INVESTIGATING THE PERFORMANCE OF SELECTED MANET ROUTING PROTOCOLS

by

Oluwatola Ayansiji

Bachelor, Computer Information System

Babcock University, 2010

Report Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Computer Science

in the Graduate Academic Unit of Computer Science

Supervisor(s): Przemyslaw R. Pochec, PhD, Computer Science

John DeDourek, PhD, Computer Science

Examining Board: Wei Song, PhD, Computer Science, Chair

Rodney Cooper, PhD, Computer Science

This report is accepted by the

Dean of Graduate Studies

MAY, 2015

THE UNIVERSITY OF NEW BRUNSWICK

ABSTRACT

A mobile ad hoc network is a dynamic and autonomous system of self-organized nodes operating without infrastructure support. MANET's topology is dynamic and can change rapidly because nodes move constantly, making the properties of such a network difficult to predict. To facilitate communication among active nodes on the network, a routing protocol is used to determine routes for forwarding data packets. A routing protocol plays an important role for the overall performance of MANETs. In this report we investigate and compare the performance of three well known routing protocols DSR, AODV and DSDV by using a number of performance metrics including the hop count, delivery ratio, end to end packet delay and node utilization. The report also discusses and analyses the impact of hypothetical Denial of Service security attacks on MANETs. The performance analysis is done using the simulation tool NS2. The experiments show that on-demand protocols AODV and DSR seem to outperform proactive protocols like DSDV.

DEDICATION

This report is dedicated to my parents for their immense support and to God for the grace his giving me to accomplish this.

ACKNOWLEDGEMENT

It's with pleasure and gratitude I thank my supervisors Prof J. Dedourek and Dr. P. Pochec for their immense contributions, assistance and guidance. This report would not have been completed without their insights and expertise.

I do like to thank my colleagues, friends for the encouragement, support and assistance. I sincerely thank you all.

Lastly to my parents thank you for the financial support and to my siblings thank you for the moral support.

Table of Contents

List of Tables

List of Figures

List of Symbols, Nomenclature or Abbreviations

AGT	Agent Traces
AODV	Ad-Hoc on Demand Vector
CBR	Constant Bit Rate
CIDR	Classless Inter-Domain Routing
CMU	Carnegie Mellon University
DoS	Denial of Service
DSDV	Destination Sequence Distance Vector
DSR	Dynamic Source Routing
IP	Internet Protocol
MAC	Medium Access Control
MANET	Mobile Ad hoc Network
QoS	Quality of Service
RREP	Route Reply
RREQ	Route Request
RTR	Reliable Transaction Router
RWP	Random Waypoint Mobility models
RWPM	Random Waypoint Model
TCL	Tool Command Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WLAN	Wireless Local Area Networks

WMN	Wireless Mesh Networks
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network

Chapter 1

Introduction

1.1 Introduction

In areas in which there is little or no communication infrastructure or where the existing infrastructure is expensive or inconvenient to use, wireless mobile users may prefer to communicate through an ad hoc network [1]. An ad hoc network is comprised of a set of mobile nodes that are connected using wireless links. These nodes can communicate and share information without a central facilitated infrastructure. Nodes in an ad hoc environment are not always stationary, but most are mobile. Hence, the network topology (the physical connectivity of communication in a network) keeps changing [2].

The hosts in an ad hoc network move according to various patterns; to make communication possible between active nodes a routing protocol is used to find path(s) to be followed by data packets, from source to destination nodes. A central challenge in the design of ad hoc networks is the development of dynamic routing protocols that can efficiently find routes between two communicating nodes [3]. Hence the performance of a routing protocol in a mobile ad hoFc network (MANET) is important.

The purpose of routing protocols is to establish the shortest, correct and most efficient route between a pair of nodes. However, not all routing protocols developed perform well in a given situation; hence factors affecting routing protocols require thorough investigation. Factors such as mobility, throughput, network size, delivery ratio, and delay, bandwidths, and signal strength and path length do affect the performance of MANET routing protocols.

1.2 Background

A routing protocol is a principle or a standard that controls how nodes come to agree in the way to route packets (using multi-hops) between computing devices in a network. Communications and formalizing agreement among nodes is crucial to the overall performance of a MANET [4]. Recently there has been a renewed interest in this field due to the common availability of low-cost laptops and palmtops with wireless interfaces. Interest is also partly fueled by growing enthusiasm in running common network protocols in dynamic wireless environments without the requirement of specific infrastructures [3].

MANETs are being extensively deployed currently since they provide features that conventional networks find impossible or difficult to emulate. A MANET uses mobile nodes to support basic networking functions like packet forwarding, routing and network management, and all these functions are carried out by all available nodes [5]. The dynamic nature of MANETs also brings about drawbacks in regards to communication link formation. The movement of nodes causes uncertainty of when nodes disappear and reappear from the network communication range, causing highly variable message delays [6]. The use of a large number of independently operating, forwarding nodes without central control, may also lead to security problems. These factors have an impact on the performance of routing protocols in MANETs.

1.3 Objectives

The research objective is to investigate and analyze the performance of reactive and proactive routing protocols in terms of their average throughput, average delay, route formation (length, frequency of changes) path length, node utilization and packet delay. Factors like node density, distance source/destination and node movement pattern/speed are considered. For the investigation portion, we compare the routing protocols using selected parameters to determine the network performance. The performance of these protocols is analyzed with the NS2 simulator. The comparison considered is with respect to these three major protocols: DSDV, DSR, and AODV. A scenario modeling a network security breach is investigated. The focus is on the evaluation of network performance in terms of a Denial of Service (DoS) attack by the introduction of rogue nodes that might affect global throughput and delay in a mobile ad hoc network operation. The rogue nodes simply try to disable the network by sending lots of DoS data.

1.4 Report Organization

Chapter 1 gives an introduction. Chapter 2 and Chapter 3 present background material. In Chapter 2, the literature on MANET routing protocols is presented. Chapter 3 describes the simulation tool. Chapter 4 describes the research methodology adopted. The experimental designs, investigation and experimental results carried out are described in Chapter 5. The conclusions and proposed improvement are presented in Chapter 6.

Chapter 2

Ad Hoc Networks

This chapter gives a brief background about MANET networks including the details of the common routing protocols used in MANETs. Additionally, various existing mobility models for MANETs are discussed.

2.1 Networking

A network is a group of two or more computers and other devices linked together by communication channels that allow sharing of information and data [7]. Networked computing devices pass data to each other along data connections; data is transferred in the form of packets. The connections between nodes are established using either cable media or wireless media.

Network communication can be divided into two main categories:

- Wired Networks,
- Wireless Networks.

Wireless networks are networks that have a number of devices connected to each other without any kind of cables to deliver the data packets. A wired network connects devices using cables. Wired networks can be created within limited area by using cables and routers that allow the sending and receiving of data. The most common wired networks use cables connected to Ethernet ports on the network router on one end, and to a computer or other device on the cable's opposite end.

In the wireless networks the links between the nodes are established without cables using radio waves. Wireless networks have very different operational characteristics from wired networks. First, packet losses in wireless networks are mostly due to physical link failures instead of network congestion. Second, the signal attenuation often causes the link to break down when environmental interferences increase or a node moves out of the maximum radio distance.

Nodes in ad hoc wireless networks play an important role in sending and receiving data packets while simultaneously acting as routers. There are six types of wireless network; wireless personal area network (WPANs), wireless local area networks (WLANs), wireless wide area networks, wireless metropolitan area networks, and wireless mesh networks [4].

2.1.1 Main Factors that impact network performance

Network performance is not always consistent across networks because there are multiple factors at play. Two main parameters that can make the difference are bandwidth and latency.

Bandwidth, or effective throughput, is the number of the packets delivered in a unit of time [8]. Another important performance parameter is the latency, it’s the time taken by a data packet to arrive at the destination. It includes the delay caused by the route discovery process and the queuing in data packet transmission [8]. When calculating latency, only the data packets successfully delivered to destinations are counted.

2.2 Routing

Routing is the process of moving a packet of data form source to destination along a specific route. Every node in a MANET can assist in the routing of packets in the network. Thus, routes between two hosts in the network may consist of hops through other hosts in the network. The dynamically changing topology where nodes may join and leave the network at any time, the multi-hop routing may keep changing as nodes join and depart from the network [9].

2.3 Ad hoc Networking

An ad hoc is originally from a Latin phrase meaning for this purpose. An ad hoc network is a connection between two or more devices without central control, and it can be either wired or wireless. An ad hoc network is a collection of possibly mobile nodes that are self- configurable to form a network without the aid of any established infrastructure. The (mobile) nodes handle the necessary control and networking tasks in a distributed manner. An ad hoc network can be tailored to specific applications and it's highly robust to single node failure and provides a high level of fault tolerance because of node redundancy and its distributed nature. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network that may not be within direct wireless transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover "multi-hop" paths through the network to any other node [1].

Figure 2.1 provides a diagram illustrating of this concept. In the example two users are highlighted showing two paths through several nodes to the router. Some examples of the possible uses of ad hoc networking include students using laptop computers to participate in an interactive lecture, business associates sharing information during a meeting, soldiers relaying information for situational awareness on the battlefield, and emergency disaster relief personnel coordinating efforts after a hurricane or earthquake.

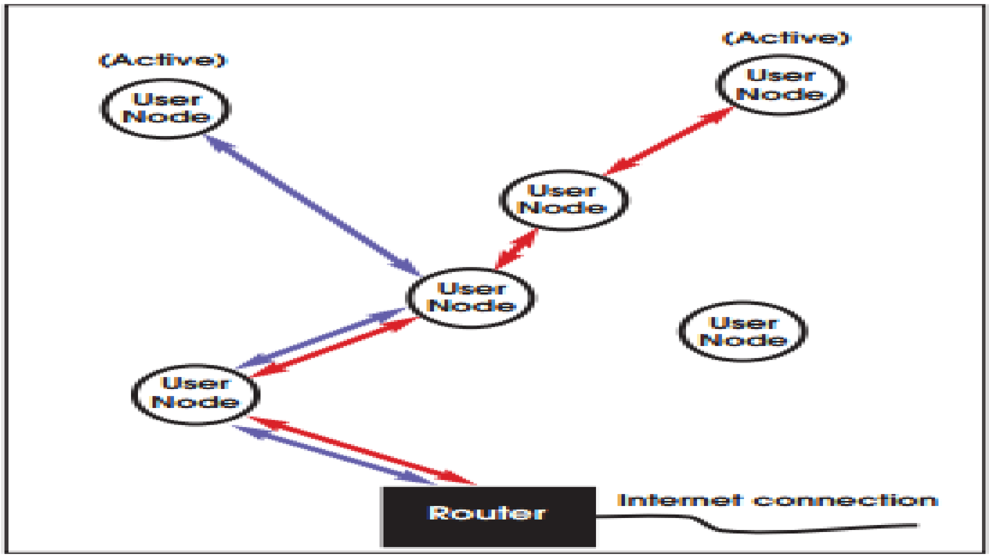

Figure 2.1: Basic Structure of an ad hoc Network [11]

There are three main applications that are based on wireless ad-hoc networks. They are Wireless Mesh Networks (WMN), Wireless Sensor Network (WSN), and Mobile Ad hoc Networks (MANET) [10].

- Wireless Mesh Network: is a communications network made up of radio nodes organized in a mesh topology. Wireless Mesh Networks often consist of mesh clients, mesh routers and gateways [10]. Wireless mesh networks have the advantage of low up-front costs, easy maintenance and good coverage service. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud.
- Wireless Sensor Network: the sensor nodes in a WSN are tiny devices operating on batteries and employing low-power radio transceivers to enable communication. It is assumed that the amount of power necessary to

communicate with the base station does not exceed the amount of power necessary to communicate with neighboring sensor nodes [12].

- Mobile Ad hoc Networks (MANET): a MANET uses mobile nodes to support basic networking functions like packet forwarding, routing, and network management. These functions are carried out by all available nodes [5].

2.4 Mobile Ad Hoc Networks (MANET)

A MANET is a sub category of ad hoc networks. MANET is a collection of wireless nodes communicating with each other in the absence of any infrastructure. Classrooms, battlefields and disaster relief activities are a few scenarios where MANETs can be used [19]. Due to concerns such as radio power limitation and channel utilization, mobile nodes may not be able to communicate directly (Figure 2.2).

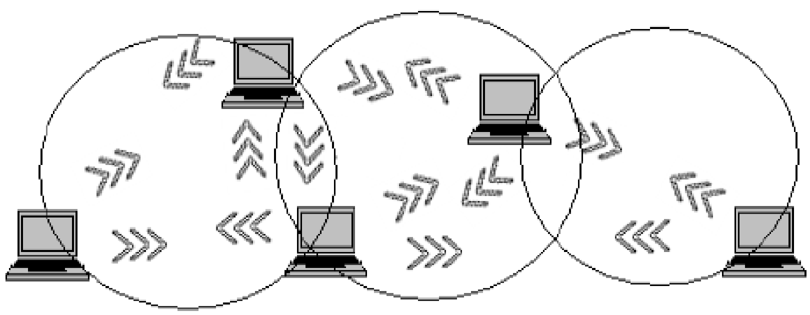

Figure 2.2: Mobile Ad hoc Network [10]

In ad-hoc networks, all nodes are mobile and connect dynamically in an arbitrary manner because the range of each host's wireless transmission is limited. So to communicate with hosts outside its transmission range, a host needs to enlist the aid of its nearby hosts in forwarding packets to the destination [10].

Most Ad-hoc networks are multi-hop; a message from a source node must go through intermediate nodes to reach its destination [23]. The packets sent by the source node are delayed by several intermediate nodes before reaching the destination node. The growing interest in Mobile Ad-hoc Networks has been largely influenced by current wireless technology growth and demand from a number of civil and military applications. Figure 2.3 shows some applications of MANETs. Some challenges in MANETS include power control at the physical layer, efficient routing at the network layer, quality of service (QoS) at the transport layer, and security.

MANETs present a larger security problem than other networks [27]. First, all signals go through wireless links in a MANET, which makes it more prone to physical security threats than fixed landline networks. Possible link attacks range from passive eavesdropping to active interference.

Second, mobile nodes are roaming independently and are able to move in any direction. Therefore, any security solution with a static configuration would not be adequate for the dynamically changing topology.

Finally, some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. An attacker could create a new type of DoS attack by forcing a node to replay packets to exhaust its energy supply. Due to the limited network capacity and battery power of wireless nodes, frequent disconnections are common in wireless MANETs, which makes anomalies hard to distinguish from normalcy. For instance, denial of service (DoS) can easily be launched if a malicious node floods the network with spurious routing messages [27].

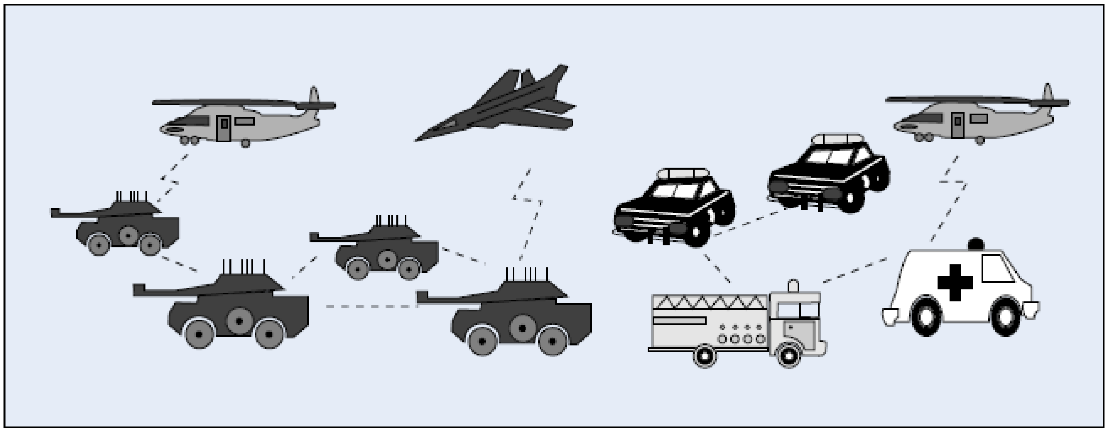

Figure 2.3: Example applications of MANETs [27]

2.5 Sensor Networks

A wireless sensor network is a group of specialized sensor nodes with a communications infrastructure that uses radio to monitor and record physical or environmental conditions [46]. Sensor networks hold the promise of facilitating large-scale, real-time data processing in complex environments. Their foreseeable applications might help protect and monitor military, environmental, safety-critical, or domestic infrastructures and resources [41].

2.6 Security in MANETS/Sensor Network

The research in security for MANETs is still in its infancy. Several security schemes for MANETs have been proposed [27]. A MANET is more vulnerable than a wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, a MANET is more prone to malicious attacks.

Attacks can be classified into passive and active attacks. A passive attack does not disrupt the operation of a routing protocol, but only attempts to discover valuable information by listening to routing traffic, which makes it very difficult to detect. An active attack is an attempt to improperly modify data, gain authentication, or procure authorization by inserting false packets into the data stream or modifying packets transiting through the network. Active attacks can be further divided into external attacks and internal attacks. An external attack is one caused by nodes that do not belong to the network. An internal attack is one from compromised or hijacked nodes that belong to the network [27].

Internal attacks are typically more severe, since malicious nodes already belong to the network as authorized parties. Therefore, such nodes are protected with the network security mechanisms and underlying services.

Some types of active attacks that are performed against MANETs are:

Black Hole: In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [28].

Denial of Service (DoS): The DoS attack results when the network bandwidth is hijacked by a malicious node. It has many forms. The classic way is to flood any centralized resource so that the network no longer operates correctly or crashes. For instance, a route request is generated whenever a node has to send data to a particular destination. A malicious node might generate frequent unnecessary route requests to make the network resources unavailable to other nodes [27].

Routing table overflow: The attacker attempts to create routes to nonexistent nodes. The goal is to have enough routes so that creation of new routes is prevented or the implementation of the routing protocol is overwhelmed.

Impersonation: A malicious node may impersonate another node while sending the control packets to create an anomaly update in the routing table [27].

Energy consumption: Energy is a critical parameter in the MANET. Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. Battery-powered devices try to conserve energy by transmitting only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node.

Information disclosure: The malicious node may leak confidential information to unauthorized users in the network, such as routing or location information. In the end, the attacker knows which nodes are situated on the target route [27].

2.7 Routing Protocol

Design of the efficient routing protocol in the MANET environment is difficult because of the route "short live" nature and as the network topologies are dynamically changing [10]. In ad hoc networks, the routing protocol is expected to implement three main functions: determining and detecting networking changes (e.g. breakdown of nodes and link failures), maintaining network connectivity, and calculating for proper routes.

