Simulation, Analysis and Comparison of DSDV Protocol in MANETS

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

Master of Engineering
in
Computer Science & Engineering

By:
Jyotsna Rathee
(80732007)

Under the supervision of:
Dr. A. K. Verma
Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

MAY 2009

Certificate

I hereby certify that the work which is being presented in the thesis entitled, **"Simulation, Analysis and Comparison of DSDV Protocol in MANETS"**, in partial fulfilment 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.

(Jyotsna Rathee)

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

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

Countersigned by:

02/07/2009

(HEAD)
Computer Science & Engineering Deptt.,
Thapar University,
Patiala.

(R. K. Sharma) 9/7/09
Dean (Academic Affairs)
Thapar University,
Patiala.

Acknowledgement

No volume of words is enough to express my gratitude towards my guides, **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, CSED, **Dr. Seema Bawa, 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 colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis.

Most importantly, I would like to thank my **Family, Friends** 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.

Jyotsna Rathee

80732007

Abstract

Mobile ad hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end system, but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. These nodes change position frequently. To accommodate the changing topology special routing algorithms are needed. For relatively small networks flat routing protocols may be sufficient. However, in larger networks either hierarchical or geographic routing protocols are needed. There is no single protocol that fits all networks perfectly. The protocols have to be chosen according to network characteristics, such as density, size and the mobility of the nodes. MANET does not require any fixed infrastructure, such as a base station; therefore, it is an attractive option for connecting devices quickly and spontaneously.

A comparison of performance of DSDV (Destination Sequenced Distance Vector) routing protocol has been made between various parameters like: packets sent, packets received, throughput, and average end-to-end delay by varying the number of nodes.

Keywords: MANETS, DSDV, NS2- network simulator

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ACK	Acknowledgement
CBR	Continuous Bit Rate
DSDV	Destination Sequenced Distance Vector
DARPA	Defence Advanced Research Project Agency
EPPCSIT	Emerging Principles and Practises of Computer Science and Information Technology
ETSI	European Telecommunications Standards Institute
FC4	Fedora Core 4
FTP	File Transfer Protocol
GUI	Graphical User Interface I
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
MAC	Medium Access Control
MANET	Mobile Ad hoc Network
MH	Mobile Hosts
NAM	Network Animation
NS	Network Simulator
OSI	Open System Interconnect
OTcl	Object Oriented Tool Command Language
PAN	Personal Area Network
PHY	Physical
Tcl	Tool Command Language
TCP/IP	Transmission Control Protocol/Internet Protocol
Tx	Transmission
UDP	User Datagram Protocol
VINT	Virtual Inter Network Test-bed
WPAN	Wireless Local Area Network

CHAPTER 1
INTRODUCTION

1.1 MOTIVATION

Recent technological advancements enable portable computers to be equipped with wireless interfaces, allowing networked communication even while mobile. Wireless networking greatly enhances the utility of carrying a computing device. It provides mobile users with versatile and flexible communication between people and continous access to networked services with much more flexibility than cellular phones or pagers. With these performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth-constrained wireless links.

Within the Internet community, routing support for mobile hosts is presently being formulated as "mobile IP" technology. This is a technology to support nomadic host "roaming", where a roaming host may be connected through various means to the Internet other than its well known fixed-address domain space. The host may be directly physically connected to the fixed network on a foreign subnet, or be connected via a wireless link, dial-up line, etc. Supporting this form of host mobility (or nomadicity) requires address management, protocol interoperability enhancements and the like, but core network functions such as hop-by-hop routing still presently rely upon pre-existing routing protocols operating within the fixed network. In contrast, the goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes--which may be combined routers and hosts--themselves from the network routing infrastructure in an ad hoc fashion. An ad hoc wireless network should be able to handle the possibility of having mobile nodes, which will most likely increase the rate at which the network topology changes. Accordingly the network has to be able to adapt quickly to changes in the network topology. This implies the use of efficient handover protocols and auto configuration of arriving nodes.

A MANET is an autonomous collection of mobile users that communicate over relatively “slow” wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity, including discovering the topology and delivering messages must be executed by the nodes themselves. Hence routing functionality will have to be incorporated into the mobile nodes. Since the nodes communicate over wireless links, they have to contend with the effects of radio communication, such as noise, fading, and interference. In addition, the links typically have less bandwidth than a wired network. Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes.

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 in general in terms of motivation followed by the whole thesis outline. In Chapter 2, we discuss the background information relating to MANETS and what are the various routing protocols that are used in MANETS. Chapter 3, we study the state of the art of DSDV (Destination Sequenced Distance Vector) proactive routing protocol in MANETS. DSDV protocol in detail has been discussed covering the description of protocol, its working, how route discovery is done; how routing table information is updated. In Chapter 4, we discuss 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 INFORMATION

2.1 MANETS

In situations where networks are constructed and destructed in ad-hoc manner, mobile ad-hoc networking is an excellent choice. The idea of mobile ad-hoc or packet radio networks has been under development since 1970s. Since the mid-90s, when the definition of standards such as IEEE802.11 helped cause commercial wireless technology to emerge, mobile ad-hoc networking has been identified as a challenging evolution in wireless technology .

A MANET is an autonomous collection of mobile users communicating over a relatively bandwidth-constrained wireless link with limited battery power with highly dynamic environments[1]. The network topology, due to the mobility in the network, is dynamic and may change rapidly and unpredictably over time. Hence, the connectivity among the nodes may vary with time because of node departures, new node arrivals, and the possibility of having mobile nodes. To maintain communication between the nodes in the network, each node works as a transmitter, host, and, a router. The management and control functions are also distributed among the nodes.

2.1.1 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 2.1, 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.2.1, 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. [2]

OSI MODEL	**TCP/IP SUITE**	**MANET PROTOCOL STACK**	
APPLICATION	APPLICATION	APPLICATION	
PRESENTATION			
SESSION			
TRANSPORT	TRANSPORT	TRANSPORT	
NETWORK	NETWORK	NETWORK	ADHOC ROUTING
DATA LINK	DATA LINK	DATA LINK	
PHYSICAL	PHYSICAL	PHYSICAL	

Fig.2.1: 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 Destination Sequenced Distance Vector (DSDV).

2.1.2 CHARACTERISTICS OF MANETS

MANETs have several salient characteristics:

2.1.2.1 Dynamic topologies

Nodes are free to move arbitrarily; thus, the network topology--which is typically multihop--may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

2.1.2.2 Bandwidth-constrained, variable capacity links

Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications--after accounting for the effects of multiple access, fading, noise, and interference conditions, etc.--is often much less than a radio's maximum transmission rate.

2.1.2.3 Energy-constrained operation

Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

2.1.2.4 Limited physical security

Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered.

These characteristics create a set of underlying assumptions and performance concerns for protocol design which extend beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed Internet.

2.1.3 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[3]. 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 infrastructured environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include:

2.1.3.1 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 organising 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.

2.1.3.2Sensor Networks [4]

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.

2.1.3.3 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 optimise traffic flow.

2.1.3.4 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.

2.1.3.5 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.

2.1.4 Challenges Facing MANETS

The ad hoc networks have its own share of challenges which are listed below:

2.1.4.1 Spectrum allocation [5]

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.

2.1.4.2 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.

2.1.4.3 Routing

Routing of data between devices 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.

2.1.4.4 Existing IP Usage

For a mobile host to be able to communicate as it moves from one location to other, one of the following of the two things have to be in place:

-- Mobile Hosts must changes its IP address whenever it moves to new place

-- Host specific routes must be propagated throughout Internet Routing fabric.

There are problems with either of these options. If a host has an open TCP [6] session with another host, that session will be terminated if the IP address changes. Also, if other hosts must be able to initiate communication with a mobile host, how can they do so if their IP address changes every time they move? How does the host obtain a new IP address as it joins a network?

What is also of concern and it not addressed in this IETF draft [3] or in any publications is the convergence of two separate auto configured ad-hoc networks, merging together to form one larger ad-hoc network. Depending on the amount of participating hosts in each network and given the size of the address space given to link local addressing in IPv4[7] (65,563 possible hosts), there is a possibility of hosts having duplicate addresses. The main issue with using TCP in MANETs comes from the assumption that a packet being dropped is an indication of congestion occurring, not an indication of a lossy link or a data transmission error. This is due to the observation that that packet error/ loss rates over the internet due to transmission errors are of the order of 1%. However, in a wireless network, the amount of transmission errors is of a much higher order. The factors affecting the percentage of transmission errors include interference from other radio signals, device mobility, the sharing of a wireless link with other devices.

All these can affect the delivery of TCP segments to the receiver, the timely return of ACK packets from the receiver and give variations in the RTT compared to the estimated value. Any of these occurring will result in the sender assuming that congestion is occurring and will use TCP’s mechanisms to drastically reduce its transmission rate. MANETs also provide additional challenges to TCP operation. The mobility of hosts means that routes between hosts are open to change. When a route is broken due to host mobility, a route reconstruction procedure is invoked. This reconstruction results in a delay that the TCP sender is unaware of. Overall data throughput has had to suffer initially because of the route reconstruction delay, but TCP has now further drastically decreased the data throughput on false pretences.

2.1.4.5 Security and Privacy

Following are the security and privacy challenges in the area of ad hoc networks:

-- Firstly, use of wireless links renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation.

-- Secondly, nodes, roaming in a hostile environment (e.g., a battlefield) with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, we should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within the network by compromised nodes. Therefore, to achieve high survivability, ad hoc networks should have a distributed architecture with no central entities. Introducing any central entity into our security solution could lead to significant vulnerability; that is, if this centralized entity is compromised, then the entire network is subverted.

-- Thirdly, an ad hoc network is dynamic because of frequent changes in both its topology and its membership (i.e., nodes frequently join and leave the network). Trust relationship among nodes also changes, for example, when certain nodes are detected as being compromised. Unlike other wireless mobile networks, such as mobile IP, nodes in an ad hoc network may dynamically become affiliated with administrative domains. Any security solution with a static configuration would not suffice. It is desirable for our security mechanisms to adapt on-the-fly to these changes.

-- Finally, an ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

2.2 Routing in Mobile Ad hoc Networks

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration [8]. Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes [9]. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multihop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network [10].

In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes [11, 12].

2.2.1 Problems in routing with Mobile Ad hoc Networks

-- Asymmetric links: Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad-hoc networks as the nodes are mobile and constantly changing their position within network. For example consider a MANET (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 [13].

– 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 [13]. This updating frequency might be very low for ad-hoc networks.

2.2.2 Classification of Routing Protocols

Classification of routing protocols in MANET's can be done in many ways, but most of these are done depending on routing strategy and network structure[9, 14]. According to the routing strategy the routing protocols can be categorized as Table-driven and source initiated, while depending on the network structure these are classified as flat routing, hierarchical routing and geographic position assisted routing [9]. Both the Table-driven and source initiated protocols come under the Flat routing see fig2.2.

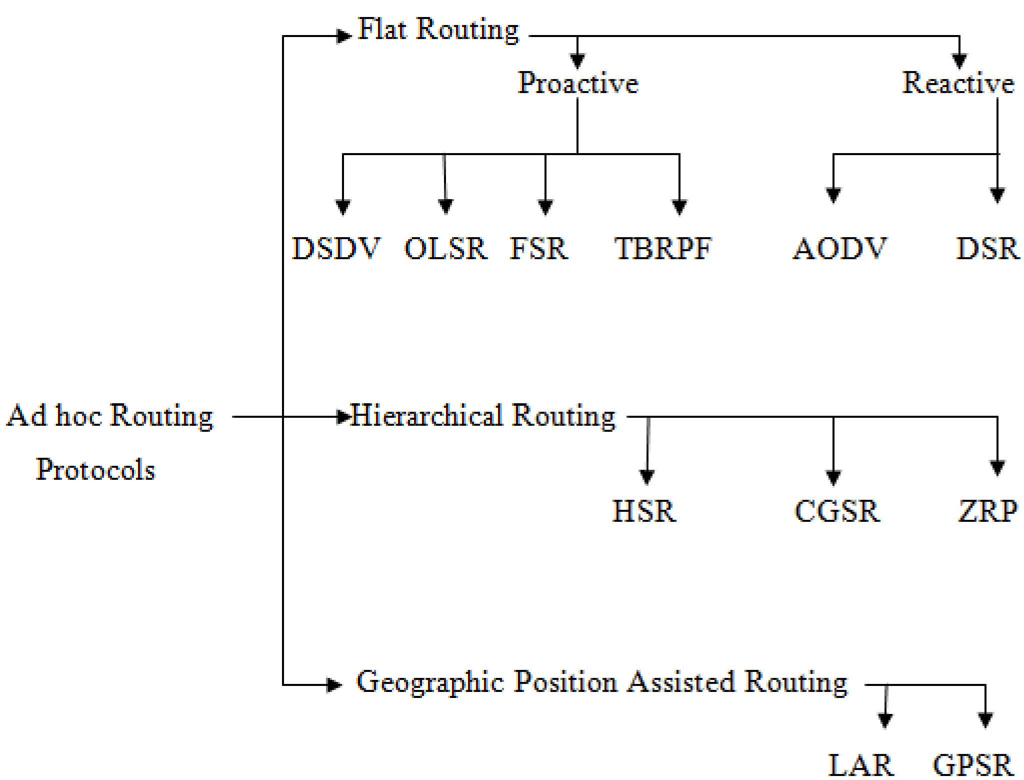


Fig.2.2: Classification of Routing Protocols in Mobile Ad hoc Networks

2.2.2.1 FLAT ROUTING PROTOCOLS

Flat routing protocols are divided into two classes; **proactive routing (table driven) protocols** and **reactive (on-demand) routing protocols**. Common for both protocol classes is that all nodes participating in routing play an equal role. They have further been classified after their design principles; proactive routing is mostly based on LS (link-state) while on-demand routing is based on DV (distance-vector).

2.2.2.1a Pro-Active / Table Driven routing Protocols

Proactive MANET protocols are table-driven and will actively determine the layout of the network. Through a regular exchange of network topology packets between the nodes of the network, a complete picture of the network is maintained at every single node. There is hence minimal delay in determining the route to be taken. This is especially important for time-critical traffic.

However, a drawback to a proactive MANET of protocol is that the life span of a link is significantly short. This phenomenon is brought about by the increased mobility of the nodes, which will render the routing information in the table invalid quickly.

Proactive MANET protocols work best in networks that have low node mobility or where the nodes transmit data frequently.

Examples of **Proactive MANET Protocols** include:

--Optimized Link State Routing, or OLSR [15]

-- Topology Broadcast based on Reverse Path Forwarding, or TBRPF [16]

-- Fish-eye State Routing, or FSR [17]

--Destination-Sequenced Distance Vector, or DSDV [18]

--Landmark Routing Protocol, or LANMAR [19]

--Clusterhead Gateway Switch Routing Protocol, or CGSR [20]

2.2.2.1b Reactive / On Demand Routing Protocols

On-demand routing is a popular routing category for wireless ad hoc routing. It is a relatively new routing philosophy that provides a scalable solution to relatively large network topologies. The design follows the idea that each node tries to reduce routing overhead by only sending routing packets when communication is requested. Common for most on-demand routing protocols are the route discovery phase where packets are flooded into the network in search of an optimal path to the destination node in the network.

Examples are:

--Ad hoc On-Demand Distance Vector, or AODV

--Dynamic Source Routing. Or DSV

--Temporally Ordered Routing Algorithm, or TORA

2.2.2.2 HIERARCHICAL ROUTING PROTOCOLS

As the size of the wireless network increases, the flat routing protocols may produce too much overhead for the MANET. In this case a hierarchical solution may be preferable. CGSR, HSR, ZRP and LANMAR are four hierarchical routing protocols that have different solutions to the organization of the routing of nodes in a MANET.

--CGSR (Clusterhead-Gateway Switch Routing)

--HSR (Hierarchical State Routing)

--ZRP (Zone Routing Protocol)

--LANMAR (Landmark Ad Hoc Routing Protocol)

2.2.2.3 GEOGRAPHICAL ROUTING PROTOCOLS

There are two approaches to geographic mobile ad hoc networks:

1. Actual geographic coordinates (as obtained through GPS – the Global Positioning System).
2. Reference points in some fixed coordinate system.

An advantage of geographic routing protocols is that they prevent network-wide searches for destinations. Control and data packets can be sent in the general direction of the destination if the recent geographical coordinates are known. This reduces control overhead in the network. A disadvantage, however, is that all nodes must have access to their geographical coordinates all the time to make the geographical routing protocols useful. The routing update must be done faster than the network mobility rate to make the location-based routing effective. This is because the nodes' locations may change quickly in a MANET.

Examples are:

--GeoCast (Geographic Addressing and Routing)

--DREAM (Distance Routing Effect Algorithm for Mobility)

--GPSR (Greedy Perimeter Stateless Routing)

CHAPTER 3

LITERATURE REVIEW

3.1 ROUTING PROTOCOL

The Destination Sequenced Distance Vector (DSDV) routing protocol is a proactive routing protocol, developed in 1994 by C. Perkins. It is a modification of conventional Bellman-Ford routing algorithm. This protocol adds a new attribute, sequence number, to each route table entry at each node. Routing table is maintained at each node and with this table, node transmits the packets to other nodes in the network. This protocol was motivated for the use of data exchange along changing and arbitrary paths of interconnection which may not be close to any base station.

3.2 BELLMAN-FORD ALGORITHM

The **Bellman–Ford algorithm**, a label correcting algorithm [21], computes single-source shortest paths in a weighted digraph (where some of the edge weights may be negative). Dijkstra's algorithm solves the same problem with a lower running time, but requires edge weights to be non-negative. Thus, Bellman–Ford is usually used only when there are negative edge weights. The algorithm was developed by Richard Bellman and Lester Ford, Jr.

According to Robert Sedgewick, "Negative weights are not merely a mathematical curiosity; [they] arise in a natural way when we reduce other problems to shortest-paths problems" [22]. If a graph contains a cycle of total negative weight then arbitrarily low weights are achievable and so there's no solution; Bellman-Ford detects this case.

If the graph does contain a cycle of negative weights, Bellman-Ford can only detect this; Bellman-Ford cannot find the shortest path that does not repeat any vertex in such a graph.

