An Investigation of Routing Protocols in Wireless Mesh Networks under certain Parameters

Blekinge Institute of Technology, Karlskrona Campus, Sweden

Authors

1- Waqas Ahmad (830516-2557)
   waqasab007@yahoo.com

2- Muhammad Kashif Aslam (800203-8498)
   kashif_akash4@yahoo.com

Supervisor

1- Alexandru Popescu (PhD Student), BTH Sweden
   alexandru.popescu@bth.se

Examiner

1- Professor Adrian Popescu, BTH Sweden
   adrian.popescu@bth.se
Abstract

Wireless Mesh Networks (WMNs) are bringing revolutionary change in the field of wireless networking. It is a trustworthy technology in applications like broadband home networking, network management and latest transportation systems. WMNs consist of mesh routers, mesh clients and gateways. It is a special kind of wireless Ad-hoc networks. One of the issues in WMNs is resource management which includes routing and for routing there are particular routing protocols that gives better performance when checked with certain parameters. Parameters in WMNs include delay, throughput, network load etc. There are two types of routing protocols i.e. reactive protocols and proactive protocols. Three routing protocols AODV, DSR and OLSR have been tested in WMNs under certain parameters which are delay, throughput and network load. The testing of these protocols will be performed in the Optimized Network Evaluation Tool (OPNET) Modeler 14.5. The obtained results from OPNET will be displayed in this thesis in the form of graphs. This thesis will help in validating which routing protocol will give the best performance under the assumed conditions. Moreover this thesis report will help in doing more research in future in this area and help in generating new ideas in this research area that will enhance and bring new features in WMNs.
Preface

This report is written in the context of final year master’s thesis that is carried out at Blekinge Institute of Technology (BTH), Karlskrona, Sweden. As it is a final year thesis so it is also a last requirement for our degree of Master’s of science in Electrical Engineering with specialization in Telecommunications.

BTH is a well known and among the respectable universities of Sweden. It is one of the high ranking universities in Sweden and in Europe as well. BTH is well equipped with all the necessary laboratories and has very good faculty as well. This master’s thesis has been carried out under the sophisticated environment of BTH and the completion of this thesis has become possible due to the cooperation of BTH and their whole staff.

Our master’s thesis is consisted of the study of Wireless Mesh Networks (WMNs), Routing Protocols (RPs) in WMNs, Design Parameters (DPs) and the simulation of few routing protocols in WMNs under certain parameters. We randomly chosen three routing protocols and tested them under certain parameters in WMNs using OPNET tool. This useful contribution has made it possible to share our thoughts and ideas relating to this topic with everyone.

We would like to thank all the BTH’s staff especially we would like to thank Mr. Mikael Asman, Lena Magnusson, Lina Berglind, our supervisor Mr. Alexandru Popescu and our examiner Mr. Adrian Popescu at Blekinge Institute of Technology, Sweden. Also we would like to thank our parents who have given us feedback in completing our thesis report in an efficient manner.
Acknowledgements

To my parents (mom and dad), you did a big sacrifice by sending their elder son overseas for getting higher education. Your sacrifice was beyond measures to me. Without your brave step, it would become impossible for me to complete my education. I am really very thankful to both of you and will always remember your sacrifice. I would also like to thank my supervisor, Mr. Alexandru Popescu, without his guidance and support; I cannot be able to achieve my goal. He never denied helping us in difficult time. In the end I would also like to thank Mr. Mikael Åsman, Lena Magnusson and all the staff of BTH, without their cooperation it was difficult to achieve the target.

--- Waqas Ahmad

Firstly I am really thankful to my elder brother Shahid Aslam, my parents and my friends who have encouraged me and give me great spirit and enthusiasm to achieve my goal. Secondly I am also grateful to my supervisor Mr. Alexandru Popescu who has given me great learning space and research oriented environment. Finally I acknowledge the credibility of Mr. Mikael Åsman, Lena Magnusson and all the staff of BTH.

--- Muhammad Kashif Aslam
Acronyms

WMNs ------------------------------------------ Wireless Mesh Networks
OPNET ------------------------------------------ Optimized Network Evaluation Tool
AODV ------------------------------------------- Ad-hoc On-Demand Vector
DSR ---------------------------------------------- Dynamic Source Routing
OLSR -------------------------------------------- Optimized Link State Routing
LANs -------------------------------------------- Local Area Networks
MANETs --------------------------------------- Mobile Ad-hoc Networks
PCI ---------------------------------------------- Peripheral Component Interconnect
PCMCIA --------------------------------------- Personal Computer Memory Card International Association
OSI --------------------------------------------- Open System Interconnection
WLAN ----------------------------------------- Wireless Local Area Network
RF ---------------------------------------------- Radio Frequency
PP ---------------------------------------------- Peer to Peer
IS ----------------------------------------------- Infrastructure
AP ---------------------------------------------- Access Point
BW --------------------------------------------- Bandwidth
NLOS ------------------------------------------ Non Line of Sight
LOS -------------------------------------------- Line of Sight
HO --------------------------------------------- Hand Over
QOS ------------------------------------------- Quality of Service
FCA ------------------------------------------- Fixed Channel Allocation
DCA ------------------------------------------ Dynamic Channel Allocation
US -------------------------------------------- United States
MWNs --------------------------------------- Multi Hop Wireless Networks
HWNs --------------------------------------- Hybrid Wireless Networks
WANs --------------------------------------- Wireless Ad-hoc Networks
WSNs --------------------------------------- Wireless Sensor Networks
IDS --------------------------------------- Intrusion Detection System
IPS --------------------------------------- Intrusion Prevention System
MAC -------------------------------------- Medium Access Control
PDe -------------------------------------- Processing Delay
QD -------------------------------------- Queuing Delay
TD -------------------------------------- Transmission Delay
PD -------------------------------------- Propagation Delay
*WANs -------------------------------- Wide Area Networks
IP --------------------------------------- Internet Protocol
TCP -------------------------------------- Transmission Control Protocol
BGP -------------------------------------- Border Gateway Protocol
IGRP ------------------------------------- Interior Gateway Routing Protocol
EIGRP ------------------------------------ Enhanced Interior Gateway Routing Protocol
OSPF ------------------------------------- Open Shortest Path First
RSVP ------------------------------------- Resource Reservation Protocol
RIP --------------------------------------- Routing Information Protocol
SMRP ------------------------------------- Simple Multicast Routing Protocol
CISCO ------------------------------------ Computer Information System Company
SNA -------------------------------------- System Network Architecture
RTMP ------------------------------------- Routing Table Management Protocol
RTP --------------------------------------- Routing Table Protocol
NLSP ------------------------------------- Network Link Service Protocol
ISO --------------------------------------- International Standard Organization
IETF -------------------------------------- Internet Engineering Task Force
ZRP -------------------------------------- Zone Routing Protocol
TORA -------------------------------------- Temporary Ordered Routing Algorithm
CBRP ------------------------------------- Cluster Based Routing Protocol
CEDAR ------------------------------------ Core Extraction Distributed Ad-hoc Routing
AM Route ---------------------------------- Ad-hoc Multicast Routing Protocol
WRP -------------------------- Wireless Routing Protocol
RReq -------------------------- Route Request
MRP -------------------------- Mesh Routing Protocol
RHS -------------------------- Right Hand Side
List of Figures

Figure 2.1 (Wired Network) ----------------------------------------------- 19
Figure 2.2 (Wireless Network) ----------------------------------------------- 20
Figure 2.3 (Nodes and Links in Mesh Network) ------------------------------- 20
Figure 2.4 (Peer to Peer) -------------------------------------------------- 22
Figure 2.5 (Infrastructure) ----------------------------------------------- 22
Figure 2.6 (Wireless Mesh) ----------------------------------------------- 22
Figure 2.7 (Wireless Mesh Network) ----------------------------------------- 24
Figure 2.8 (Point to Point Network) ----------------------------------------- 24
Figure 2.9 (Point to Multipoint Network) ------------------------------------ 25
Figure 2.10 (Bridging and Routing in OSI Model) --------------------------- 26
Figure 2.11 (Non Line of Sight) -------------------------------------------- 28
Figure 2.12 (Branches of Wireless Networking) ----------------------------- 29
Figure 2.13 (Classification of MWN) ---------------------------------------- 30
Figure 2.14 (Security Model) ----------------------------------------------- 32
Figure 3.1 (Split Horizon Technique Preventing Loops) ---------------------- 36
Figure 3.2 (IP Multicasts) ----------------------------------------------- 37
Figure 3.3 (Larger Internetwork that requires hold-downs) ------------------ 40
Figure 3.4 (SMRP scenario runs from multicast group to end-point) -------- 41
Figure 3.5 (Router running both RIP and IGRP Protocols) ------------------- 42
Figure 4.1 (Steps in Research Methodology) ------------------------------- 54
Figure 5.1 (Showing Load on Network) -------------------------------------- 56
Figure 5.2 (Received Signal with Jitter) ----------------------------------- 56
Figure 5.3 (Graphs showing behavior after Simulation) ---------------------- 57
Figure 5.4 (Highest level; Designing of Network) ------------------------- 59
Figure 5.5 (Middle Level; Simple Server Node) ----------------------------- 59
Figure 5.6 (Low Level; Making of FSM) ------------------------------------ 60
Figure 5.7 (Levels of Simulation Project) ---------------------------------- 60
Figure 5.8 (Flow Chart of work in OPNET) ----------------------------------------------- 61
Figure 6.1 (Thesis Simulation Scenario with 15 Nodes) --------------------------------- 65
Figure 6.2 (Thesis Simulation Scenario with 30 Nodes) --------------------------------- 65
Figure 6.3 (Thesis Simulation Scenario with 60 nodes) --------------------------------- 66
Figure 6.4 (DES Execution Window (50mins)) ------------------------------------------ 67
Figure 6.5 (DES Execution Window (3mins)) ------------------------------------------- 67
Figure 6.6 (Showing Graphs of all Parameters when Nodes=15 (AODV)) ----------- 68
Figure 6.7 (Showing Graphs of all Parameters when Nodes=15 (DSR)) -------------- 69
Figure 6.8 (Showing Graphs of all Parameters when Nodes=15 (OLSR)) ----------- 69
Figure 6.9 (Showing Graphs of all Parameters when Nodes=30 (AODV)) -------- 70
Figure 6.10 (Showing Graphs of all Parameters when Nodes=30 (DSR)) ---------- 71
Figure 6.11 (Showing Graphs of all Parameters when Nodes=30 (OLSR)) ------ 71
Figure 6.12 (Showing Graphs of all Parameters when Nodes=60 (AODV)) --------- 72
Figure 6.13 (Showing Graphs of all Parameters when Nodes=60 (DSR)) ---------- 72
Figure 6.14 (Showing Graphs of all Parameters when Nodes=60 (OLSR)) -------- 73
Figure 6.15 (AODV All Parameters) ----------------------------------------------------- 74
Figure 6.16 (DSR All Parameters) -------------------------------------------------------- 74
Figure 6.17 (OLSR All Parameters) ------------------------------------------------------- 75
Figure 6.18 (Showing Delay, Network Load and Throughput (15nodes)) ------------ 75
Figure 6.19 (Showing Delay, Network Load and Throughput (30nodes)) ------------ 76
Figure 6.20 (Showing Delay, Network Load and Throughput (60nodes)) ------------ 76
List of Tables