The routes between two hosts in the network may consist of hops through other hosts in the network. The nodes in the network may be static (e.g. nodes dropped from an aircraft to a remote terrain or a toxic environment), static most of the time (e.g., books, projectors, furniture), or moving (vehicles, people, small robotic devices) [16]. A routing protocol is a principle or standard that controls how nodes come to agree in the way to route packets (using multi-hops) between computing devices in MANETs. Communications and formalizing agreement among nodes is crucial to the overall performance of a MANET [6].

2.8 Routing approaches for MANETs

Routing Protocol for MANETs can be broadly classified into two categories. These are:

- Proactive or table-driven routing protocols,
- Reactive or on-demand routing protocols.

Proactive routing protocols are table driven and actively determine the layout of the network. Through a regular exchange of network topology control packets between each node, a complete picture of the network is maintained at every single node [10]. Every node in this routing protocol maintains information of only active paths to the destination nodes. Packets are transmitted to the next node along a predefined route as in routing table. The packet forwarding is done faster but the routing overhead is greater because all the routes have to be defined before sending any packet [17]. DSDV, OLSR are example of proactive protocols.

On-demand [reactive] 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. This routing protocol doesn't keep the record of a route in the routing table so there is no overhead for maintaining the routes to the nodes [17]. The design follows the idea that each node tries to route the packets when communication is requested [10]. A route to a specific destination is computed on demand, which is only when needed. To efficiently use resources in controlling large dynamic networks, hierarchical routing, including cluster based and dominating set based, is normally used [12]. Common for most on-demand routing protocols is the route discovery phase where packets are flooded in to the network in search of an optimal path to the destination node in the network. Some reactive MANET protocols include: DSR, AODV and TORA.

2.8.1 Destination Sequence Distance Vector Routing (DSDV)

This protocol is based on the classical Bellman-Ford routing algorithm [10] designed for MANETs. DSDV is a table driven routing protocol, and as in all table driven protocols each node maintains a table that contains the next hop to reach all destinations [13]. DSDV packets are routed between nodes of an ad-hoc network using routing tables stored at each node. Each entry is marked with a sequence number.

The sequence number is used to distinguish stale routes from new ones and thus it avoids the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So the update is both time driven and event-driven. After receiving an update, a neighboring node utilizes it to compute the routing table entries [10].

One disadvantage of DSDV is that it constantly uses energy and bandwidth through regular updates of the routing table. This is due to new sequence numbers being generated along with the changes in topology. Therefore it is unsuitable on a highly dynamic or large-scale network scenario [14].

2.8.2 Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is an easy and an effective reactive routing protocol. The routing processes of the DSR protocol are composed of the main mechanisms of “Route Discovery” and “Route Maintenance”, which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network [10].

Route Discovery

Route Discovery is used whenever a source node desires a route to a destination node. First, the source node looks up its route cache to determine if it contains a route to the destination. If the source finds a valid route to the destination, it uses this route to send its data packets. If the node does not have a valid route to the destination, it initiates the route discovery process by broadcasting a route request message. The route request message contains the address of source and the destination, and a unique identification number. An intermediate node that receives a route request message searches its route cache for a route to the destination. If no route is found, it appends its address to the route record of the message and forwards the message to its neighbors. The message propagates through the network until it reaches either the destination or an intermediate node with a route to the destination. Then a route reply message, containing the proper hop sequence for reaching the destination, is generated and unicast back to the source nodes [12].

Route Maintenance

Route Maintenance is used to handle route breaks, when a node encounters a fatal transmission problem at its data link layer; it removes the route from its route cache and generates a route error message. The route error message is sent to each node that has sent a packet routed over the broken link. When a node receives a route error message, it removes the hop in error from its route cache. Acknowledge messages are used to verify the correct operation of the route links [10].

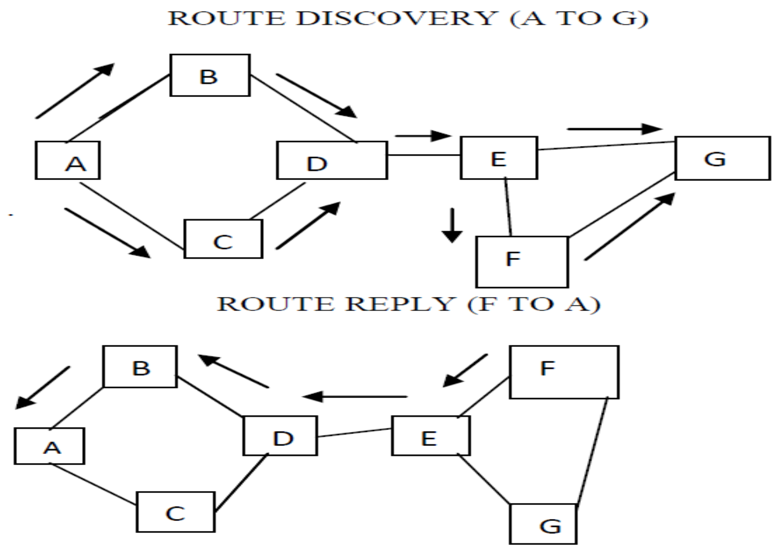

Figure 2.4: DSR Request and Reply [15]

2.8.3 Ad hoc On Demand Vector (AODV)

The Ad-hoc On Demand Vector routing protocol uses an on-demand routing algorithm, that builds routes between nodes only as desired by source nodes. AODV includes route discovery and route maintenance [10]. In this protocol, when a node starts a connection it broadcasts a request for a connection. This protocol also uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting and scales to a large number of mobile nodes. For example, when node S intends to find a route to node D, the process is shown in the Figure 2.5.

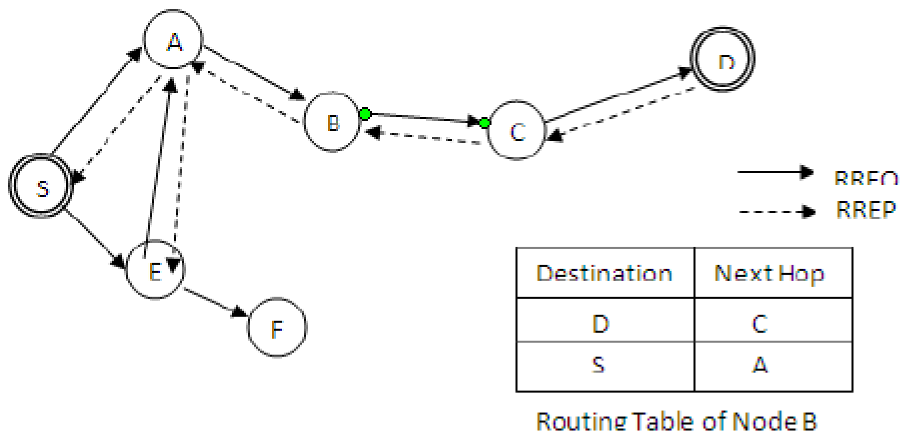

Figure 2.5: AODV Routing Protocol Model [10]

AODV builds routes using route request (RREQ) and reply query (RREP) cycle, when a link fails, a routing error is passed back to a source node, and the process repeats. Nodes receiving the RREQ may send a RREP if it is the destination, or if it has a route to the destination, with the corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case it unicasts a RREP back to the source node, otherwise it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID [10].

2.9 Comparison of routing protocols

Every routing protocol reacts differently to enable connections and routes. The task of routing protocols is to establish and enable transfer of data packets from a source to a destination node in a MANET. The three routing protocols (DSDV, DSR, and AODV) have similar properties and are also distinct in their own ways.

When using proactive routing (i.e. DSDV), one is certain to use valid routes. Each route is stored in a route cache, or a route table, for a period of time. In most reactive routing (i.e. DSR, AODV) the route maintenance is carried out by real time monitoring, rather than periodic updates and only entries for the active destination are monitored. Table 2.2 is presented to compare the three routing protocols:

Table 2.1: Comparison for Routing Protocols (DSDV, DSR, and AODV) [16]

Parameter	**DSDV**	**DSR**	**AODV**
Route maintained	Route table	Route cache	Route table
Route computation	Table-Driven	On demand	On- demand
Route updates	Periodically	As needed (event driven)	As needed (event driven)
Mechanism of routing	One hop	Source routing	Next hop
Update information on route	Neighbours link state	Route error	Route error

2.10 Mobility Models

Many mobility models were designed in order to simulate the real world scenarios better for MANET applications. A mobility model tries to mimic the movement of real mobile nodes that change the speed and direction with time and how their location, velocity and acceleration change over time [18].

In ad hoc wireless mobile networks, the mobility models focus on the individual motion behavior between mobility epochs, which are the smallest time periods in a simulation in which a mobile host moves in a constant direction at a constant speed [2].

One intuitive method to create realistic mobility patterns would be to construct trace-based mobility models, in which accurate information about the mobility traces of users could be provided. A trace is where actual node movements have been experienced and observed in real life systems. In this type of model, accurate information can be captured when the simulations include a large number of mobile nodes over a long observation period of time. However, since MANETs have not been implemented and deployed on a wide scale, obtaining real mobility traces becomes a major challenge. Therefore, various researchers proposed different kinds of mobility models, attempting to capture various characteristics of mobility and represent mobility in a somewhat 'realistic' fashion. Much of the current research has focused on the so-called synthetic mobility models that are not trace-driven [12]. One popular example of synthetic mobility is the random mobility model. According to this model, the speed and direction of motion in a new time interval have no relation to their past values in the previous epoch. This model can generate unrealistic mobile behavior such as sharp turning or sudden stopping [29].

Based on specific mobility characteristics, the random mobility models can be classified into three categories.

2.10.1 Random-based Mobility Models

In random-based mobility models, the mobile nodes move randomly and freely without restrictions. The destination, speed and direction are all chosen randomly and independently of other nodes [12]. This kind of model has been used in many simulation studies.

2.10.2 The Random Waypoint Model

The node movements in Random Waypoint Models (RWP) are random and independent of each other, and the nodes use pause time between changing direction and velocity. This model became a 'benchmark' mobility model to evaluate the MANET routing protocols, because of its simplicity of implementation and analysis. To generate the node trace of the random waypoint model the setdest tool from the CMU Monarch group may be used. This tool is included in the widely used network simulator NS2 [18]. This model was used for the experiments in this report.

In the Random Waypoint model nodes normally stay for a certain period of time, known as pause time, before moving toward the destination. After the pause time passes, a mobile node randomly chooses a destination within an allocated simulation area. The minimum and maximum velocities of a node are chosen, hence a mobile node moves toward a destination with a particular constant velocity, which is uniformly distributed between the minimum and maximum velocities. When a destination is reached, a mobile node pauses for a specific time before repeating the random process.

Some limitations of Random waypoints are [19].

1) Temporal dependency: Due to physical constraints of the mobile entity itself, the velocity of a real mobile node changes continuously and gently instead of abruptly, i.e. the current velocity is dependent on the previous velocity. However, the velocities at two different time slots in the RWP model are independent in the random waypoint model.

2) Spatial dependency: The movement pattern of a real mobile node may be influenced by and correlated with nodes in its neighborhood. In random waypoint, each mobile node moves independently of others.

3) Geographic restrictions: In many cases, the movement of a real mobile node may be restricted along the street or a freeway. In the RWP model the movement is restricted by the geographical boundary only.

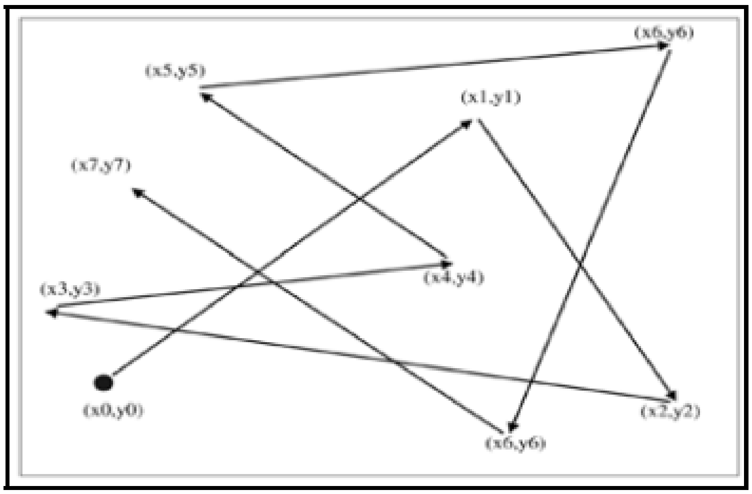

Figure 2.6: Example of node movement in the Random waypoint model [31].

2.10.3 Random Walk Model

The Random Walk model was originally proposed to emulate the unpredictable movement of particles in physics. It is also referred to as the Brownian motion. Because some mobile nodes are believed to move in an unexpected way, random walk mobility model is proposed to mimic their movement behavior [12] [3]. In this model, the nodes choose their location, velocity and direction at each time randomly. The random walk model has similarities with the random waypoint model because the node movement has strong randomness in both models. We can think of the random walk model as the specific random waypoint model with zero pause time [18]. An example of random waypoint model is shown in Figure 2.7.

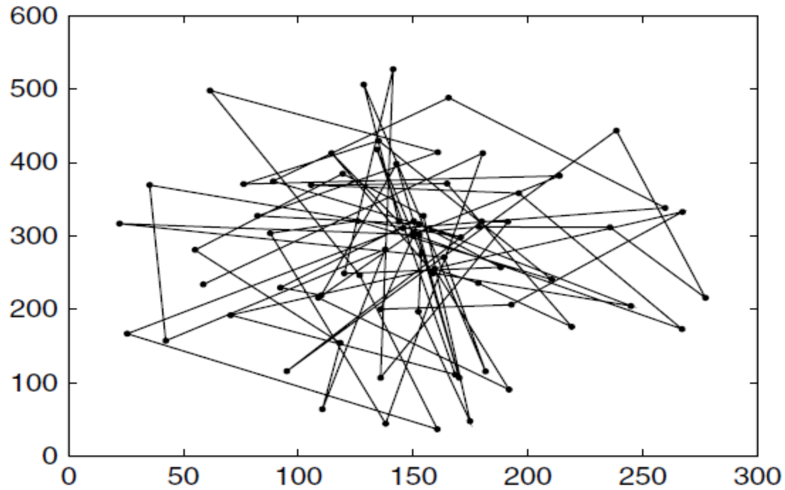

Figure 2.7 : Traveling pattern of an MN using the 2-D Random Walk Mobility Model [12].

Chapter 3

Network Simulator and Simulation

Chapter 3 describes network simulation and the tool used for simulation. The simulator used for the research is discussed in Section 3.1, and Section 3.2 shows architectural design of NS2. Features and simulation steps are explained in 3.3 and finally the setdest command and tool of NS2 is described in 3.5.

3.1 Overview

The network simulator (NS2) is an object-oriented simulator developed as part of the VINT project at the University of California in Berkeley. NS2 is extensively used by the networking research community [20]. It provides substantial support for simulation of TCP, UDP, routing, multicast protocols over wired and wireless (local and satellite) networks, etc. The popularity and the number of users of this tool have increased in recent years.

NS2 allows simulating MANETs. It is an object oriented open source simulator written in OTcl and C++ [29]. NS2 helps to debug problems in a controlled environment. NS2 also helps in performing analysis of hypothetical changes. Figure 3.1 shows the architectural view of NS2 simulator.

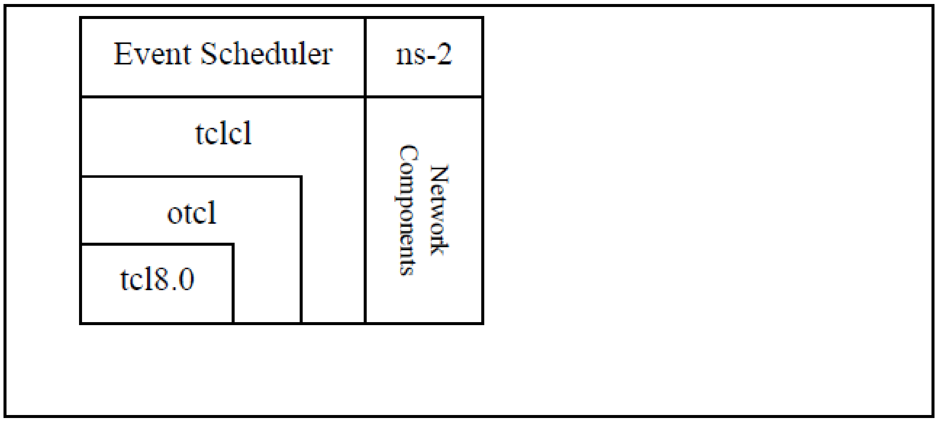

Figure 3.1: Architecture of NS2 [21]

3.3 NS2 Features

In NS2, network simulation is set up using a scripting language (TCL) which defines simulation objects. At the end of simulations a trace file is generated which contains the record of all events during the simulation.

As shown in Figure 3.1, NS2 is composed of TCL, OTCL, TCLCL, event scheduler and network component. TCL stands for Tool Command Language which is used for creating various simulation scenarios in NS2. OTCL is an object-oriented TCL programming language. In NS2, programs are written in OTCL as it provides object-oriented support in order to link the simulation scenario script written in TCL and programs written in C++. Above all of this is the simulator co-ordinates with models of various network components and the event scheduler implemented in C++. In order to create a simulation, OTCL is used to line these C++ files to the simulation script written in TCL and simulation program which is generated with OTCL [21].