3.2.1 ALGORITHM

Bellman–Ford is in its basic structure very similar to Dijkstra's algorithm, but instead of greedily selecting the minimum-weight node not yet processed to relax, it simply relaxes *all* the edges, and does this $|V| - 1$ times, where $|V|$ is the number of vertices in the graph. The repetitions allow minimum distances to accurately propagate throughout the graph, since, in the absence of negative cycles, the shortest path can only visit each node at most once. Unlike the greedy approach, which depends on certain structural assumptions derived from positive weights, this straightforward approach extends to the general case. Bellman–Ford runs in $O(|V|\cdot|E|)$ time, where $|V|$ and $|E|$ are the number of vertices and edges respectively. The Bellman Ford Algorithm is as follows:

```
procedure BellmanFord(list vertices, list edges, vertex source)
  // This implementation takes in a graph, represented as lists of vertices
  // and edges, and modifies the vertices so that their distance and
  // predecessor attributes store the shortest paths.

  // Step 1: Initialize graph
  for each vertex v in vertices:
     if v is source then v.distance := 0
     else v.distance := infinity
     v.predecessor := null

  // Step 2: relax edges repeatedly
  for i from 1 to size(vertices)-1:
     for each edge uv in edges: // uv is the edge from u to v
        u := uv.source
        v := uv.destination
        if u.distance + uv.weight < v.distance:
           v.distance := u.distance + uv.weight
           v.predecessor := u

  // Step 3: check for negative-weight cycles
  for each edge uv in edges:
     u := uv.source
     v := uv.destination
     if u.distance + uv.weight < v.distance:
        error "Graph contains a negative-weight cycle"
```

3.3 DESIGN GOALS OF DSDV

The Bellman Ford Routing Algorithm is computationally efficient and easy to implement. This algorithm can cause routing loops that can occur if the internetwork's slow convergence on a new configuration causes inconsistent routing entries. Another problem that cannot be handled by this algorithm is counting to infinity. This condition continuously loops packets around the network, despite the fundamental fact that the destination network is down. While the routers are counting to infinity, the invalid information allows a routing loop to exist. Modifications eliminate the problem of loops but need some inter-nodal coordination mechanisms which imply few topological changes. Now, this algorithm is not designed to handle rapid topological changes.

So, the design goals of DSDV are:

-- Keep the simplicity of Bellman Ford algorithm.

-- Avoid the looping problem.

Therefore, the approach that is followed to attain these goals is:

-- Model each host as a router.

-- Tag each routing table entry with a sequence number.

3.4 ROUTING TABLE

Each node in the network maintains routing table for the transmission of the packets and also for the connectivity to different stations in the network. These stations list for all the available destinations, and the number of hops required to reach each destination in the routing table. The routing entry is tagged with a sequence number which is originated by the destination station. In order to maintain the consistency, each station transmits and updates its routing table periodically. The packets being broadcasted between stations indicate which stations are accessible and how many hops are required to reach that particular station. The packets may be transmitted containing the layer 2 or layer 3 address [23].

The data broadcast by each node will contain its new sequence number and the following information for each new route:

-- The destination address

-- The next hop for each destination

-- The number of hops required to reach the destination and

-- The new sequence number, originally stamped by the destination

-- Install Time

-- Stable Data

The transmitted routing tables will also contain the hardware address, network address of the mobile host transmitting them. The routing tables will contain the sequence number created by the transmitter and hence the most new destination sequence number is preferred as the basis for making forwarding decisions. This new sequence number is also updated to all the hosts in the network which may decide on how to maintain the routing entry for that originating mobile host.

Destination	Next Hop	Hops/Metric	Seq. No.	Install Time	Stable Data

Fig.3.1: Fields of Routing Table

3.5 TRANSMITTING ROUTE INFORMATION

Routing information is advertised by broadcasting or multicasting the packets which are transmitted periodically as when the nodes move within the network. The DSDV protocol requires that each mobile station in the network must constantly, advertise to each of its neighbours, its own routing table. Since, the entries in the table my change very quickly, the advertisement should be made frequently to ensure that every node can locate its neighbours in the network. This agreement is placed, to ensure the shortest number of hops for a route to a destination; in this way the node can exchange its data even if there is no direct communication link.

After receiving the route information, receiving node increments the metric and transmits information by broadcasting. Incrementing metric is done before transmission because, incoming packet will have to travel one more hop to reach its destination. Time between broadcasting the routing information packets is the other important factor to be considered. When the new information is received by the mobile host it will be retransmitted soon effecting the most rapid possible dissemination of routing information among all the cooperating mobile hosts. The mobile host cause broken links as they move from place to place within the network. The broken link may be detected by the layer2 protocol, which may be described as infinity. When the route is broken in a network, then immediately that metric is assigned an infinity metric there by determining that there is no hop and the sequence number is updated. Sequence numbers originating from the mobile hosts are defined to be even number and the sequence numbers generated to indicate infinity metrics are odd numbers. The broadcasting of the information in the DSDV protocol is of two types namely:

1. Full dump

Full dump broadcasting will carry all the routing information and requires multiple NPDU's (network protocol data units).

2. Incremental dump

The incremental dump will carry only information that has changed since last full dump. Incremental dump requires only one NPDU to fit in all the information**.**

3.6 SELECTION OF ROUTES

If new routing information is received, selection of routes is done as follows:

1) Any route with a more recent sequence number is used.

2) If the new route has equal sequence number but better metric, then this route is chosen.

3) Newly recorded routes are scheduled for immediate advertisement.

3.7DAMPING FLACTUATIONS

There can be fluctuations of routing table entry advertisements. The general problem arises because route updates are selected according to the following criteria:

--Routes are always preferred if the sequence numbers are newer;

--Otherwise, routes are preferred if the sequence numbers are the same and yet the metric is better (lower).

To see the problem, suppose that two routes with identical sequence numbers are received by a Mobile Host, but in the wrong order. In other words, suppose that MH4 receives the higher metric next hop first, and soon after gets another next hop with a lower metric but the same sequence number. This could happen when there are a lot of Mobile Hosts, transmitting their updates not quite regularly. Alternatively, if the Mobile Hosts are acting independently and with markedly different transmission intervals, the situation could occur with correspondingly fewer hosts.

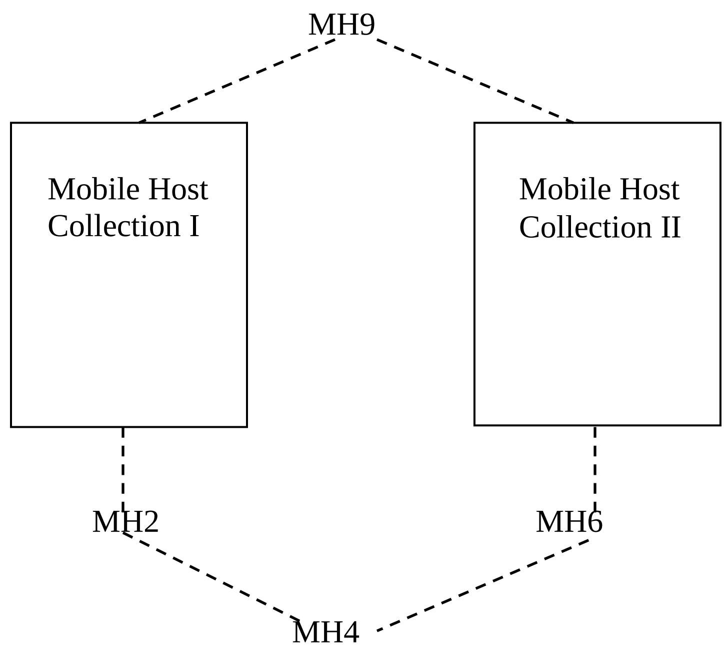


Fig. 3.2: Receiving Fluctuating Routes

Suppose, in any event, in Fig.3.2 there are enough Mobile Hosts to cause the problem, in two separate collections of Mobile Hosts both connected to a common destination MH9, but with no other Mobile Hosts in common. Suppose further that all Mobile Hosts are transmitting updates approximately every 15 seconds, that Mobile Host MH2 has a route to MH9 with 12 hops, and Mobile Host MH6 has a route to MH9 with 11 hops, Moreover, suppose that the routing information update from MHZ arrives at MH4 approximately 10 seconds before the routing information update from MH6. This will occur every time that a new sequence number is issued from Mobile Host MH9. In fact, the time differential can be drastic if any Mobile Host in collection II begins to issue its sequence number updates in multiple incremental update intervals, as would happen, for instance, when there are too many hosts with new sequence number updates for them all to fit within a single incremental packet update. In general, the larger the number of hops, the more drastic differentials between deliveries of the updates can be expected.

3.7.1 SETTLING TIME

The solution for damping fluctuations is to keep a route settling time table in each node with a time to wait for a route with a better metric before advertising the update message. The settling time data is stored in a table with the following fields, keyed by the first field:

--Destination address

--Last settling time

--Average settling time

The settling time is calculated by maintaining a running, weighted average over the most recent updates of the routes, for each destination [24]. Suppose a new routing information update arrives at MH4. The sequence number in the new entry is the same as the sequence number in the currently used entry, and the newer entry has a worse (i.e., higher) metric. Then MH4 must use the new entry in making subsequent forwarding decisions. However, MH4 does not have to advertise the new route immediately and can consult its route settling time table to decide how long to wait before advertising it. The average settling time is used for this determination. For instance, MH4 may decide to delay (average.settling_time x 2) before advertising a route. This can be quite beneficial, because if the possibly unstable route were advertised immediately, the effects would ripple through the network, and this bad effect would probably be repeated every time Mobile Host MH9's sequence number updates rippled through the ad-hoc network. On the other hand, if a link via Mobile Host MH6 truly does break, the advertisement of a route via MH2 should proceed immediately. To achieve this when there is a history of fluctuations at Mobile Host MH4, the link breakage should be detected fast enough so that an intermediate host in Collection II finds out the problem and begins a triggered incremental update showing an ∞ metric for the path along the way to Mobile Host M H9. Routes with an ∞ metric are required by this protocol to be advertised immediately, without delay.

In order to bias the damping mechanism in favour of recent events, the most recent measurement of the settling time of a particular route must be counted with a higher weighting factor than are less recent measurements. And, importantly, a parameter must be selected which indicates how long a route has to remain stable before it is counted as truly stable. This amounts to specifying a maximum value for the settling time for the destination in the settling time table. Any route more stable than this maximum value will cause a triggered update if it is ever replaced by another route with a different next hop or metric.

When a new routing update is received from a neighbour, during the same time that the updates are applied to the table, processing also occurs to delete stale entries. Stale entries are defined to be those for which no update has been applied within the last few update periods. Each neighbour is expected to send regular updates; when no updates are received for a while, the receiver may make the determination that the corresponding computer is no longer a neighbour. When that occurs, any route using that computer as a next hop should be deleted, including the route indicating that computer as the actual (formerly neighbouring) destination.

Increasing the number of update periods that may transpire before entries are determined would result in more stale routing entries, but would also allow for more transmission errors. Transmission errors are likely to occur when a CSMA-type broadcast medium is used, as may well be the case for many wireless implementations. When the link breaks, an ∞ metric route should be advertised for it, as well as for the routes that depend on it.

3.8 EXAMPLE OF DSDV

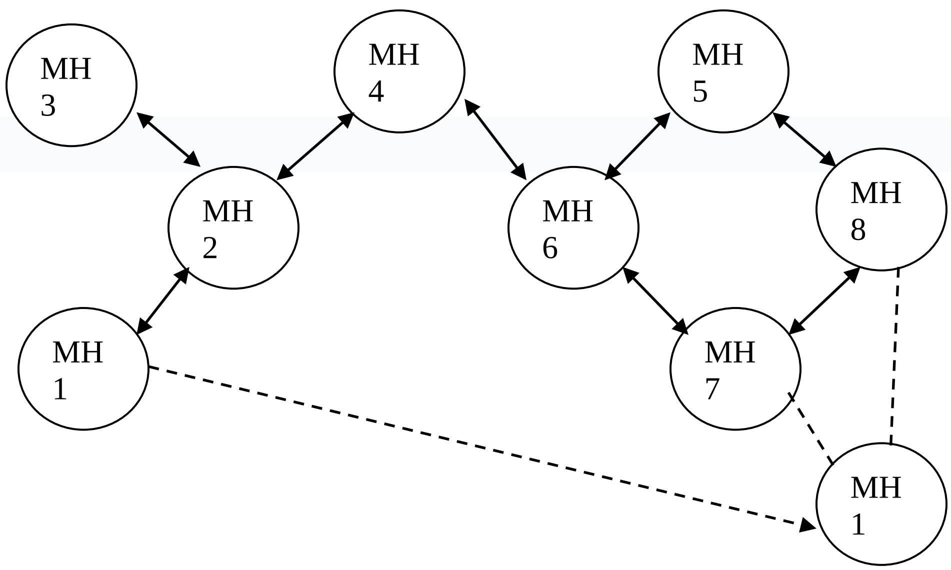


Fig. 3.3: Movement of Mobile Hosts in Ad hoc Network

Consider the above fig. 3.3 which has 8 hosts in the network. We will have a look at the changes to the MH4 routing table with reference to the movements of MH1. Initially, all the nodes advertise their routing information to all the nodes in the network and hence the routing table at MH4 initially looks like

Table 3.1: Routing Table of MH4

Destination	Next Hop	Metric	Sequence Number	Install Time	Stable Data
MH1	MH2	2	S-406	T001_MH4	Ptr_MH1
MH2	MH2	1	S-128	T001_MH4	Ptr_MH2
MH3	MH2	2	S-584	T001_MH4	Ptr_MH3
MH4	MH4	0	S-710	T001_MH4	Ptr_MH4
MH5	MH6	2	S-392	T002_MH4	Ptr_MH5
MH6	MH6	1	S-076	T001_MH4	Ptr_MH6
MH7	MH6	2	S-128	T002_MH4	Ptr_MH7
MH8	MH6	3	S-050	T002_MH4	Ptr_MH8

The forwarding table at MH4 would look like:

Table 3.2: Forwarding Table at MH4

Destination	Metric	Sequence Number
MH1	2	S-406
MH2	1	S-128
MH3	2	S-584
MH4	0	S-710
MH5	2	S-392
MH6	1	S-076
MH7	2	S-128
MH8	3	S-050

But, when the host MH1 moves its location as shown in the fig. 3.3 nearer to MH7 and MH8 then, the link between MH2 and MH1 will be broken resulting in the assignment of infinity metric at MH2 for MH1 and the sequence number will be changed to odd number in the routing table at MH2. MH2 will update this information to its neighbour hosts.

Since, there is a new neighbour host for MH7 and MH8; they update their information in the routing tables and they broadcast. Now, MH4 will receive its updated information from MH6 where MH6 will receive two information packets from different neighbours to reach MH1 with same sequence number, but different metric. The selection of the route will depend on less hop count when the sequence number is the same. Now the routing table will look like

Table 3.3: Routing Table after MH1 movement

Destination	Next Hop	Metric	Sequence Number	Install Time	Stable Data
MH1	MH6	3	S-516	T001_MH4	Ptr_MH1
MH2	MH2	1	S-238	T001_MH4	Ptr_MH2
MH3	MH2	2	S-674	T001_MH4	Ptr_MH3
MH4	MH4	0	S-820	T001_MH4	Ptr_MH4
MH5	MH6	2	S-502	T002_MH4	Ptr_MH5
MH6	MH6	1	S-166	T001_MH4	Ptr_MH6
MH7	MH6	2	S-238	T002_MH4	Ptr_MH7
MH8	MH6	3	S-160	T002_MH4	Ptr_MH8

And the forwarding table would be:

Table 3.4: Forwarding Table at MH4 after movement of MH1

Destination	Metric	Sequence Number
MH1	3	S-516
MH2	1	S-238
MH3	2	S-674
MH4	0	S-820
MH5	2	S-502
MH6	1	S-166
MH7	2	S-238
MH8	3	S-160

In this example, one node has changed its routing information, since it is in a new location. All nodes have transmitted new sequence numbers recently. If there were too many updated sequence numbers to fit in a single packet, only the ones which fit would be transmitted. These would be selected with a view to fairly transmitting them in their turn over several incremental update intervals. There is no such required format for the transmission of full routing information packets. As many packets are used as are needed, and all available information is transmitted. The frequency of transmitting full updates would be reduced if the volume of data began to consume a significant fraction of the available capacity of the medium.

CHAPTER 4

PROBLEM STATEMENT & OBJECTIVE

4.1 PROBLEM STATEMENT

A mobile ad-hoc network (MANET) is a kind of wireless ad-hoc network, and is a self-configuring network of mobile routers (and associated hosts) connected by wireless links – the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably.

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. 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 which is known as packet switching is straight forward, but the path determination could be very complex. 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.

Proactive protocols maintain the routing information even before it is needed. Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. Many of these routing protocols come from the link-state routing. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node.

The destination sequenced distance vector routing protocol is a proactive routing protocol which is a modification of conventional Bellman-Ford routing algorithm. This protocol adds a new attribute, sequence number, to each route table entry at each node. Routing table is maintained at each node and with this table; node transmits the packets to other nodes in the network. This protocol was motivated for the use of data exchange along changing and arbitrary paths of interconnection which may not be close to any base station. DSDV has advantages that it guarantees loop free path and count to infinity problem is also reduced. DSDV maintains the best path instead of maintaining multiple paths to every destination. With these advantages, DSDV also have some limitations, like: Wastage of bandwidth due to unnecessary advertising of routing information even if there is no change in the network topology and it doesn't support Multi path Routing.

4.2 OBJECTIVE AND SUB- TASKS

The primary objective of this thesis is:

To analyze, implement and perform comparative analysis of Destination Sequenced Distance Vector routing protocol with the parameters like packets sent, packets received, throughput, end to end delay when the network grows larger. what changes happen in these four parameters when we increase the number of nodes while implementing DSDV.

To achieve primary objective, following tasks must be done:

-- Get a general understanding of ad -hoc networks.

-- Get a general understanding of simulation environment that could be used for analyzing evaluating and implementing ad hoc routing protocols

-- Implement DSDV with different number of nodes for wireless ad-hoc networks.

-- Analyze the protocol theoretically and through simulation based on above mentioned parameters.

CHAPTER 5

INSTALLATION, SIMULATION & DESIGN

5.1. Fedora Core 4

Fedora Core [25] is a free operating system base on Linux. Red Hat and being developed by the open source community and the Red Hat engineers sponsor the development of Fedora. Fedora Core 4 (FC4) is the latest release of the Fedora Project currently. Some primary features of FC4 are extensive performance improvements, support for Intel-based Macs and a new Graphical User Interface (GUI) virtualization manager.

5.2. The Network Simulator (NS2)

Simulation can be defined as “Imitating or estimating how events might occur in a real situation” [26]. It can involve complex mathematical modelling, 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. NS2 Overview

NS [27] is an event driven network simulator developed at University of California at Berkeley, USA, as a REAL network simulator projects in 1989 and was developed at with cooperation of several organizations. Now, it is a VINT project supported by DARPA. NS is not a finished tool that can manage all kinds of network model. It is actually still an on-going effort of research and development. The users are responsible to verify that their network model simulation does not contain any bugs and the community should share their discovery with all. There is a manual called NS manual for user guidance.

NS is a discrete event network simulator where the timing of events is maintained by a scheduler and able to simulate various types of network such as LAN and WPAN according to the programming scripts written by the user. Besides that, it also implements variety of applications, protocols such as TCP and UDP, network elements such as signal strength, traffic models such as FTP and CBR, router queue management mechanisms such as Drop Tail and many more.

There are two languages used in NS2 C++ and OTcl (an object oriented extension of Tcl). The compiled C++ programming hierarchy makes the simulation efficient and execution times faster. The OTcl script which written by the users the network models with their own specific topology, protocols and all requirements need. The form of output produce by the simulator also can be set using OTcl. The OTcl script is written which creating an event scheduler objects and network component object with network setup helping modules. The simulation results produce after running the scripts can be use either for simulation analysis or as an input to graphical software called Network Animation (NAM).

