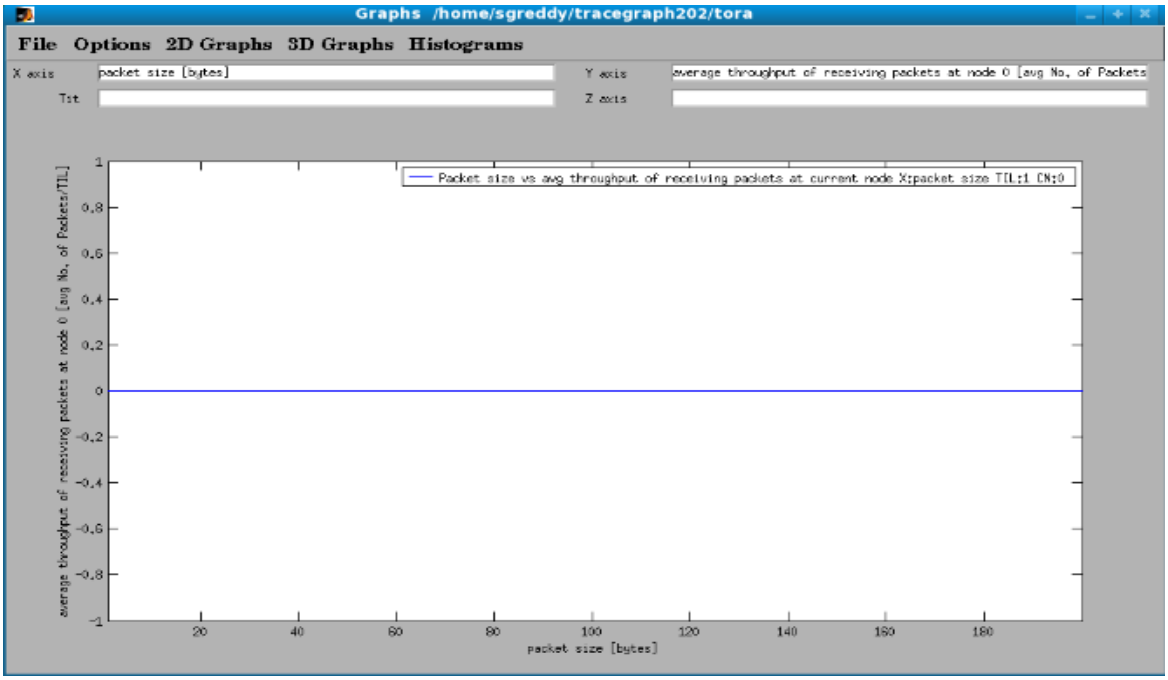


Figure.6.12 (TORA): Average throughput of receiving packet at node verses packet size(bytes)

Table 6.1 Outputs of the Simulation under Scenario 1

Metrics	**AODV**	**DSR**	**TORA**
No of Packets Received	104480	17864	16684
No of Packets Drop	203600	58698	38657
Packet Delivery Ratio	50.431	50.73	50.62

6.2. Scenario 2:

In the second simulation scen_20node_1s_10mps_150sim_1000x1000 and cbr_20node_20con_3rate scenario files have been used as movement scenario and traffic scenario respectively. This simulation may enable us to see what would be the performances of the protocols when the number of nodes increased. After the simulation and analyzing the trace files, we have obtained the graphs from which we concluded that; the performances of the protocols are approximately similar with the first simulation

performances. Again DSR protocol is extremely reliable when look at throughput and packet delivery fraction.

6.2.1. Simulation of AODV routing protocol: The following figures are the execution of the nam files instances created. We can view the output on the network simulator with 20 nodes of AODV routing protocol and also analyzing the trace files, we have obtained the graphs from which we concluded that; the performance of the AODV routing protocol.