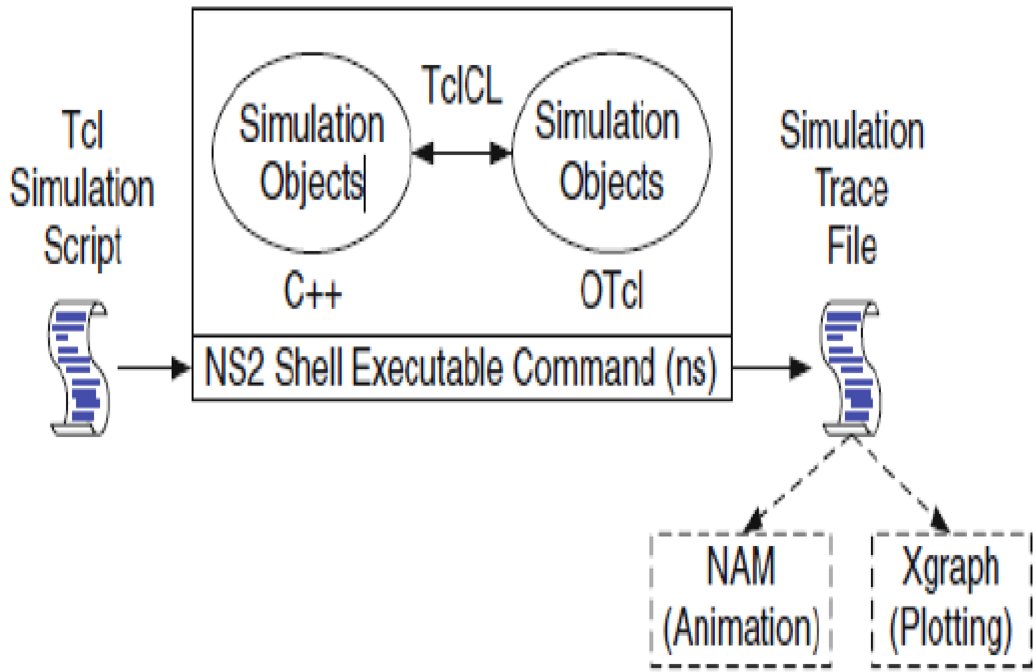

Figure 3.2: NS2 simulation Execution [10]

Figure 3.2 shows the procedure of executing the simulation in NS2. First, we create a simulation script which contains the simulation scenario and parameters which are to be applied. This simulation script is the TCL file in which parameters like protocol to be used, energy model to be used, and physical layer are specified. These parameters are modeled in NS2 using object oriented extension of C++ that is linked the current simulation script using OTCL linkage.

NS2 is utilized for three broad reasons in research [10]: selecting a mechanism or protocol variant, investigating the performance of composite networks, and exploring unanticipated connections of various protocols. For this research we used it to investigate the performance of routing protocols.

3.4 Main NS2 Simulation Steps

The following shows the three-step used in defining a simulation scenario in an NS2

Step 1: Simulation Design*:* The first step in simulating a network is to design the simulation. In this step, the user determines the simulation purposes, network configuration and assumptions, the performance measures, and the type of expected results.

Step 2: Configuring and Running Simulation: This step implements the design in the first step. It consists of two phases:

Network configuration phase: In this phase network components (e.g. node, TCP and UDP agents) are created and configured according to the simulation design. Also, the events such as packet size, data transfer and number of nodes that are scheduled to start at a certain time (simulation time).

Simulation Phase: This phase starts the simulation which was configured in the network configuration phase. It maintains the simulation clock and executes events chronologically. This phase usually runs until the simulation clock reaches a value specified in the network configuration.

Step 3: Post Simulation Processing: The main tasks in this step include verifying the integrity of the program and evaluating the performance of the simulated network. While, the first task is referred to as interpreting the script, the second one is achieved by properly collecting and compiling simulation results [10]. After the completion of simulation, a trace file is generated. The output can now be fetched from the trace file. An AWK or Perl script may be coded that extracts the required output from that trace file. We used AWK scripts. From these results, direct generation of charts and graphs is possible using x-Graph or excel, and x-Graph is a tool supported by NS2. NS2 also provides support for visualization of the network with the help of NAM, which is the

Network Animator tool. Figure 3.3 shows the graphical interface used by NAM. NAM uses the trace file generated by the simulation carried out in NS2 and generates an animation based on it [21].

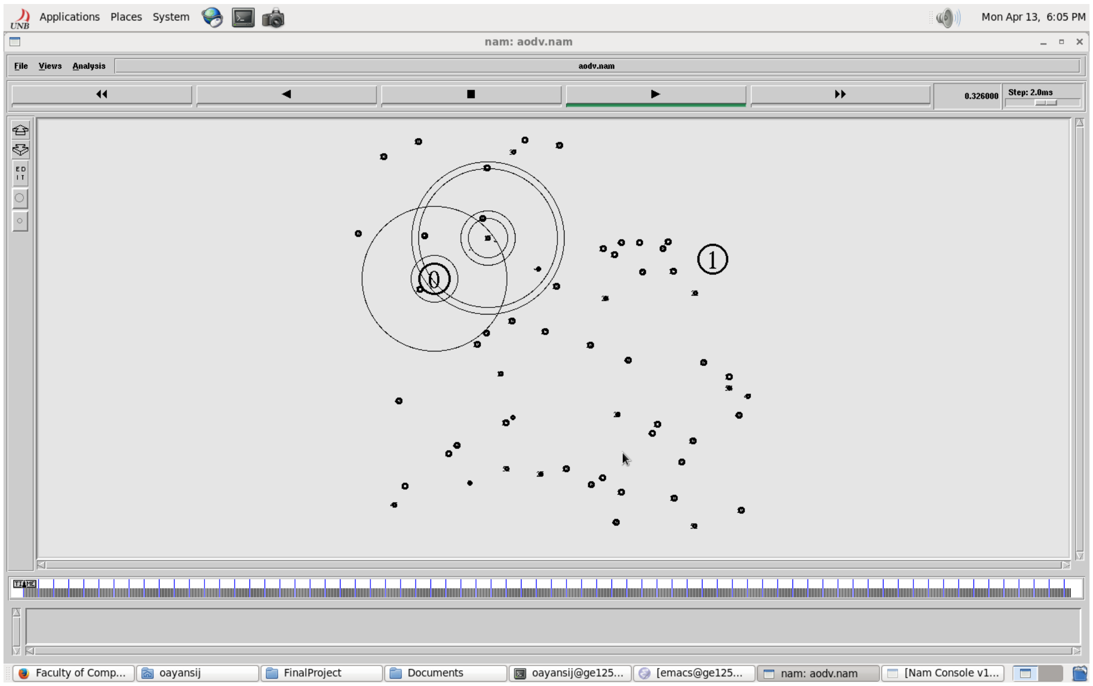

Figure 3.3: Graphical Network Animator (NAM)

However, there is a problem with setting up large simulation experiments in NS2: performance testing requires large numbers of nodes and packets. This would require a lot of work to set up manually the position and movement of all the nodes. To conquer this we use the setdest tool which is included in the NS2.

3.5 Setdest Tool & Command

NS2 simulation requires the ability to generate node movements for a large number of nodes. A utility called setdest is supplied with the simulator. It was developed in C++ to address the mobility simulation issues in NS2. It uses system dependent/dev/random and calls the library functions initstate() for generation of random numbers [10]. The setdest utility is a tool used to generate the positions of nodes and their moving speed and moving directions, by first generating the nodes in the specified boundary and then using the Random Waypoint Mobility (RWP) model algorithm to create random movements for the mobile nodes [22]. This tool is under "NS2_home/indep-utils/cmu-scen-gen/setdest. This program randomly generates a random waypoint mobility scenario and sends it to stdout in the form of a TCL script that NS2 will later use.

Setdest uses the following parameters: setdest version number, node number, pause time, maximum speed of the movement, simulation time, x coordinate, and y coordinate. It has two versions.

The Syntax is:

. /setdest [-n num_of_nodes] [-p pausetime] [-s maxspeed] [-t mintime] [-x maxx] [-y maxy] > [outdir/movement-file]

In the first version v1 of setdest there was no setting for the nodes minimum speed. For this the node could use random speed that can be too small for a node to reach its destination. This was not helpful in providing a true simulation scenario. In the second version v2 of setdest this problem was fixed by adding the option to set a minimum speed, along with some other features. The utility file must be called by NS2 to get the simulation to run with the random movement, using the waypoint mobility model.

3.6 Trace File

Trace files are text-based results of packet tracing in NS2. Trace files are generated during the simulation and are created to collect the detail of all packets traversing the network. Once the trace file is extracted it is useful in processing and analyzing data. AWK and Perl are the most popular languages used in analyzing the output from the trace file. They are coded to extract the required output from the trace file. Let's consider these two lines of code from the trace file:

r 149.397366557 _1_ AGT --- 13652 ack 60 [13a 1 0 800] ------- [2:0 1:1 29 1] [4217 0] 2 0

s 149.399632637 _0_ RTR --- 13674 tcp 1060 [0 0 0 0] ------- [0:0 1:0 30 1] [2605 0] 0 0

Table 3.1 shows the interpretation of every field in the sample trace file example.

Table 3.1: Trace File description

Field &Value	Description
r,s,f,D	Represent "received", "sent", "forwarded" and "dropped", respectively.
149.397366557	The second field is the time.
0,1,2, ...	The third field is the node number.
AGT,RTR, IFQ	The fourth field is MAC address to indicate if the packet concerns a MAC layer. AGT indicates the transport layer (e.g. tcp) packet, or RTR if it concerns the routing packet. It can also be IFQ to indicate events related to the interference priority queue(like drop of packets)
13652	After the dashes, there comes the global sequence number of the packet (this is not the tcp sequence number).
tcp,ack	At the next field there comes more information on the packet type.
500,1060	Then comes the packet size in bytes.
[13a 1 0 800]	The four numbers in the first square brackets concern the MAC

	layer information. The first hexadecimal number, 13a, specifies the expected time in seconds to send this data packet over the wireless channel. The second number, 1, stands for the MAC-id of the sending node, and the third, 2, is that of the receiving node. The fourth number, 800, specifies that the MAC type is ETHERTYPE_IP.
[2:0 1:1 29 1]	The next numbers in the second square brackets concern the IP source and destination addresses, then the ttl (Time To Live) of the packet.
[4217 0]	The third bracket concerns the tcp information: its sequence number and the acknowledgment number.

Chapter 4

Performance Evaluation of MANETS

This chapter outlines the methodology used in investigating the performance of selected MANET routing protocols. This chapter is divided into three sections. Section 4.1 presents the introduction. Section 4.2 outlines the goals. Section 4.3 describes the performance metrics, 4.5 the parameters used in carrying out the experimental research. Section 4.6 summaries the chapter.

4.1 Introduction

In networking, the methods used for evaluation of routing protocols are analytical modeling, real experiment and computer simulation. Analytical modeling is based on mathematical computation and analysis. In a MANET, the nodes move and the topology changes dynamically and unpredictably [23], therefore using a real experiment might be too expensive. As a result performance evaluation using analytical methods or real methods is not attempted in this study.

Simulation is the process of constructing a model of a system which represents a system under investigation and conducting experiments with the model on a computer for a specific purpose of experimentation to solve the problem [24]. The goal of using any simulator is to accurately model and predict the behavior of a real world problem in a system. The simulator used in this study is NS2.

4.2 Goals

The experiments aim to observe the performance of different routing protocols (AODV, DSDV and DSR) on a MANET. Performance metrics are used to analyse the performance of each protocol under two broad scenarios. The impact of a DoS attack on a network, as compared to there no DoS attached is investigated. A DoS attack diminishes or eliminates a network's capacity to perform its expected function. Although attackers commonly use Internet but here we are considering a rogue node (or malicious node) that might generate frequent unnecessary route requests thereby limiting the resources available to the legitimate node or other nodes. These malicious nodes will flood the network with enough messages to impede its proper use.

4.3 Performance Metrics and Criteria

To evaluate the performance of routing protocols, both qualitative and quantitative metrics are needed. A Metric is a standard measurement used in a routing algorithm to determine the best possible, effective and efficient route to a destination. There are many performance metrics that can be used to observe the performance of routing protocols. This experiment is evaluated based on the following performance metrics: effective bandwidth/throughput, node utilization, end to end delay, packet delivery ratio, and hop count.

4.3.1 Effective Bandwidth or Throughput

Throughput or effective bandwidth can be defined as how many data packets are received by receiver within data transmission time or simulation time. It is the average rate of successful data packets received over a communication channel and is measured in bits per second (bits/s). Throughput measures the effectiveness and efficiency of routing protocols usage (performance) over the network. In any network higher throughput is the most essential factor.

4.3.2 Packet delivery ratio

Packet delivery ratio is defined as the number of data packets received by the destination node divided by the number of data packets transmitted by the source node. It is used to calculate the loss rate of packets during transmission in the network. A higher packet delivery ratio gives a better network. This number presents the effectiveness of a protocol.

4.3.3 Average end-to-end delay

It is the average time taken by a data packet to arrive at the destination. It includes the propagation delay, delay caused by route discovery process, retransmission delays at medium access control (MAC) and the queue in data packet transmission. Only the data packets successfully delivered to destinations are counted [8].

The end to end delay for packet p which was sent by the node n, as a source node and received successfully at destination node is:

End-to-end $\text{delay}_{np} = \text{starttime}_{np} - \text{endtime}_{np}$

where starttime_{np} is the time when sending of packet p at node n starts. Endtime_{np}, is the time when packet p is received successfully at destination node [15].

The lower the value of end to end delay means the better performance of the protocol. End to end delay evaluates the ability of routing protocols to make efficient use of network resources.

4.3.4 Hop Count

Hop count is the number of hops it took each packet from the source node before it got the destination node. Hop count also refers to the number of intermediate devices (like routers) through which data must pass between source and destination, rather than flowing directly over a single wire. Each router along the data path constitutes a hop [25].

4.3.5 Node Utilization

In order to address the issue of routing in wireless networks consideration must be given to minimize the energy consumption on nodes that is how many times a node participates during routing. This could have a significant effect on the batteries of the node and ultimately the performance of the network. Node utilization is an important metric since battery power at each node is limited. Due to limited battery power, the communication overhead must be minimized if the number of routing tasks is to be maximized. A longer path that passes through nodes that have plenty of energy may be a better routing strategy. Alternatively, some nodes in the network may be temporarily inactive and the power consumption metric may be applied on active nodes [26].

4.4 Processing Simulation Results

The first two metrics (packet delivery ratio and Effective bandwidth) are the most important for best-effort traffic. Note, however, that these metrics are not completely independent. For example, the larger the hop counts or the longer path lengths, the higher the end to end delays.

Now that we know the performance metrics the post simulation process can be down. After the completion of simulation, a trace file is generated, the output is fetched from the trace file, and AWK scripts were coded to extract the required output from that trace file.

From these results, direct generation of charts and graphs is possible by using x-Graph or excel. Note that x-Graph is supported by NS2 and that excel is widely available.

For example the number of packets sent by the source node and the number of packets received by the destination nodes can be extracted from the trace file using the following AWK and grep scripts. Counting the sent packets from the source node, the command below executes that

```
awk /s -t/ out.tr> sent.out
```

To print the received and sent packets from source node (0) and destination node (1)

```
BEGIN{
sent=0;
received=0;
}
$1~/s/&&/AGT/&&$31~/0.0/{sent++}
 $1~/r/&&/AGT/&&$33~/1.0/{received++}
 END{
 print(sent,received);
}
```

NS2 also provides support for visualization of the network with the help of NAM, which is a Network Animator tool. From this tool we can see (i.e. visualize interactively) the packets sent, received and some that have been dropped.

4.4 Assumptions

The assumptions made for experimental investigation are: 1) only the source node in a network is supposed to generate CBR traffic at any given time. Others nodes act as a forwarding nodes to the destination node; 2) dropped packets were not considered in calculating some metrics, such as delay. 3) all nodes are mobile and follow the RWP model, except the source and destination which are stationary; and 4) not all the nodes in a network are moving at a given time (pause time).

4.5 Simulation Environment and Set up

The network scenarios to be examined were chosen to mimic the common scenarios chosen to test MANET routing protocols. The three routing protocols AODV, DSDV and DSR are used in investigating a network based on the analysis of performance metrics. Network Simulator2 (NS2) is used to investigate the scenario. The three routing protocols are used in investigating varying network sizes with a bounded 1000 x 1000 meters area, the same node speed and 802.11 as the network standard.

Each wireless node uses Wireless Channel with 802.11 MAC and a WirelessPhy layer implemented in NS2. The simulation uses the TwoRayGround propagation model and an omnidirectional antenna. The random node mobility for the experiments is generated using a node movement generator “setdest” built into NS2. The setdest application generates a node movement file using the random way-point algorithm. The maximum speed is set to 2 m/s and the pause time is 2s the node speed of 2 m/s reflects the movement of people. We use a 1000m x 1000m square area as stated before wherein the source and the destination wireless nodes (nodes 0 and 1, Figure 4.1) are stationary, at locations (200, 650) and (900,700).

In setting up the Denial of Service (DoS) and Distributed Denial of Service (DDoS) Figure 4.1 shows the graphical set up on a NAM interface. The DoS has a rogue node sending packets across the legitimate traffic, DDoS has two rogue nodes (nodes 2 and 4, Figure 4.1) sending packets across the legitimate traffic all at the same time. The rogue nodes are set at locations (600,900) and (500,800), the nodes are sending at 0.05Mbps (20packets sent every 1 second). Every packet has a size of 512 bytes.

Data in the MANET are transmitted from the source to the destination node over a UDP connection at a constant bit rate and are generated using the NS2 built-in CBR traffic generator at the rate of 0.05Mbps (20 packets sent every 1second). Every packet has a size of 512 bytes. The buffer size at each node is 50 packets, the number of nodes used in the experiments varied from 20 to 120 and all simulations are carried out in 300 seconds of simulation time.

NS2 has parameters that help change the network settings and control the simulation process. Some of the parameters are listed Table 4.1.