Table 2.1 (Showing difference b/w WANs and WMNs) -------------------------------- 31
Table 4.1 (Situations of Different Research Strategies) ---------------------------------- 54
Table 6.1 (Statistical Information; Mean Calculation) ------------------------------------ 77
# Table of Contents

1 **Introduction**
   1.1 Background ............................... 15
   1.2 Objective of this Thesis .................. 15
   1.3 Related Work ............................ 16
   1.4 Research Questions ...................... 16
   1.5 Thesis Layout ............................ 16
   1.6 Scope of this Thesis ........................ 17

2 **Introduction to Wireless Mesh Networks**
   2.1 Wired Networks vs. Wireless Networks ............. 18
      2.1.1 Wireless Networks .................... 19
   2.2 Mesh Networking Defined ..................... 20
      2.2.1 Nodes and Links ....................... 20
      2.2.2 Control Issues ........................ 21
      2.2.3 Modern Mesh Networking ................. 21
      2.2.4 Wireless Networking Structure ............. 21
      2.2.5 Conquering Transmission Distance Limitations ...... 21
   2.3 Network Progression .......................... 22
      2.3.1 Types of Wireless Networks ............. 23
         2.3.1.1 Wireless Mesh Networks .......... 23
         2.3.1.2 Point to Point Networks .......... 24
         2.3.1.3 Point to Multi Point Networks ....... 25
   2.4 Types of Networking Addressing ............... 25
      2.4.1 Unicast Addressing .................. 25
      2.4.2 Broadcast Addressing ................. 25
      2.4.3 Multicast Addressing ................. 26
   2.5 Bridging and Routing ........................ 26
   2.6 Advantages of WMNs .......................... 27
      2.6.1 Non Line of Sight .................. 27
      2.6.2 Seamless Communication ............... 28
   2.7 Resource Management in WMNs ................... 28
   2.8 Taxonomy .................................. 29
      2.8.1 Mobile Adhoc Networks (MANETs) .......... 29
      2.8.2 Classification of Multihop Wireless Networks .... 30
      2.8.3 Difference b/w WANs and WMNs .......... 31
   2.9 Security in WMNs ........................... 31
      2.9.1 Security Model for WMNs ............... 32

3 **Routing Protocols- Protocols in WMNs**
   3.1 Routing .................................. 33
   3.2 Types of routing ........................... 33
      3.2.1 Static Routing ....................... 33
      3.2.2 Dynamic Routing ..................... 34
   3.3 Protocols ................................ 34
      3.3.1 Routing protocols .................... 34
      3.3.2 Comparison of Interior and Exterior Routing Protocols ...... 35
   3.4 Common Types of Routing Protocols ............... 35
      3.4.1 Border Gateway protocol ............... 35
3.4.2 Dec-net routing Protocol ............................................. 35
3.4.3 Enhanced IGRP ...................................................... 36
3.4.4 Interior Gateway protocol ........................................ 36
3.4.5 IBM Routing Protocols ............................................. 37
3.4.6 IP Multicast ......................................................... 37
3.4.7 Open Shortest Path First ......................................... 37
3.4.8 Resource Reservation Protocol .................................. 38
3.4.9 Routing Information Protocol .................................... 38
3.4.10 Simple Multicast Routing Protocol ......................... 40
3.4.11 Netware Link Service Protocol ............................. 41
3.4.12 Open System Interconnection Routing .................... 41
3.5 Redeveloping Route Information Between Protocols ........... 41

3.6 Common Routing in Mobile Ad-hoc Networks .................... 42
3.6.1 Link State Routing ................................................ 42
3.6.2 Distance Vector Routing ........................................ 43
3.6.3 Source Routing .................................................... 43
3.6.4 Flooding .......................................................... 43

3.7 Basic Properties of Protocols in MANETs ......................... 43
3.7.1 Distributed Nature ................................................. 43
3.7.2 Loop Free Environment .......................................... 43
3.7.3 Demand Based Criteria ......................................... 43
3.7.4 Optimum uni-directional link ................................ 44
3.7.5 Alternating Route Policy ....................................... 44
3.7.6 Maintains Quality of Service ................................. 44

3.8 Protocols Used in MANETs ........................................... 44
3.8.1 Ad-hoc on-demand Distance Vector ......................... 45
3.8.1.1 Process to find out Route .................................. 45
3.8.1.2 Route Management Policy ................................ 45
3.8.2 Dynamic Source Routing Protocol ......................... 46
3.8.2.1 Route Analysis ............................................... 46
3.8.2.2 Route Control Mechanism ................................. 46
3.8.3 Optimized Link State Routing Protocol .................. 46
3.8.4 Destination Sequenced Distance Vector Routing ......... 47
3.8.5 Temporarily Ordered Routing Algorithm .................. 47
3.8.6 Zone Routing Protocol .......................................... 47

3.9 Wireless Mesh Network Protocols ................................ 48
3.9.1 Pre-requisite/General Perspective for WMNs Routing ..... 48

4 Introduction to Research Methodology
4.1 Introduction of Research ........................................... 50
4.1.1 A Way of Thinking .............................................. 50
4.2 Types of Research .................................................. 50
4.2.1 Qualitative Research ............................................ 51
4.2.2 Quantitative Research ......................................... 51
4.3 What is Research Methodology .................................... 51
4.3.1 Methods of Knowing ............................................ 51
4.3.1.1 Method of Obstinacy ..................................... 52
4.3.1.2 Method of authority ...................................... 52
4.3.1.3 Method of Perception ..................................... 52
4.3.1.4 Method of Science

4.4 Combination of both Research Types

4.4.1 Thesis Research Type

4.5 Steps in Research Methodology

4.5.1 Identify a Problem

4.5.2 Build the Questions

4.5.3 Literature Study of Topic

4.5.4 Start Writing New Research

4.5.5 Getting Started With Simulation Environment

4.5.6 Implement the Simulation

4.5.7 Simulation Results

4.6 Research Strategies

5 Design Parameters; Guide to Simulation Environment

5.1 Design Parameters

5.1.1 Delay/End to End Delay

5.1.2 Throughput

5.1.3 Network Load

5.1.4 Jitter

5.1.5 Packet Loss

5.1.6 Routing Overhead

5.1.7 Packet Delivery Ratio

5.2 What is Simulation

5.2.1 Why Simulation

5.2.2 Simulation Environment Used

5.2.3 What can be Learnt from OPNET

5.3 Division of Simulation Work

5.3.1 Highest Level

5.3.2 Middle Level

5.3.3 Low Level

5.4 Diagram Showing Traffic

5.5 Flow of Work in OPNET

5.6 Application Areas of OPNET

5.6.1 Evaluation of Routing Algorithms

5.6.2 Protocol Management

5.6.3 Wireless & Satellite Communication Protocols

5.6.4 Network Management

5.6.5 Network Planning

5.7 Tabs in OPNET

5.7.1 Scenario Tab

5.7.2 Topology Tab

5.7.3 Traffic Tab

5.7.4 Protocols Tab

5.7.5 Simulation Tab

5.7.6 Result Tab

5.7.7 DES Tab

6 Simulation Results and Analysis

6.1 Introduction

6.2 First Scenario
6.2.1 Second Scenario ................................. 65
6.2.2 Third Scenario ................................. 66
6.3 Simulation Results ................................. 66
  6.3.1 When Nodes=15, AODV Performance ........ 67
  6.3.2 When Nodes=15, DSR Performance ........... 68
  6.3.3 When Nodes=15, OLSR Performance .......... 69
6.4 Increasing the Nodes ............................. 70
  6.4.1 When Nodes=30, AODV Performance ......... 70
  6.4.2 When Nodes=30, DSR Performance .......... 70
  6.4.3 When Nodes=30, OLSR Performance ......... 71
  6.4.4 When Nodes=60, AODV Performance ......... 72
  6.4.5 When Nodes=60, DSR Performance .......... 72
  6.4.6 When Nodes=60, OLSR Performance .......... 73
6.5 All Parameters; All Scenarios ................... 73
  6.5.1 AODV Performance ............................ 73
  6.5.2 DSR Performance ............................ 74
  6.5.3 OLSR Performance ............................ 74
6.6 Performance Comparison .......................... 75
  6.6.1 All Protocols, 15 Nodes ...................... 75
  6.6.2 All Protocols, 30 Nodes ...................... 76
  6.6.3 All Protocols, 60 Nodes ...................... 76
6.7 Final Comparison and Statistical Information .... 77