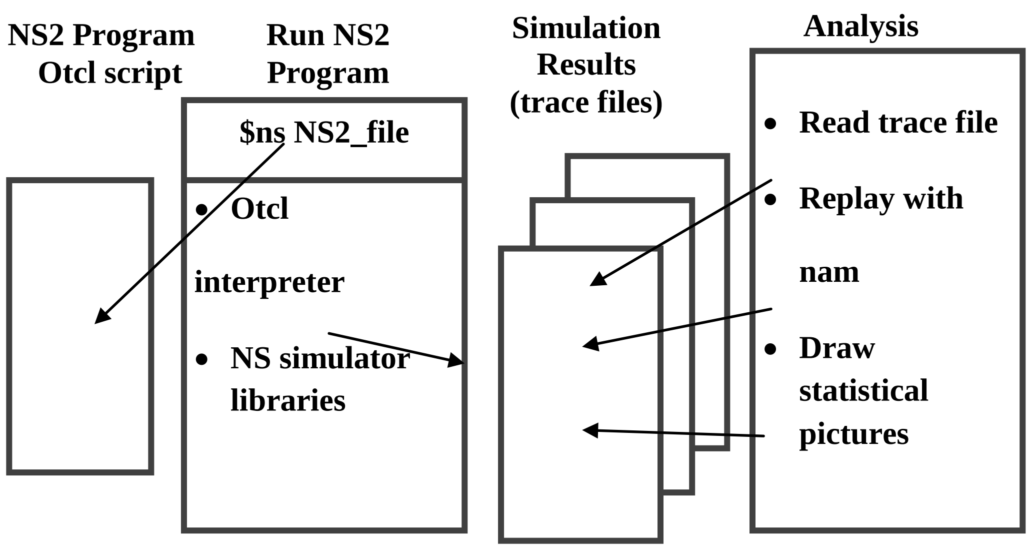


Fig.5.1: Running NS2 Program

NS2 is an event driven network simulator, which can be implements in Linux-based platform. This report will explain on how to install NS2 in Fedora Core platform. The NS2 files (recommended to download a piece of file which includes all the needed files called ns-allinone-2.xx from http://www.isi.edu/nsnam/ns/ must be downloaded into any media storage, most preferred is inside the computer itself where the NS2 is going to be installed. Since, we are using NS 2.33. It is not recommend logging in as a root because installation at root may interfere with any important Linux files.

5.2.2. Tool Command Language (Tcl)

Short for Tool Command Language, Tcl [28] 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.

5.2.3. The Network Animation (NAM)

The network animator began in 1990 as a simple tool for animating packet trace data. This 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.

5.2.4. The Trace File

The trace file is an ASCII code files and the trace is organized in 12 fields as in Figure 5.2. below.

Event	Time	From node	To node	Pkt type	Pkt size	Flags	Fid	Src addrs	Dst addrs	Seq num	Pkt id

Fig. 5.2. 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, dequeued 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 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.

5.2.5. The Tracegraph

It is a data presentation system for Network Simulator NS2. The simulator doesn’t have any options implemented to analyse simulations results so it’s hard to use it. Trace graph [29] 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 NS2 trace file formats; wired, satellite, wireless (old and new trace), wired-cum-wireless. Trace file loading stage is divided into 4 stages; automatic trace file format recognition, trace file parsing to extract necessary simulation data which is saved to a temporary file, trace files can contain much more data than is needed by the system, so unnecessary information is omitted to speed up trace file loading, temporary file loading, constants calculations (packets types, packets sizes, flows IDs, trace levels, number of nodes, simulation time) – in order to speed up data processing. Wireless and wired-cum-wireless trace files are parsed and saved in Trace graph format.

5.3. Simulation of Routing Protocols

Simulation of DSDV routing protocols has been carried over to evaluate the performance. Various parameters that are considered for simulation are listed in table 5.1.

Table 5.1: Network Parameter Definition

Parameter Name	**Value**
Channel Type	Channel/Wireless Channel
Netif	Phy/Wireless Phy
Mac Protocol	Mac/802_11
Queue Length	50
Number of Nodes	5/10/15/25
Routing Protocol	DSDV
Grid Size	600 x 600
Packet Size	512
Simulation Time	50
Topology	Random

CHAPTER 6

RESULTS, PERFORMANCE EVALUATION & ANALYSIS

In this chapter, we discuss the simulation results of the DSDV protocol. On the basis of results of *.nam file and *.tr file, the analysis is being done. We also evaluate the performance of DSDV by taking number of nodes as a parameter. 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 DSDV 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 four parts basis on the number of nodes that vary:

1. DSDV with 5 nodes.
2. DSDV with 10 nodes.
3. DSDV with 15 nodes.
4. DSDV with 25 nodes.

The comparison of performance of DSDV, based on the number of nodes is done on following parameters like packet sent, packet received, throughput and average end-to-end delay.

6.1 Simulation of DSDV with 5 Nodes

Simulation of DSDV is performed with 5 nodes in the beginning. Nodes in the simulation scenario are at same position initially. With the passage of time they started moving to different positions (i.e. mobile). Here, the nodes transmit their routing table information to nodes that are covered under their range of communication. Now, when a particular node goes out of range of a particular node then the packets received by the other node are less than the packets sent by the source(sender) node. In Fig.6.1, we can see the route discovery between various nodes at a particular instant and the packets that are transferred among them.

As the position of the nodes changes, some nodes are out of range for each other. Then packets sent by them to those out of range nodes are being dropped. In Fig.6.2, we can see the change of positions of the nodes and also the dropping of packets. The nodes which are in range, still communicate with each other having a low rate of packets dropped.

The tracegraph snapshots have been taken with simulation time of 50 seconds. In Fig.6.3, the entire simulation information is shown with end-to-end delay. The throughput of sending and receiving, sending packets are shown in fig.6.4, and fig.6.5. In Fig.6.6, number of dropped packets at every node is shown.

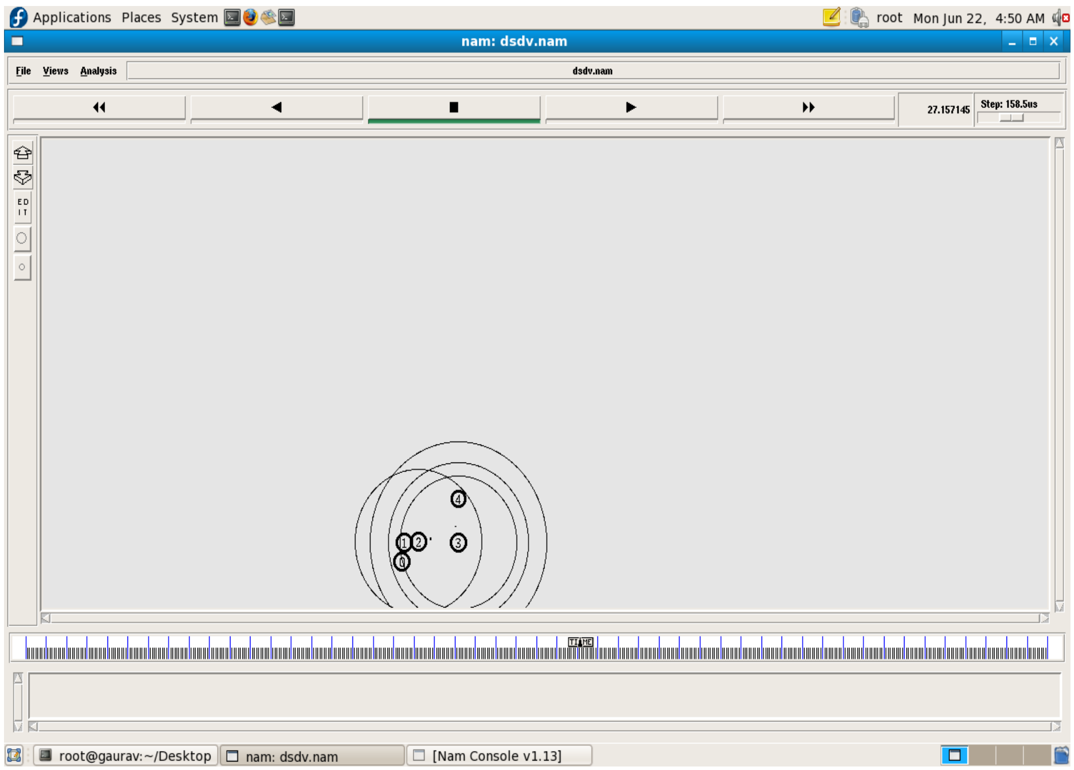


Fig.6.1: DSDV with 5 nodes: Sending and Receiving Packets and Route Discovery

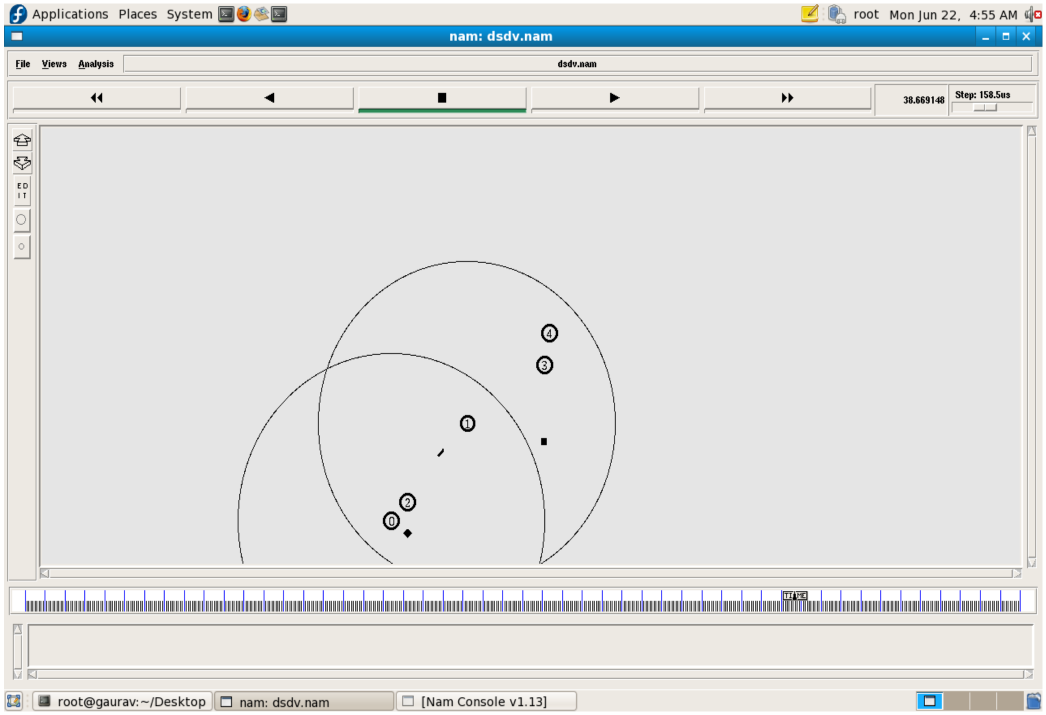


Fig.6.2: DSDV with 5 nodes: Dropping of Packets

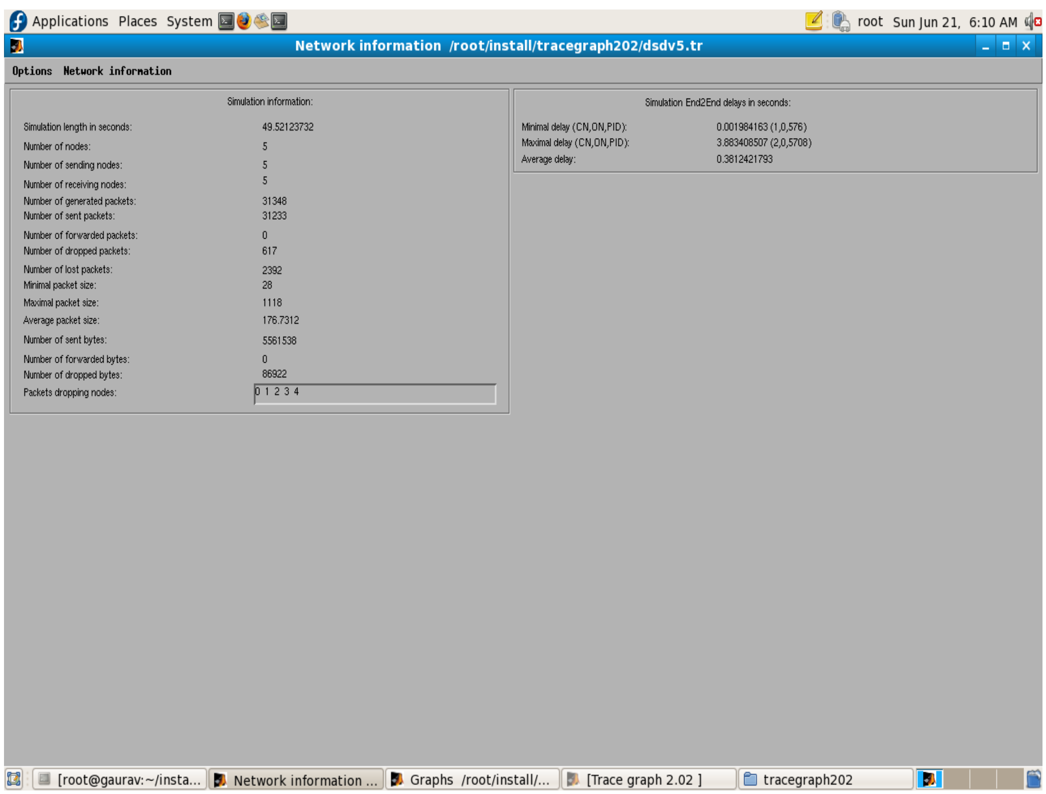


Fig6.3: Simulation Details (Tracegraph File)

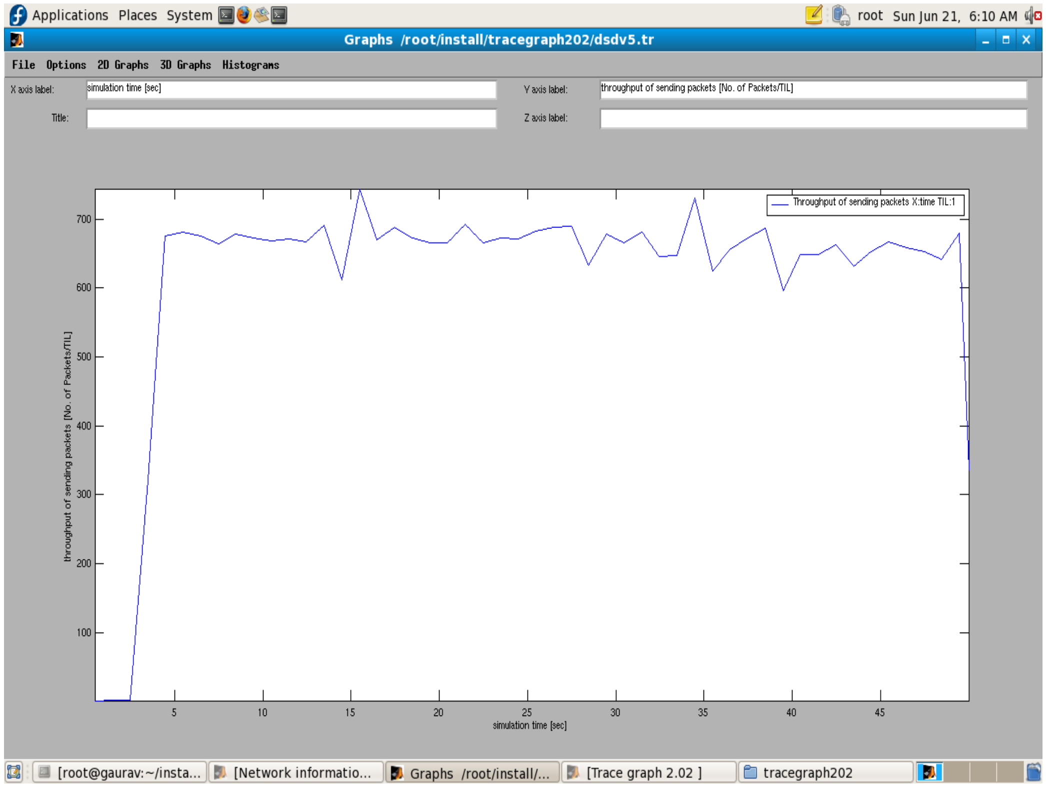
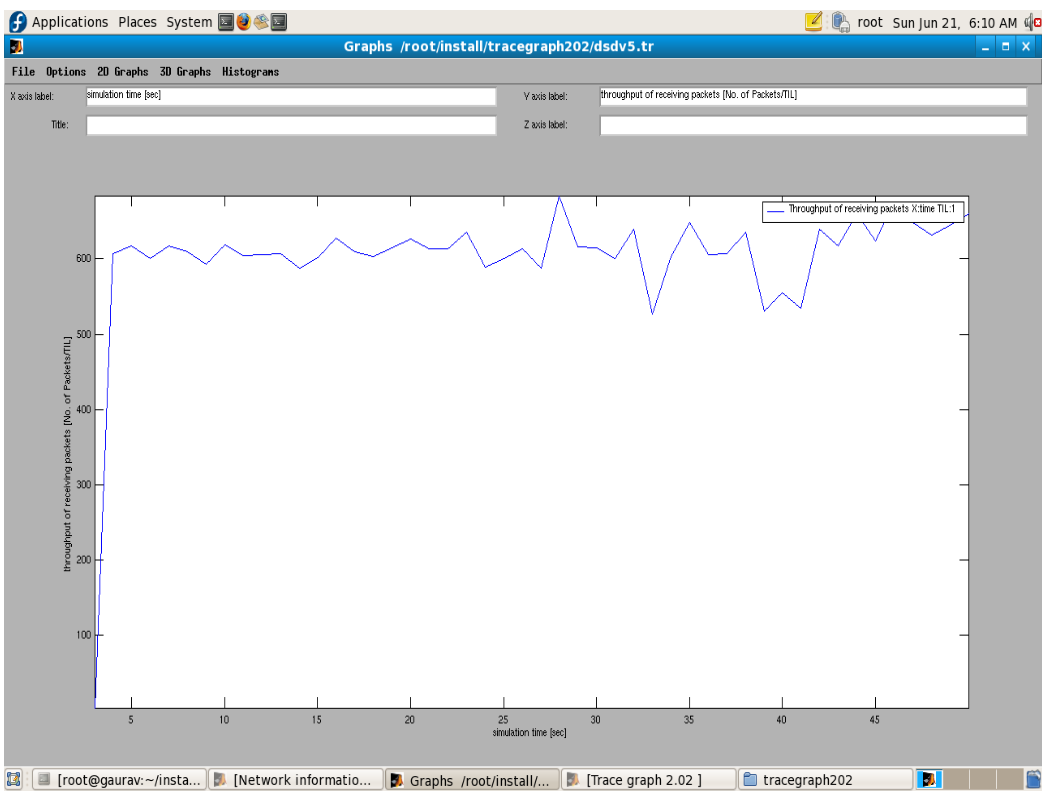