Table 4.2: General parameters used in simulation

Parameter	**Value**
Channel Type	Channel / wireless channel
Network interface type	Phy / wireless channel
Simulation time	300.0 s
Simulation model	Two Ray Ground
MAC Type	802.11
Antenna	Antenna/Omni Antenna
Traffic Source	CBR
Packet size	512bytes

Topography	1000m*1000m
Node Speed	2m/s
Pause Time	2s
Number of nodes	20,40,60,80,100,120
Interval	0.05

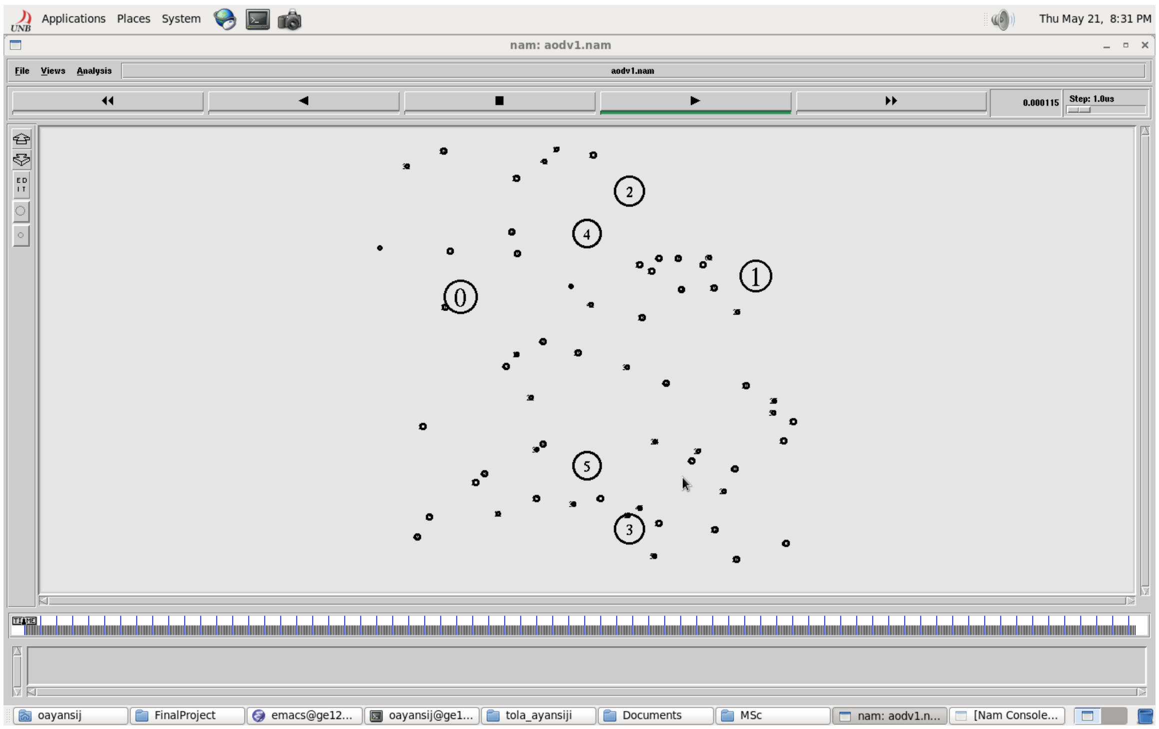

Figure 4.1: DoS &DDoS graphical illustration

Table 4.3: Traffic loads experimental scenarios

Scenario 1	NO DoS Attack Scenario 1 consists of experiments with No DoS attack. Each experiment implementss AODV, DSR, and DSDV. All experiments are implemented using the network environment and configuration illustrated in Figure 4.1 with a network size varying from 20-120, speed of 2 m/s and packet size of 512 bytes.
Scenario 2	DoS Attack Scenario 2 consists of experiments with DoS attack. MANET seems to be more vulnerable to security attacks due to mobile nodes. It has same parameters as in Scenario 1 but now with malicious nodes added to the network. The node speed and packet size are kept constant.

Chapter 5

Results and Comparative Analysis

This chapter reports on experimental results and the summary of the report.

5.1 Experimental Results

Figure 5.1 compares the packet delivery ratio of AODV, DSDV and DSR. As shown in this figure the delivery ratio of AODV and DSR performs best in delivering above 80% of data packets as compared to 60% of the DSDV protocol. This can be attributed to the nature of the algorithm in DSDV; it maintains node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth which in turn reduces the network performance. With varying network sizes from 20-120, packet delivery ratio of DSDV increases as the network size increases, i.e., with 20 nodes, we get only a delivery ratio of 30%.

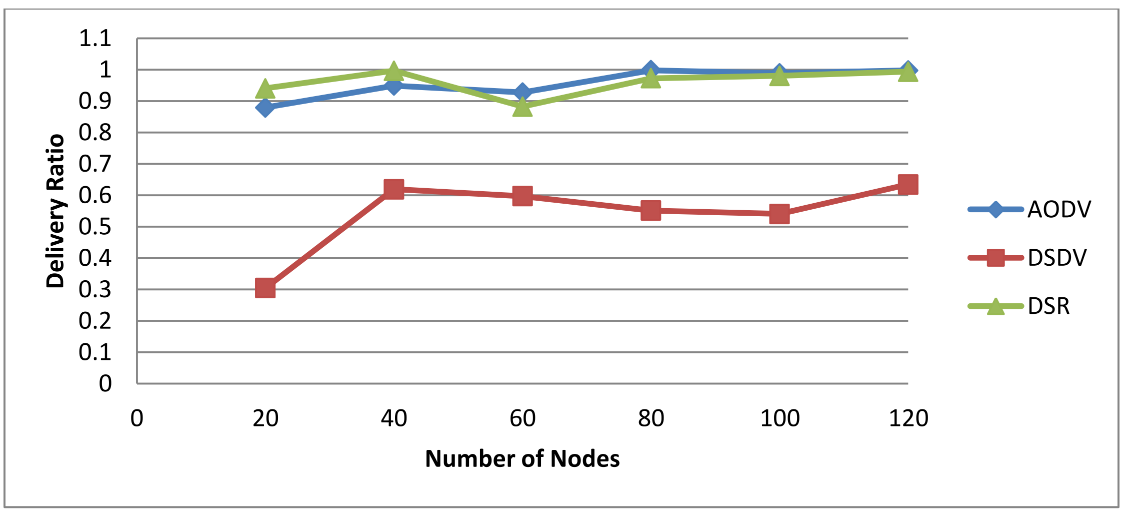

Figure 5.1: Packet delivery ratio for varying network sizes

Figure 5.2 shows the packet delivery ratio with Denial of Service (DoS). The delivery performances of the routing protocols were distorted, since The network resources were unavailable because of the compromised or hijacked nodes in the network. The protocols performed similarly but DSDV seems the worst affected maintaining low delivery ratio, while the highest delivery ratio stands at 50%, because all the routes have to be defined before sending the packet. AODV seems to perform better than DSR because of the algorithm used in AODV.

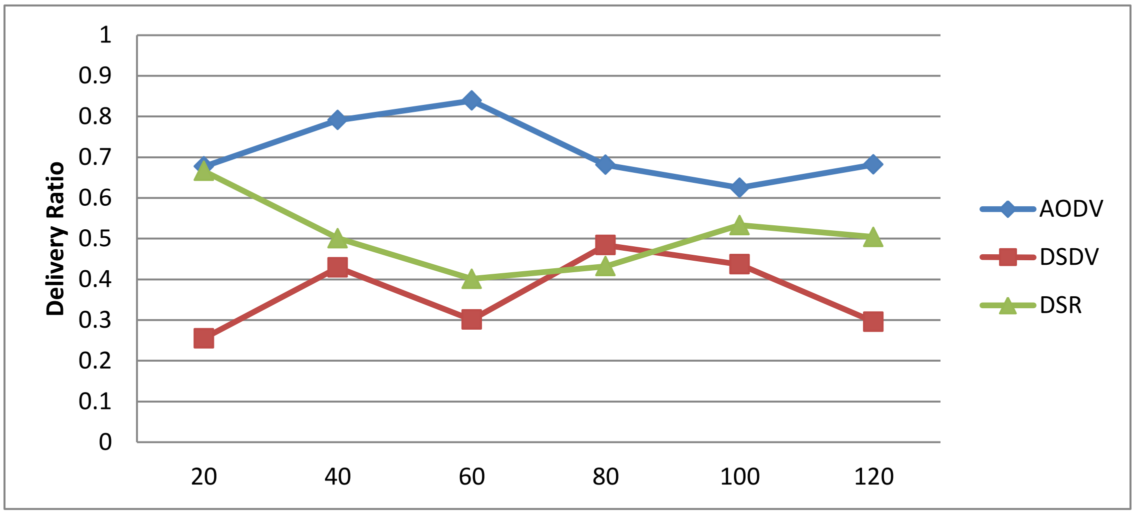

Figure 5.2: Packet delivery ratios for varying network sizes with DoS

Figure 5.3 shows average end to end delay. DSDV protocol has a lower delay, DSR approach has the highest delay, while AODV maintains a consistency in this metric. The reason for this is DSR uses source routing, i.e., the source must know the complete hop sequence to the destination. A mobile node continues to use a route to a gateway until it is broken. But in DSDV, periodic information sent by the gateways allows the mobile node to update their route entries for the gateways more often, resulting in fresher and shorter routes.

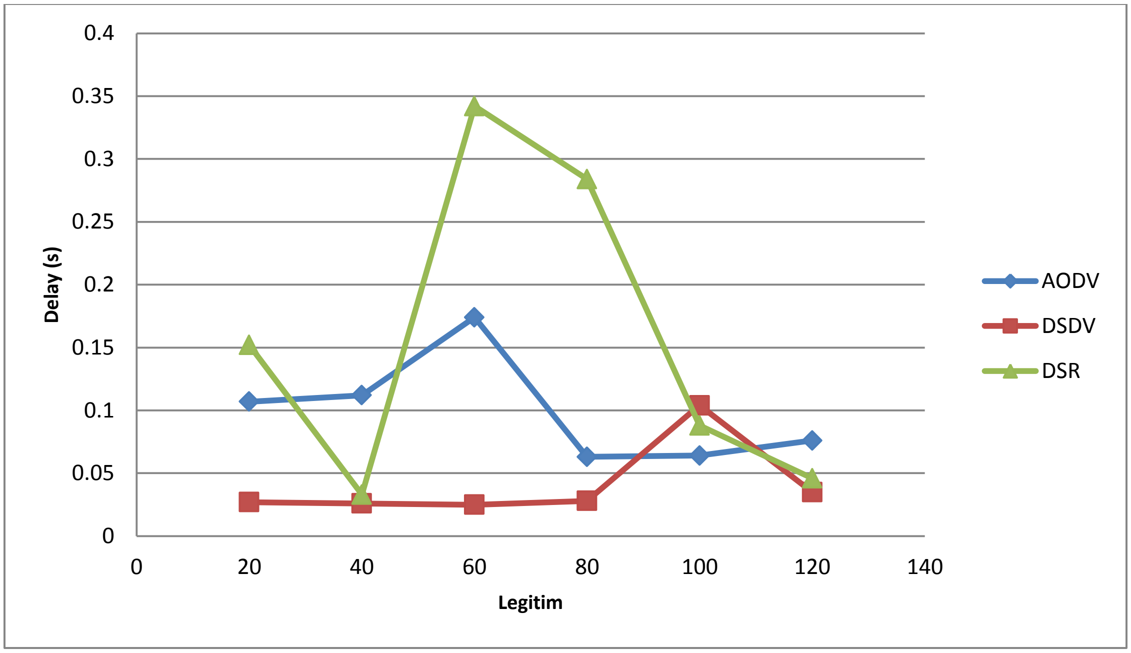

Figure 5.3: Average delay for varying network sizes

Figure 5.4 shows average delay for varying network sizes with DoS attack on the network. As we already know, a DoS attacks tries to shut down the target (victim) preventing authorized users from using any of the resources. Figure 5.4 show that DSR has a high delay of 5.5s at 80 nodes for instance. Other protocols however, have lower delays than that of DSR. DSDV and AODV have 0.965s and 0.386s of delay, respectively. The reason for the good performance of AODV is it gets new route to the destination node faster when the network is under attack than other routing protocols. DSR takes longer time to find new routes.

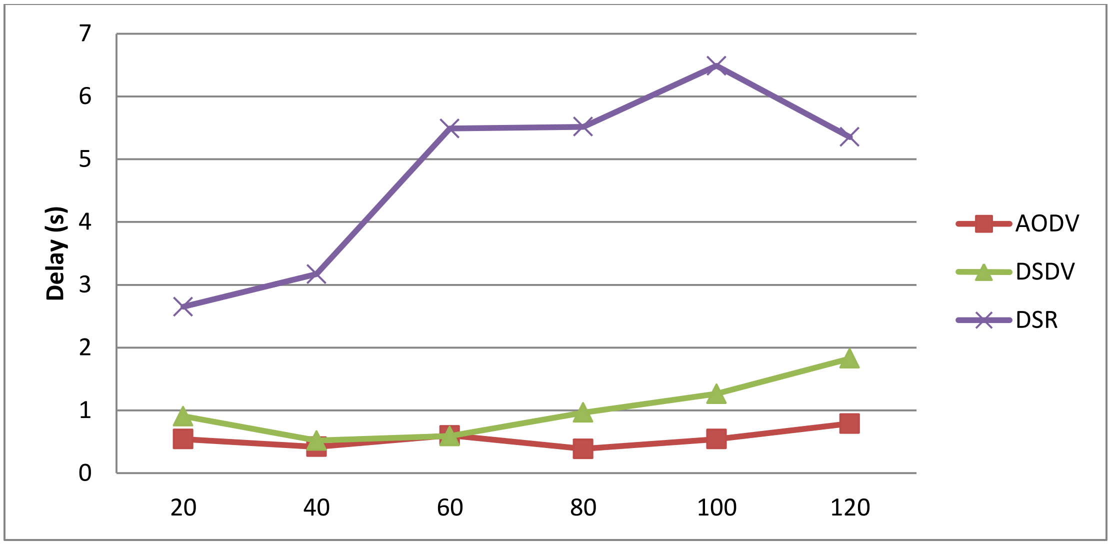

Figure 5.4: Average delay for varying network sizes with DoS

Figure 5.5 shows the effective throughput for the AODV protocol with the number of nodes NN = 60 and packet size PS= 512bytes. The graph shows throughput in MBits/s against time from 0-300s. The protocol performance is good with the average throughput of 85Mbit/s. Although the network transmission seems to breakdown (rerouting) at time 90s likely because of the movement of the nodes, but pick up within 10s of transmission. A high throughput from 0s in transmission means that the routes are found very early in this protocol. Also, the throughput shoots up to 120Mbit/s between time 110s to 120s.

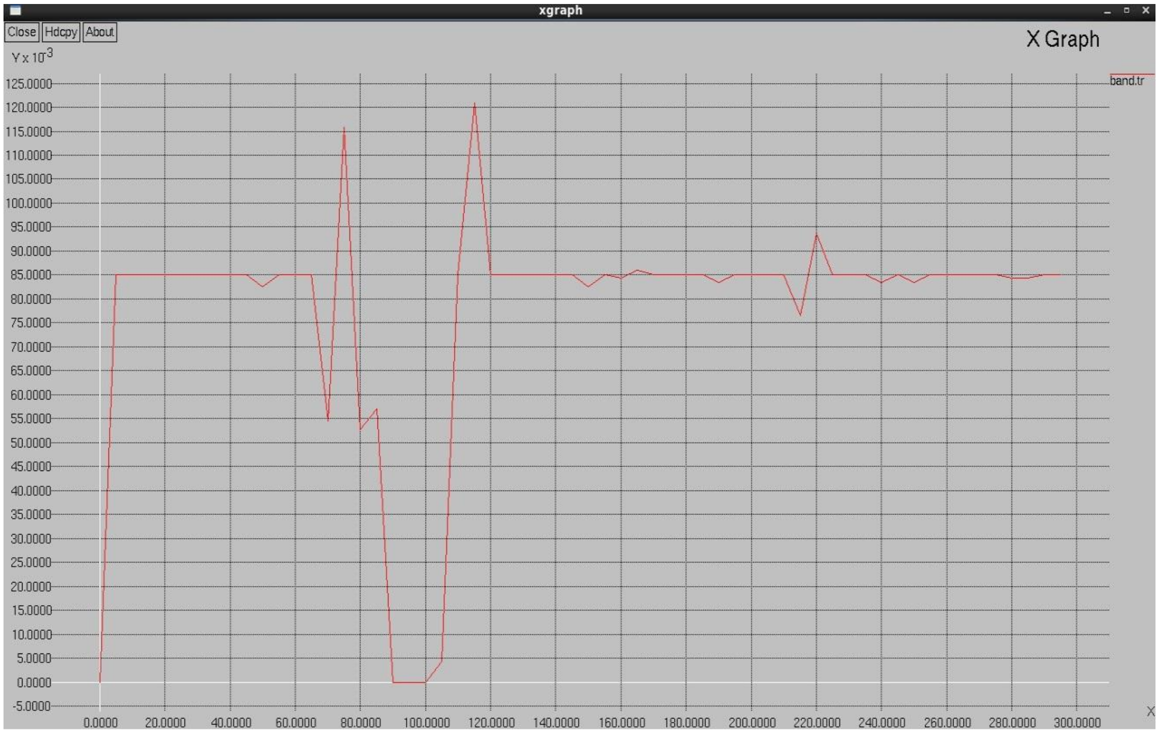

Figure 5.5: AODV Effective Bandwidth (NN=60, PS 512bytes)

Figure 5.6 shows the effective throughput for DSDV protocol. As shown in the figure, DSDV gives a fluctuating throughput performance, with best throughput at 85Mbit/s. Another time the network doesn't seem to be stable. This is a result of the mechanism that DSDV employs. Mobile nodes update their route entries for the gateways more often, resulting in fresher and shorter routes. DSDV protocol doesn't start transmission early. As shown in Figure 5.6, its first transmission seems to start at time 35s with very low effective throughput, though it begins to perform better as the transmission continues. It also shows that the packet delivery ratio is 60% as packets didn't get to the destination until about 40s. We can confirm this in Figure 5.1.

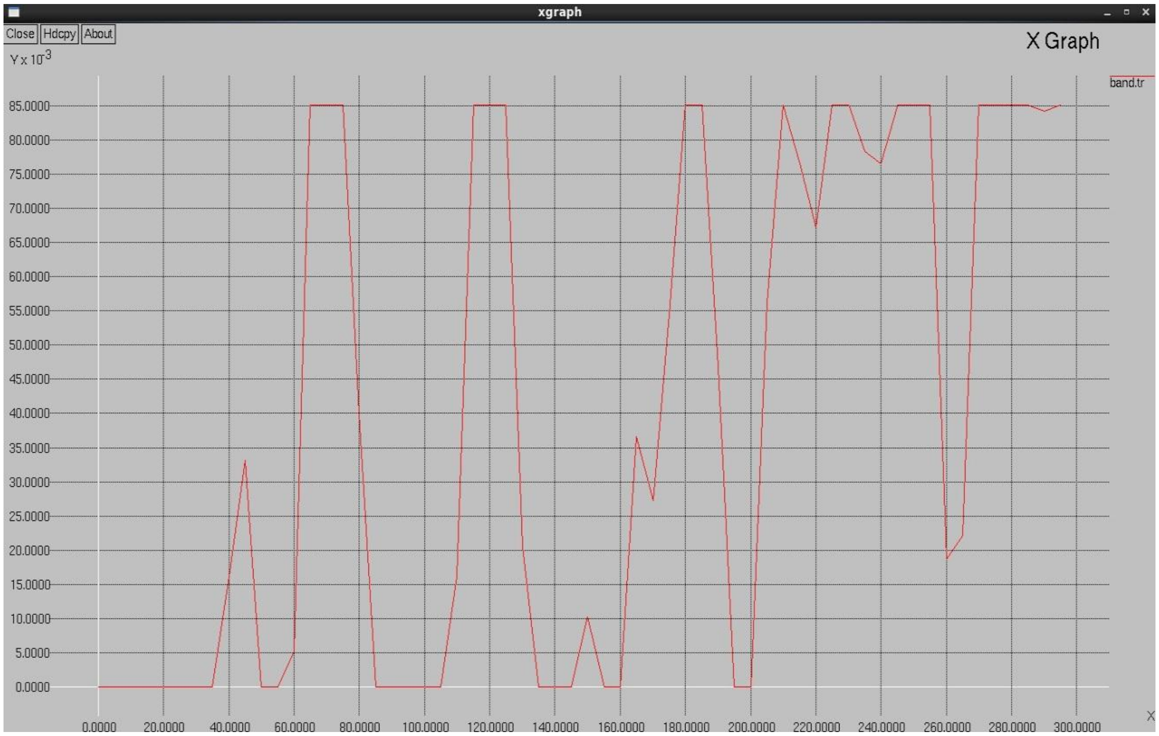

Figure 5.6: DSDV Effective Bandwidth (NN=60, PS 512bytes)

Figure 5.7 shows the effective bandwidth for DSR protocol. It performs much better than DSDV with good throughput from 0s and maintained for a long transmission time until till it breaks at 80s. Because it's an on-demand protocol (the routes are created when required) it maintains the route until it's no longer needed.