Conclusion ................................................................ 79

Future Work ......................................................... 79

Appendix- Simulation Steps ................................. 81

References ........................................................... 85
Chapter 1 - Introduction

1.1 Background

Wireless communication has an enormous use these days and is still becoming popular from times immemorial. This is because of the latest technological demands nowadays arising from laptops, wireless devices such as wireless local area networks (LANs), etc. Because of its fast growing popularity day by day, it has led wireless communication data rates higher and it has made its prices cheaper, that is why wireless communication is growing so fast. Wireless communication can work between hosts by two different methods; one method is to allow the existing network carry data and voice, and second method is to make ad-hoc network so that hosts can communicate with each other [1]. Wireless Mesh Networks (WMNs) are one of the types of ad-hoc networks. Ad-hoc networks are also called as mobile ad-hoc networks (MANETs). Companies use wireless mesh networks for making large coverage area of wireless local area networks. WMNs are the latest technology that has lot of things in common with MANETs. Basically WMNs are consisted of wireless nodes; each node with its own packet, these nodes can communicate with each other by forwarding the packets to one another. This is very similar to MANETs; each node acts as a host and a router, which is basically a wireless router. In WMNs, if clients want to communicate with routers, they use the networking interfaces like Ethernet 802.11 and Bluetooth. There are some cases when WMNs router lies inside the network card, then clients can use the networking interfaces like peripheral component interconnect (PCI) or personal computer memory card international association (PCMCIA) bus, for the sake of communication. WMN nodes can provide internet connectivity and these nodes are termed as gateways. There are lot of advantages of WMNs over different other technologies, one of them is its least deployment time and other includes reliability and market coverage [2]. Different companies like Nokia, Motorola, Ericson, and Siemens etc have great trust in WMNs technology as it provides full IP solution [3]. Because of the fast developments in the field of wireless communication (laptops, PDAs) the demand for getting internet access from anywhere, anytime has increased. Wireless stations are the current technology that can provide internet to wireless devices by making a route between them. These wireless stations are so called access points. Network is created by access points among wireless devices and provides a bridge between internet and this network. Access points have some coverage area; this coverage area can be extended by allowing wireless devices to pass packets towards access points. This kind of multi-hop wireless access networks are called WMNs [4]. Routing protocols have great importance in WMNs. Without routing protocols WMNs cannot be implemented. Routing protocols help routers in a network to know how they can communicate with each other. They work on the third layer of the Open System Interconnection (OSI). They prevent routing loops and select preferred routes [5]. Lot of routing protocols during the communication process might encounter certain parameters such as delay, jitter, throughput, latency and network load in WMNs. Researchers have been working on this issue, finding a suitable and efficient protocol that can give best performance under these certain conditions.

1.2 Objective of this thesis

The objective of this master thesis in electrical engineering was to get the deep understanding of wireless mesh networks and the routing protocols that can be used in it; by studying previous research papers that gives some related material about them. Routing protocols in WMNs should be evaluated
theoretically as well as some of the routing protocols should be evaluated for WMNs through simulation to see which protocol gives best performance under the certain conditions that are delay, throughput, network load. It was needed to see the results of those protocols in the form of graphs that were obtained from the simulation work. Initially in this master thesis in electrical engineering, all the necessary topics like wireless mesh networks, routing protocols and other relating material for these two topics had been studied and discussed theoretically. After this the routing protocols had been implemented in wireless mesh network keeping in mind the conditions (delay, throughput and network load) through a simulation environment. This thesis also had a plus point that it could give the future researchers a clear idea that the routing protocols can be tested for other criteria also using this kind of simulation, and this could be of great interest for the field of wireless mesh networks. The simulation was carried out on a very sophisticated tool named optimized network evaluation (OPNET) Modeler 14.5. The study of this master thesis tested the protocol that gave best performance under specific conditions.

1.3 Related Work

Routing protocols have been tested for wireless mesh networks in past, but for some other conditions. In this master thesis, routing protocols have been tested for delay, throughput and network load altogether. Routing protocols have been studied in past individually and collectively also but the combinations of those were different to these protocols that have been used in this master thesis. The simulation of different protocols has been done on the software NS-2 keeping in mind the conditions that were overhead, optimal path etc [1]. Study thesis that was done in university of Canada has also some unique features and the useful information about routing in WMNs made us possible to discuss and to evaluate the performance of our chosen routing protocols in WMNs under certain conditions [3]. Another study thesis with only 10 credits has discussed the two protocols AODV and DSDV performance under the conditions bandwidth, throughput and packet loss altogether, but no simulation work is shown [6]. Definitely routing protocols in WMNs have been tested for delay, throughput also but in our thesis three different parameters (delay, throughput and network load) is tested together for the first time, and its simulation has been done on OPNET Modeler 14.5. Moreover, routing protocols used in our master thesis were AODV, DSR and OLSR. Among these three protocols AODV and DSR were reactive protocols while OLSR was a proactive protocol.

1.4 Research Questions

- What are the various protocols used in WMNs?
- Which protocol gives the best performance under assumed conditions in WMNs?
- What are the effects of various protocols in WMNs or MANETs?
- Which simulation tool is used and why it is used?

1.5 Thesis Layout

- Chapter 2 will define a detail study about wireless mesh networks. Also this chapter will differentiate between wireless mesh networks and wireless networks. Moreover it will also emphasis on the difference between wired and non-wired networks including their advantages and disadvantages and much more.
• Chapter 3 will give a deep understanding of routing protocols in Mobile Ad-hoc networks or in Wireless Mesh Networks. This chapter will also discuss in brief for most of the routing protocols that are being used these days.

• Chapter 4 will explain about the research methodology of our thesis. It will describe about that particular method/approach that we have used in our thesis.

• Chapter 5 will have a look on design parameters of WMNs and it includes a guide to simulation environment that is used in this thesis. Design parameters will be discussed and all the important things are discusses relating to the simulation environment. Before performing simulation, this guide to the simulation tool is very much helpful.

• Chapter 6 describes the simulation results performed in our thesis. The results are shown in the form of graphs. And it also includes the final analysis and statistical information of the three routing protocols used, in the form of mean calculation.

• Appendix shows all the necessary steps that are done in our simulation work.

• In the end there is a conclusion, the work that is done in this thesis is written briefly in conclusion. And also it includes an article for future work, which is telling about the challenges of future in this research.

1.6 Scope of this thesis
Routing protocols in WMNs are of two types i.e. reactive and proactive. The protocol that is reactive as well as proactive is usually referred to as hybrid protocol. Hybrid protocol is the one that has combine features of both reactive and proactive. In this thesis, three routing protocols were taken into account for checking their performance in WMNs in terms of delay, throughput and network load through simulation in OPNET Modeler 14.5. Three routing protocols are AODV, DSR and OLSR, where AODV and DSR are reactive protocols while OLSR is a proactive, neither of all is a hybrid protocol. Already mentioned before that in this thesis the network performance has been checked using three different routing protocols. Every routing protocol evaluated in this thesis might have some edge on each other, but this thesis emphasizes on three parameters (delay, throughput and network load) and the effect of routing protocols under these parameters. Only one routing protocol outperforms the other two protocols in most of the chosen parameters in this thesis.
Chapter 2- Introduction to Wireless Mesh Networks

In this chapter we are beginning with the explanation of wired vs. wireless networks and then later we have discussed in detail about the wireless mesh networks (WMNs) and it’s all relating topics. WMNs are gaining fame day by day because it has lot of advantages as compared to other wireless networks. It is fine addition in the field of wireless networks. The main topics of this chapter include the advantages of WMNs, taxonomy of wireless networking, network progression, and security issue in WMNs and resource management in WMNs.

2.1 Wired vs. Wireless Networks

The network that uses wires is known as a wired network. Initially the networks were mostly wired networks. When there is a use of wire in a network, definitely it also requires network adapters, routers, hubs, switches if there are more than two computers in a network. The installation of a wired network has been a big issue because the Ethernet cable should be connected to each and every computer that makes a network. Definitely this kind of connection takes time, in fact more time than expected, because when we connect wires with computers we have to take care of lot of things like wire should not come under the feet, it should be under ground or it should be under the carpet if computers are in more than one room. However in new homes nowadays, the wiring is being done in such a way that it will look like as it is a wireless connection, greatly simplifying the process of cables. Similarly the wiring of a wired network depends on lot of things like what kind of devices are being used in a wired network, whether the network is using external modem or is it internal, the type of internet connection and many other issues. As we know making a wired network is not an easy task, but still there are many other tasks that are more difficult than making a wired network, but we are not going to discuss these tasks here. In configuring the wired network, the hardware implementation is a main task. Once the hardware implementation is finished in a wired network, the remaining steps in a wired network do not differ so much from the steps in a wireless network. There are some advantages of wired network that include cost, reliability and performance. While making a wired network, Ethernet cable is the most reliable one because the makers of Ethernet cable continuously improving its technology and always produces a new Ethernet cable by removing the drawbacks of previous one. That is why Ethernet cable is the most preferable in making a wired network, as its reliability is kept on growing from the past few years. In terms of performance, wired networks can provide good results. In the category of Ethernet, there is Fast Ethernet too, that provides enormous performance if a wired network is built in home for some features like data sharing, playing games and for the sake of high speed internet access. Still it is not false to say that Fast Ethernet can fulfill the need of network that is built in home for these kinds of purposes, till many years in future. Security in wired LANs can be a little problem because a network that is wired and is connected with internet must have firewall also in it, but unfortunately wired network does not have tendency to support firewalls, which is a big issue. However this problem can be solved by installing firewall software on each individual computer in a network [7].
The nodes of wired network does require power, as they get that power from the alternating current (AC) source that is present in that particular network.