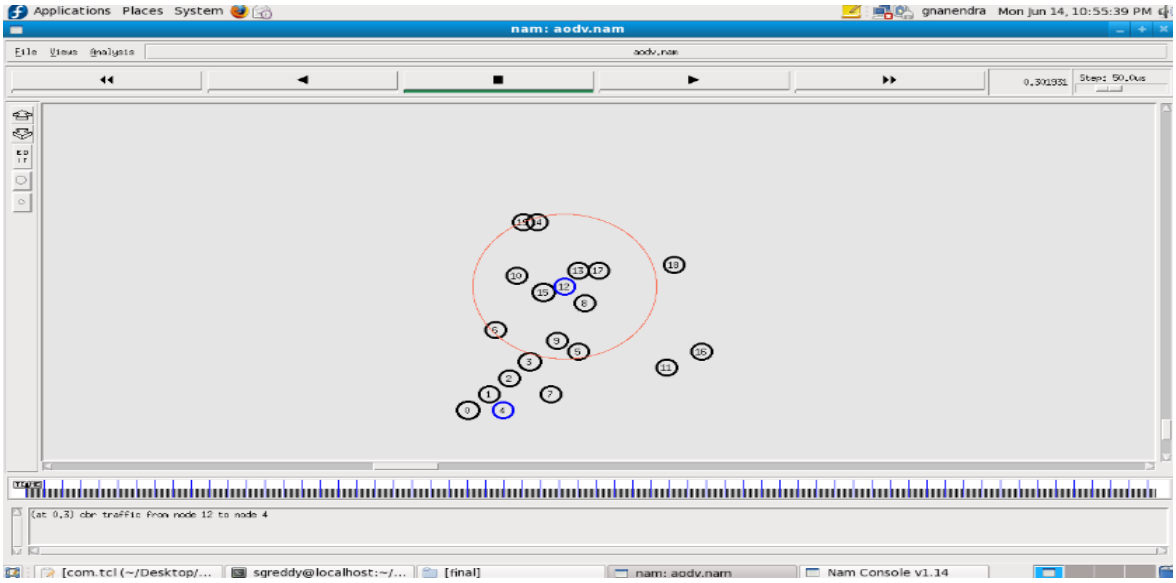


Figure.6.13. AODV (Random Topology): Simulation Environment (NAM)

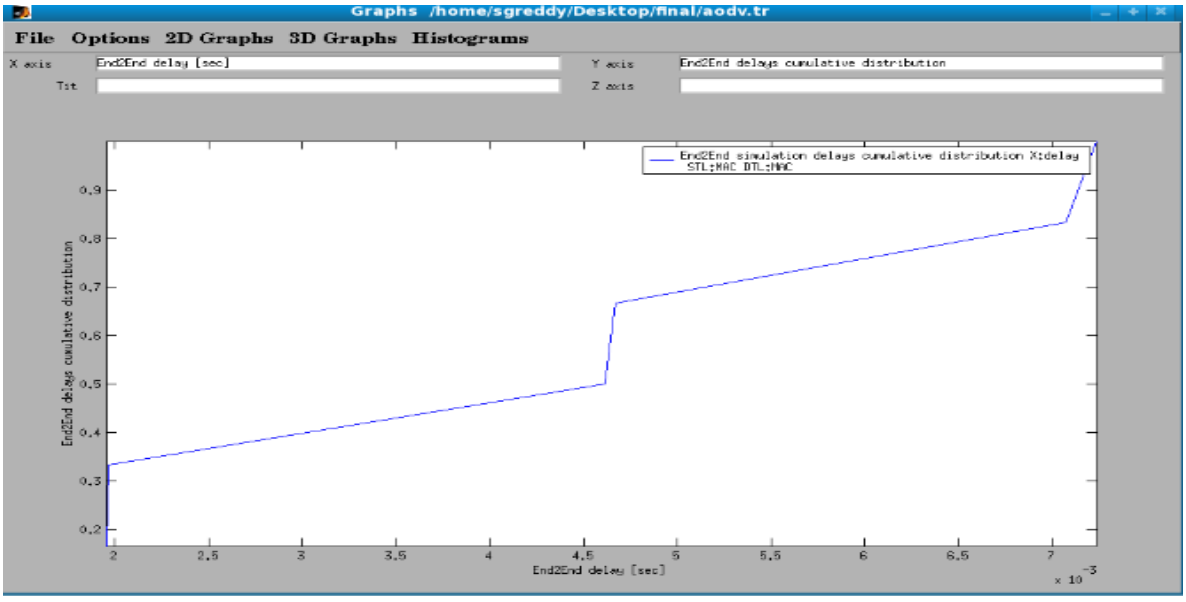


Figure.6.14. AODV (Random Topology): End-to-end Simulation Delay Cumulative Distribution