Next, let's consider the three protocols AODV, DSR, and DSDV under DoS attack, where Figure 5.8, 5.9 and 5.10 shows the results respectively,

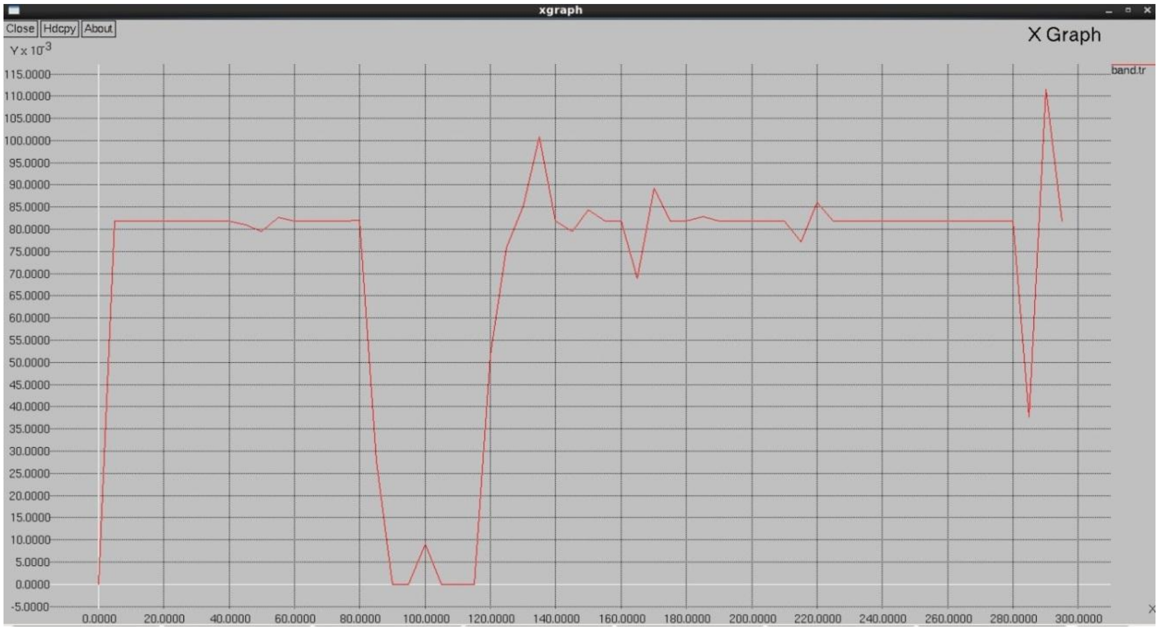

Figure 5.7: DSR Effective Bandwidth (NN=60, PS 512bytes)

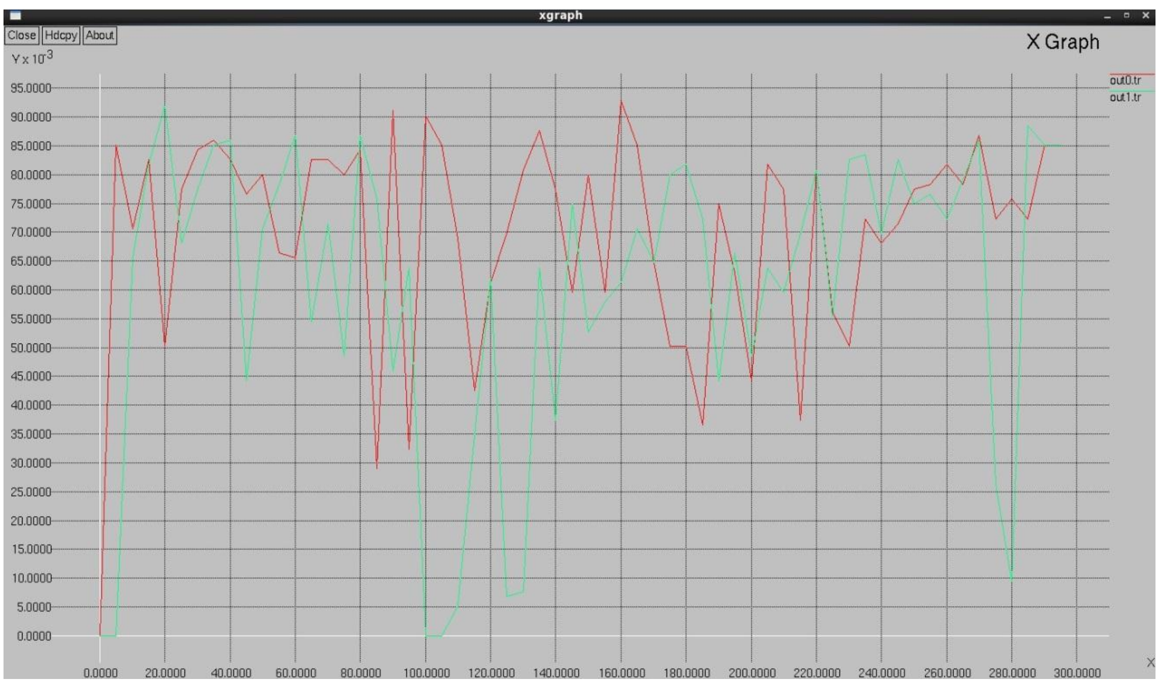

Figure 5.8: AODV DOS Effective Bandwidth

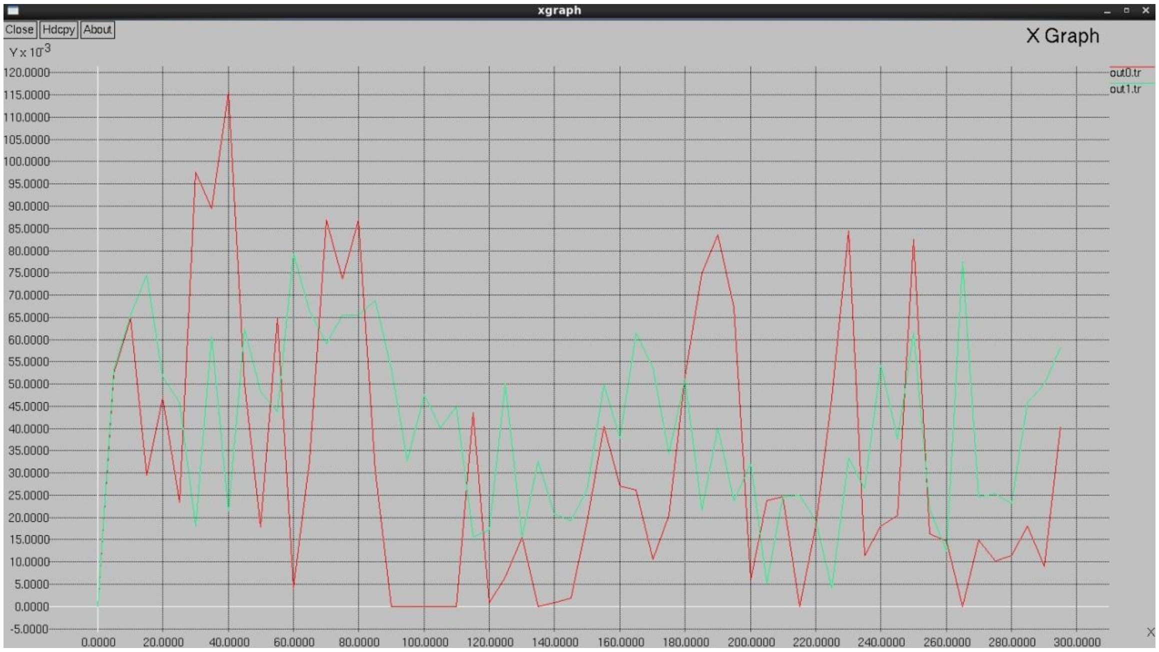

Figure 5.9: DSR DOS Effective Bandwidth

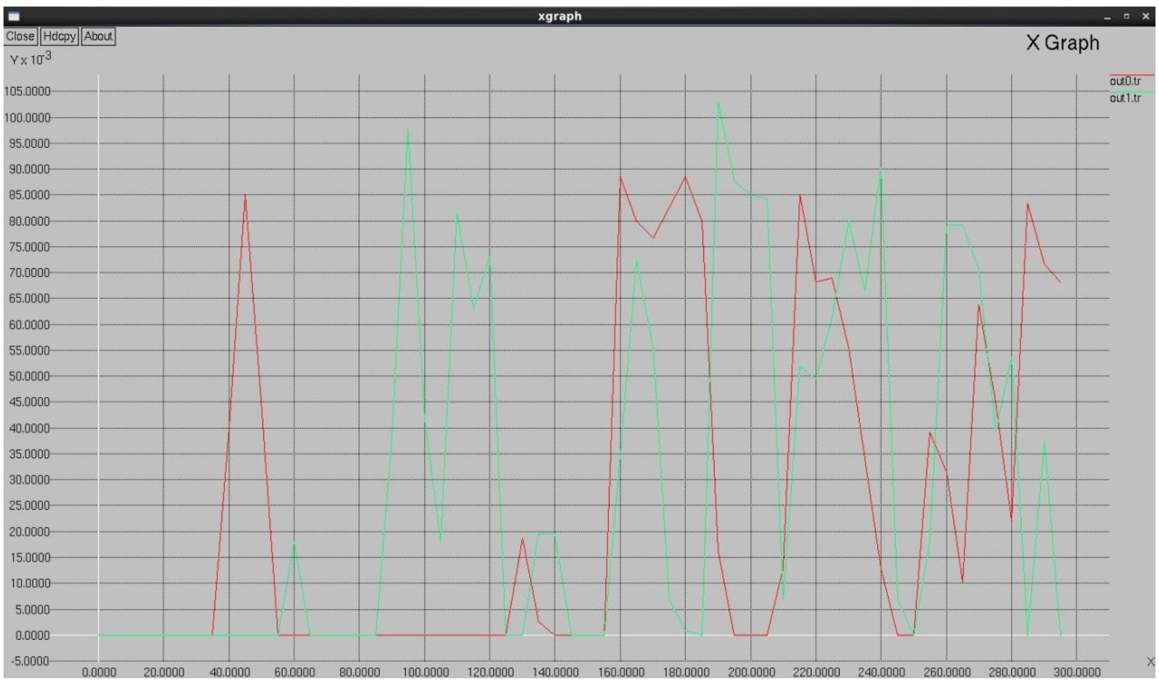

Figure 5.10: DSDV DOS Effective Bandwidth

The red line graph signifies the legitimate network, the green line graph represents the malicious traffic. The graphs show the division of the available bandwidth between the legitimate and DoS traffic. AODV transmits the legitimate traffic better than DSR and DSDV.

Figure 5.11 shows the node utilization for AODV plotted against the number of nodes. As expected, the source (0) and destination nodes (1) have higher node utilization, whereas node 16 for instance has low utilization. So we didn't consider node 1 and 0 in the calculation of average utilization. Utilization is how many times a node has been used during packet transmission, which could also be called the usage frequency of each node. The higher the node usage the less the battery power and vice versa. Node utilization affects the battery life of a node.

The average node utilization for AODV is 780. It means that for this protocol to perform effectively, each node needs at least enough battery life that can be utilized for retransmitting data over 780 times. For comparison with protocols DSDV and DSR, graphical illustration are given in Figure 5.12 and in Figure 5.13.

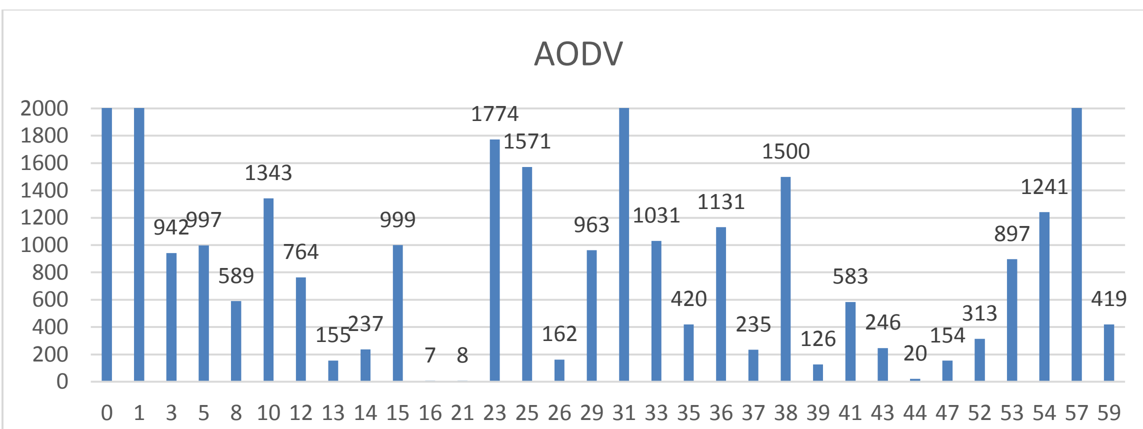

Figure 5.11: Node Utilization AODV (NN= 60, ST = 300s), Average Utilization =780

Figure 5.12 shows node utilization for DSDV protocol. The average node utilization for DSDV is 500, which is better than AODV protocol. DSDV needs less battery power to run the same simulation.

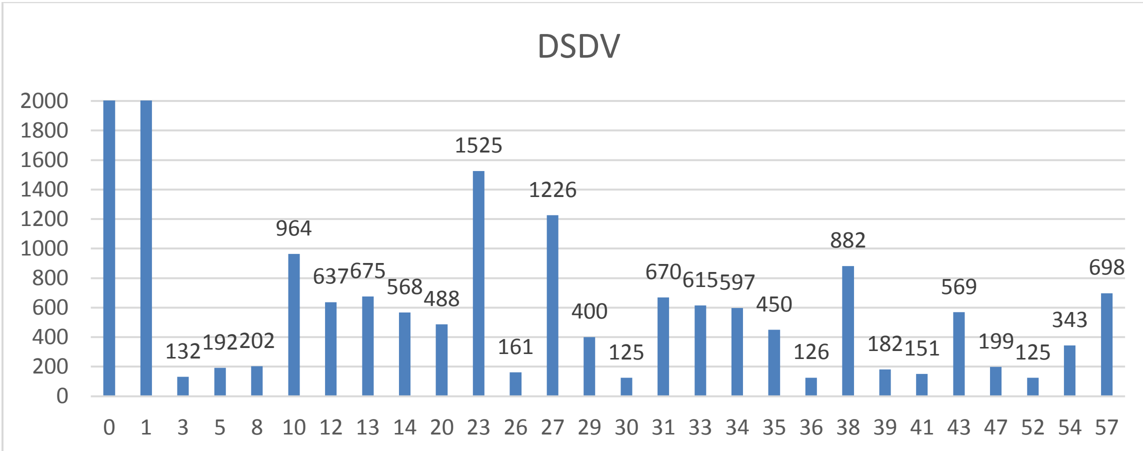

Figure 5.12: Node Utilization DSDV (NN= 60, ST = 300s), Average Utilization = 500

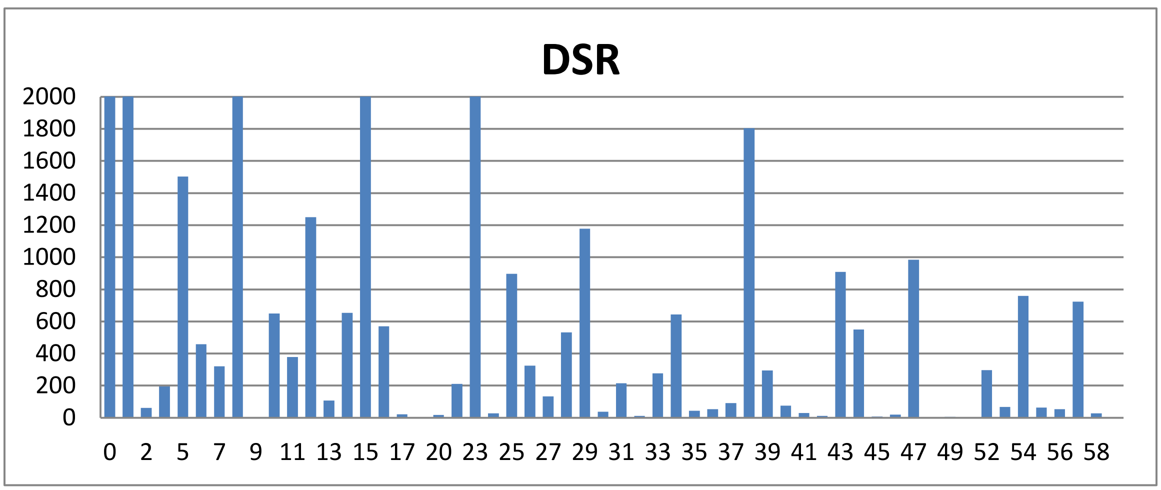

Figure 5.13: Node Utilization DSR (NN= 60, ST = 300s), Average Utilization = 450

Figure 5.13 shows the Node utilization for DSR routing protocols. The average utilization for DSR is 450. DSR has the least node utilization.

An attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node.

Figures 5.14, 5.15, 5.16 show the node utilization with DoS attack for each protocol. The average utilizations are DSR = 393, DSDV = 385 and AODV = 483. These averages are less than those without DoS network.