2.1.1 Wireless Networks

On the other hand, wireless network is such kind of network that does not use wires to build a network. It uses radio waves to send data from one node to other node. Wireless networks lie under the category of telecommunications field. It is also known as wireless local area network (WLAN). It uses the Wi-Fi as a standard of communication among different nodes or computers. There are three types of Wi-Fi communication standard.

- 802.11b
- 802.11a
- 802.11g

802.11b was the oldest standard that was being used in WLAN. After 802.11b, the standard being introduced was 802.11a. It offers better speed than previous one and is mostly used in business networks. The latest standard is 802.11g that removes the deficiencies of previous two standards. Since it offers best speed from other two standards, also it is the most expensive one.

The installation of this kind of network can be done by two ways. First one is ad-hoc mode and the second one is infrastructure mode. Ad-hoc mode allows wireless devices in a network to communicate on the logic of peer to peer with each other. However the second mode is the most required mode as it allows wireless devices in a network to communicate with a central device which in turn communicates with the devices that are connected with central device through wire. But both these modes have one similarity that they use wireless network adapters, termed as WLAN cards.

Wireless LAN costs more than the wired network as it requires wireless adapters, access points that makes it three or four times expensive than Ethernet cables, hubs/switches for wired network. Wireless network faces reliability problem also as compared to wired networks, because while installing the wireless network it may encounter the interference that can come from the household products like microwave ovens, cordless phone etc. Wi-Fi communication standard’s performance is inversely proportional to the distance between the computers and the access points. Larger the distance between the computers and access point, smaller will be Wi-Fi performance and hence smaller will be performance of
wireless network. Similarly, security wise it is less secure than the wired network because in wireless communication data is sent through the air and hence there are more chances that data can be intercepted [7].

Figure 2.2 Wireless Network [9]

2.2 Mesh Networking Defined

To understand the concept of mesh networking it is necessary to know what the mesh topology is, how it can be implemented in a network. In a communication network, node is a term that is very common and the meaning of node in a networking environment is a device that has the ability of transmit and receive the data. If there are n nodes in a communication network and that network is said to be a mesh network if each node can communicate with every other node i.e. a network following a mesh topology. If a deep and clear understanding of a mesh network is required, the n nodes is reduced to some understandable form because n is a general form of representing total number of nodes. If n nodes are reduced to a number of 5 or any number the structure of mesh network can easily be understandable [10].

2.2.1 Nodes and Links

Devices that are in a communication network are known as nodes and the connection between these nodes is known as a link. In a mesh network the nodes are unfeasible with the interconnection of the nodes. To connect two nodes we need one link, to connect three nodes we need three links, to connect four nodes we need six links. This means that there is no direct relationship between the number of nodes and their links in a mesh network. Initially a physical interface was required by nodes for connection with each link and this interface performed parallel to serial and serial to parallel conversions because at that time data flows bit by bit on a serial link. In a mesh network every node has physical constrictions that put limitations on the number of nodes that are to be connected [10].

Figure 2.3 Nodes and Links in Mesh Network [10]
2.2.2 Control Issues

In early ages there were such kind of networks that have hundreds and thousands of nodes that were not connected with each other but they used more than two links towards other nodes so that they could adjust traffic and could provide better routing capacity. Since they had two or more links towards other nodes, the data could not travel directly from one node to another, they had to choose that links for communication with destination node. This kind of network structure is termed as partial mesh network structure. This kind of network was usually used in the early 1970s and 1980s. Since they used the two or more links for communication with destination node, its routing operation were also bit different and required synchronization with control messages that came from nodes [10].

2.2.3 Modern Mesh Networking

Modern mesh net workings these days are wireless, and are called wireless mesh networking. In a wireless network each node has one Radio Frequency (RF) transmitter/receiver that has the tendency to communicate with all wireless nodes connected inside a network. RF has made the communication process very easy as compared to the wired networks. Because in wireless mesh network RF fulfils all the process of communication but in wired network it is opposite, this single interface has to be converted into multiple interfaces. Nodes should lie inside the range of transmission for the sake of successful communication [10].

2.2.4 Wireless Networking Structure

There are two common types of wireless LAN networking structures i.e. Peer to Peer (PP) and Infrastructure (IS). These two types are somehow different with each other. In PP structure each node can communicate with other node directly and these nodes should be inside the range of transmission. But in infrastructure, each incoming data has to pass through the Access Point (AP). AP is just like a two port bridge, its one port is connected with a wired network while the other port is connected with a RF transmitter/receiver. This means in infrastructure network, if two nodes want to communicate with each other they will first communicate with AP and then AP will generate the data for them. AP acts as a relay station for the communicating nodes, when two nodes are communicating with each other, their distances can be doubled as compared to the PP network. This AP acts like a central server for the communicating nodes, when this AP stops working, nodes cannot communicate with each other. Similarly if a node is out of the range of transmission the communication will also suffer [10].

2.2.5 Conquering Transmission Distance Limitations

This limitation that every node has to be in the transmission range is one of the drawbacks in wireless networks and it must be removed. So there is one solution for this that each and every node will act as a relay. When considering WMNs, the nodes of WMNs act as routers and repeaters. Routers are used to transmit and receive the information. In PP network the transmission has a limitation of two nodes i.e. two nodes can communicate with each other, while in infrastructure network, communication is dependent on AP. But in WMNs each node can communicate with every other node. Moreover WMNs is said to be a combination of PP transmission series in which each node can act like a router and repeater. No central device or server is required in WMNs and nodes can communicate with each other on the basis of PP.
2.3 Network Progression

As the terms “nodes” and “links” have been discussed, they are the initial terms in field of networking to understand the different types of networking that includes WMNs, PP and infrastructure. The field of networking has got progress steps by steps. Every new technology needs the study of previous material. Similarly there are few things that came first i.e. topology. In wireless networking there are different topological networks.
2.3.1 Types of Wireless Network

There are various types of wireless networks that are discussed in detail below.

- Wireless Mesh Network
- Point to Point Network
- Point to Multipoint Network

2.3.1.1 Wireless Mesh Network

A network that is wireless, made in the form of mesh and uses radio waves between nodes for the sake of communication is known as wireless mesh network (WMN). It is a special kind of wireless ad-hoc networks which are also called as mobile ad-hoc networks (MANETs). This kind of network is made up of mesh clients, mesh routers and gateways. The devices like laptops, mobile phones, wireless mouse, wireless keyboards, PDA etc come under the category of mesh clients, while mesh routers have the duty to send the data from one end to another which has to pass to and from the gateways. Gateways may connect with the internet but there is no specific need of the connection of gateways with the internet. There is one more concept in it i.e. mesh cloud. Definitely the nodes that lie in a mesh network have some coverage area. This coverage area that constitutes of all the radio nodes in that particular network is sometimes referred as mesh cloud [11]. A wireless mesh network does not work on the logic of predefined paths, and that is why mesh routers are being introduced in these types of network. Mesh routers have made the implementation of wireless mesh networks extremely easy as mesh routers have the tendency to select and adjust the path on the spot to which they can communicate [12]. An advantage of wireless mesh network is that it offers superfluity and it is quite reliable. If there will be a problem in one node of a network, the network will not come onto its knees, the whole network will keep on working except that one particular node. The other nodes will find an alternate path either directly or through the neighboring nodes using a routing protocol. Moreover it is a self-organizing network. These kinds of features make WMN more advantageous like robustness, low cost and easily maintenance property. WMN can be classified into three types.

- Infrastructure wireless mesh network
- Client wireless mesh network
- Hybrid wireless mesh network

In the first type of WMN, mesh routers form an infrastructure for the clients. In client WMN, client nodes form network to perform routing. In hybrid WMN, clients form mesh functions plus accessing the network [11].

As WMN is a self configuring network that has many cool features in it like low power consumption, sensing ability and controlling ability. As in WMN all the nodes can communicate with each other nodes without going back to the central device. Since it cannot get back to the central device, node to node communication requires less power as compared to the traditional wireless network’s transmitter. Because of its less power consumption, it can save lot of power in it and in this way battery lasts for a year or so without recharging. Since in WMN all nodes can transmit data and receive, therefore it is good for sensing and controlling also [13].
2.3.1.2 Point to Point Network

Point to point network is a type of wireless network. As its name suggests that it is a point to point connection, only one node can communicate with other one node at a time in a network. It is just like a one to one function, where one element can make a pair with other one element only. Hence for bigger networks where speed and performance is a core issue, this kind of topology is not a good option. In this kind of network if one connection breaks the whole network will stop working. It will cost more wire to build a network and it is the most difficult network in terms of configuring. It follows the tree topology.
2.3.1.3 Point to Multipoint Network

As its name suggests in this kind of network, one node can communicate with one or more nodes in a network. It includes a central device in a network which controls the communication process of all nodes. If one node has to communicate with some other node, it will send data to the central device and then central device will look the receiver node and deliver that data to receiver. This network is made up of star topology. The performance of this network depends on the quality of link between central device and all nodes.

Figure 2.9 Point to Multipoint Network [16]

2.4 Types of Networking Addressing

There are several types of networking addressing which are described and shown as follows.

- Unicast Addressing
- Broadcast Addressing
- Multicast Addressing

2.4.1 Unicast Addressing

In this type of addressing, packets sent to unicast address are delivered to one device/node. The meaning of unicast is to cast the packet to only one node. At a time only one node can transmit a data towards destination node. In simple words it is said in this type of addressing, there will be only one sender and one receiver.

2.4.2 Broadcast Addressing

Address will be given and single node will transmit packets towards all other nodes that belong to this address. The meaning of broadcast is to transmit data to all the hosts/nodes that lie in a network. In simple words it is said that in this type of addressing there will be one sender but the data will be transferred to all the destinations.
2.4.3 Multicast Addressing

In this kind of addressing, single device will transmit the packets/data not to all devices in a network but to specific devices. Example of this kind of communication is a conference call in which multicast addressing takes place i.e. only specific users can communication with each other. In simple words it is said that there is one sender that sends data but the receivers can be more than one but not all.