Fig.6.4: Throughput of sent packets v/s simulation time



6.5: Throughput of received packets v/s simulation time

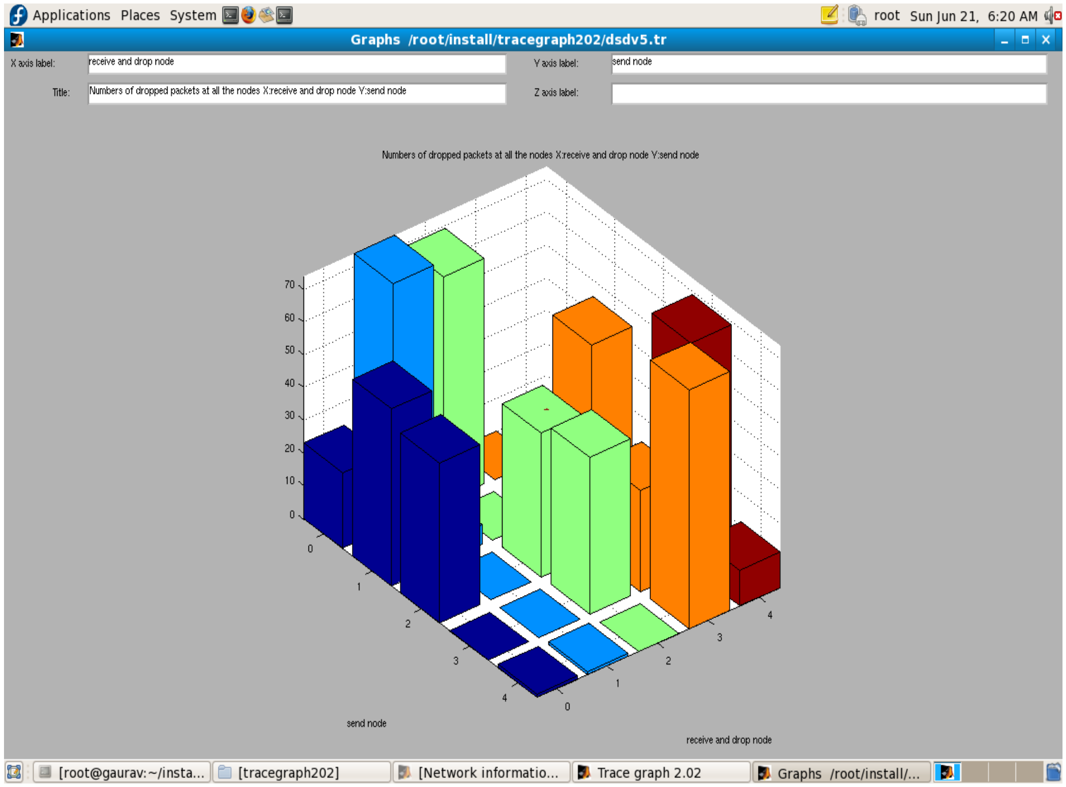


Fig.6.6: Dropped Packets.

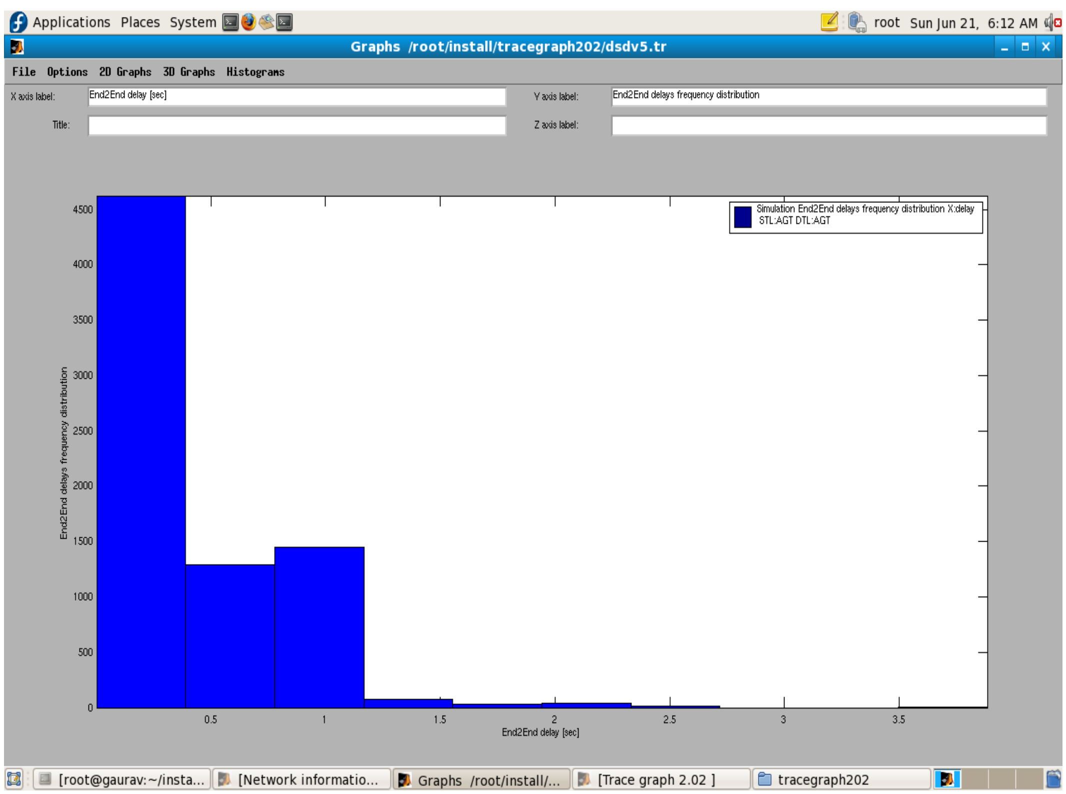


Fig.6.7: End-to-End Delay: Frequency Distribution

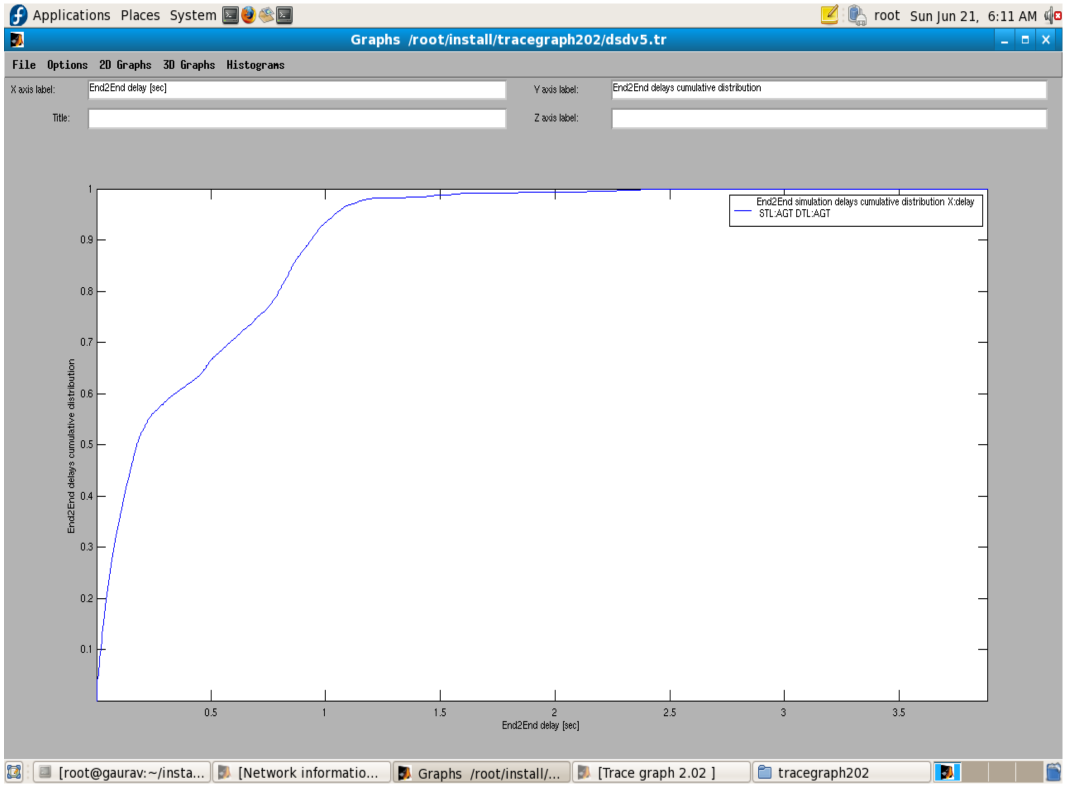


Fig.6.8: End-to-End Delay: Cumulative Distribution

Fig.6.7 shows the end-to-end delay for frequency distribution. The frequency distribution is at peak at starting but till last it decreases to minimum as end-to-end delay time increases. In Fig.6.8, cumulative distribution is shown. With delay time increasing, cumulative delay increases invariably till 1.5 sec and then becomes constant.

6.2 Simulation of DSDV with 10 Nodes

In this case, we perform the simulation for 10 nodes. Here, also nam file and dsdv10.tr files are generated when we execute the dsdv10.tcl file.

Fig.6.9 and Fig.6.10 shows the flow of packets between various nodes at certain position and route discovery and dropping of packets when nodes change their respective positions. Fig.6.11 shows the simulation details of the protocol with 10 nodes. Fig.6.12 and Fig.6.13 shows the throughput of sending and receiving packets versus simulation time, respectively. Fig.6.14 shows the dropped packets at various nodes.

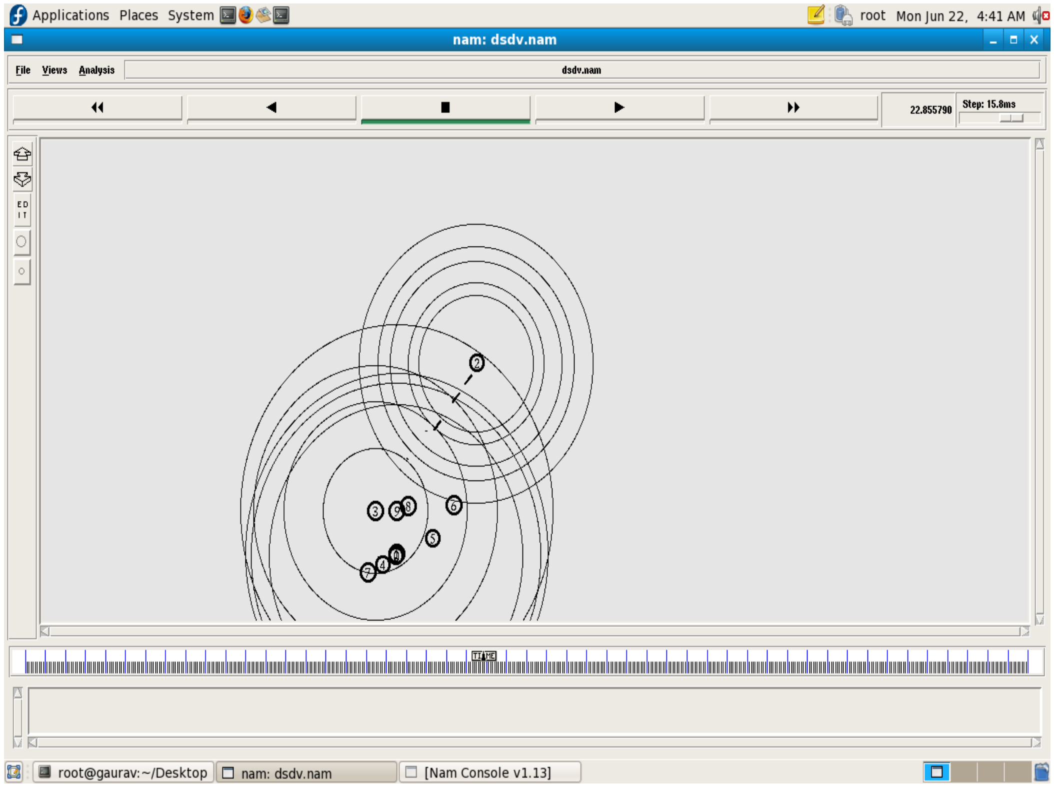


Fig.6.9: DSDV with 10 nodes: Sending and Receiving packets and route discovery

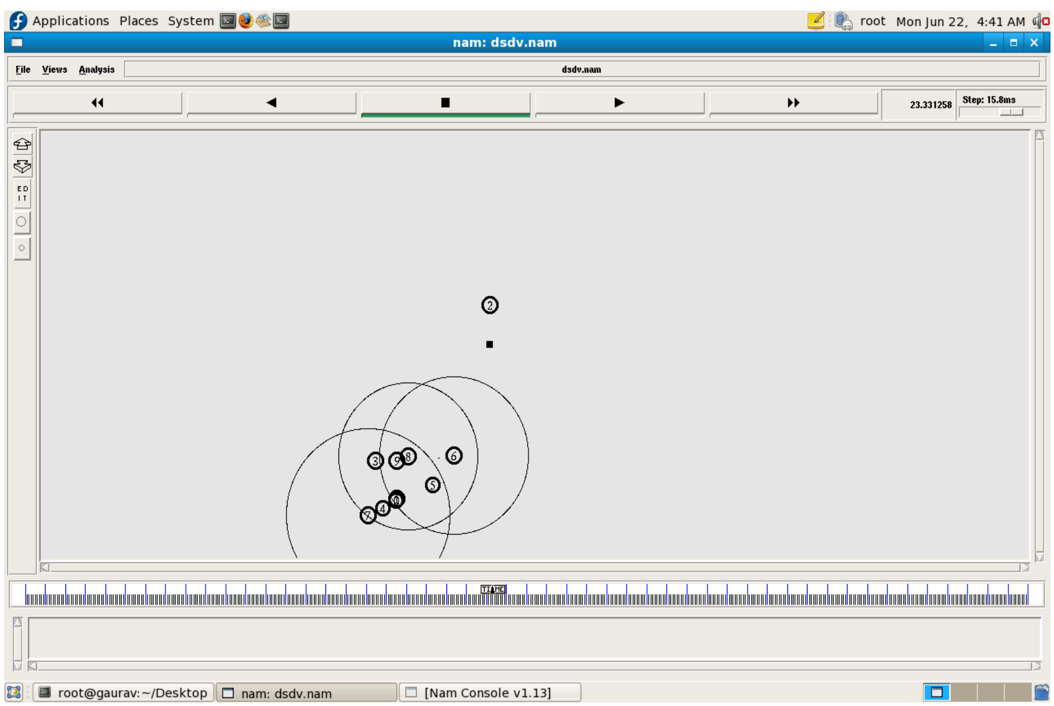


Fig.6.10: DSDV with 10 nodes: Dropping of Packets

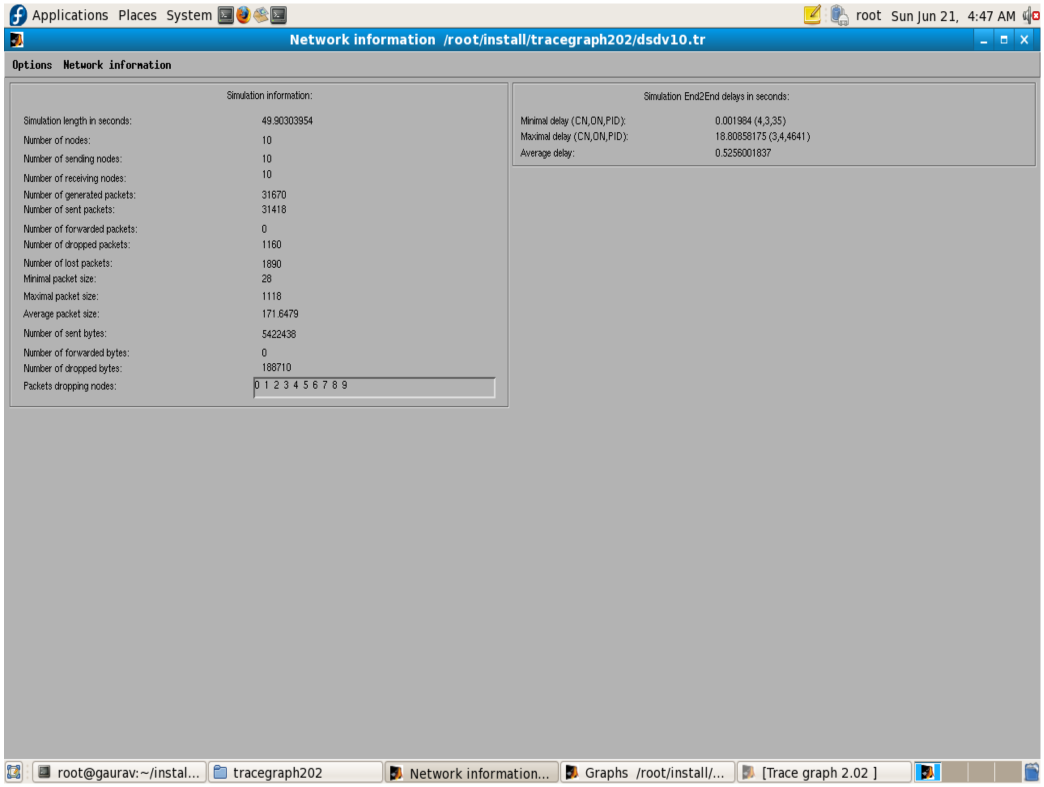


Fig.6.11: Simulation Details (Tracegraph File)