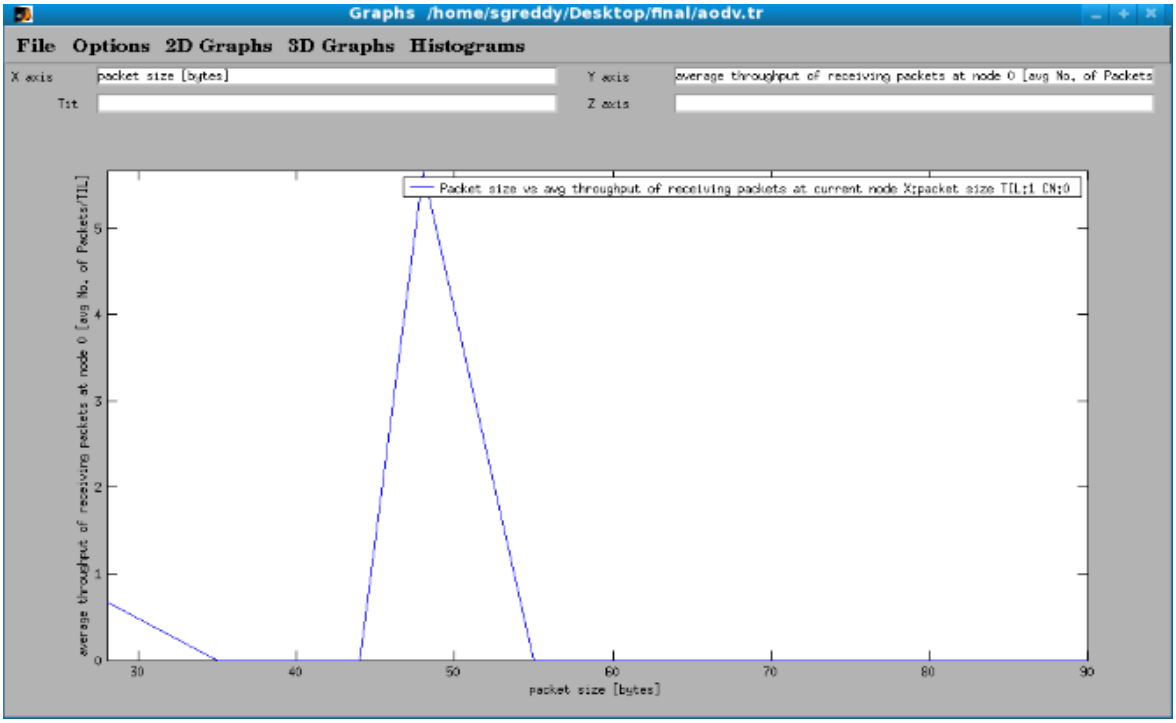


Figure.6.15 (AODV): Average throughput of receiving packet at node verses packet size (bytes)