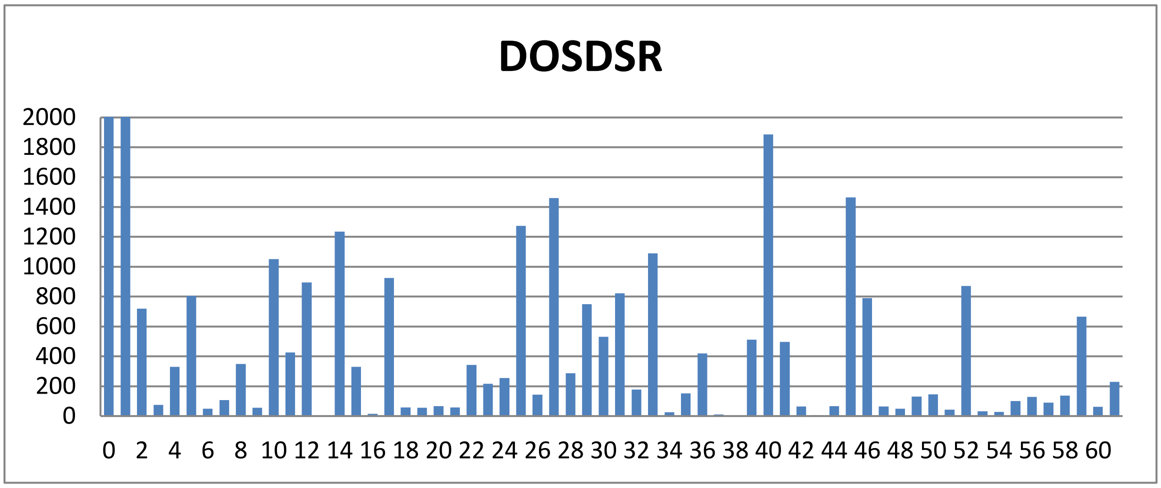

Figure 5.14: Node Utilization DSR with DOS, Average Node Utilization 393

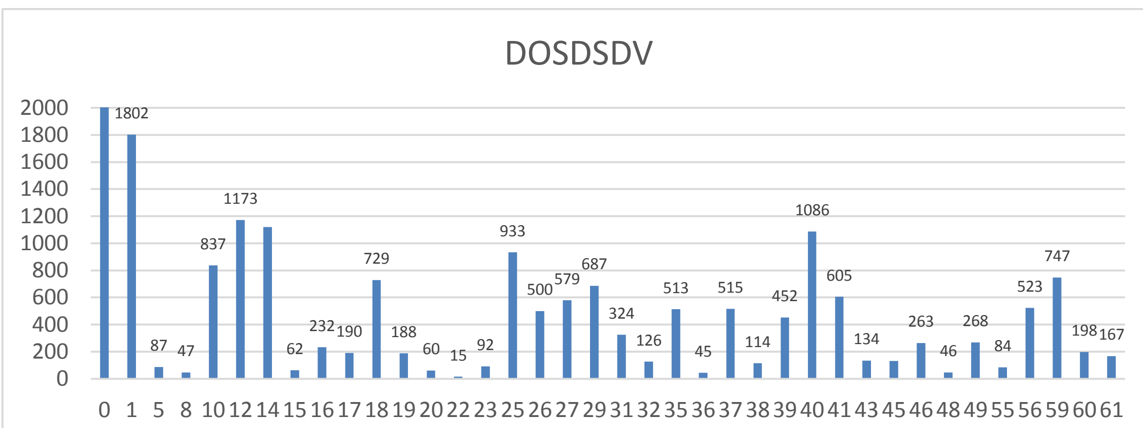

Figure 5.15: Node Utilization DSDV with DOS, Average Node Utilization 385

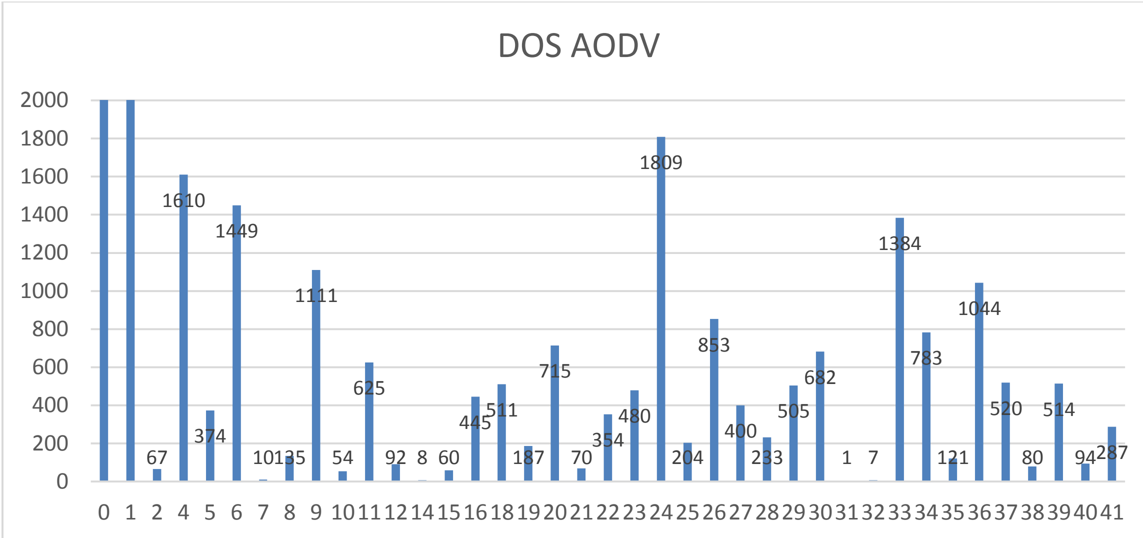

Figure 5.16: Node Utilization AODV with DOS, Average Node Utilization 483

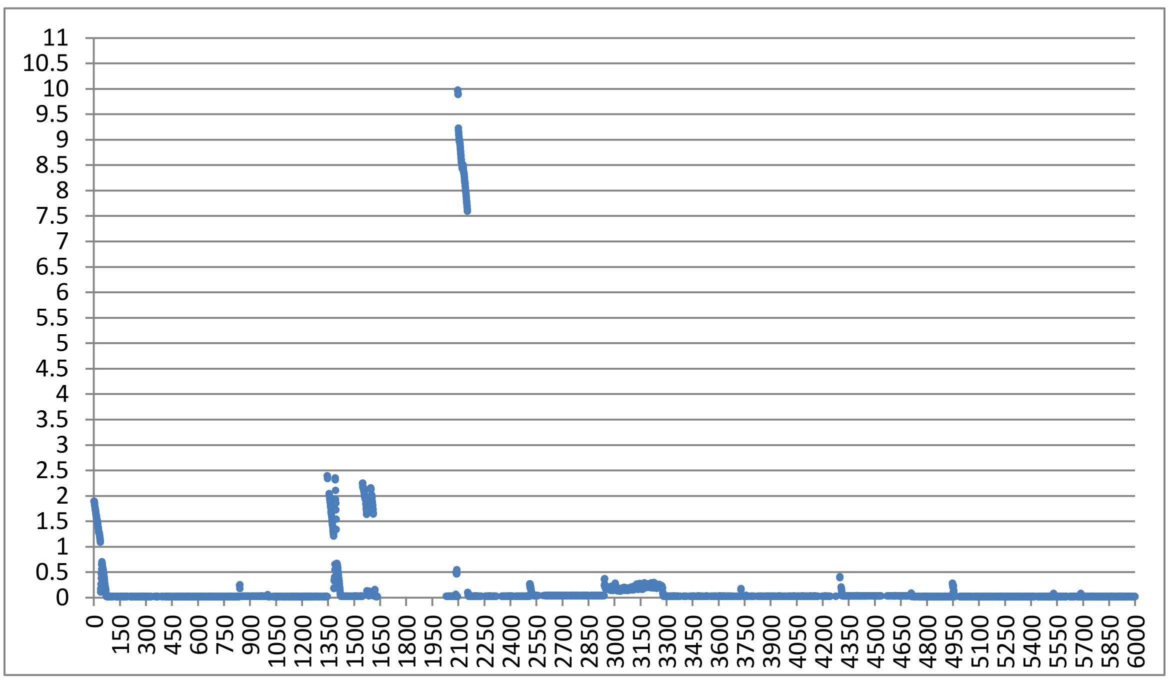

Figure 5.17: AODV Delay per packet, Average Delay per packet = 0.17487s

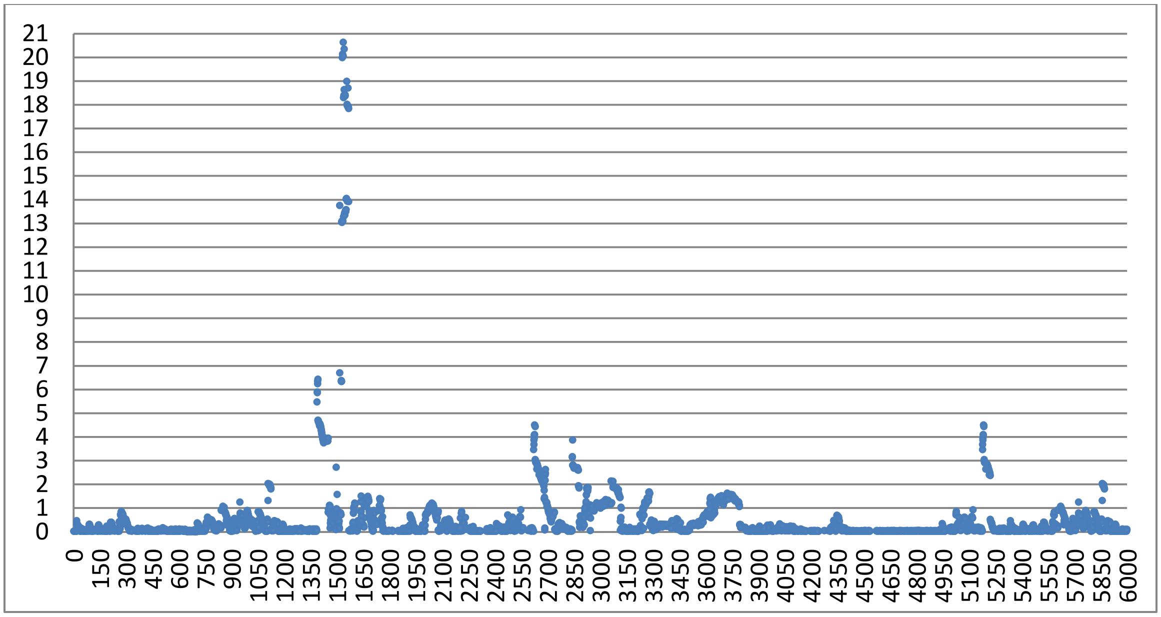

Figure 5.18: DOS AODV delay per packet, Average delay per packet = 0.5413s

Figures 5.17 and 5.18 present the delay for each packet in a no-DoS network and a DoS network for AODV routing protocol. Network size is 60 nodes, delay (s) is on the vertical axis and individual packets are on the horizontal axis.

From the Figures 5.17 and 5.18 we can see a significant difference in delay when the network is under attack. Because of the aggressive flooding in the network, it is difficult to establish a valid route and as a result the packets have more delay.

Figures 5.19 and 5.20 show the path length for DoS and no DoS network. Path length is the number of hops it took each packet from the source node before it got the destination node. From the figures, the path length average for no DoS is lower than DoS. Also from these figures, we can relate the path length to the delays in packet delivery which are shown in Figure 5.17 and Figure 5.18.

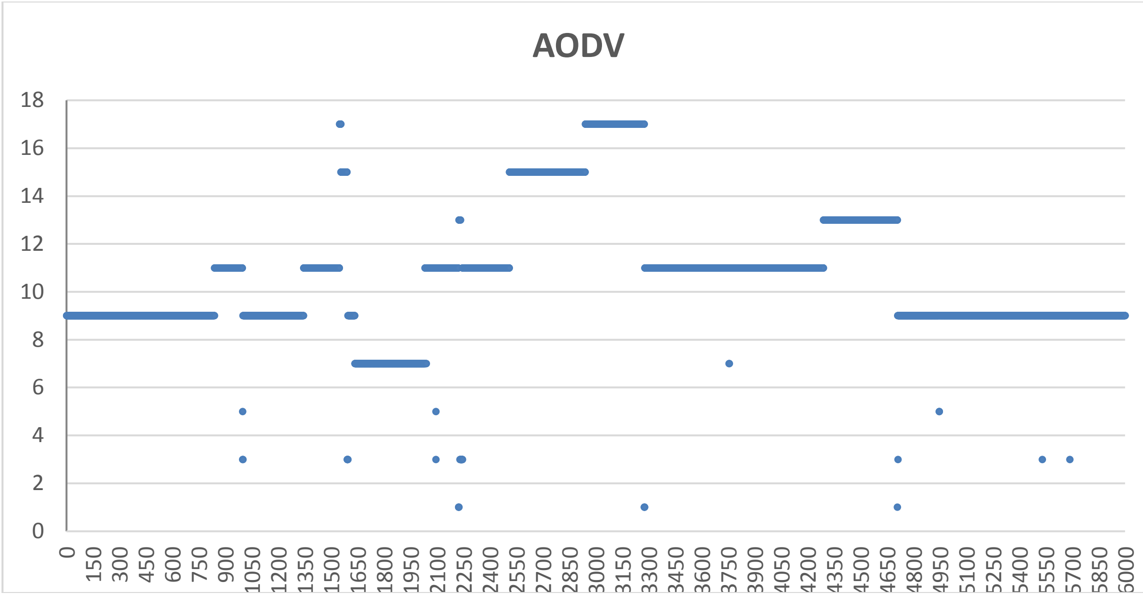

Figure 5.19: AODV Path length, Average Path length = 10.642

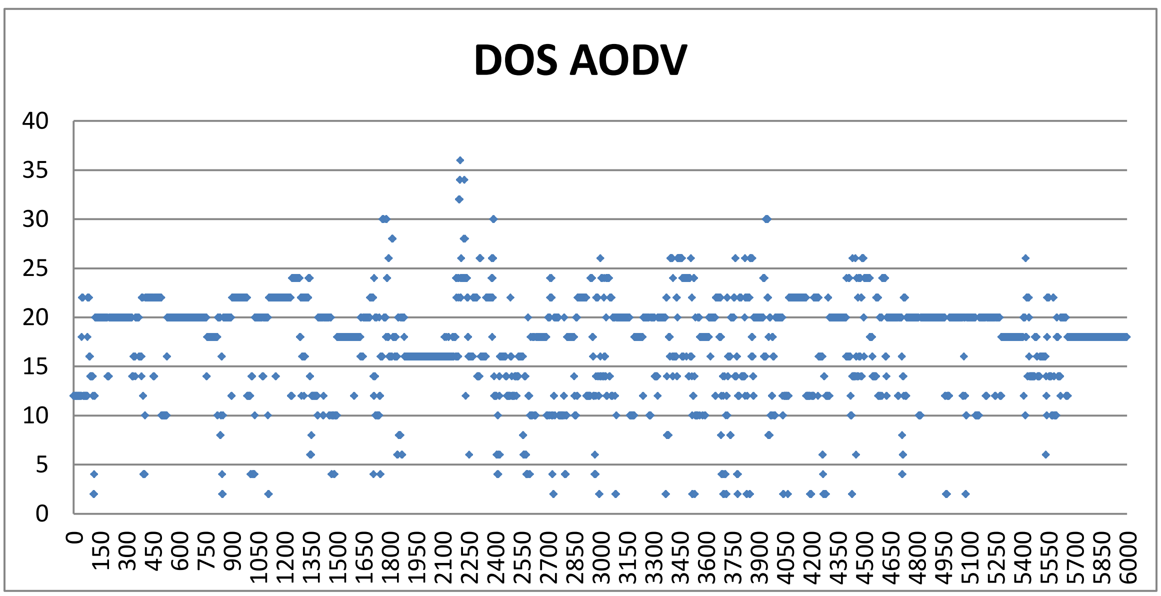

Figure 5.20: DoS Path lengthAverage Path length = 17.51267

Figure 5.21 shows the degradation of delay per packet in AODV. The degradation in this case is defined as the difference between the no DoS delay per packet and the DoS delay per packet. It shows the delay difference in seconds on the vertical axis and individual packets on the horizontal axis.

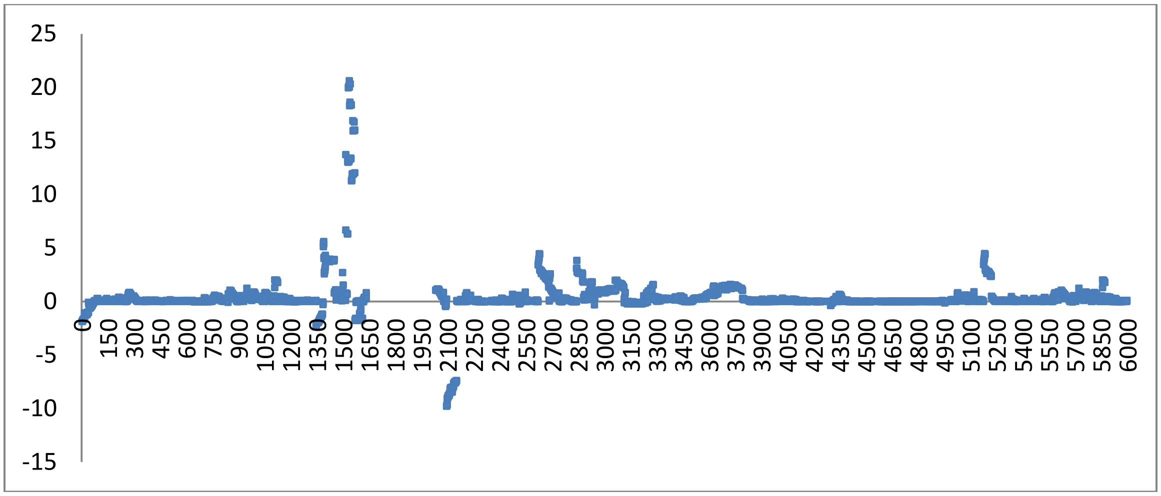

Figure 5.21: Degradation of delay per packet in AODV

DSDV

Figures 5.22 and 5.23 show the delay per packet in a no-DoS network and a DoS network for DSDV routing protocol. Delays (s) is on the vertical axis and individual packets on the horizontal axis. The average delay for DSDV with DoS 0.025263s is higher than the delay DSDV with no DoS 0.6643s. Though the delay in DSDV is not as high as AODV, there is still a significant difference when the network is attacked. We can confirm this from Figures 5.24 and 5.25: the path length averages are 6.27 and 11.7, the lower path length shown means less delay for each packet.