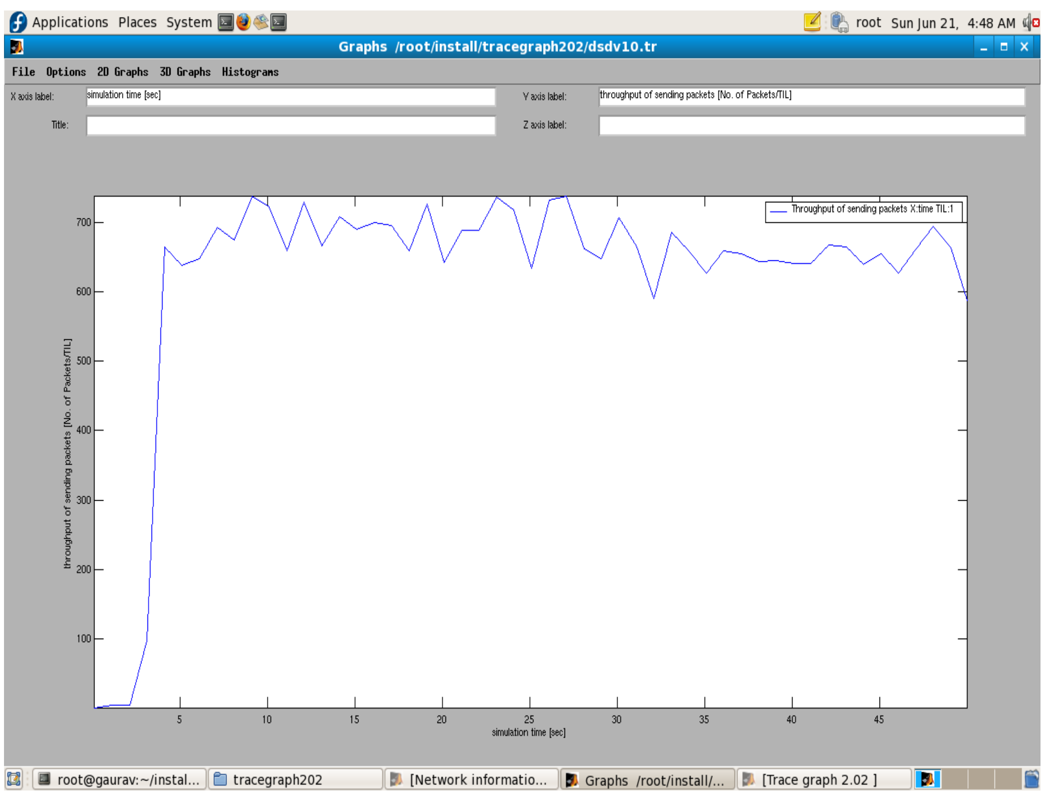


Fig.6.12: Throughput of sent packets v/s simulation time

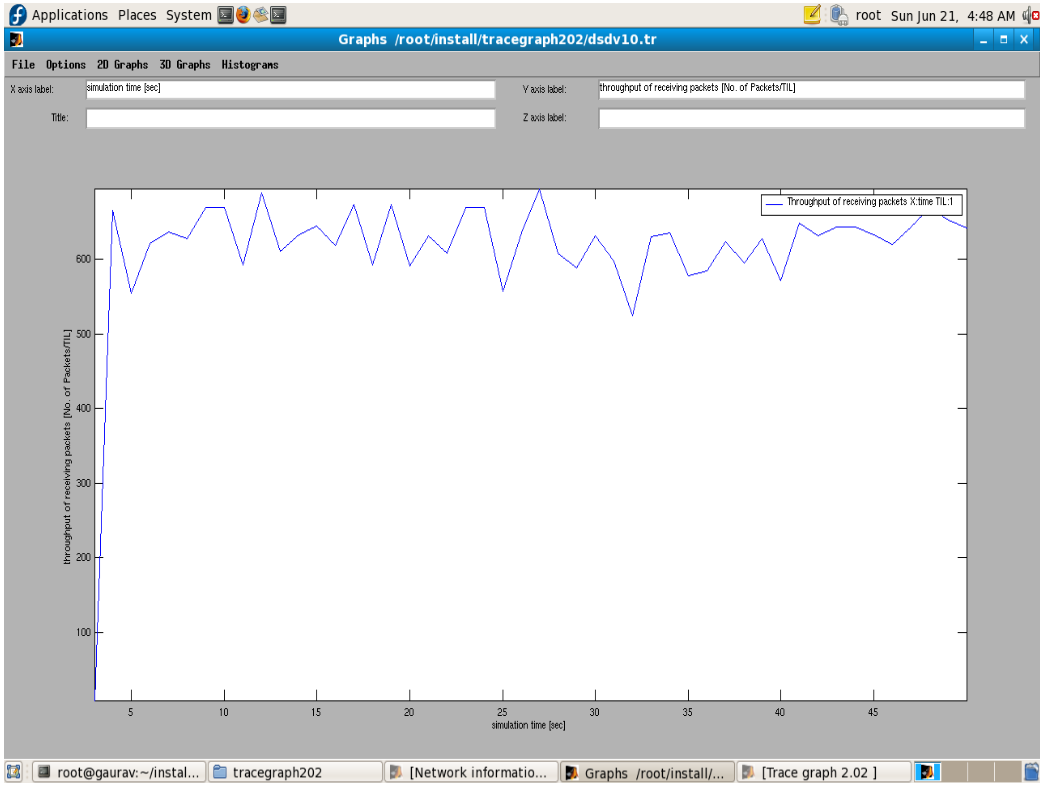


Fig6.13: Throughput of received nodes v/s simulation time

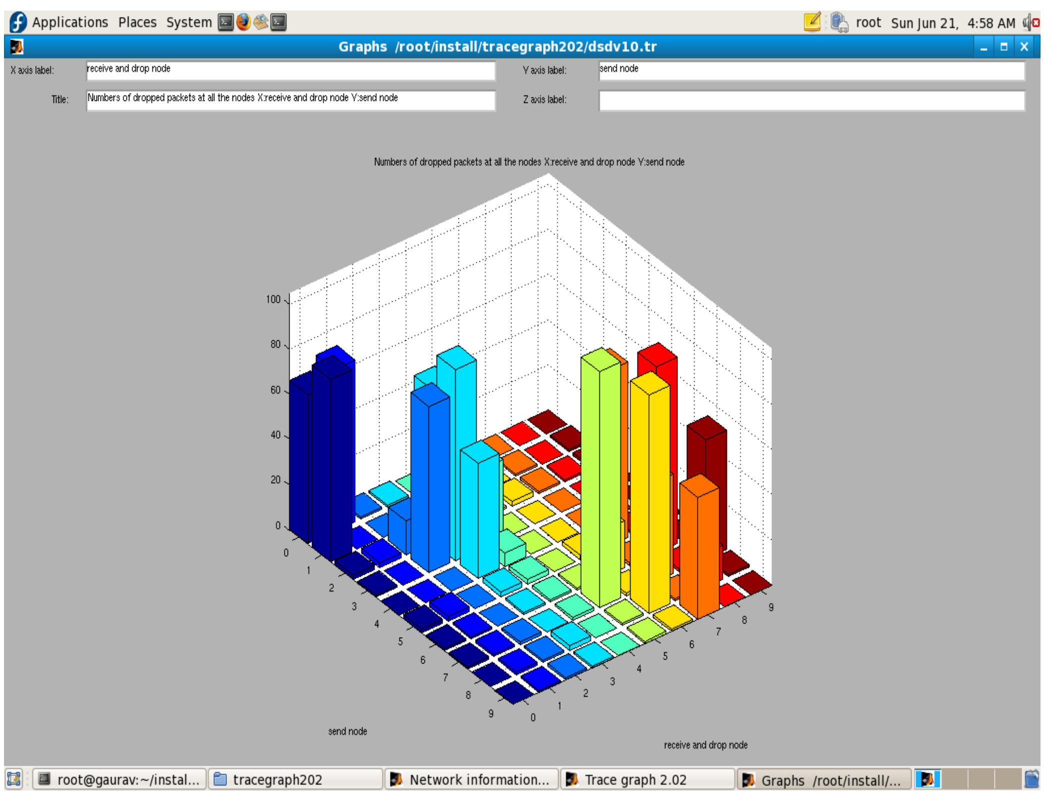


Fig. 6.14: Dropped Packets

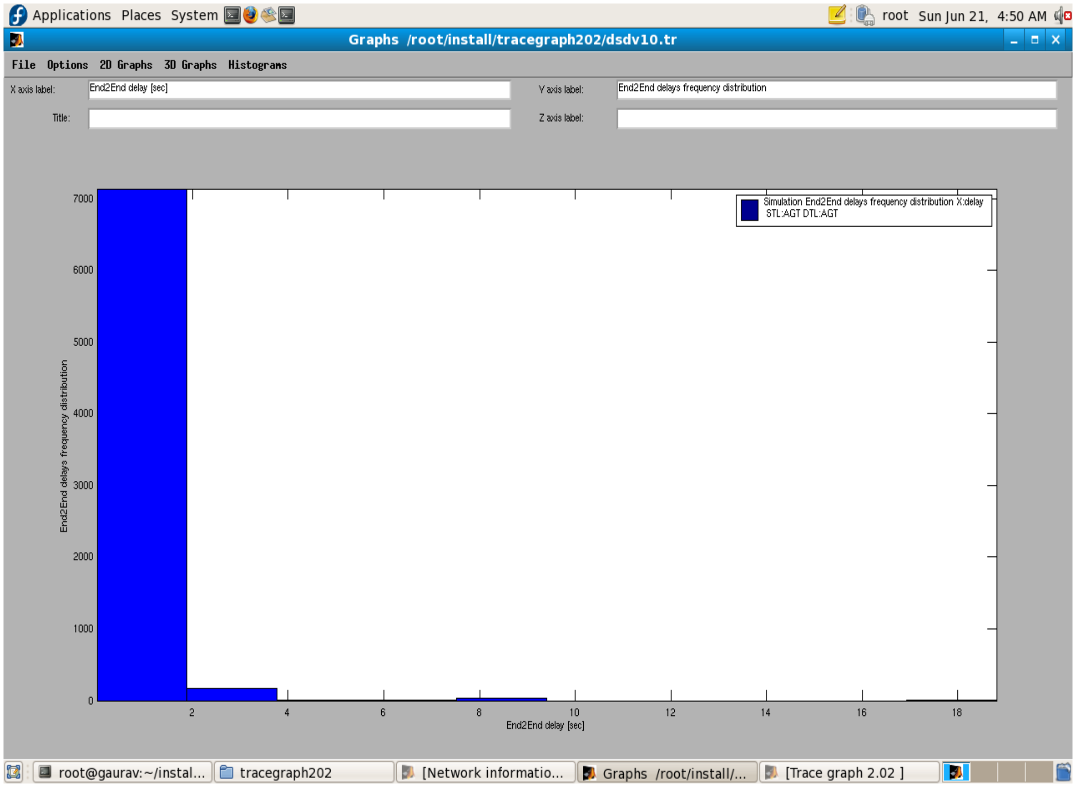


Fig. 6.15: End-to-End Delay: Frequency Distribution

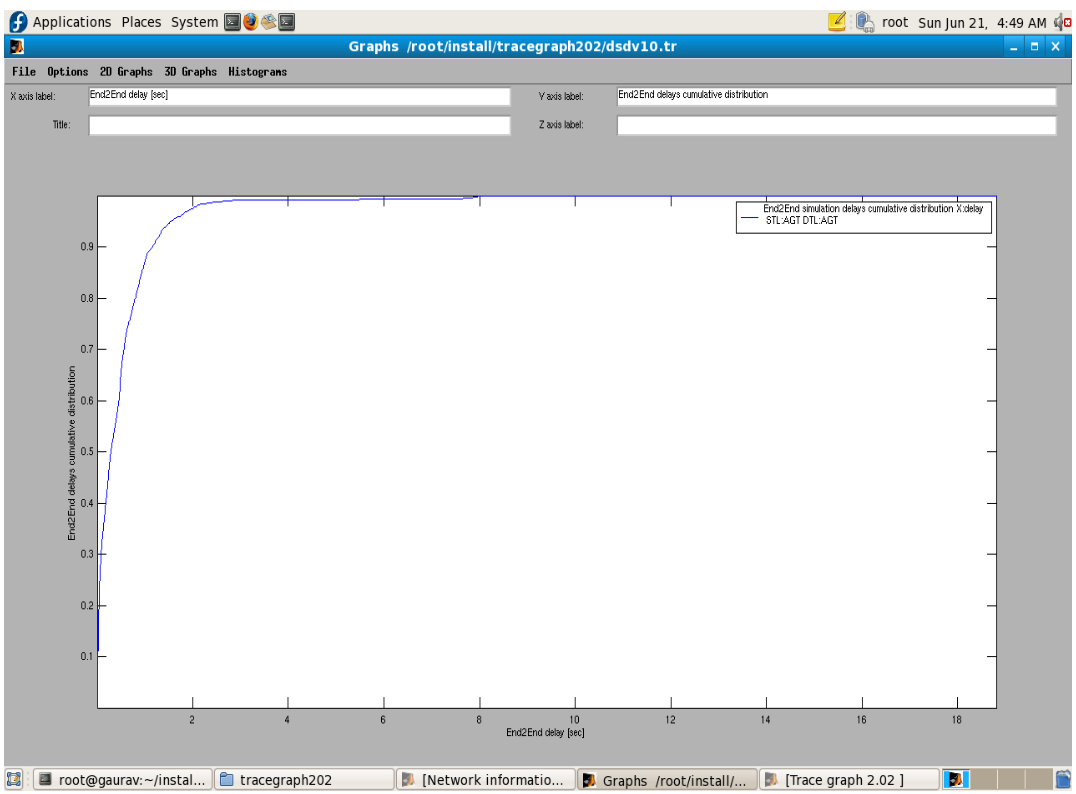


Fig. 6.16: End-to-End Delay: Cumulative Distribution

Fig. 6.15 shows the end-to-end delay frequency distribution. Fig.6.16 shows the end-to-end delay cumulative distribution, which after increasing to maximum, become constant after end-to-end delay of 3 sec.

6.3 Simulation of DSDV with 15 Nodes

After performing the simulation of DSDV protocol with 5 and 10 nodes, we again increases the number of nodes to 15. We consider the parameters like throughput , end-to-end delay, dropped packets, for 15 nodes now.

Fig. 6.17 shows the packets flow between different nodes and route discovery. Fig. 6.18 shows dropping of packets while various nodes change their positions. Fig. 6.19 shows simulation details. In Fig. 6.20 and Fig. 6.21, throughput of sending and receiving packets are shown.

Fig. 6.22 shows 3D graph of the dropped packets. Fig. 6.23 shows the end-to-end delay frequency distribution and end-to-end delay cumulative distribution s shown in fig.6.24.

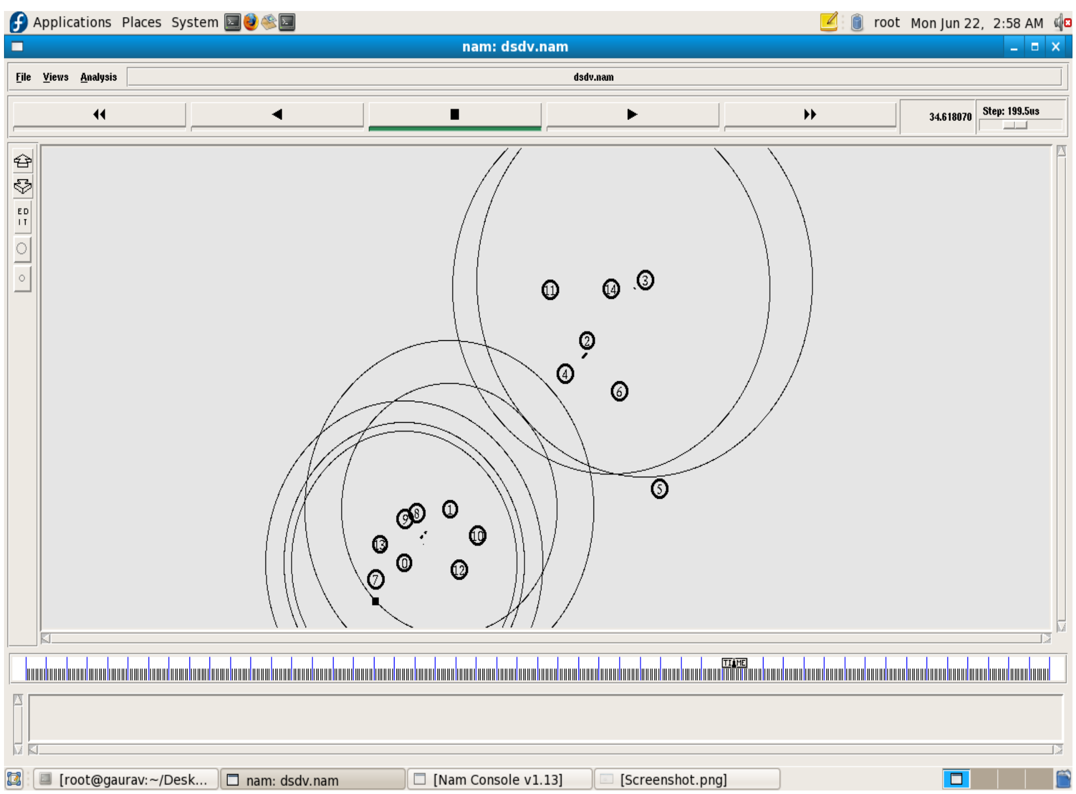


Fig. 6.17: DSDV with 15 nodes: sending and receiving packets and route discovery

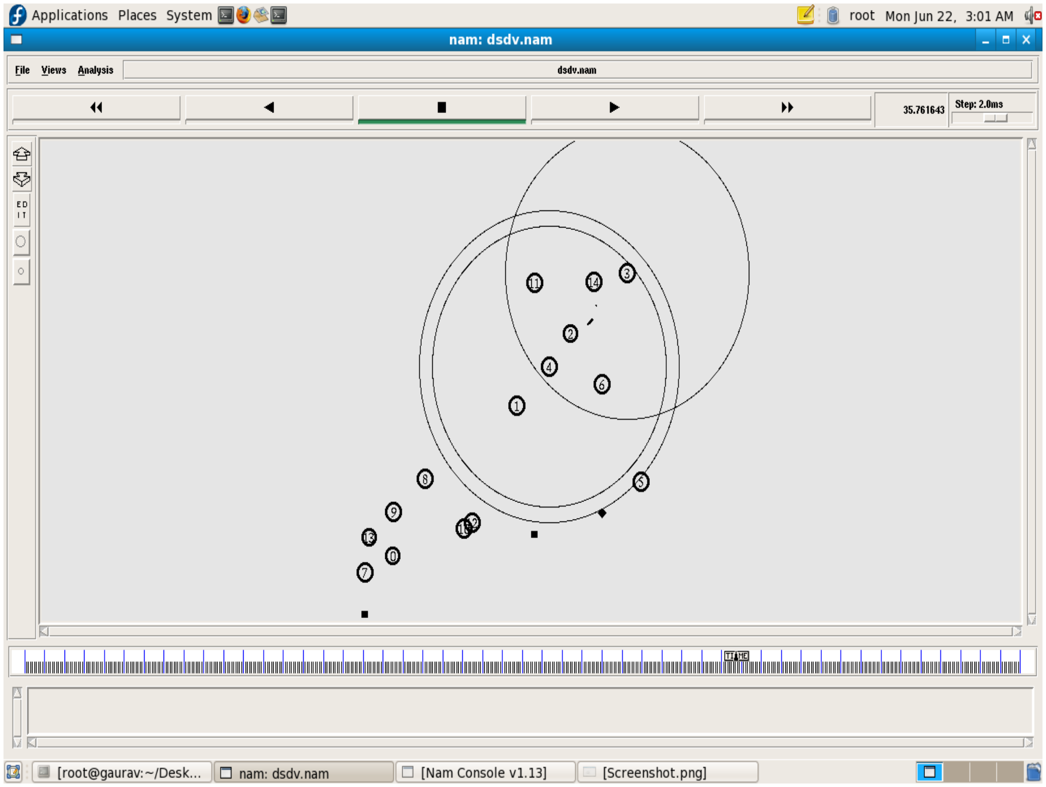


Fig. 6.18 : DSDV with 15 nodes : dropping of packets

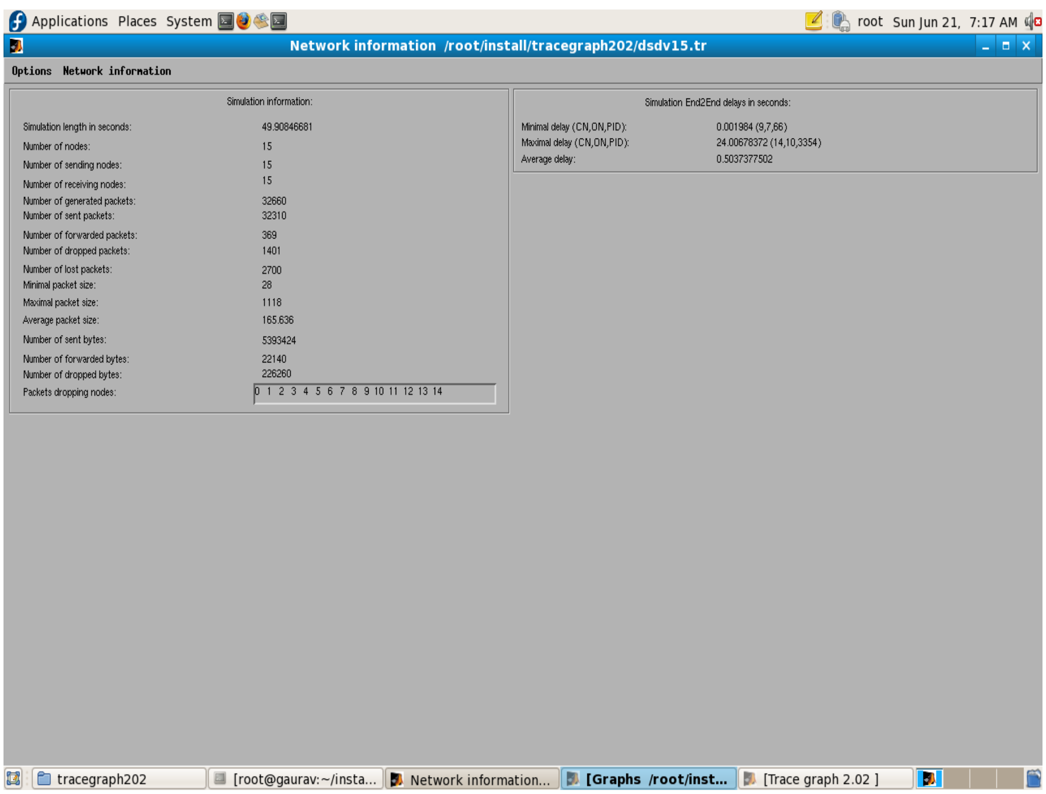


Fig. 6.19 : Simulation Details (Tracegraph File)