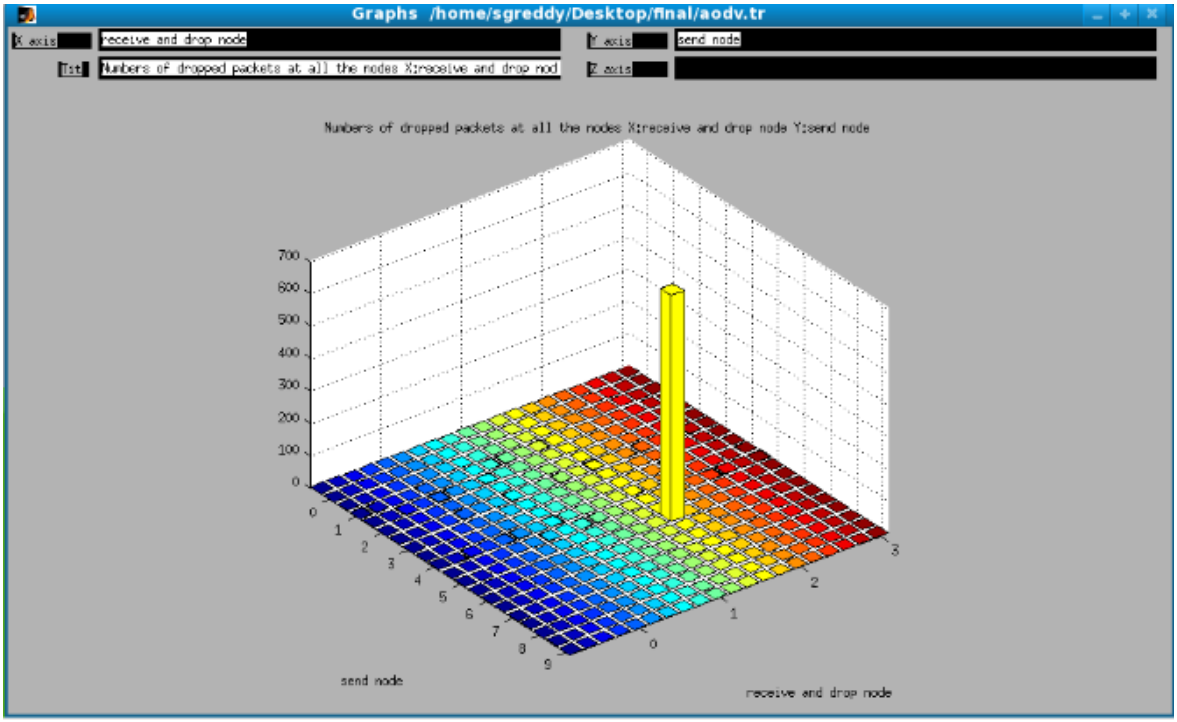


Figure.6.16. AODV (Random Topology): Dropped Packets

6.2.2. Simulation of DSR routing protocol:

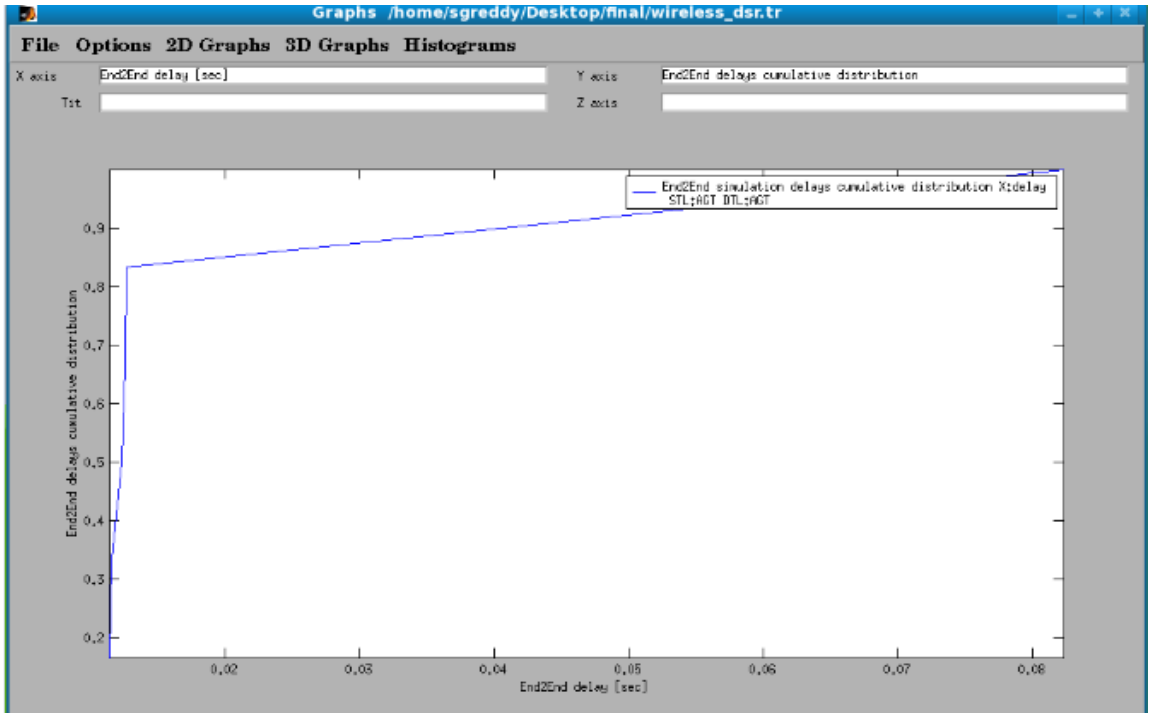


Figure.6.17. DSR (Random Topology): End-to-end Simulation Delay Cumulative Distribution

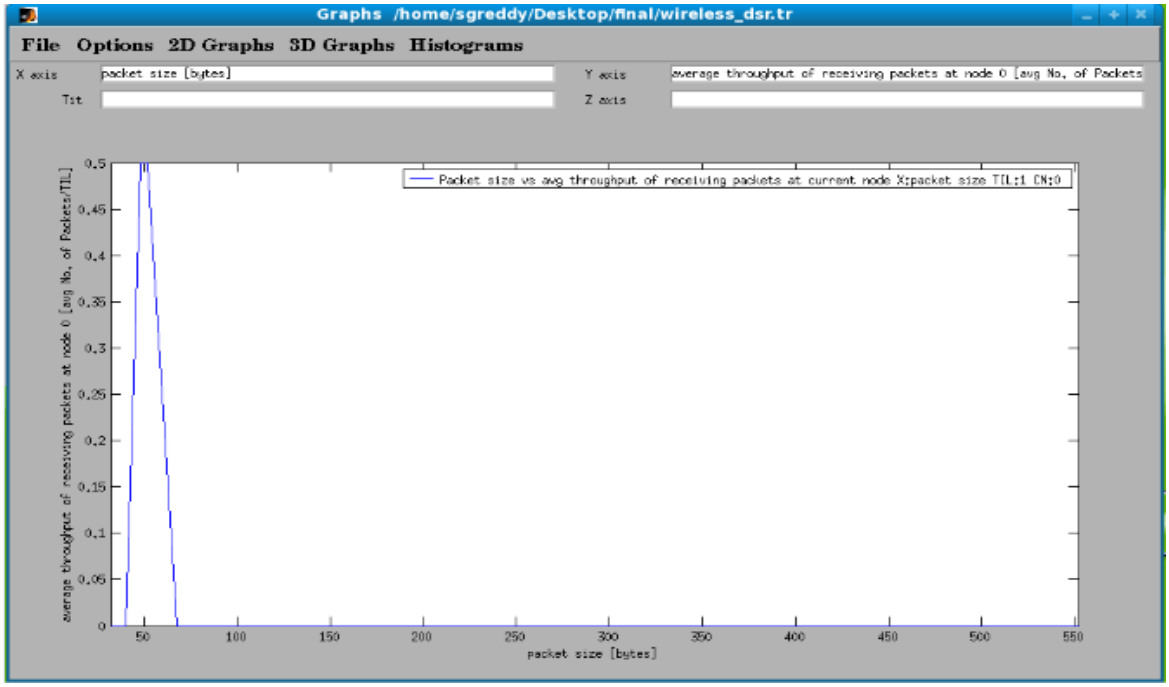


Figure.6.18 (DSR): Average throughput of receiving packet at node verses packet size (bytes)