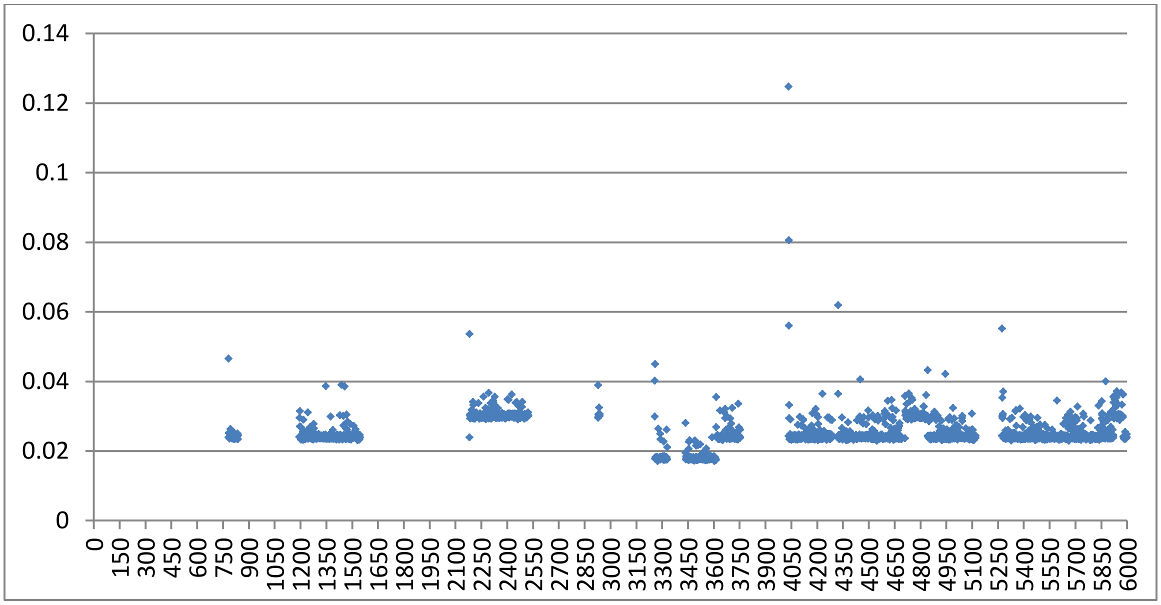

Figure 5.22: DSDV Delay per packet, Average packet delay: 0.025263s

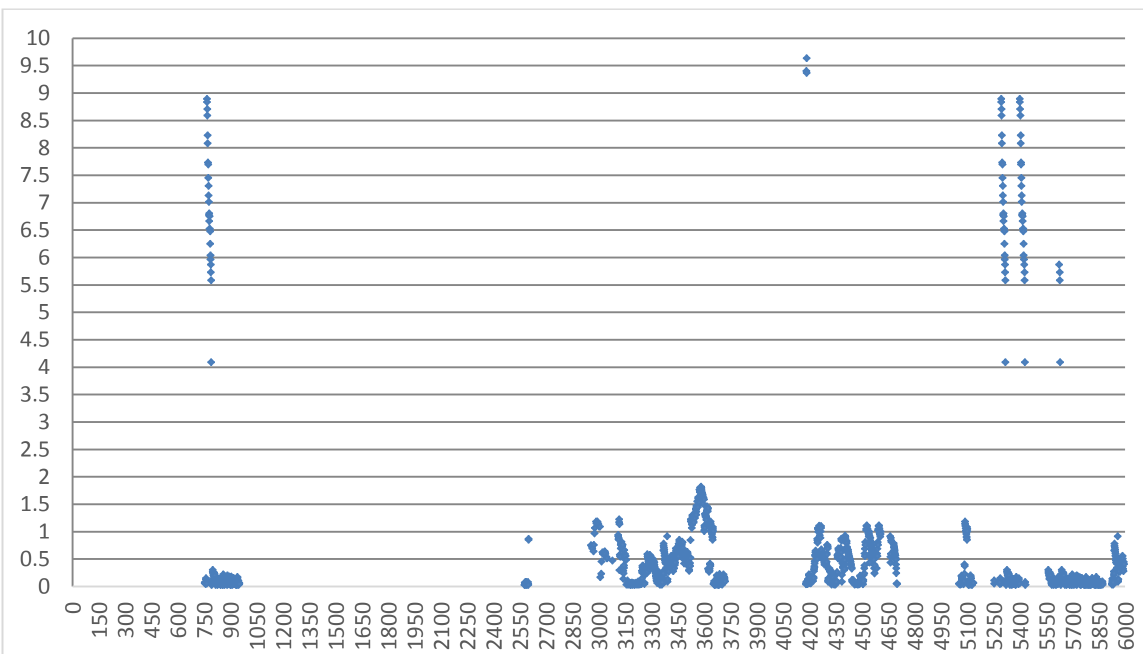

Figure 5.23: DOS DSDV delay per packet, Average delay per packet 0.6643s

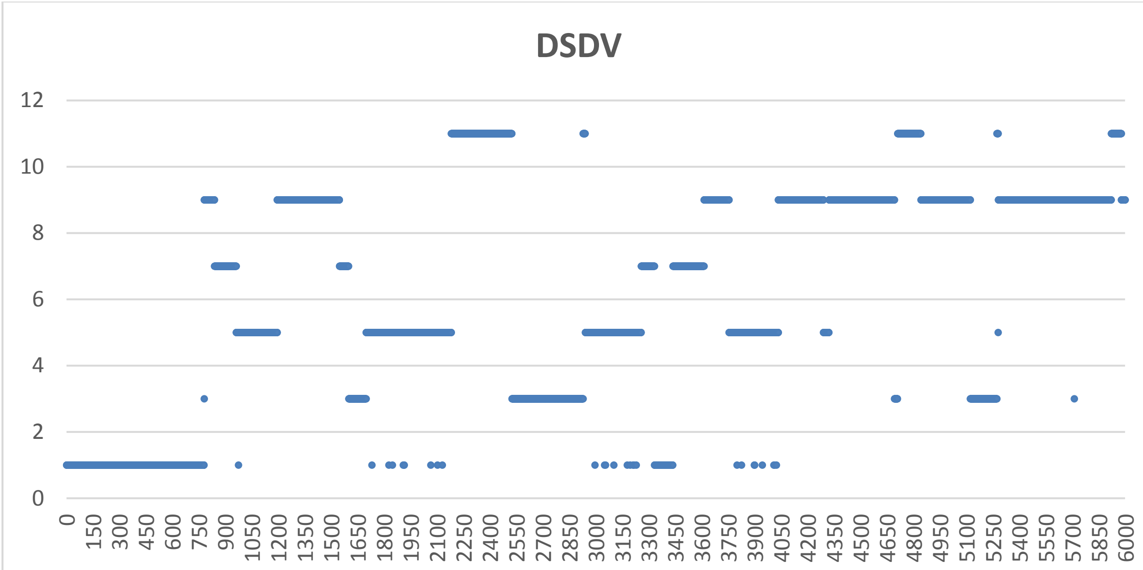

Figure 5.24: DSDV Path length, Average path length =6.275333

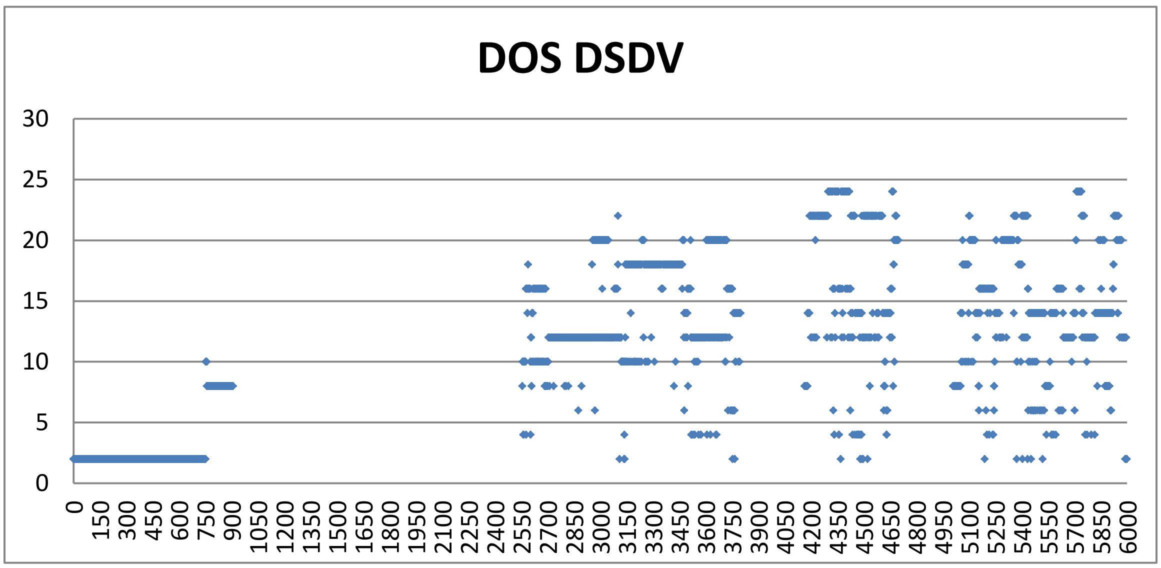

Figure 5.25: DOS Path length, Average Path length= 11.72133

Figure 5.26 shows the degradation of delay per packet in AODV. The degradation in this is the difference in the packets delivered in No DoS delay per packet and the DoS delay per packet. It shows the delay difference in seconds on the vertical axis and individual packets on the horizontal axis.

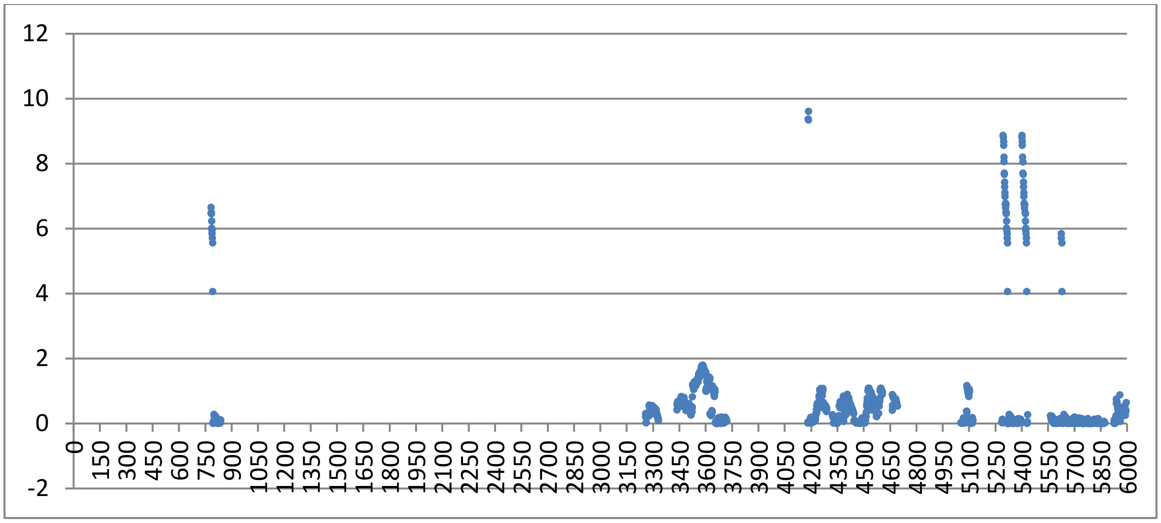

Figure 5.26: Degradation of delay per packet DSDV

DSR

Figures 5.27 and 5.28 present the delay time for each packet in a no-DoS network and a DoS network for DSR routing protocol. Network size of 60 nodes, delay (s) is shown on the vertical axis, while individual packets are indicated on the horizontal axis. DoS with DSR has higher delays, and it also has the highest delay among the three routing protocols.

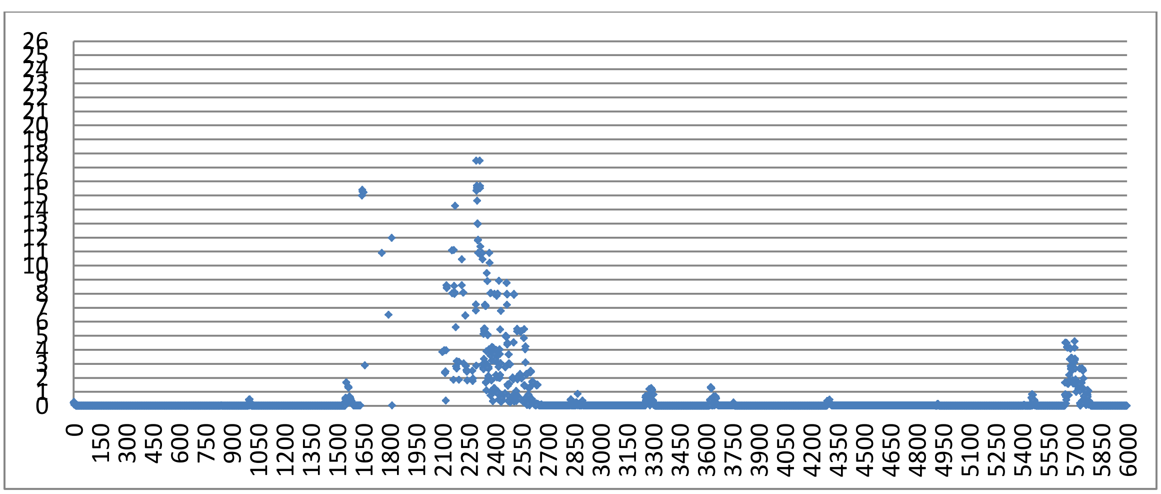

Figure 5.27: DSR delay per packet, Average delay packet = 0.34227s

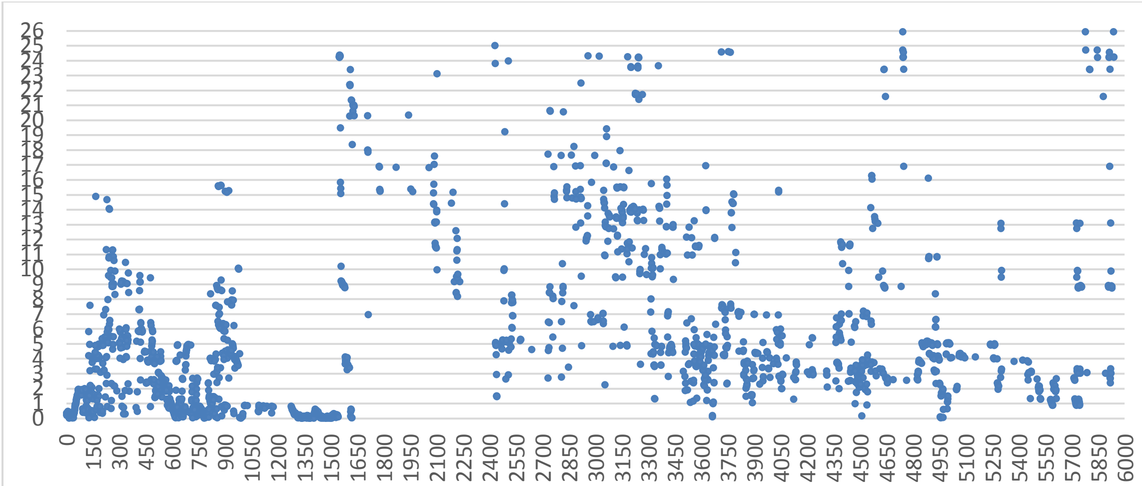

Figure 5.28: DOS DSR delay per packet, Average delay per packet = 5.7671s

Figures 5.29 and 5.30 show the path length for DSR with no DoS and DoS. The average path length also differ as a result, the DoS attacks make the path longer which causes more delay to the destination node.