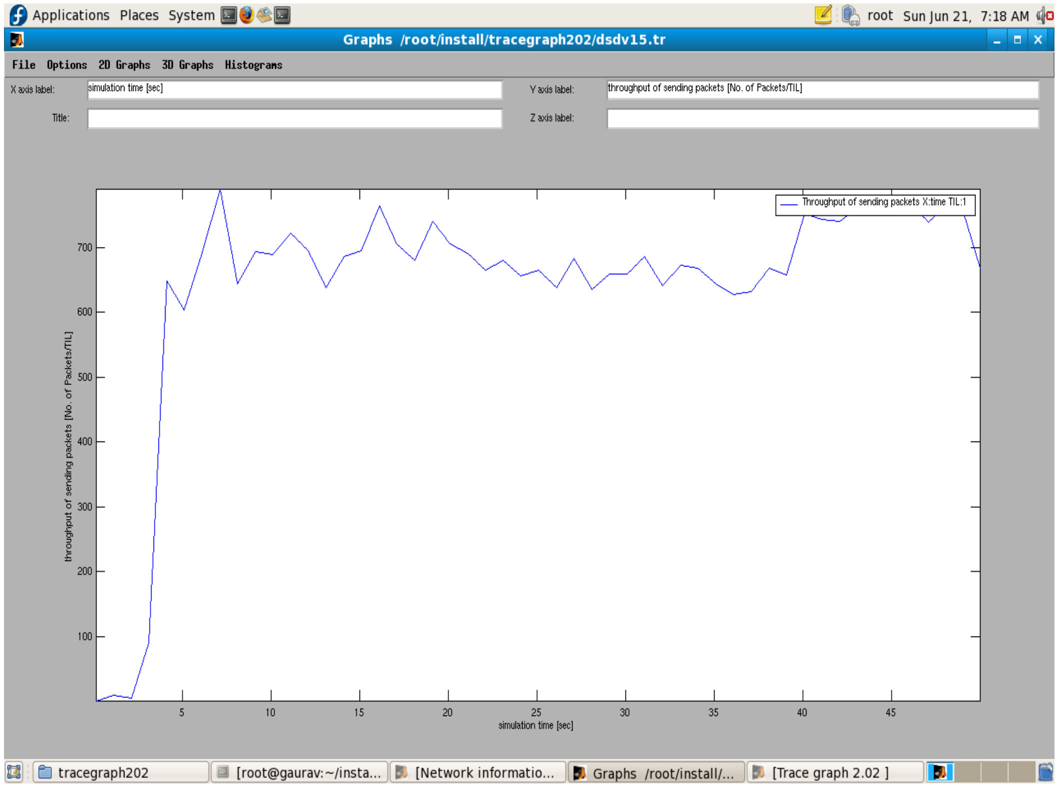


Fig. 6.20 : Throughput of sent packets v/s simulation time

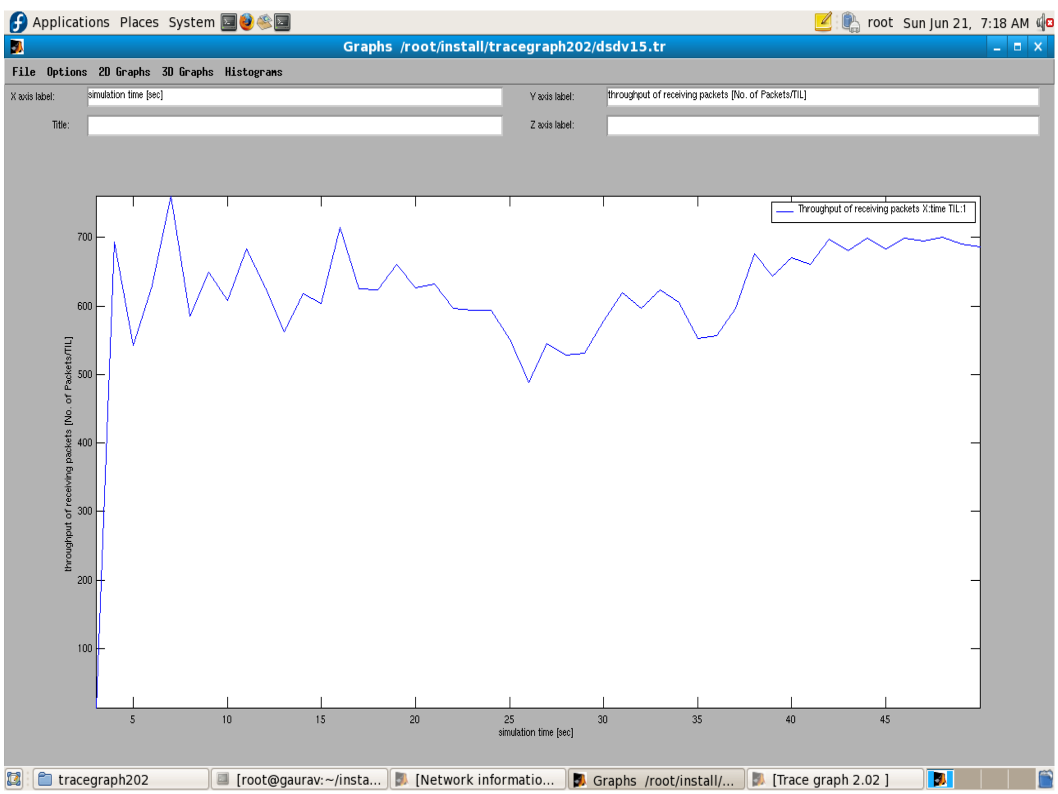


Fig. 6.21 : Throughput of received packets v/s simulation time

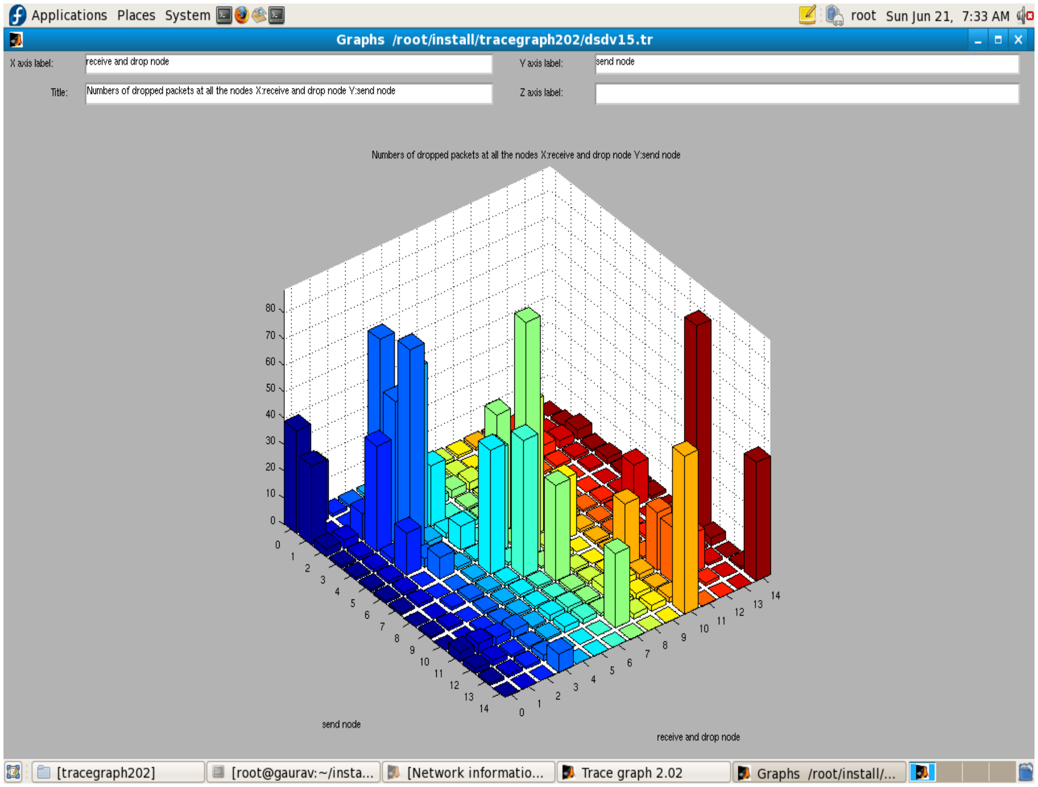


Fig. 6.22: Dropped Packets

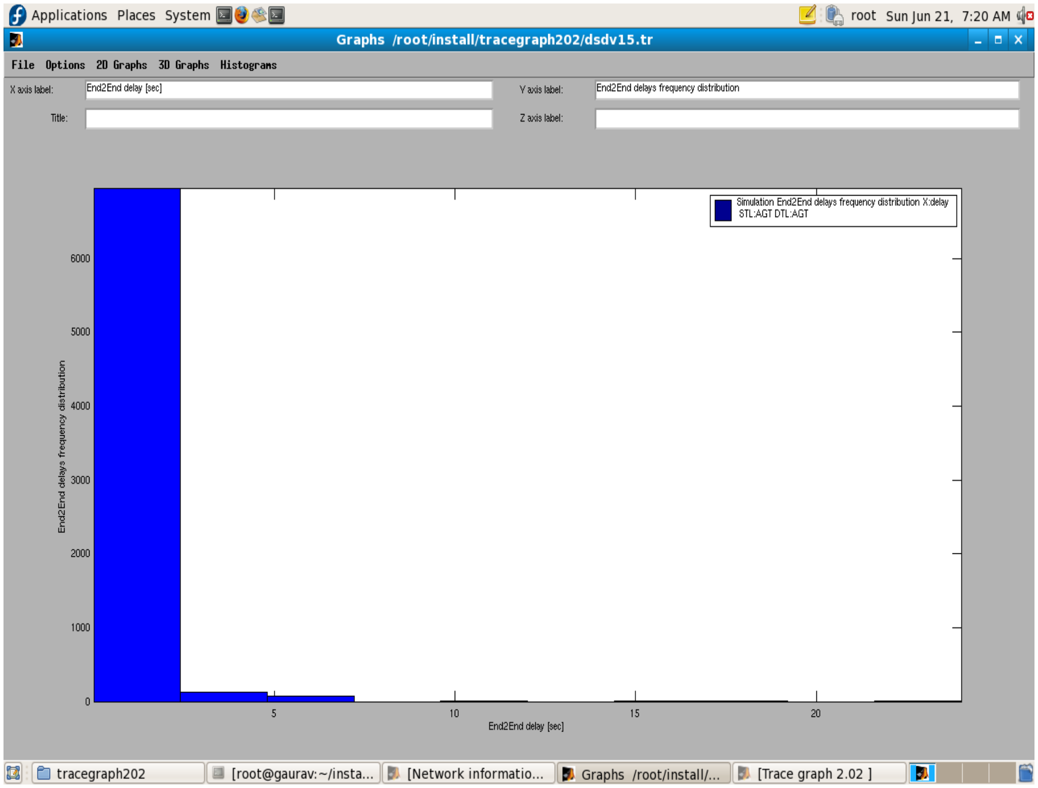


Fig.6.23: End-to-End Delay: Frequency Distribution

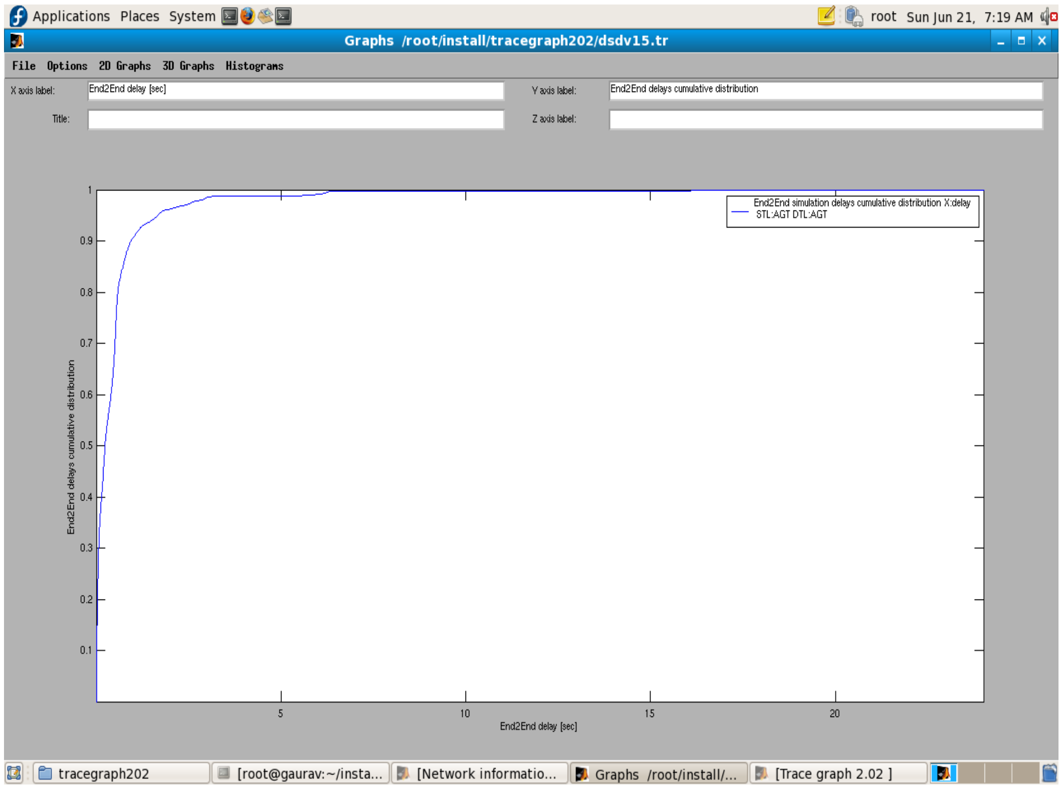


Fig. 6.24: End-to-End Delay: Cumulative Distribution

6.4 Simulation of DSDV with 25 Nodes

Finally, we increase the number of nodes to 25 to perform the DSDV simulation in ns2. The same parameters like throughput, delay are taken. Fig. 6.25 shows the route discovery and sending and receiving packets. Fig. 6.26 shows the dropping of packets. Simulation details are shown in Fig. 6.27.

In Fig. 6.28 and Fig. 6.29, throughput of sending and receiving packets are shown. Fig. 6.30 shows 3D graph of the dropped packets. Fig. 6.31 shows the end-to-end delay frequency distribution and end-to-end delay cumulative distribution as shown in fig.6.32.