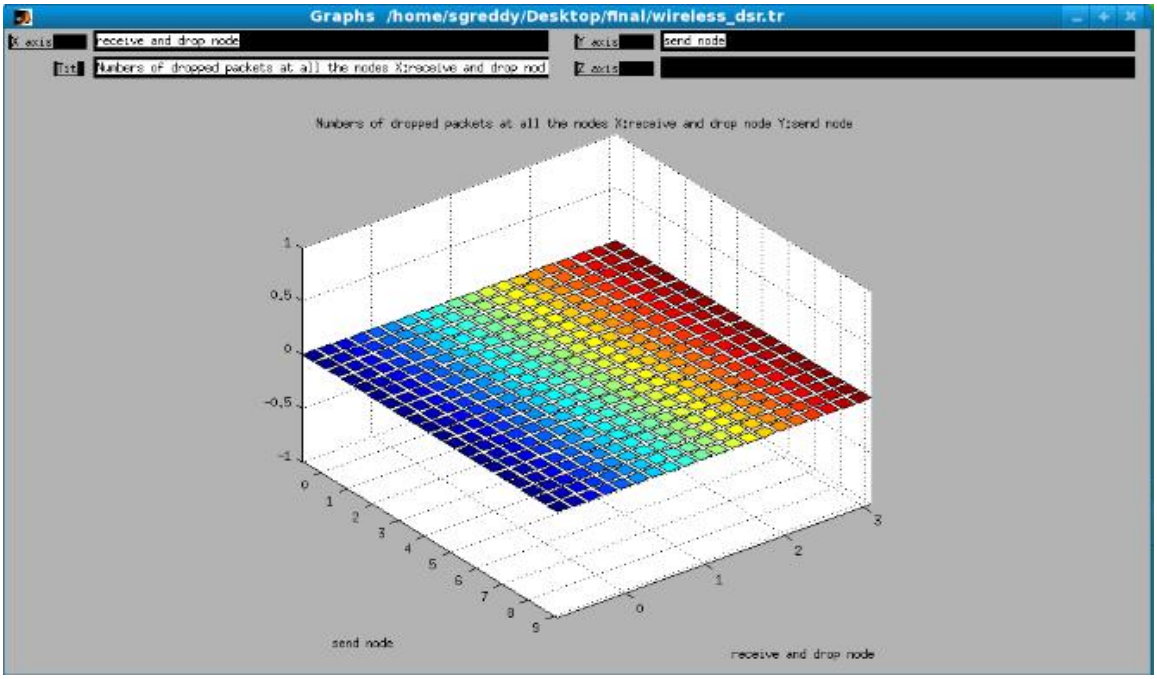


Figure.6.19. DSR (Random Topology): Dropped Packets

6.2.3. Simulation of TORA routing protocol:

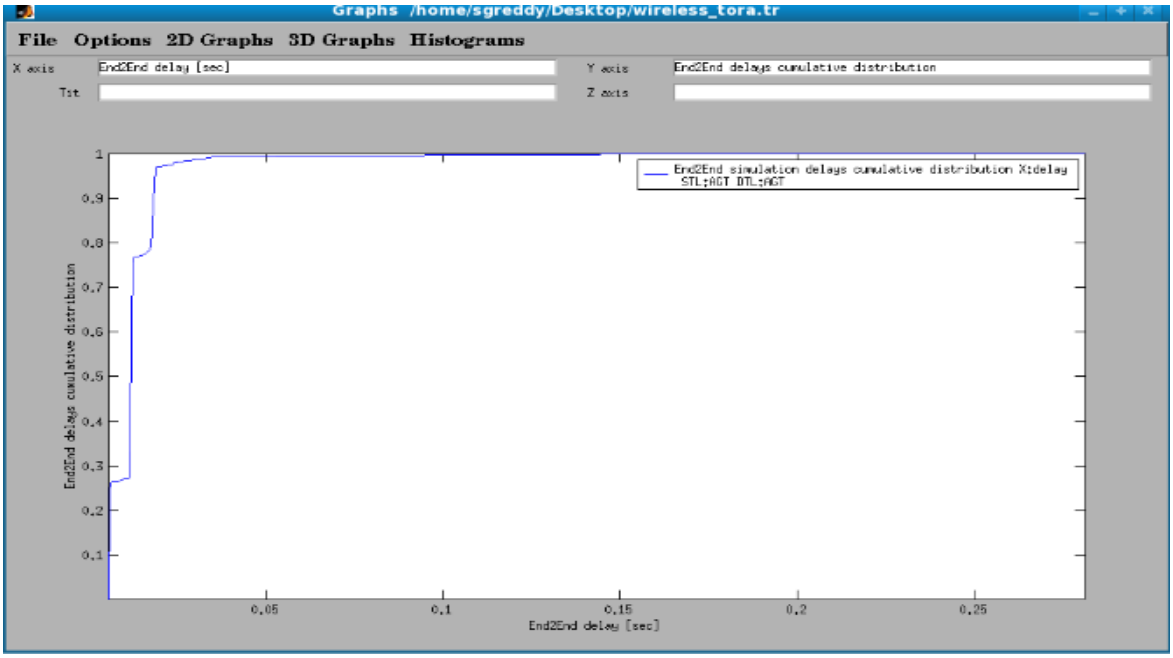


Figure.6.20. TORA (Random Topology): End-to-end Simulation Delay Cumulative Distribution

6.3. Comparison of the Three Routing Protocols:

The simulation results are revealed in the following section in the form of line graphs. Graphs illustrate comparison between the three protocols by varying different numbers of sources on the basis of the above-mentioned metrics as a function of pause time.