2.5 Bridging and Routing

Bridge and router are the devices that connect two different networks with each other so that successful communication becomes possible between these networks. Bridge operates at the second layer of OSI model while router operates at the third layer of OSI model. Bridging is used when there is a matter of connecting same kinds of networks and on the other hand routing is used when there is a matter of connecting two or more different networks with each other. From both of them, it is always recommended to use routing as routing is more professional then bridging. However bridging is not complicated, it is easier then routing but still bridging has some more weak points than routing in terms of call management and performance. Since bridging uses broadcasting, it transfers data to every node in a network, and hence transfers data to those nodes also that do not require it. On the other hand routing is done on the network layer of OSI, hence it is more sophisticated and efficient than bridging because it transfers packets from source to destination by having a look on the addresses of each packet that has to be transmitted over a network. The most important thing in routing is that it only transfers packets to those nodes that require data at that time. Routing makes better use of a bandwidth (BW); it does not waste bandwidth because it cannot send packets unnecessarily [17].
2.6 Advantages of WMN

The advantages of wireless mesh network over other networks are very significant and have great importance. While building a network, WMN offers unique features as compared to other networks.

- No use of wire
- Less cost effective
- More nodes, More speed
- Useful for Non Line of Sight (NLOS)
- No need for network administrator
- Fast data processing
- Easy to install and uninstall
- Don’t require new Wi-Fi standard
- Tolerant to faults

Using no wire to build a network is a great advantage. Nowadays bigger networks do not prefer to use wire. Our internet is a real example of this; many networks are connected with each other wirelessly having a mesh topology, which in other words also called as seamlessly [18].

Since it uses no wire that is why it is cheap.

It is very useful for those networks where there is no direct communication between sender and receiver. Such kind of communication is termed as NLOS communication.

In WMN the nodes automatically adjust themselves according to the situation; therefore there is no need for the network administrator if there is any problem in the nodes or network.

WMN nodes can communicate with their neighboring nodes as well without going back to the central device, which increases its data processing speed.

WMN nodes can easily be installed or uninstalled according to the requirement.

Like all other wireless networks standards, WMN also uses one of those standards. Being a new technology it does not require new Wi-Fi standard.

WMNs are very much tolerant to faults, if couple of nodes in a network fails, the communication will always keep on going.

2.6.1 Non Line of Sight

NLOS is a term used for communication between transmitter and receiver where there is no direct path for data transmission. Some obstacles are there between transmitter and receiver. The obstacles may be anything i.e. buildings, trees, mountains etc. When transmitter sends any data, it will reflect from these paths and then reaches the receiver. However NLOS is extracted from the term line of sight (LOS) which means that there is direct communication between transmitter and receiver, no obstacles will be there between them. But in NLOS when data reaches the receiver from different reflections it may experience a weak signal at its end. This is known as fading. But fading is no longer a very big problem these days. It can be minimized or bring to that level up to almost zero. To minimize/remove the signal fading the most common way is to increase the strength of a signal at the transmitter side and to increase the bandwidth of that signal. Bandwidth is the range of frequencies in a signal.
Increasing the range of frequencies will increase the bandwidth of a signal. WMN is used for NLOS networks as it the best suited option. WMN is a mesh network which uses NLOS communication, so definitely during the transmission of data from one end to another; the data strength does not remain same when it reaches to its destination. So WMN has the ability to automatically configure and handle this kind of problem also, it automatically increases the signal strength to that level that it does not experience a fade at receiver’s side. Because WMN has dozens of nodes in it, and that is why these dozen of nodes help to find a clear signal at the receiver side. No other network has the ability to do this.

![Figure 2.11 Non Line of Sight](image)

**2.6.2 Seamless Communication**

Seamless communication works on the basis of always best connected anywhere anytime. Definitely in a WMN there are many nodes, and the goal of seamless is to always keep these nodes connected whatever the change will occur. User should not be disconnected during the ongoing communication. This offers handover (HO) management and location management. HO management means to keep nodes connected when the position or direction will change. Location management means that network will find from where the node is connected to it. Since WMN is best for NLOS networks, wirelessly connected mobiles with some access points also come under the category of NLOS communication. Because signal from the base station experiences reflection from different things and then reaches mobile node. This means it is another advantage of WMNs that it also provides seamless communication.

**2.7 Resource Management in WMN**

In wireless mesh networks the main thing to keep in mind always is the satisfaction of users in terms of quality of service (QOS). Users always demand good quality and it is increasing day by day. A network is considered to be good and successful that offers quality service to their users. If there is no QOS, that network is just useless. To meet the users QOS criteria there are some very important things that have to keep in mind while building a network, and these things should be there in a network,
only in this case a network can fulfill the requirement of QOS. The most important things that should be in WMN are:

- Channel Diversity
- Routing
- Mobility Management

Sometimes in WMNs there can be interference in a network, which puts bad impact on users. Hence to remove this interference, channel diversity has to be done. To gain channel diversity in WMN it is highly required to do channel allocations. Channel allocations can be done by two methods i.e. fixed channel allocation (FCA) and dynamic channel allocation (DCA). However these days DCA scheme is preferred. In DCA, the call blocking probability is low as compared to FCA.

By following the routing the QOS criteria in WMN can be obtained easily. Routing helps users connect with a network that is consisted of access points and gateways. This is the best technique in terms of achieving QOS in WMN. Previous researches have used routing technique for getting QOS in WMN and have led to lot of routing protocols.

The third way to obtain QOS in WMN is to do mobility management. Mobility management includes HO management and Location management. HO management is responsible for keeping the nodes always connected when the direction or place of the node is changed. Location management is responsible for watching from where the node is connected with network [3].

2.8 Taxonomy

![Figure 2.12 Branches of Wireless Networking](image)

### 2.8.1 Mobile Ad-hoc Networks (MANET’s)

Mobile ad-hoc networks (MANETs) are also type of wireless ad hoc networks that is why MANETs and WMNs are correlated with each other. Even sometimes MANET is also called as mobile mesh network and it can also be called as a wireless mesh network. It is not necessary that mesh network can also be mobile or wireless mesh network. As previous diagram is showing that MANETs are
infrastructure less but when the definition of WMNs is applied it is found that MANETs are the subset of WMNs as both of them are self-organizing. Also the study of different research papers reveals that WMNs and MANETs can be taken as same kind of networks. So like WMN, MANET is also useful for larger coverage area like internet worldwide. MANET is made on the logic that each node is independent and free to move in every direction. Since it works dynamically that is why while routing, routing protocols can easily find and update the selected paths dynamically. Moreover MANET supports multi hop communication same like WMN [20]. The term ad hoc came from Latin language which means “for this purpose only”. Since MANETs are very much in common with WMNs, the plus points of MANETs are also very much similar to WMNs. The communication is done through wireless links. Nodes that constitute this network can perform the functions of routers and hosts. They use dynamic network topology. Free of infrastructure like WMNs. It can be made at any place as it is a wireless network. The applications of MANETs are also same like WMNs. Nowadays United States (US) military has more interest in using MANETs. Information can be accessed easily as compared to wired networks. The main disadvantage of MANETs is that because of its wireless feature there are more chances of attacks on it. Attacker might attack easily to wireless networks as compared to wired networks. As in MANETs the nodes can communicate with their neighboring nodes also without the use of a central server, therefore when some node is affected or not working properly, it is hard to find that infected node as it has volatile network topology [21].

2.8.2 Classification of Multihop Wireless Networks

The classification of Multihop Wireless Networks (MWNs) has been done beautifully. To understand the concept of MWNs clearly, the figure is drawn [22]. MWN is a superset of Hybrid Wireless Networks (HWNs), Wireless Ad-hoc Networks (WANs), Wireless Sensor Networks (WSNs) and WMNs. WANs have no infrastructure and posses dynamic topology, WSNs are made of tiny sensor nodes and they can follow single hop wireless communication or Multihop wireless communication. On the other hand HWNs can follow both single and multi hop communications. WMNs follow Multihop communication.

Figure 2.13 Classification of MWNs [22]
2.8.3 Difference between WANs and WMNs

Wireless Adhoc Networks and Wireless Mesh Networks are very much similar with each other. Only problem is with the routing protocols. Those routing protocols that give best performance in WANs do not give reasonable performance when it comes to use in WMNs [22]. Both of them use different protocols. They differ with each other in some matter which can be illustrated in following table.

<table>
<thead>
<tr>
<th>Number</th>
<th>Issues</th>
<th>Wireless Adhoc</th>
<th>Wireless Mesh</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Network Topology</td>
<td>Highly Dynamic</td>
<td>Relative Static</td>
</tr>
<tr>
<td>2</td>
<td>Mobility of nodes</td>
<td>Medium to High</td>
<td>Low</td>
</tr>
<tr>
<td>3</td>
<td>Energy Constraint</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>4</td>
<td>Routing Performance</td>
<td>Fully Distributed on-demand Routing</td>
<td>Partially Distributed with table driven Routing</td>
</tr>
<tr>
<td>5</td>
<td>Deployment</td>
<td>Easy to Deploy</td>
<td>Planning Required</td>
</tr>
<tr>
<td>6</td>
<td>Traffic Characteristics</td>
<td>User Traffic</td>
<td>User and Sensor Traffic</td>
</tr>
<tr>
<td>7</td>
<td>Relaying</td>
<td>By mobile nodes</td>
<td>By fixed nodes</td>
</tr>
<tr>
<td>8</td>
<td>Infrastructure Requirement</td>
<td>Infrastructure less</td>
<td>Fully fixed or partial infrastructure</td>
</tr>
</tbody>
</table>

Table 2.1 Showing difference b/w WANs and WMNs [22]

2.9 Security in WMNs

There are various challenges in WMNs on which it is necessary to overcome and hence making the WMN more and more ideal. While making an efficient network, there exist these kinds of challenges, on which it is necessary to tackle. The challenges that arise in WMNs are authentication, authorization, encryption, key management, attacks, intrusion detection and prevention, secure routing and security policies [23]. Authentication is one of the core issues in network security. When there is no interruption in our network, it is said that network is providing authentication or in other words data cannot be made stop by any third party. In WMNs thousands of nodes are being connected wirelessly with each other and as it is already said that stealing the data from a wireless network is easier than a wired network. Hence while building a WMN it is necessary to keep in minds that it must provide authentication so that users gain more confidence on a network.