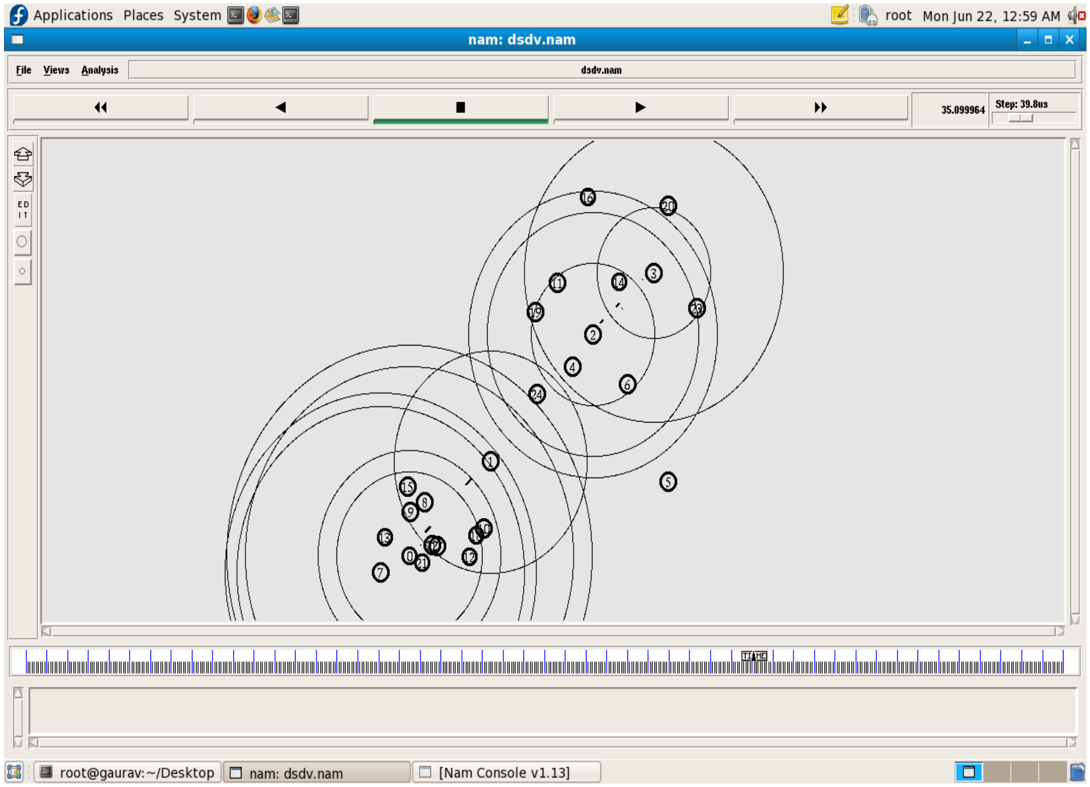


Fig. 6.25: DSDV with 25 nodes: sending and receiving packets and route discovery

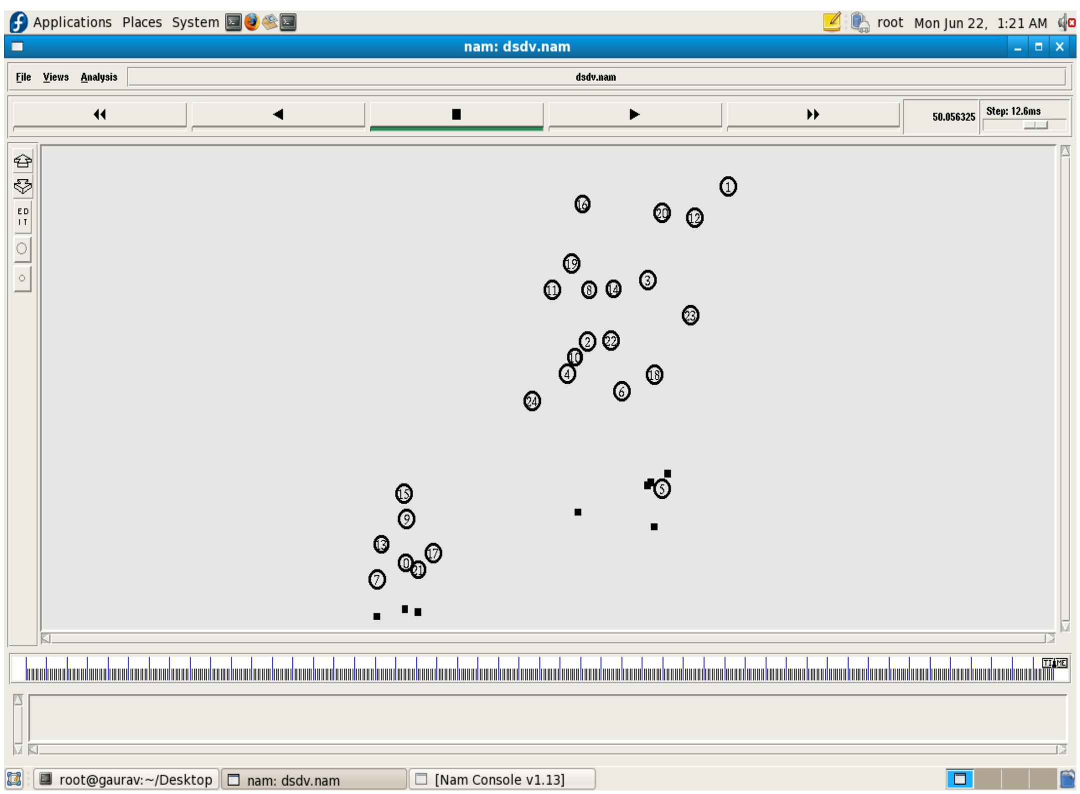


Fig. 6.26: DSDV with 25 nodes : Dropping Packets

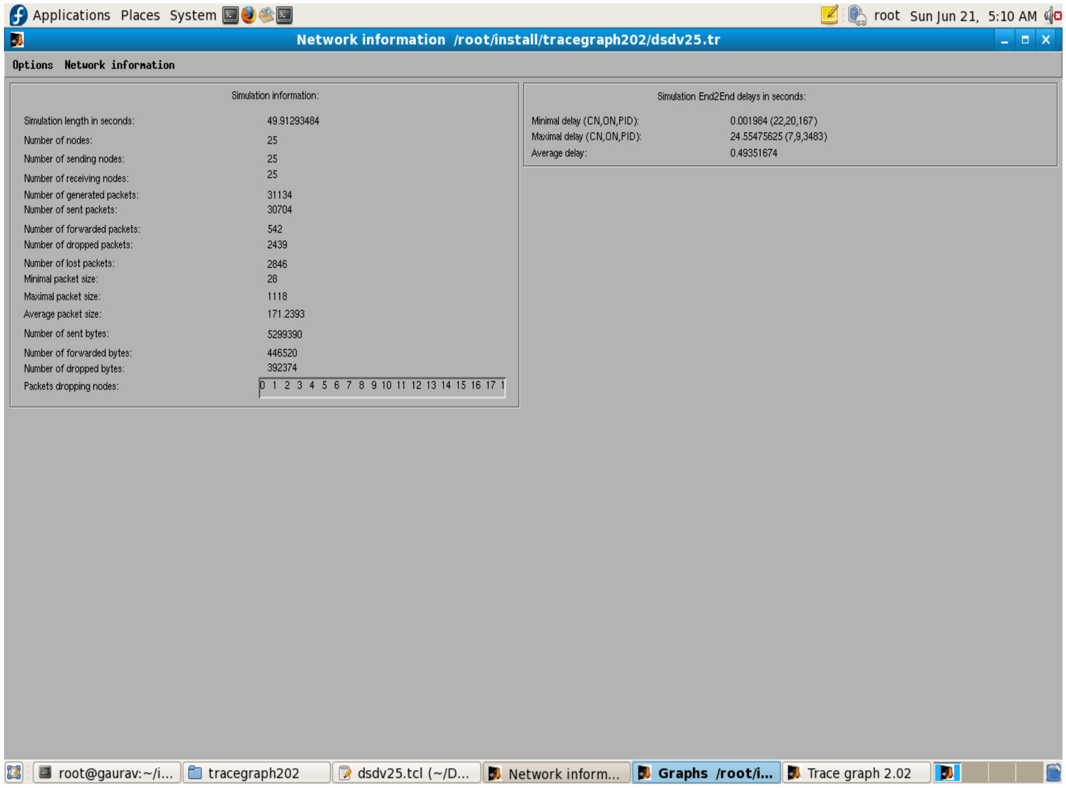


Fig.6.27: Simulation details (Tracegraph File)

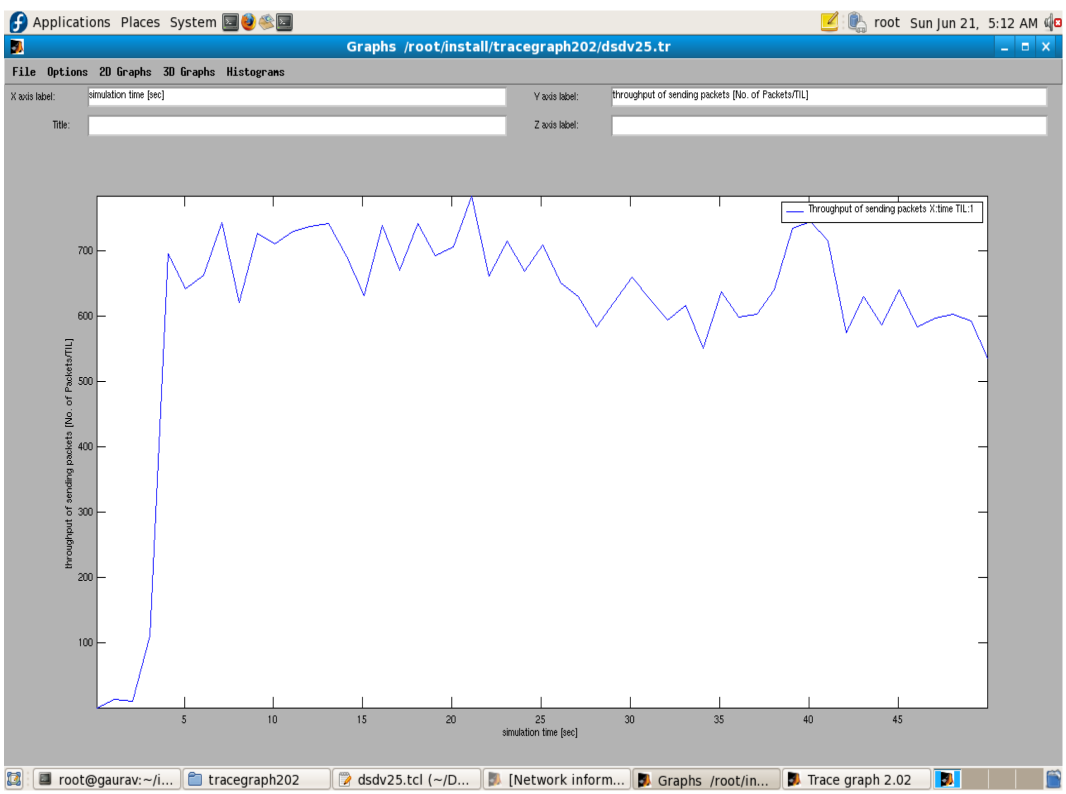


Fig. 6.28 : Throughput of sent nodes v/s simulation time

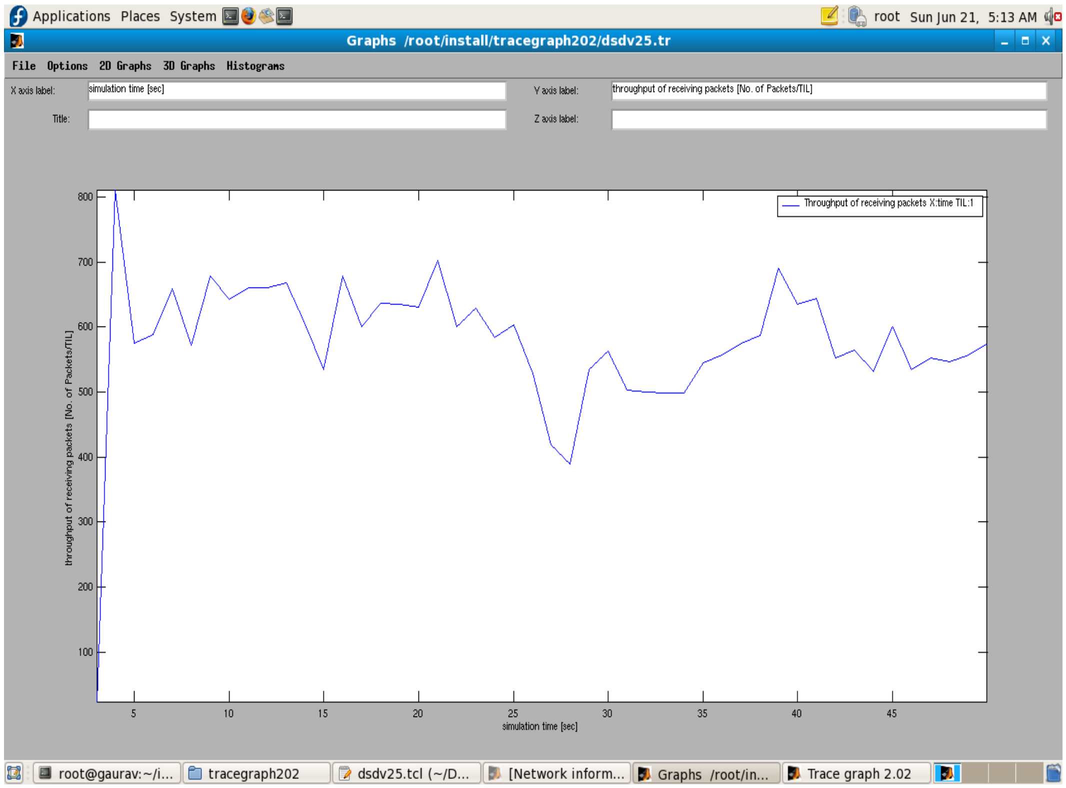


Fig. 6.29 : Throughput of received nodes v/s simulation time

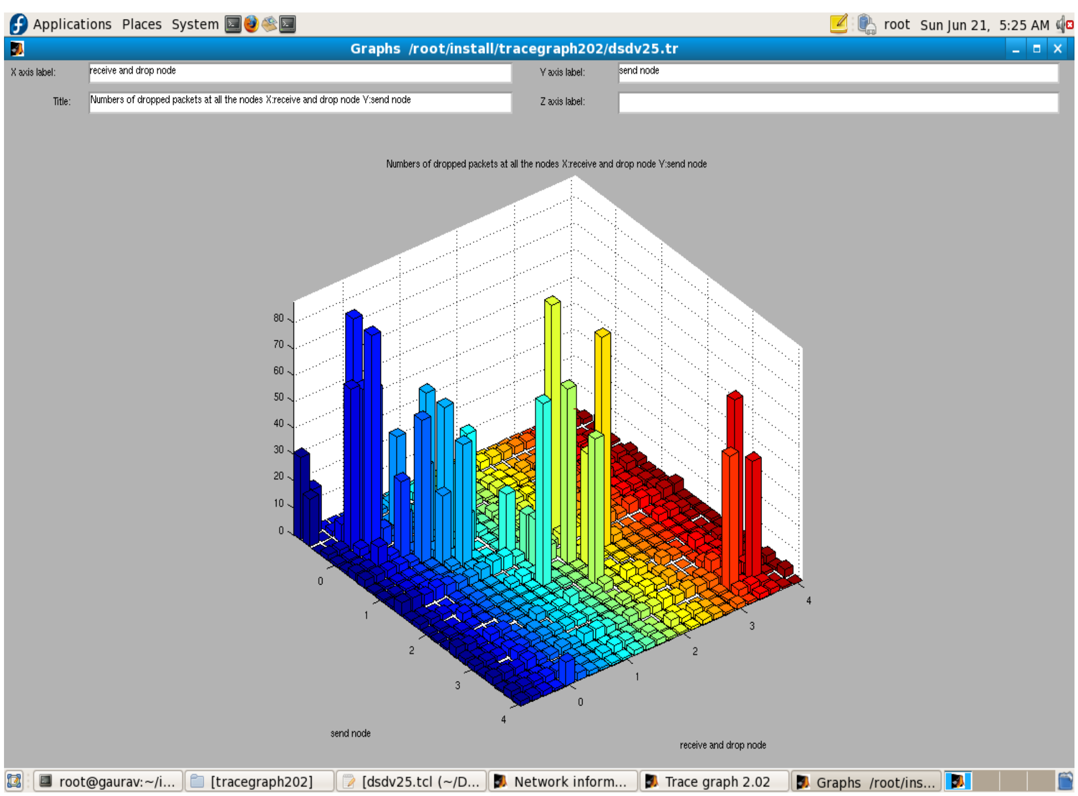


Fig. 6.30 : Dropped Packets

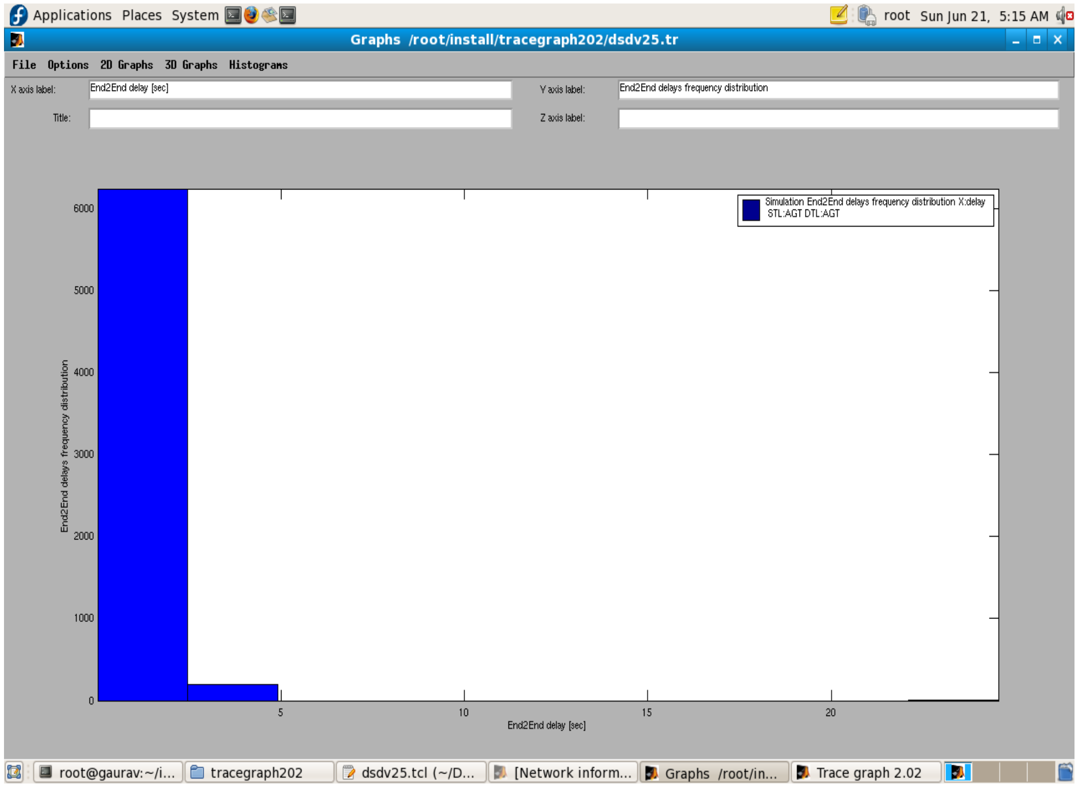


Fig. 6.31: End-to-End Delay : Frequency Distribution

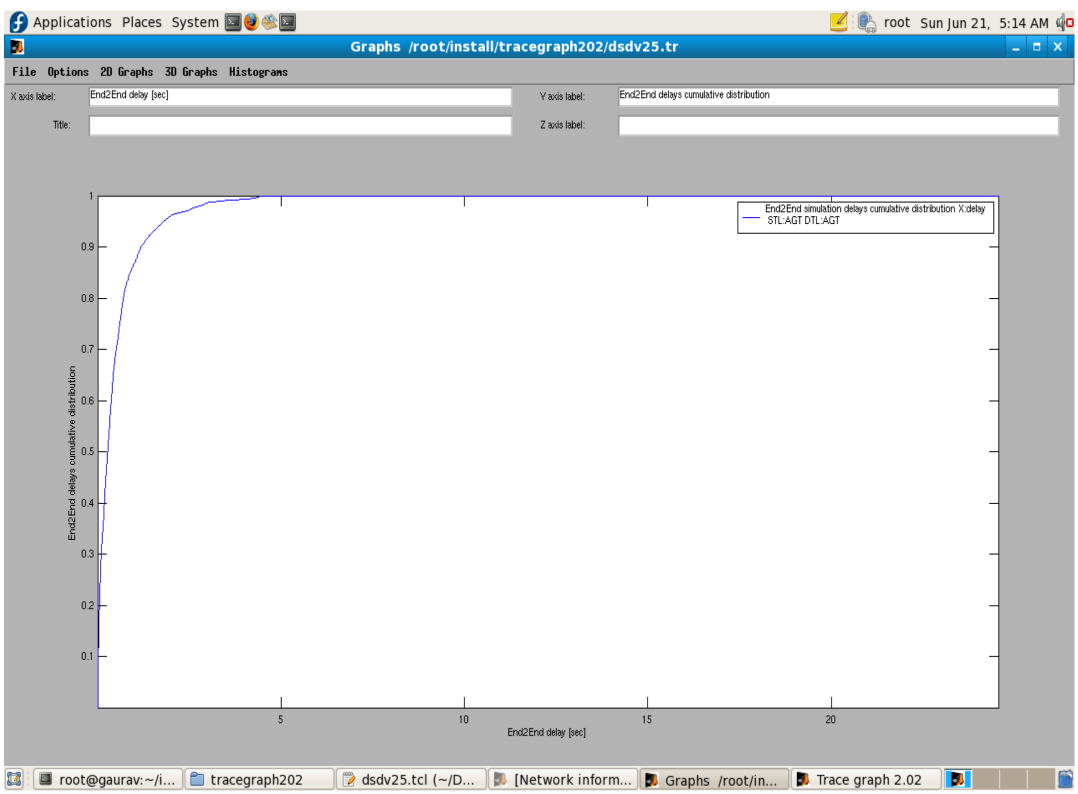


Fig. 6.32 : End-to-End Delay : Cumulative Distribution

6.5 Comparison of Performance of DSDV based upon Number of Nodes

As we increase the number of nodes for performing the simulation of DSDV protocol, number of sent and delivered packets changes, which in turn changes the throughput and average end-to-end delay. Throughput is defined as the ratio of data delivered to the destination to the data sent out by the sources. Average end-to-end delay is the average time a packet takes to reach its destination. The table 6.1 shows the difference between sent packets, received packets, lost and dropped packets, average end-to-end delay when number of nodes is increased.