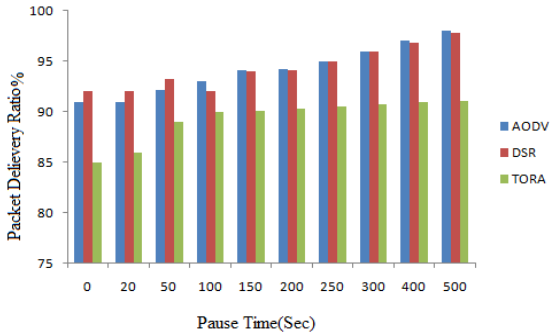


Figure6.21: Packet delivery fraction vs. Pause time for 15-node model with10 sources

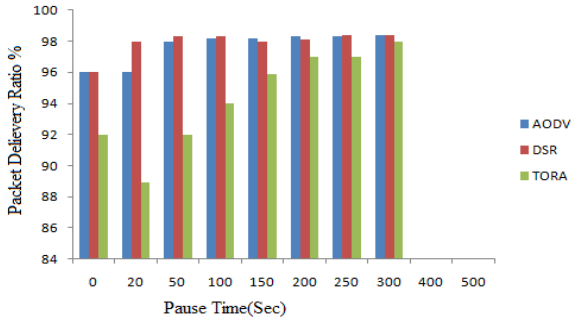


Figure.6.22: Packet delivery fraction vs. Pause time for 20-node model with20 sources

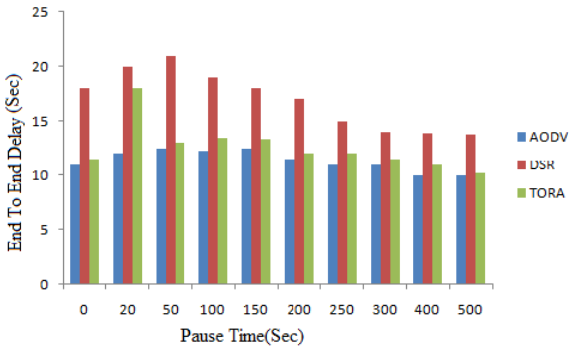


Figure6.23: End to End Delay vs. Pause time for 15-node model with10 sources

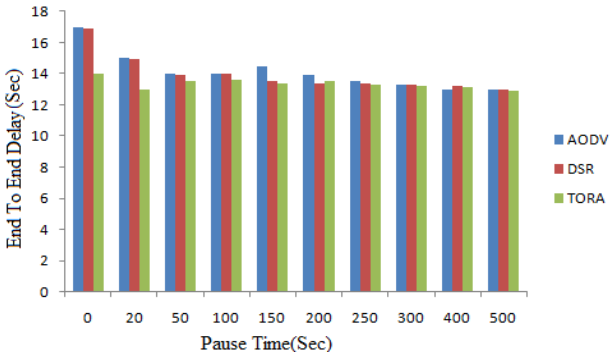


Figure.6.24: End to End Delay vs. Pause time for 20-node model with20 sources

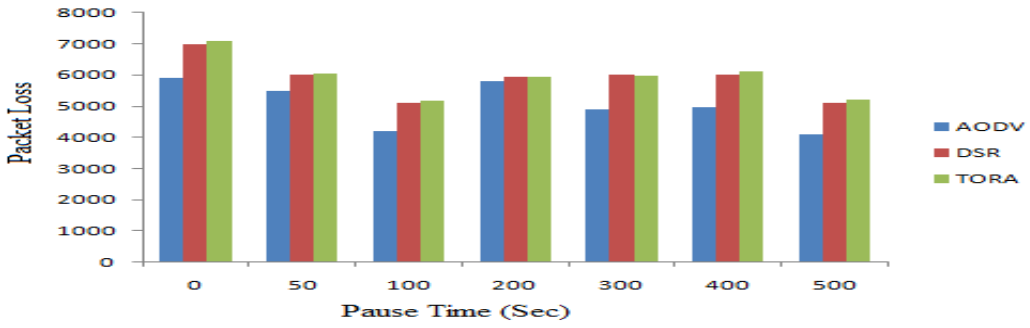


Figure6.25: Pocket Lose vs. Pause time for 20 nodes

6.4. Performance of Ad hoc Routing Protocols

This section presents a conversation on the performance of the previously described ad hoc routing protocols. The interpretation are based on various studies that have been done to compare the performance of routing protocols for MANETs

6.4.1 Performance of DSR

When low mobility DSR performs very well and delivers close to 95% of its packets. At high mobility, the throughput drops to about 70%. The throughput in DSR also decreases as a function of the number of nodes in the network. At high load, high mobility and large number of nodes, the throughput can be as low as 50%. The per-packet overhead in DSR is high because it embeds the complete source route in the packet header. This overhead can reach 100% for small sized data packets. DSR tend to keep the routing overhead relatively low even under high loads and large number of nodes. DSR finds close to optimal routes in most cases. Underneath low network loads, the average end-to-end delay in DSR is very low. However, the average delay can increase 5-6 times for modest to high network loads.