Authorization is the kind of permission that particular thing is accessible. In WMN when nodes communicate with each others, there are some confidential data relating to each node, and if there is no authorization in a network, someone’s data can be readable. It is one of the key challenges that arise in WMN.

It is necessary that communication is not hacked by the third party so an efficient encryption method should be used. There are two encryption schemes used nowadays depending upon the requirements of a network i.e. symmetric encryption or asymmetric encryption. Symmetric encryption uses one key and asymmetric encryption uses two keys.

Key management is the method of managing the exchange of keys between nodes or systems. It also lies under the category of cryptography. Probably is the most difficult part of cryptography. In a huge network like WMN, this challenge should not be ignored.
Some kinds of attacks also disturb the communication of network. That includes active attacks and passive attacks. Lot of measures had been taken to prevent the network from attacks. It is always desirable that a network is so secure that attacker cannot gain access of anything.

In WMN secure routing is the biggest issue among all. When nodes are connected with each other and having a communication, definitely this is being done by routing, and to make it secure routing protocols are used nowadays. There are various routing protocols. Lot of security policies must be taken to increase the security features of WMN.

2.9.1 Security Model for WMNs

In every network there are key issues i.e. availability, integrity, authenticity and confidentiality. If some actions attempt to disturb these issues, they are called intrusions. There is one system by which intrusions can be detected i.e. Intrusion Detection System (IDS). Intrusions can be prevented by using different kind of software. There is intrusion prevention system (IPS) which is a sub part of IDS that prevents the network from intrusions. In simple words to make the WMNs secure from attacks it is necessary to do intrusion detection and prevention. There is a proposed security model for WMNs that explains how the security services are put together [24]. In the intrusion prevention model, first three including authentication, integrity and data confidentiality works on Medium Access Control (MAC) layer while integrity, data confidentiality, authorization and source routing works on network layer. The right model shows that availability, intrusion detection and automated response can work on both layers i.e. network and MAC layers.

![Security Model](image-url)
Chapter 3- Routing Protocols; Protocols in WMNs

3.1 Routing

Routing is the process of choosing paths through which network traffic flows. Routing is implemented in different sort of networks, for instance telephone network, electronic data networks and internet network. In electronic data networks routing uses packet switching technology. In packet switching networks, routing makes the path for packet forwarding, and also supports for the transportation of addressed packets from source to destination through intermediate nodes by using hardware devices like routers, bridges, gateways, firewalls or switches. Ordinary computers with multiple network cards may forward packets and activate routing, regardless of limited performance. The routing process usually adopts forwarding in terms of routing tables. Therefore for the manufacturing of routing tables memory is necessary for precise routing.

Routing schemes have different attributes in their delivery.

- **Unicast** \(\rightarrow\) Sends message to a single special node.
- **Broadcast** \(\rightarrow\) Sends message to all the nodes in the network.
- **Anycast** \(\rightarrow\) Sends message to anyone which is not included in node’s groups, probably the closest to source.

Unicast is the prominent kind of message delivery in internet [25]. Routing plays the vital role in the internet, to support messages to pass from one to another computer and consequently reach the destination. Each middle computer performs routing. This procedure includes analyzing a routing table to find the best path. Routing is mostly being mixed with bridging, as the functions of both the techniques are identical. The basic difference between them is that bridging takes place at low level in which hardware component performs main role, whereas the routing occurs at high level in which software component has vital role. Routing creates complex analysis to determine the suitable path for the packet [26].

3.2 Types of Routing

There are mainly two types of routing which are as follows.

- Static Routing
- Dynamic Routing

3.2.1 Static Routing

Static routing is exactly opposite to dynamic routing; it basically reveals the procedure by which network administrator by hand not automatically construct network routers for forwarding packets. The administrator configure routing table for this purpose. Static routes are permanent; they are not being changed by any administrator [27]. Static routing has lot of benefits for autonomous systems, for instance create relaxation for subnets and next hop routers. Static routing creates the environment to prevent routing protocol traffic on link connected to autonomous systems. As there is no routing protocol is operating on Autonomous system link, then the possibility of fault router is finished. One
of the big advantages of static routing is that it prevents link failure, although static routing has some disadvantages yet it is familiar selection for administrators. To connect two autonomous systems, some commands are required to achieve static routing [28].

### 3.2.2 Dynamic Routing

Dynamic Routing demonstrates different routes using for forwarding data which depends on given situations of network. This routing is more flexible and feasible than static routing. It has the capability to overcome overloaded traffic and can control congestion. As dynamic routing uses different paths to forward the packets that is why it is more versatile whereas static routing uses fixed paths that is why it has less worth [29].

### 3.3 Protocols

Protocols have great importance in every kind of communication, e.g. in human communication there are different set of rules for speaking, listening and understanding. These rules represent protocols of conversation. They are helpful for the people to successfully communicate. The protocols also play great rule in network devices. In computer network systems, protocol has the standard rule which is being followed by computers to communicate with each other. Protocol defines and maintains the connection as well as data transfer between computers. Protocol develops the synchronization in the system. Protocols can be implemented in terms of hardware, software or in both forms. The extensive and comprehensive use of protocols in internet systems spread prosperity and strength. The internet protocol (IP) and transmission control protocol (TCP) are the important ones in this context. The most common protocols are listed below.

- IP, TCP, DHCP, HTTP, FTP, TELNET, SSH, POP3, SMTP, IMAP, SOAP, PPP [30]

### 3.3.1 Routing Protocols

Before going into the detail of routing protocol, it is necessary to know about the routing protocol. What it performs actually, and what is their importance in the field of telecommunication. Generally routing protocol represents the relation or formula that is being used by routers to find the suitable way through which data can be forwarded. Routing protocol is also helpful in exchange of information between routers. Routing protocol plays vital role to adjust the network according to variable conditions [28]. So the role of routing protocol in reliable and predictable communication is indispensable. In other words routing protocol is the implementation of routing algorithm in the form of software or hardware. Routing protocol uses different matrices to find out the path which is used to transfer the packet across the network. The numbers of network layer devices along the path are given below.

- Hop count
- Bandwidth
- Delay load
- MTU
- Cost

Generally Routing protocols are categorized by interior and exterior routing protocols.
3.3.2 Comparison of Interior and Exterior Routing Protocols

Routing protocols which are intended to be used within an organization are known to be interior routing protocols, for instance the lead interior gateway protocol IGP is OSPF. Other interior gateway protocols include IS, RIP, and EIGRP. Whereas the routing protocols which are designed for use between organization and networks, they are called as exterior routing protocols. The main exterior gateway protocol is BGP. The BGP is upgraded to BGP4 [31]. Now for the further study of routing protocols and their critical importance in communication systems, it is important to discuss some important routing protocols and their functions in networking or telecommunication systems.

3.4 Common types of Routing Protocols

The common routing protocols which have great impact on the communication systems are listed below [32].

- Border gateway protocol (BGP)
- Dec-net Routing protocol
- Enhanced IGRP (EIGRP)
- Interior gateway protocol (IGRP)
- IBM routing protocols
- IP multicast
- Open shortest Path first (OSPF)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)
- Simple Multicast Routing Protocol (SMRP)
- Net ware Link Service Protocol (NLSP)
- Open System interconnection Routing

Now the brief description of these routing protocols is listed below.

3.4.1 Border gateway protocol

Basically BGP is used to transfer the information through the internet; it is helpful for Internet service providers to connect with each other. It is also useful for numerous connections which create complexity with in network, also useful for unrelated domains. BGP was initially became an internet standard in 1989, now it is being updated to BGP4. BGP supports the efficient, reliable and controlled criteria to complex and difficult routing schemes. BGP also promises the system to be secure and stable [33]. BGP was developed to improve EGP. BGP ensures reliability by introducing route updates. BGP has very unique quality that it carries out keep-alive mechanism. BGP does not rely on metric transmission, but transmit path messages for autonomous systems. BGP follows the rule of enforcing policies. This policy is configured to permit BGP-enabled router to other autonomous systems by choosing the best path [28].

3.4.2 Dec-net Routing protocol

Dec net routing protocol is used in decent scenario for reliable communication [32].
3.4.3 Enhanced IGRP

It is an integrated routing protocol which is improved form of IGRP with greater techniques and more efficient than IGRP [32]. EIGRP uses the identical technology found in IGRP for the measurement of metric. The only difference is the method of route advertisement, and the manipulation of entries into the routing table. These methods are same like link state protocol. The main parameters of EIGRP are [28].

- Neighbor discovery/recovery
- Consistent transport protocol
- Dual finite state machine
- Variable-length subnet masks

3.4.4 Interior Gateway Routing Protocol

IGRP was developed by Cisco in 1980. The basic goal of Cisco is to create a vigorous and strong protocol for autonomous systems. In the middle of 1980, the famous IGRP was Routing information Protocol. The reliability and strength of IGRP motivated many organizations to replace RIP into IGRP. The quality of IGRP is that it is a distance vector routing protocol, which measures vector distances. IGRP also uses a metric to calculate mathematical values for delay, bandwidth, load and efficiency. IGRP has the ability to enhance its stability and strength. The main qualities of IGRP are hold downs, split horizons and poison reverse updates. Hold downs are basically used to stop continuous message updates from unsuitable reinstalling route that might have damaged. Split horizons originate from the supposition that it is not useful to send information about a route back to the direction from which it came. Split horizons are also implemented in IGRP, useful for algorithms stability. IGRP has been acknowledged as the most advantageous routing protocol; due to its functional similarity to RIP, it has great qualities. Nowadays it has the deficiency of variable length subnet mask, so Cisco developed an enhanced version of IGRP for further improvement [34].