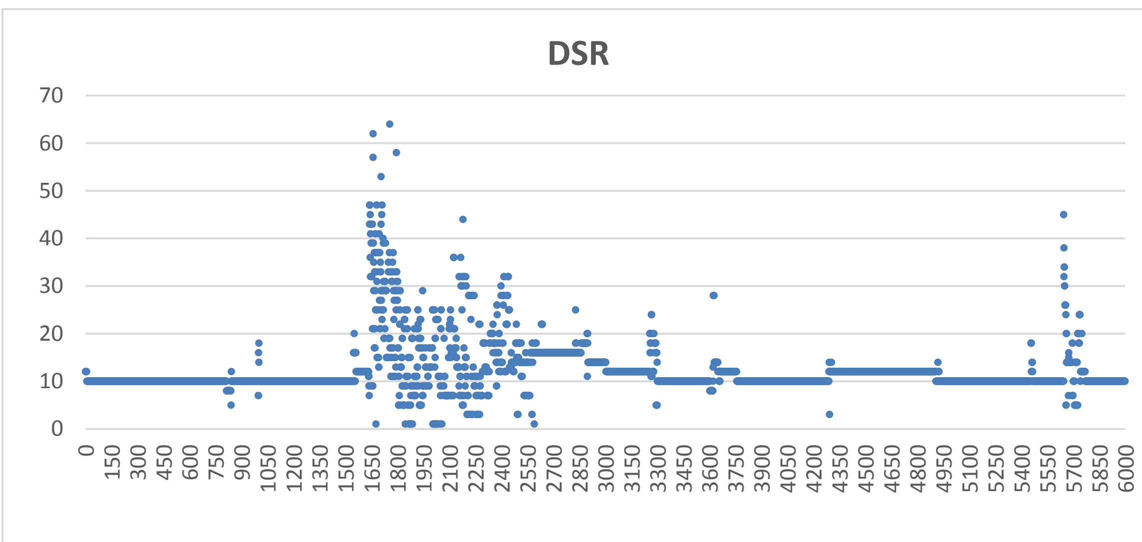

Figure 5.29: DSR Path length, Average Path length = 11.80717

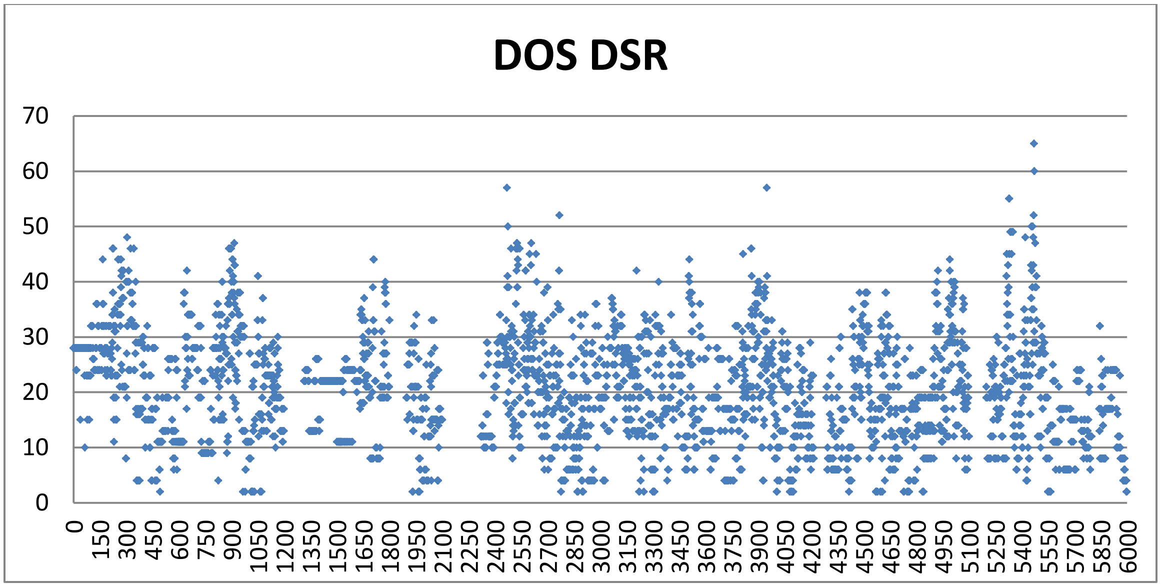

Figure 5.30: DOS Path length, Average Path length = 19.33833

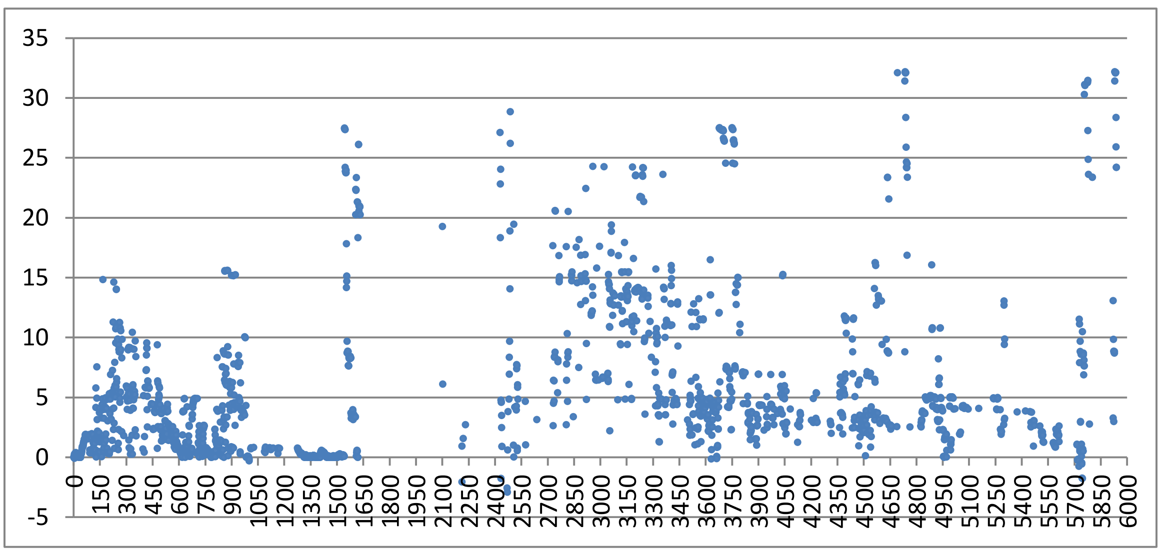

Figure 5.31: Degradation of delay per packet DSR

5.2 Summary

In comparing the three protocols AODV, DSR and DSDV, the simulation results gave important findings, especially on those which have impacted the performance of routing protocols in MANETs. The presence of varying network size and security attacks in the network gave different response to DSDV, DSR, and AODV routing algorithms.

These routing protocols were compared in terms of packet delivery ratio, average end-to-end delay, effective bandwidth, node utilization and path length. Our simulations have shown that performance of a routing protocol varies across different performance metrics. Figure 5.32 gives a summary of the packet delivery ratio of the three routing protocols, in a scenario of a legitimate network and the same network with multiple DoS attacks. From this figure AODV performs better than DSR and DSDV respectively. AODV performs better by having a prior knowledge of neighbors, hence preventing loops and determining the freshest routes. In DSR, where RREQ and RREP messages are used every node in this routing protocol will be able to communicate by maintaining information of only active routes to the destination node [25].

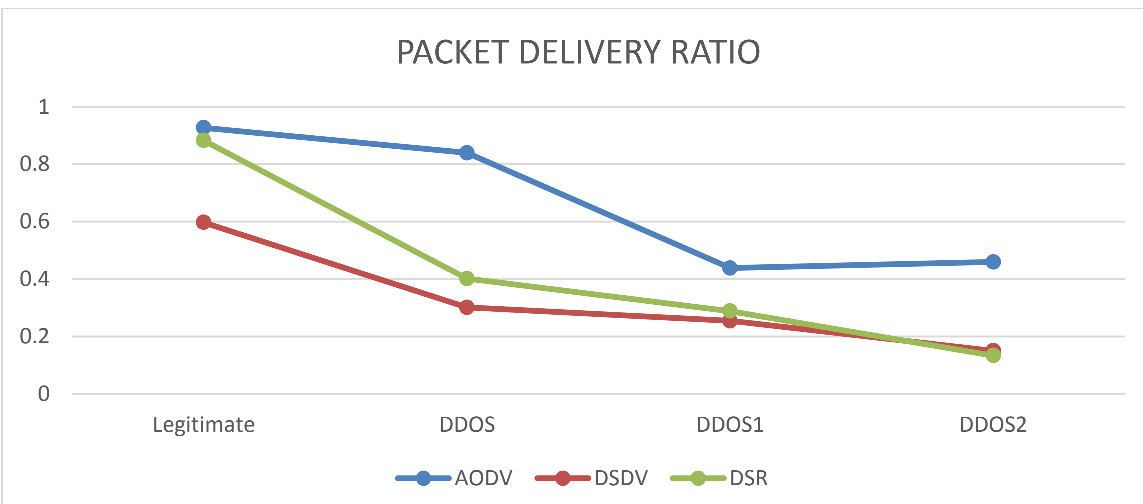

Figure 5.32: PDR with DDOS1, 2.

End to end delay plays an effective role in the scalability of routing protocols. The time it takes a packet to arrive at its destination has an impact on routing protocol performance. Regarding the average end to end delay for varying network size, as shown in Figure 5.3

DSDV has the least delay for large, medium or small network sizes. One factor for this is that it uses full dump or incremental update on nodes, resulting in fresher and shorter routes.

AODV has a lower delay than DSR because of its RREQ mechanism. In DSR when a RREQ message is sent, a destination replies to all RREQ when it receives which therefore resulting in difficulty in determining the least congested route. whereas in AODV a destination replies only to the first RREQ it receives.

The presence of DoS on the network, as shown in Figure 5.4, increases the delay of each routing protocol. DSR still has the highest delay and AODV the lower delay.

For the node utilization metric some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. Nodes of a mobile ad hoc network are often battery-powered, thus, energy is a precious resource that they may not want to waste for the benefit of other nodes [14]. In Figures 5.11, 5.12 and 5.13 DSR has the least average node utilization at 450 while AODV has the highest average node utilization which means it requires more battery power.

Figures 5.14, 5.15 and 5.16 show the reaction of routing protocol to MANET's performance in node utilization under DoS attack. An attacker forces a node to replay packets to exhaust its energy. An attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node.

The addition of malicious nodes makes the node utilization lower in our experiment, which implies that DoS disrupts the network thereby reducing the routing function of each node rather than serving the network the rogue nodes were been used. AODV has the highest utilization and DSDV has the least. The average utilizations are DSR = 393, DSDV = 385 and AODV = 483.

For the path length and the delay per packet metric, in routing protocols the path length, in terms of the number of hops, determines the delay of each packet. Figures 5.19, 5.24 and 5.29 show the path length for AODV, DSDV and DSR respectively. DSDV has the least hop count with an average of 6.3 hops for each packet to reach its destination, while DSR has the highest hop count with an average hop count of 11.8 and AODV has an average hop count of 10.6. Figures 5.17, 5.22 and 5.27 show the delay per packet for different protocols, which indicate that DSDV outperformed the other routing protocol AODV and DSR with very low delay. This delay is dependent on the hop count. DSDV has the least hop count because every node in this routing protocol maintains information of only active paths to the destination nodes and the packet forwarding is done faster, therefore the delays are also the least.

AODV has lower hop count and lower delay than DSR because we have only one source node and one destination in our network. It is only the source node that caches the route to the destination when the DSR protocol is used, while with AODV each node on the discovered route maintains a routing entry.

DSR's higher hop count may be attributed to the fact that it maintains and uses non optimal routes from the cache [23]. As transmission increases, DSR becomes more aggressive in its caching, therefore hop count increases, and thereby delay increases. In the DoS scenario the results were still the same, DSDV still the least and DSR having the highest hop count.

In summary on-demand protocols AODV and DSR seems to outperform proactive protocols DSDV.

Table 5.1: Result comparisons

	Packet delivery Ratio	Packet delay	Node utilization	Path length
AODV	Highest	Medium	medium	Medium
DSR	Medium	Highest	lowest	Highest
DSDV	Lowest	Lowest	Highest	lowest

Chapter 6

Conclusions and Recommendations

The simulation based study of the impact of routing protocols DSDV, DSR, and AODV in MANET has been conducted to evaluate the performance of each of them based on CBR traffic. The results of the comparative analysis show that our performance evaluation mechanisms are effective enough in NS2. The routing protocols were compared in terms of packet delivery ratio, average end to end delay, effective throughput, node utilization and path length. Our simulations have shown that performance varies across different performance metrics. It is observed that AODV and DSR perform better in simulations than DSDV. These results not only help by doing a comparative analysis but also an insight into the variables that are affecting routing performances.

In any network size where the resources are not distorted (by a DoS attack) the AODV protocol performs well in most cases. One of the contributing factors towards the good performance of AODV protocol could be due to the type of data traffic used, AODV employs the algorithm that prevents loops and determines the freshest routes. From the results, in the throughput/delivery ratio metrics, the performance of the routing protocols varied with varying network sizes. DSR and AODV performed very well, while the performance of DSDV was poor. Mobility in MANETs makes end to end delay metric important. The results suggest that DSR have high delays in small, medium or large network size which is not good for an ad hoc network, but the DSDV and AODV protocol perform much better. For the utilization metric, battery life (energy) of each node in an ad hoc network is very important. According to the results DSR will maintain the least battery usage in any network size. AODV will still maintain the energy of each node but will run out much earlier than the two other protocols.

The results also provide some insights to the effect of security attack in MANETs. The presence of a security attack (DoS) causes a decline in performance of each protocol. Our results suggest that in any network size, traffic load and mobility, an ad hoc network will be very low. The throughput/delivery ratio metric of an ad hoc network under DoS attacks shows that AODV performs better, DSR decreases performance while DSDV is hugely affected. The average delay metric in a distorted network shows that AODV and DSDV have the least delays, DSR in a small network size may perform well but with medium or large network size it will have a woeful performance. The utilization metric shows that DSR reacted favorably since it requires the least energy needed for the network. DSDV can also be recommended. AODV didn't react well as the node consumes more energy under the attack.

In all, AODV protocol reacted favorably under DoS attack, which makes it more recommended at such a time. DSDV performs well in average delay and energy needed. It performs poorly in delivery ratio, which makes the protocol not suitable during DoS attacks. Though DSR protocol has the least amount of energy needed, the end to end delay is very high and delivery ratio is very low. Thus, it won't be a good protocol when ad hoc network is under attack.

Security attacks should be taken into account at the early stages of a routing protocol design. When no countermeasures are taken, the network performance is distorted and could be very damaging to the network operation. The analysis has proven that AODV can perform better using our metrics with least delays in packet delivery, less path length from source node to destination node, less amount of energy needed, and packets delivered safely to the destination. The on-demand protocol AODV performs better, being an improvement from DSR and DSDV, and turns out to be a highly versatile protocol. We attribute a slight advantage in the performance of the AODV protocol to the specifics of our experiment and to a different way the three protocols maintain and update the route information.

6.1 Future Work

The report focuses on investigating the performance of MANETs routing protocol, and impact of security attacks (DoS) in MANETs. Further investigations and research on security issues in MANETs are possibilities in future work. Since we can conclude that AODV and DSR perform better than DSDV in implementing a new protocol the features of AODV should be improved upon. Conduct future investigation of routing protocols under different mobility models and different DoS scenarios (other than RWP).

Bibliography

[1] A. K. Sharma, and N. Bhatia, "Behavioral study of MANET routing protocols by using NS-2", IJCEM International Journal of Computational Engineering and Management, Vol. 12, 2011, pp. 100-104.

[2] C. Newport, Simulating mobile ad hoc networks: a quantitative evaluation of common MANET simulation models, Dartmouth College Science, 2004.

[3] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks", Personal Communications, IEEE, Feburary 2001, pp. 16-28.

[4] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research", Wireless communications and mobile computing, Vol. 2(5), 2002, pp. 483-502.

[5] P. Michiardi and R. Molva, "Simulation-based analysis of security exposures in mobile ad hoc networks", In European Wireless Conference. Feb.2002

[6] W. G. Lol, An investigation of the impact of routing protocols on MANETs using simulation modelling (Doctoral dissertation, Auckland University of Technology).2008

[7] J. V. E. Molsa, "Increasing the DoS attack resiliency in military ad hoc networks", Military Communications Conference, IEEE. Vol.4, Oct. 2005, pp. 2282-2288.

[8] D. Muhit, "Performance Evaluation of Aodv, Dsr, Dsdv Mobile Ad-Hoc Protocols on Different Scenarios: An Analytical Review", International Journal of Advances in Computing and Information Technology, Vol. 1, Feb. 2012, pp. 26-45.

[9] A. Ferreira, A. Goldman, and J. Monteiro, "Performance evaluation of routing protocols for MANETs with known connectivity patterns using evolving graphs", Wireless Networks, Vol.16 (3), 2010, pp. 627-640

[10] F. Bai, and A. Helmy, A survey of mobility models. Wireless Adhoc Networks University of Southern California, USA, 206, 2004.

[11] G. J. Moses, D. S. Kumar, P. S. Varma, and N. Supriya, "A Simulation Based Study of AODV, DSR, DSDV Routing Protocols in MANET Using NS-2", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2(3), March 2012, pp. 43-51.

[12] J. K. Parmar, and M. Mehta, "PERFORMANCE EVALUATION OF NS2 AND OMNET++ SIMULATORS FOR AODV PROTOCOL IN MANET", International Journal of Research in Engineering and Technology, Vol.3(2), Feb.2014, pp. 609-615.

[13] S. D. Khatawkar, K. K. Pandyaji, R. M. Patil, V. M. Sali, and U. L. Kulkarni, "Performance Comparison of DSDV, AODV, DSR, Routing protocols for MANETs", International Conference on Computer Networks and Communication Systems, IPCSIT, Vol. 35, 2012, pp. 44-48.

[14] R. P. Reena, and V. Richariya, "Performance Evaluation of Routing Protocols for MANET using NS2", International Journal of Computer Applications, 2013, pp. 12-16.

[15] C. Bettstetter, and C. Wagner, "The Spatial Node Distribution of the Random Waypoint Mobility Model", WMAN, Vol.11, 2002, pp. 41-58.

[16] I. Stojmenovic, and X. Lin, “Power-aware localized routing in wireless networks. Parallel and Distributed Systems”, IEEE Transactions on, Vol.12 (11), 2001, pp. 1122-1133.

[17] A. Shrivastava, A.R. Shanmogavel, A. Mistry, N. Chander, P. Patlolla, and V. Yadlapalli, Overview of Routing Protocols in MANET’s and Enhancements in Reactive Protocols, Department of Computer Science Lamar University. 2005

[18] X. Hong, M. Gerla, G. Pei, and C. C. Chiang, “A group mobility model for ad hoc wireless networks”, Proceedings of the 2nd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems, 1999, pp. 53-60.

[19] E. M. Royer, and C. K. Toh, “A review of current routing protocols for ad hoc mobile wireless networks”, Personal Communications, IEEE, Vol.6 (2), 1999, pp. 46-55.

[20] J. Hortelano, M. Nácher, J. C. Cano, C. Calafate, and P. Manzoni, “Evaluating the goodness of MANETs performance results obtained with the ns-2 simulator”, Proceedings of the 2nd international conference on Performance evaluation methodologies and tools, 2007, pp. 13.

[21] G. Lin, G. Noubir, and R. Rajaraman, “Mobility models for ad hoc network simulation”, INFOCOM, Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, Vol.1, 2004, pp. 454-463.

[22] B. Ishibashi, and R. Boutaba, “Topology and mobility considerations in mobile ad hoc networks”, Ad hoc networks, Vol 3(6), 2005, pp. 762-776.

[23] O. Balci, “Principles and techniques of simulation validation, verification, and testing”, Simulation Conference Proceedings, Feb. 1995, pp. 147-154.

[24] Margaret Rouse (2006) TechTarget. Retrieved 05 May 2015, from http://searchdatacenter.techtarget.com/definition/sensor-network

[25] H. Li, and M. Singhal, “A secure routing protocol for wireless ad hoc networks”, Proceedings of the 39th Annual Hawaii International Conference, Jan. 2006, Vol. 9, pp. 225-225.

[26] A. Wood, and J. A. Stankovic, “Denial of service in sensor networks”, Computer, Vol.35 (10), 2002, pp. 54-62.

[27] M. Al-Shurman, S.M. Yoo, and S. Park, “Black hole attack in mobile ad hoc networks”, Proceedings of the 42nd annual southeast regional conference, 2004, pp. 96-97.

[28] K. Patel, J. DeDourek, and P. Pochec, “Investigation of Channel Formation in a MANET”, Fifth International Conference on, August 2010, pp. 229-231.

[29] Marc Greis. NS-2, The ns Manual (formally known as NS Documentation) Retrieved 02 December. 2014, from http: //www.isi.edu/nsnam/ ns/doc.

[30] P. Garg and A. Tuteja, “Comparative Performance Analysis of Two Ad-hoc Routing Protocols”, International Conference on Network and Electronics Engineering, Vol. 11, 2011, pp. 99-104.

Vita

Candidate's full name: AYANSIJI oluwatola

Universities attended (with dates and degrees obtained): Babcock University 2006- 2010, Computer Information System & University of New Brunswick 2013-2015, Computer Science.