6.4.2 Performance of AODV

The AODV shows well performance in networks of up to 100 nodes regardless of node mobility and network load. Under these conditions, it delivers close to 95% of its packets and the throughput can approach 100% in fairly static networks. The throughput decreases as the number of nodes increases due to longer routes and higher collision rate. At number of nodes becoming more, the throughput becoming low .The packet delivery ratio also drops with increase in nodal mobility. The routing overhead is lower than proactive protocols but is high compared to DSR. However, AODV outperforms DSR in terms of per-packet overhead. Under conditions of high mobility, high load and larger number of nodes, the throughput can drop to 70%. Unlike many protocols, AODV does not find the optimal route in most cases and the difference in the optimal route and the route found by AODV can be up to four hops. It is interesting to note that the average delay in AODV decreases as the mobility increases.

6.4.3 Performance of TORA

When the numbers of nodes are low, TORA performs very well even at the highest rate of node mobility and delivers about 93% of its packets. TORA is based on the theory of link reversal and this can build the configuration of short lived routing loops. This problem is responsible for greater part of the packet drops in TORA. The performance of TORA suffers a ruthless joggle as the number of nodes increases and the packet delivery ratio can fall to about 9% in huge networks. TORA fails to converge in huge networks with high mobility rates and can undergo a congestive collapse. However, the performance of TORA is poor compared to protocols like DSR and AODV and it has been found that TORA had the most overhead compared to these protocols. The routing overhead in TORA is the sum of constant mobility-independent overhead (due to neighbor sensing) and variable mobility-dependent overhead.

Chapter 7

CONCLUSION & FUTURE SCOPE

Mobile Ad hoc Networks (MANETs) have received increasing research attention in recent years. There are many active research projects concerned with MANETs. Mobile ad hoc networks are wireless networks that use multi-hop routing instead of static networks infrastructure to provide network connectivity. MANETs have applications in rapidly deployed and dynamic military and civilian systems. The network topology in MANETs usually changes with time. Therefore, there are new challenges for routing protocols in MANETs since traditional routing protocols may not be suitable for MANETs. Researchers are designing new MANETs routing protocols, comparing and improving existing MANETs routing protocols before any routing protocols are standardized using simulations. In the presented work, we have discussed a comparison of three routing protocols (AODV,DSR and TORA) for Mobile ad hoc (MANETs) network in two scenarios with varying of nodesWe sincerely hope that our work will contribute in providing further research directions in the area of routing.

This comparison study is an attempt towards a comprehensive performance evaluation of three commonly used mobile ad hoc routing protocols (DSR, TORA and AODV) .Simulation was done with simulation time of 150 seconds and with some varying parameters, using the latest simulation environment ns-2. For short-range wireless communication in MANETs, AODV, DSR and TORA are used and the results are compared on the issues like throughput of sent packets, dropped packets, end-to-end delay and are very important for detailed performance evaluation of any networking protocol. We can summarize our final conclusion from our experimental results as follows:

• Increase in the density of nodes yields to an increase in the mean End-to-End delay.

• Increase in the pause time leads to a decrease in the mean End-to-End delay.

• Increase in the number of nodes will cause increase in the mean time for loop detection.

In short, AODV has the best all round performance. DSR is suitable for networks with moderate mobility rate. It has low overhead that makes it suitable for low bandwidth and low power network. TORA is suitable for operation in large mobile ad hoc networks having dense population of nodes. The major benefit is its excellent support for multiple routes and multicasting.

For the future work, this area will investigate not only the comparison between AODV, DSR and TORA routing protocols but more on the vast areas, extensive complex simulations could be carried out using other existing performance metrics, in order to gain a more in-depth performance analysis of the ad hoc routing protocols. Other new protocols performance could be studied too.

[1] Dimitri Bertsekas and Robert Gallager, "Data Networks - 2nd ed". Prentice Hall, New Jersey, ISBN 0-13-200916-1.

[2] D.Johnson et al., Dynamic Source Routing for mobile Ad-hoc Networks, IETF MANET Draft, April2003.

[3] M. S. Corson, J. P. Maker and G. H. Cirincione , "Internet-Based Mobile Ad Hoc Networking," IEEE Internet Computing, Vol. 3, no. 4, July-August 1999, pp. 63-70

[4] C. Mbarushimana, A. Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), IEEE Computer Society, March 2007.

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

[6] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced distance-Vector Routing (DSDV) for Mobile Computers," Comp. Commun. Rev., Oct. 1994, pp. 234–244

[7] T. Lin, S. F. Midkiff, and J. S. Park, "A Framework for Wireless Ad Hoc Routing Protocols," in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, vol. 2, pp. 1162-1167, New Orleans, LA, March 2003

[8] RL Pickholtz, LB Milstein and DL Schilling, "Spread spectrum for mobile communications, " IEEE Transactions , 1991

[9] Scott M. Ballew. Managing IP Networks with Cisci Routers. Orilley 1st Edition 1997

[10] C. E. Perkins, E. M. Belding-Royer, and S. R. Das. "*Ad hoc on-demand distance vector (AODV)routing*". Rfc 3561, IETF, July 2003

[11] George Aggelou, "Mobile Ad Hoc Networks", 2nd edition, Mc GRAW Hill professional engineering, 2004

[12] T. Lin and S. F. Midkiff, "Mobility versus Link Stability in the Simulation of MobileAd Hoc Networks," in *Proceedings of the Communication Networks and*

Distributed Systems Modelling and Simulation Conference (CNDS), pp. 3-8, Orlando, FL, January 2003 (invite paper).