Figure 3.1 Split Horizon Technique Preventing Loops [34]
3.4.5 IBM Routing Protocols

IBM Routing technique necessarily consists of System Network Architecture (SNA). IBM routing technique supports peer based network technology [35], in which there is no central entity, so there is no single point of failure. This technique also includes advanced program to program computing. IBM SNA is also responsible for maintaining the class of service [35].

3.4.6 IP Multicast

Nowadays in the internet systems, as the telecommunication has grown up so fast, many users want to know about the same information approximately at the same time. IP multicast has great importance in this context. So by using IP multicast technique to dispense the information, appropriate bandwidth utilization is achieved. The example of this technique is audio and video Web content. There are lot of reasons to use IP multicast technique; however there are limitations of using this technique.

![Figure 3.2 IP Multicasts [36]](image)

One of the main applications of IP multicast is the video conferencing. It is very useful for the business point of view, but during the video conferencing there may be possibility of more bandwidth utilization. Other applications of IP multicast are multimedia conferencing, data replication, real time data multicast and gaming as well as simulation [36].

3.4.7 Open Shortest Path First

OSPF was determined by OSPF working group of Internet Engineering Task force. Basically OSPF is an Internet Gate way Protocol, designed for internal single autonomous system. The technology used in OSPF is primarily link state based technology. Every router has similar link sate data bases. The efficiency of link sate bases is being established by consistent flooding algorithm. OSPF helps the independent system to divide the regions in to different areas, to deliver extra level of routing protection. OSPF is also helpful for the configuration of virtual links, it restraints the topological limitations of an autonomous systems. By using this protocol flexible routing metric has been achieved. There are lot of attributes which make this protocol reliable and flexible, for example equal cost multipath, TOS based routing, variable length subnet support and subarea support. The size of OSPF seems to be very large, due to the presence of large number of external link state algorithms.
The utilization of OSPF is very large in the internet, for instance data gathering, Dijkstra’s frequency, data base turnover, LSAs per packet. The suitable available size of an OSPF router memory is almost 10,000 supported by LSAs; there are also the ways to reduce database size in domain. OSPF is reasonable for independent systems, because it carries large number of external routes. OSPF is also useful for smaller or small autonomous systems, because it has tremendous attribute like fast convergence, equal cost multipath, TOS routing, areas etc. The drawback of OSPF is that it has less capability to manage the mechanism, primarily policy mechanism is involved in the development of four layer routing hierarchy; inter area, intra area and external routes [37].

3.4.8 Resource Reservation Protocol

Resource reservation protocol is used as the tool to help for the design of integrated services architecture by reserving Internet recourses for connection oriented transfer to maintain quality of service. RSVP must be interlinked with dynamic routing, as the main purpose of an internet is to provide quality of service and send data from source to the destination in consistent and sound manner. So to avoid congestion and maintain quality of service (throughput, delay, network load) resource reservation and dynamic routing should be worked together. Internet resource reservation has different purpose whereas resource reservation may be implemented in a connection-oriented network, like ATM. So for dynamic routing is concerned, the concept of soft state is used. A soft state is simply a set of state information at a router that can be damaged unless continuously refreshed. If the route changes then the soft state are expired, then new resource reservation will be activated along the route. The protocol that has been established for the sake of resource reservation in an internet environments RSVP, defined in RFC 2205. RSVP has lot of goals and characteristics. Some of the characteristics of RSVP are listed below.

- RSVP can handle nicely changes in multicast group membership. This membership can be dynamic. Therefore reservation should be dynamic and there would be independent dynamic reservations for each multicast group.
- RSVP is also helpful to receivers to select one source from multiple sources transmitted to multicast group. This is known as channel changing capacity.
- RSVP has the ability to deal delicately with variations in routes. It would be operated by automatically redeveloping the resource reservation along new paths as long as sufficient resources are available.
- RSVP is also used as control protocol overhead, to control the traffic flow and congestion control.

RSVP uses two basic message types; Resv and path. Basically Resv is created from the multicast group receivers and spread out upstream via distribution tree. These messages are responsible for the creation of soft state along the routes of distribution tree. Path message is used to create upstream routing information. As for as all routing protocols in multicast group are concerned, the only downstream route in the form of distribution tree is maintained others are not maintained [38].

3.4.9 Routing Information Protocol

Basically Routing information protocol is distance vector protocol in which hop count is used as its metric. The application of RIP for Routing traffic is in the form of global internet and also interior gateway protocol (IGP) that states it executes routing within single independent system. On the other hand Exterior gateway protocols, such as the Border Gateway Protocol (BGP), perform routing between different autonomous systems. RIP is developed as an Internet Routing Protocol and now the
modified version of RIP is also used. The Apple talk Routing Table Maintenance Protocol (RTMP) and Banyan Vines routing table protocol (RTP) are suitable for modified version of RIP. When there is variation in network topology then it is necessary for RIP to send routing update messages at regular interval of time. When there is change to an entry, then router receives a routing update message, it automatically upgrades its routing table to create the new route. Then the metric value is also changed that is increased by one, this is the signal to the sender as the next hop. RIP prefers only the best possible route to the target, the route which has the lowest metric value. These updates are operating individually at regular schedules. RIP mostly uses single routing metric to calculate the distance between source and destination network. This single routing metric is called as hop count. Each hop in a path from source to destination is being assigned value by 1.

To control abrupt network topology changes, RIP explores lot of qualities that are similar to many routing protocols. RIP for instance uses hold-down and split-horizon to stop incorrect routing information being spread additionally, the limitation of hop-count resists routing loops to continue indefinitely. RIP has the ability to use large number of timers to synchronize its performance. The parameters which are included are routing update timer, a route timeout, and a route-flush timer. The timer clocks interval between periods. Mostly the timer is set to 30 seconds. Every routing table entry has a route timeout timer linked with it [39].

When the network spreads, it is pretty much hard to achieve all the routing tables on all the routers updated correctly. The time taken by all the routing tables to get arranged properly is known as convergence time. To fast this procedure, RIP introduces triggered updates, which demonstrates that whenever there is change in topology then link will be disappeared, so it will not wait for the next routing update, but delivered triggered update quickly. Unluckily, this process does not work for all conditions. Fig 3.3 demonstrates the happening when there is no link between A and B as well as no more connection. They will inform their neighbors that link is no more through triggered update. When this information goes to all router devices they will convey triggered update, indicating change in topology [28].

The main targets of IGRP are listed below,

- Provides stability in routing large internetworks, without routing loops.
- Synchronized with changes in network topology.
- IGRP has the ability to tackle different kinds of services.
- Less amount of overhauling in terms of bandwidth as well as router processor exertion.
- IGRP has the capability to spread the traffic along different routes.

The main difference between RIP and IGRP is in metric, poisoning algorithm, and the use of default gateway, remaining split horizon, triggered updates and hold-downs are implemented in the same way [28].
3.4.10 Simple Multicast Routing Protocol

Primarily SMRP is transport layer protocol specially manufactured for route multimedia data streams over Apple Talk networks. SMRP has the ability to help Apple computers quick time conferencing, connectionless services, best effort delivery of multicast datagram. The special attribute of SMRP is to make easier the transfer of data from single source to more than one destination [40].

SMRP is used to help routers and end stations to transfer multicast packets over different network protocols. SMRP is capable of maintaining multicast addresses and develop single source to transfer data to special multicast group address. Thus through this procedure receiver joins this group. Additionally, SMRP has large number of services, such as address management, the multicast transaction protocol, data transferring, topology setting, and node setting.

SMRP depends upon the local network that represents the end point. SMRP has two parts, 3 byte network number and 1 byte socket number. Every local network should be assigned by range of unique network numbers. The basic technique of assigning numbers is to develop multicast groups equal to the number of networks multiplied by 254. There is also the policy of SMRP to map network numbers by underlying network layer protocols. The fashions by which multicast addresses are mapped to network layer addresses depend on network layer. The multicast addresses are available for all end points, all nodes, and all entities addresses.

SMRP depends on number of node relations, for instance designated nodes, adjacent nodes, tunnel nodes to make it easy transport of multicast data grams. SMRP routers are assigned as nodes used as primary or secondary nodes. The start up process starts to find out primary and secondary nodes. The node first attempts to become the secondary node on every local net, the next time it tries to become designated primary node. So the dealing is either by primary node or secondary node requests. In this case no response showed that agreement is successful, whereas positive response shows that agreement failed [40].
3.4.11 Netware Link Service Protocol

NLSP is basically designed as a link state routing protocol to sort out the restrictions linked with IPX Routing Information Protocol and its relevant protocols like Service Advertisement Protocol (SAP). So overall to remove the deficiencies of RIP and SAP, NLSP plays vital role. Moreover NLSP delivers better routing, improved efficiency, and scalability. NLSP based routers are identical with RIP based routers. NLSP is also helpful for sound and trust worthy delivery. The decisions regarding with NLSP are really elegant due to its complete mapping network quality, not only next hop quality like RIP. In addition NLSP routers transfer service information according to changes in services, not like SAP which changes at every 60 seconds. NLSP has also several applications. It is useful for WAN link, multicast Addressing. It also supports for maintaining the load across different parallel paths and also improves link quality. Furthermore in case of scalability, NLSP has the ability to help up to 127 hops [41].

3.4.12 Open System Interconnection Routing

The international Organization for Standardization (ISO) generated a full organized methodology to use Open System Interconnection Protocol. The terms or techniques used OSI are System to Intermediate System, End system to Intermediate System and inter-domain routing protocol. End system refers to any non routing network nodes whereas intermediate system reveals a router. These terms are represented as ES-IS and IS-IS OSI protocols. The other terminologies used in OSI networking are area, domain, level 1 routing and level 2 routing [42].