Packet Size---------------------- 512

Simulation Time---------------- 50 sec

Table 6.1: Comparison of Various Parameters v/s No. of Nodes

No. of Nodes / Parameters	5	10	15	25
Packets Sent	31233	31418	32310	30704
Packets Lost	2392	1890	2700	2846
Packets Dropped	617	1160	1401	2439
Packets Delivered	28224	28368	28209	25419
Throughput	0.904	0.902	0.873	0.827
Average end 2 end delay	0.381	0.525	.504	0.493

Fig.6.33 shows total number of packets sent vary with increasing number of nodes. As the number of nodes goes on increasing, the packets sent first increases then decreases.

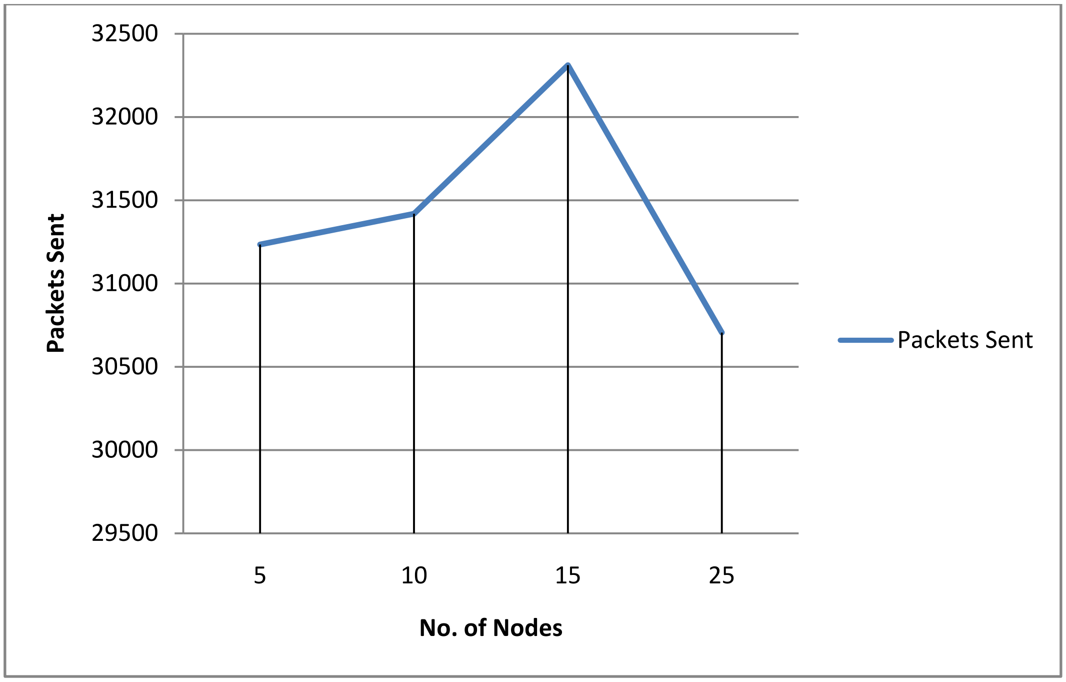


Fig.6.33: Packets Sent v/s No. of Nodes

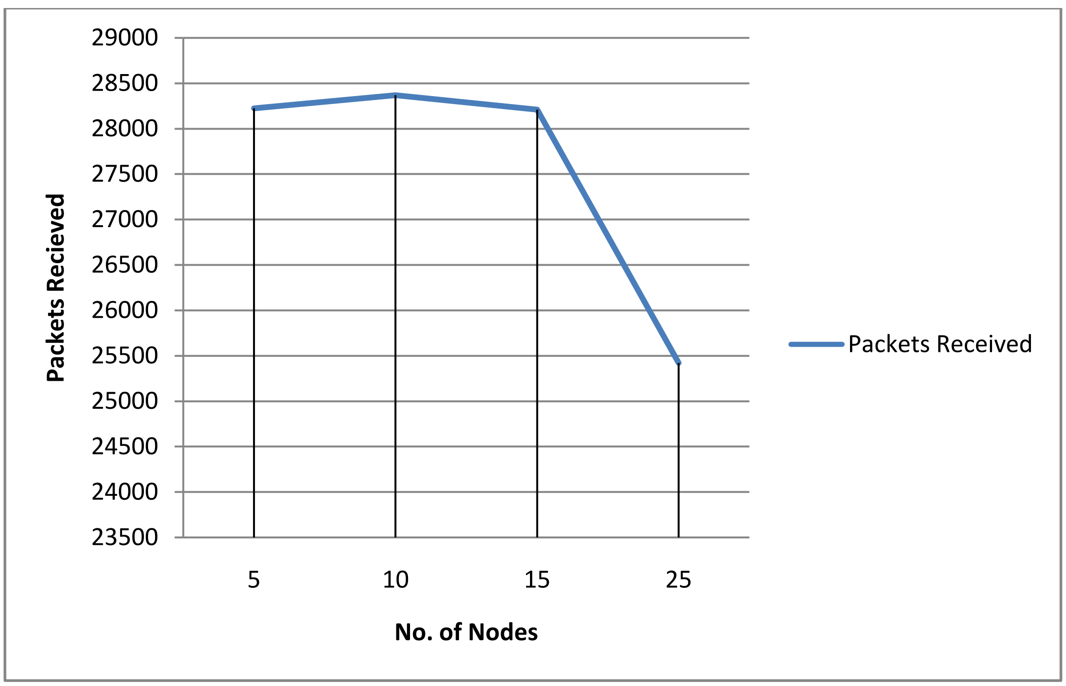


Fig.6.34: Packets Received v/s No. of Nodes

Fig.6.34 shows total number of packets received with increasing number of nodes. As there are more number of nodes, the number of packets received becomes much less, i.e., number of packets lost and dropped increased.

Fig. 6.35 shows the graphical representation of throughput versus number of nodes of DSDV protocol. From the figure and the table above, we came to know that as the number of nodes increases, the throughput of DSDV protocol decreases from 0.904 to 0.827. This means that the packet delivery ratio goes on decreasing when numbers of nodes are increased in DSDV protocol.

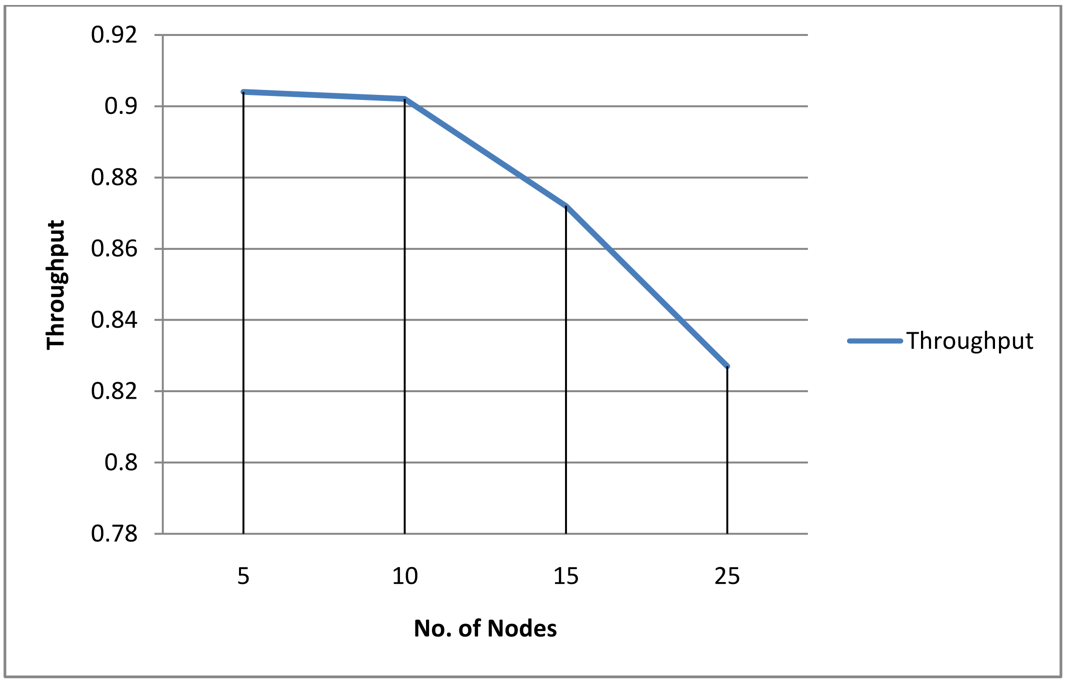


Fig. 6.35: Throughput v/s No. of Nodes

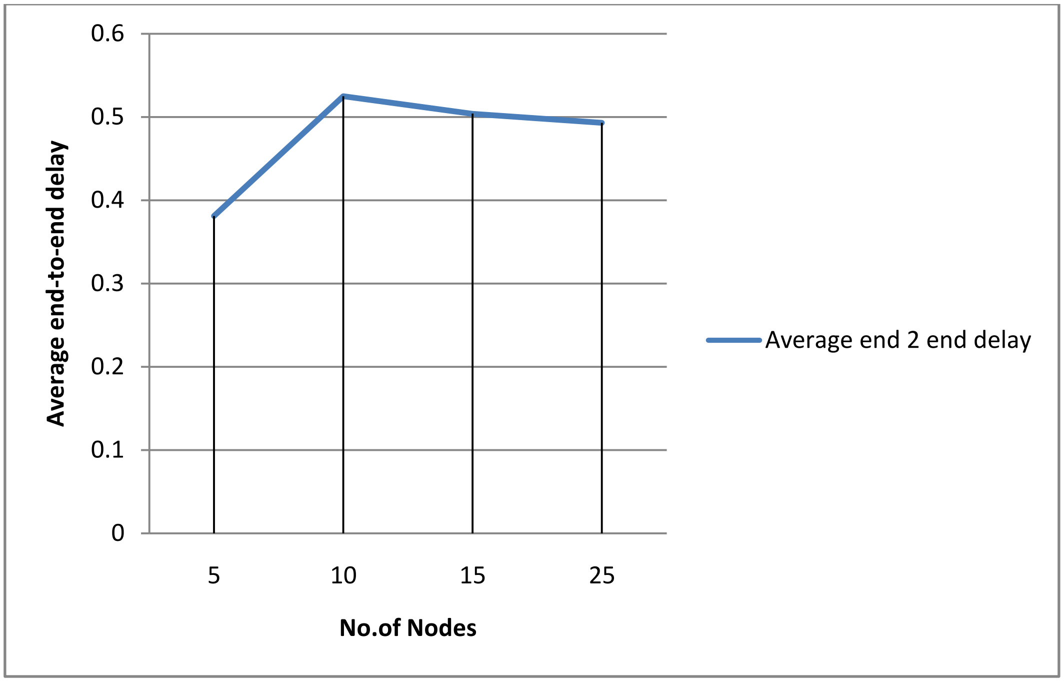


Fig. 6.36: Average End-to-End Delay v/s No. of Nodes

Fig. 6.36 shows the average end-to-end delay graph plotted against number of nodes. Average end-to-end delay, at the starting increases when numbers of nodes are increased to 10 from 5, but after that decreases as we further increase the number of nodes to 15 and 25. This means that the average time to reach its destination taken by a packet is decreased as the number of nodes increases. That is, more the number of nodes, less time will be taken by a packet to reach its final destination from the source.

CHAPTER 7

CONCLUSION & FUTURE SCOPE

Routing is a significant issue in Mobile Ad hoc Networks. The objectives listed in the problem statement have been carried out properly. In the presented work, the performance of DSDV is studied against various parameters such as, packets sent, packets received, throughput, and average end-to-end delay while increasing the number of nodes. We sincerely hope that our work will contribute in providing further research directions in the area of routing.

Our analysis of the result guides us to conclude that:

-- Numbers of packets sent are first increases and then goes on decreasing as the numbers of nodes are increased.

-- With the increase in number of nodes, number of packets received goes on decreasing.

-- Number of lost packets and dropped packets goes on increasing with the increase in number of nodes.

-- The throughput of the DSDV protocol decreases with the increase in number of nodes. The ratio of packets delivered to packets sent is low when the number of nodes is large.

-- The average end-to-end delay i.e. the average time that a packet takes to reach its destination is less for large number of nodes. DSDV behaves well in terms of average delay when number of nodes is increased.

In the presented work, we have made a simulation study; it would be interesting to note and analyze the behaviour of a MANET on a real-life test-bed. Further, we can also investigate the behaviour of other proactive routing protocols such as – FSR, OLSR and TBRPF.

[1] Sarangapani, Jagannathan, “Wireless ad hoc and sensor networks: Protocols, Performance and Control”, CRC Press.

[2] 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.

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

[4]C. Shen, C. Srisathapornphat and C. Jaikaeo, “Sensor Information Networking Architecture and Applications,” IEEE Pers. Commun., pp. 52-59, Aug. 2001.

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

[6] W. Richard Stevens, “TCP/IP Illustrated, Volume 1: The Protocols”, Addison Wesley Professional 1994 / 0-201-63346-9 /

[7] P Calhoun and C Perkins, “Mobile IP Network Access Identifier Extension for IPv4,” RFC 2794, March 2000

[8] Xiaoyan Hong, Kaixin Xu, and Mario Gerla. “Scalable routing protocols for mobile ad hoc networks”, 2002.

[9] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz, “A review of routing protocols for mobile ad hoc networks”, Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia, 2003.

[10] Laura Marie Feeney, “A taxonomy for routing protocols in mobile ad hoc networks”, Technical report, Swedish Institute of Computer Science, Sweden, 1999.

[11] Jochen Schiller, “Mobile Communications”, Addison-Wesley, 2000.

[12] Elizabeth M. Royer and Chai-Keong Toh, "A review of current routing protocols for ad hoc mobile wireless networks", Technical report, University of California and Georgia Institute of Technology, USA, 1999.

[13] 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.

[14] Dr. Uwe Roth, "Highly dynamic destination-sequenced distance-vector routing",http://wiki.uni.lu/secan-lab/Highly+Dynamic+Destination-Sequenced+Distance-Vector+Routing.html.

[15] P. Jacquet, P. Muhlethaler, A. Qayyum, A. Laouiti, L. Viennot and T. Clausen, "Optimized Link State Routing Protocol", Internet Draft, IETF MANET Working Group, draft-ietf-manet-olsr-04.txt, Mar. 2002.

[16] R. G. Ogier, F. L. Templin, B. Bellur, M. G. Lewis, "Topology Broadcast Based on Reverse-Path Forwarding (TBRPF)", Internet Draft, IETF MANET Working Group, draft-ietf-manet-tbrpf-05.txt, Mar. 2002.

[17] G. Pei, M. Gerla, and T.-W. Chen, "Fisheye State Routing in Mobile Ad Hoc Networks", Proceedings of Workshop on Wireless Networks and Mobile Computing, Taipei, Taiwan, Apr. 2000.

[18] Perkins, C.E., and P. Bhagwat, "Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers:, Computer Communications Review,1994, pp. 234–244.

[19] P. F. Tsuchiya, "The Landmark Hierarchy: a new hierarchy for routing in very large networks", Computer Communication Review, vol.18, no.4, Aug. 1988, pp. 35-42.

[20] Ching -Chuan Chiang, Hsiao-Kunag Wu, Winston Liu and Mario Gerla, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," IEEE Singapore International Conference on Networks, SICON'97, pp. 197-211, Singapore, 16.-17. April 1997, IEEE

[21] Dimitri P. Bertsekas (March 1992). "A Simple and Fast Label Correcting Algorithm for ShortestPaths"(PDF).Networks,Vol.23,pp.703-709,1993. http://www.mit.edu/people/dimitrib/SLF.pdf. Retrieved on 2008-10-01.

[22] Robert Sedgewick, "Algorithms in Java", Third Edition. ISBN 0-201-36121-3. Section 21.7: Negative Edge Weights. http://safari.oreilly.com/0201361213/ch21lev1sec7

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

[24] Charles E. Perkins, Pravin Bhagwat, "Highly Dynamic Destination-Sequenced Distance Vector Routing (DSDV) for Mobile Computers", http://www.cs.virginia.edu/~cl7v/cs851-papers/dsdv-sigcomm94.pdf

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

[26] Marc Greis. *Ns Tutorial*. http://www.isi.edu/nsnam/ns/tutorial/index.html

[27]S.McCanne and S.Floyd,"*Network Simulator",* http://www.isi.edu/nsnam/ns/

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

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

TO BE PUBLISHED

- Jyotsna Rathee, Vivek Kumar and Dr. A.K.Verma, "*Comparison of Performance of Wireless Mobile Ad-hoc Network Routing Protocols",* National Conference (EPPCSIT-09), Jalandhar, Punjab, Sept. 4-5, 2009.

COMMUNICATED

- Jyotsna Rathee and Dr. A.K.Verma, "*Simulation and Analysis of DSDV Protocol in MANETS*", International Journal of Information Technology and Knowledge Management (IJITKM) , Kurukshetra University, Kurukshetra, India.