[13] Cisco. Cisco Internetworking. Cisco Press, 2002

[14] Vincent D.Park, M.scott Corson. A highly Adaptive Distributed Routing Algorithm for Mobile wireless Networks. http://www.cs.odu.edu/skovvuri/tora.pdf cited on 11.05.2009.

[15]S. Das, C. Perkins, and E. Royer. Performance comparison of two on-demand routing protocols for ad hoc networks. In INFOCOM'2000 (1), pages 3–12, 2000.

[16] T. Lin, S. F. Midkiff, and J. S. Park, "A Dynamic Topology Switch for the Emulation of Wireless Mobile Ad Hoc Networks," in *Proceedings of the IEEE Local Computer Network (LCN), Wireless Local Network Workshop*, pp. 791-798, Tampa, FL, November 2002.

[17] Charles E. Perkins and Pravin Bhagwat, "DSDV routing over a multi hop wireless network of mobile computers", Technical report, IBM Research and University of Maryland, USA.

[18] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A.Qayyum, L. Viennot, "Optimized link state routing protocol for ad hoc networks", IEEE INMIC, Pakistan, 2001.

[19] D.Johnson. Validation of wireless and mobile network models and simulation. In DARPA/NIST Network Simulation Validation Workshop, Fairfax, Virginia, USA, May 1999.

[20] T. Lin and G. H. Sasaki, "Nonblocking WDM Networks with Fixed-Tuned Transmitters and Tunable Receivers," in *Proceedings of the 37th Annual Allerton Conference on Communication, Control and Computing*, pp. 400-401, Monticello, IL, September 1999.

[21] Bassam Halabi. Internet Routing Architectures. Cisco Press, 2000.

[22]Haas Z. J., Pearlman M. R., and Samar P., "The Zone Routing Protocol (ZRP)", IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.

[23] G.H. Sasaki and T. Lin, "A Minimal Cost WDM Network for Incremental Traffic," in *Proceedings of the IEEE Information Theory and Communication Workshop (ITW),* pp

[24] C.C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. IEEE SICON '97, Apr. 1997, pp. 197–211

[25] Tasman Networks Inc. Routing basics: Protocol evolution in enterprise and service provider networks. Technical report, 2004.

[26] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183–97

[27] S.Corson, J.Macker. MANET: Routing Protocol Performance Issues and Evaluation Considerations RFC 2501, IETF Network Working Group January1999, http://www.ietf.org/rfc/rfc2501.txt cited on 11.05.2009,

[28] P. Misra. "Routing Protocols for Ad Hoc Mobile Wireless Networks". Student Project Report, Ohio State University, 1999.

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

[30] C-K. Toh, "A Novel Distributed Routing Protocol to Support Ad-Hoc Mobile Computing", Proc. 1996 IEEE 15th Annual Int'l. Phoenix Conf. Comp. And Commun., Mar. 1996, pp. 480–86.

[31] 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 Communications, vol. 17, no. 8, pp. 1415- 1425, August 1999.

[32] T. Lin, "Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications" (phd thesis).

[33] Fedora website. http://docs.fedoraproject.org/install-guide/fc4/en/

[34] The network simulator - ns-2. http:// www. isi.edu/nsnam/ns/.

[35] K. Fall and K. Varadhan (Eds.), ns notes and documentation,1999. http://wwwmash.cs.berkeley.edu/ns/.

[36] ns by Example, http://nile.wpi.edu/ns/

[37] Speeding up ns-2 scheduler.

http://netlab.caltech.edu/~weixl/technical/ns2patch/ns2patch.htm

[38] The ns Manual. http://www.isi.edu/nsnam/ns/doc/index.html

[39] Tracegraph http://www.tracegraph.com/download.html

[40] A.K.Verma "Design and Development of a Routing Protocol for MANETs" (phd thesis).

[41] E. M. Belding-Royer and C. E. Perkins. "*Evolution and future directions of the ad hoc on-demand distance vector routing protocol*". *Ad hoc Networks Journal*, 1(1):125–150, July 2003.

PUBLISHED

- S.G.Reddy, P. kusa kumar, A .K .Verma, " Evaluation of Routing protocols for Mobile Ad hoc Networks" in Proc. Of ICSCI-2010.(pp. 682-687).

- P.kusakumar, S.G.Reddy, A.K.Verma, "Ant based Routing Algorithms for MANETs-A Review", Accepted for publication in Proc. IISN 2010(pp.133 -136).

COMMUNICATED

- S.G.Reddy, A.K.Verma "Performance comparison of three on-demand routing protocols for Mobile Ad hoc networks" communicated in IJCS.