3.5 Redeveloping Route information Between Protocols

If someone has the chance to create the network, and the device to design it operation of routing protocols take place, consequently routers are used for this purpose. There is possibility to select your
preferred protocol selectively. There may be some kind of condition, that pre-existing network is available, so UNIX machines are responsible for dealing such type of networks. There is a doubt about the network how more than one routing protocols can be operated at one time in the network, in both the cases either temporary basis or permanent basis. To solve this issue, redeveloping or redistribution phenomenon exists. There is a policy for the router to be able to run more than one routing protocol and redevelop routing information. To fix up this issue, multiple domains are used. Routers works with routing protocol and also informs the domain about others network as shown in fig 3.5. This figure demonstrates that router runs both routing protocols, and also has the responsibility to inform both the domains as well as updates both protocols. The router designates one metric to all routers that it distributes from one domain to another. It shows the most appropriate path to its target network, also illustrates redistribution of routes between RIP and IGRP [28].

3.6 Common Routing in MANETs

There is possibility of common protocols to be implemented in Mobile Ad-hoc networks. These protocols are commonly known as link state or distance vector kind of protocols. The major disadvantage of using these protocols in mobile Ad-hoc networks is that they are basically manipulated for static topology not for steady conditions in mobile Ad-hoc networks with great dynamic changing. Dynamic and Link state routing can be applied efficiently with low mobility. But these routing techniques depend on messages with periodic control. Thus it shows its static nature, when the number of nodes is large, the potential destination may also be large, which can create problem. The requirement of frequent and abrupt change of data within network increases. Therefore these routing techniques should be operated in low mobility scenarios. One of the attribute of these common protocols is that they are bidirectional, for instance the transfer of data will be in both the directions between two hosts or clients. As mobile Ad-hoc networks has their own conventional routing protocols, to understand the difficulties and problems for the usage of common protocols it is necessary to develop the concept of following terms [43].

3.6.1 Link State Routing

In this state, every node develops the consistency to analyze complete topology and show the cost of each link. For the persistence of costs, every node periodically spreads costs of output links to other nodes by using the process of flooding. Flooding is the process to transfer updated version of packets to all nodes within network without any obstacle. When the node gets the information, it upgrades the network policy and utilize shortest path to select the next hop for every target i.e. the path that delivers the lowest cost. There may be some problems may arise to view the node due to long spreader delays, distributed networks, such undetermined network topology may result into loop formation, but these loops are temporary they are vanished when the message is transferred to network [43].
3.6.2 Distance Vector Routing

In this routing scheme, every node views the cost of outgoing link. It disseminates periodically information to its neighbors and helps out to find the shortest path to every other node in the network, instead of promulgating information to all the nodes. The information received by nodes estimate routing table again through shortest path algorithm. Distance vector routing is more reliable, feasible to implement and short storage space is required for this routing, but one of the drawback of distance vector is the creation of short and large routing loops. Due to these loops nodes have to select their next hops in full distributed way depends on the information that should be refreshed [43].

3.6.3 Source Routing

In case of source routing, every packet has complete route information to the target or destination. This phenomenon or technique has the ability to remove the presence of routing loops. As source determines the routing path and information about the packet which travels through specified route, this technique is called as source routing technique. Moreover the addition of overhead in this approach is actually the larger packets which contain complete path information [43].

3.6.4 Flooding

The basic phenomenon to distribute routing or control information by usage of spreading or disseminating method, in which source nodes have the responsibility to send packets to all nodes in the network. Flooding is basically the implementation of broadcast method in wireless scenario. The source node sends the information to all neighbor nodes in wireless network. The neighbor nodes then forward this information to the entire node within their approach. So in this way, all the packets spread or flood within entire network. The packets are sequenced in number form to avoid staling information and loops [43].

3.7 Basic Properties of Protocols Used in MANETs

Routing protocols should have following qualities to become appropriate for Mobile Ad-hoc networks.

3.7.1 Distributed Nature

Routing protocols should not be centralized control; they should be distributed in nature in both environments static and mobile. In case of ad-hoc or WMNs environment, the difference is that nodes can be entered or leave the network in random way as well as generate distributed or partitioned network due to mobility [43].

3.7.2 Loop free Environment

It is also the criteria of Ad-hoc networks that protocols generate loop free routes and has some mechanism to deliver loop conditions. Due to loop free environment bandwidth consumption becomes low [43].

3.7.3 Demand-Based Criteria

In order to control overhead, save important network and node resources the protocol must be reactive. The protocols also need to disseminate control information in a periodic way [43].
3.7.4 Optimum unidirectional Link

Many routing algorithms are bidirectional. The wireless environment offers mostly unidirectional links, and the ability of using them is really reasonable.

3.7.5 Alternating Route Policy

To avoid the number of effects due to topology changes and traffic congestion, different routes can be used. If the specific route is disrupted, alternate routes can be used without choosing route discovery mechanisms [43].

3.7.6 Maintains quality of service

Routing protocols should have qualities to maintain quality of service such as delay, throughput, network load and jitter etc. The research explores that all routing protocols have no such attributes ideally. They are still in evolution to find the best path to the destination node and control appropriate routing tables [43].

3.8 Protocols used in Mobile Ad-hoc Networks

Internet Engineering Task Force (IETF) introduced MANETs to create such type of network in which there is no central entity. The main purpose of MANETs is to improve IP routing protocol used for both static and dynamic techniques. There are lots of routing protocols which are working under this category, but few of them are listed below.

- AODV (Ad-hoc on-Demand Distance Vector)
- ZRP (Zone routing Protocol)
- TORA (Temporally Ordered Routing Algorithm)
- DSR (Dynamic source Routing)
- CBRP (Cluster Based Routing Protocol)
- CEDAR (Core Extraction Distributed Ad-hoc Routing)
- AM Route (Ad-hoc Multicast Routing Protocol)
- OLSR (Optimized Link State Routing Protocol)

Although all the routing protocols used in MANET are very important in their functionality, they have their own attributes and contributions for reliable communication and flexibility, yet here the brief description of some the protocols would be listed. The main motive for description is to understand the basic concept of these protocols and know about the importance of their functionality. There are lot criteria to classify Mobile Ad-hoc routing protocols, but the most acknowledged criteria is to categorize them as reactive or proactive protocols in behavior. The routing which is pre calculated or pre defined or the tables are manipulated for such routing is known as proactive routing. To know about the routes, nodes should store half or full information for the network topology. The benefit of predetermined route environment when the message is to be sent to destination, the route is update and up to the mark, with the consequences of low delay and synchronization. The proactive routing protocols use shortest path algorithms. The proactive protocols include OLSR (Optimized Link State Routing Protocol), DSDV and WRP (wireless Routing Protocol). The main drawback of these routing is that the information used by these routing protocols cannot be used. The other major drawback is the broadcasting of information utilizes bandwidth and energy in terms of control packets. On the
other hand the routing which represents on demand policy is referred as reactive routing. In contrast with proactive routing there is no pre computed routing here to the target, but on demand, when necessary. When a source is going to deliver packets to target, it is needed to first determine the route or many routes. This phenomenon is known as resource discovery. So totally opposite to proactive routing the policy 1 to first determine the route, then the source is in position to deliver packets along the determined path. There is the possibility to have some obstacles in the way of communication, may be there exists breakage of routes due to the movement of nodes along the path up and down. The procedure adapt to control such breakage is route maintenance. The reactive routing has the edge that it maintains the bandwidth. The disadvantage of on demand or reactive routing the latency is increased due to route determination. The route determined is not being assured to be useable by on demand routing. There are also some problems may be created due to increase in mobility rate. Dynamic source routing, TORA, AODV protocols are included in reactive routing policy [43].

3.8.1 Ad-hoc on-Demand Distance Vector

The Ad-hoc on-demand is basically reactive protocol which supports multi routing between nodes which are playing their roles to form an Ad-hoc network. AODV is the improved version of DSDV protocol, but the main difference is that AODV is reactive whereas DSDV is proactive. It has great advantages, for instance, for disseminating information through routes on demand basis requirement for maintenance is not necessary. One of the main qualities of AODV is that it is free from hops. The environment where AODV is activated, target sequence numbers confirm the route, to be refreshed properly. The algorithm use d in AODV considers two messages, one is route request, to establish the route request message is being activated by AODV, and the other is hello message. These messages support nodes to strengthen neighbor nodes. Without the presence of hello messages, the identification of nodes is difficult. AODV has the ability to provide lot of information about the following technical aspects [43].

- Target IP addresses, where the packets should be sending.
- Sequence numbers.
- Counting of hops, that packet has passed.
- Next hop, stability of routes
- Neighbor nodes activity
- Request, the request should be on at a time.

3.8.1.1 Process to Find out Route

The node starts to find out the path, the path is necessary for determining and travelling of data. The source finds out the path and sends the message towards the destination. The request message is also activated to find out the appropriate route for sending the message [43].

3.8.1.2 Route Management Policy

To manage the route, it is necessary to point out the route that lacks its validity, then the removal of route entry exists and link failure message is conveyed. This message is also transferred to nodes which are using the same route which has been suffering from breakage. The neighbor’s nodes are properly updated. This process is repeated again and again. The main benefit of AODV is the limitation of routing messages as compared to ordinary protocols. This is all due to the reactive behavior of AODV [43].
3.8.2 Dynamic Source Routing Protocol

Dynamic Source Routing Protocol represents source route which is implemented on demand basis. Every node should control its route cache. The node regularly updates the route cache if there is a better route, and then it can adopt new routes. In dynamic source routing process every packet has to know about the route direction, to avoid periodic route findings. DSR has the quality to find out the route and control the path for routing. MAC layer helps DSR to detect link failures [43].

3.8.2.1 Route Analysis

The finding of node is important when mobile node transfers message to specific target same like AODV. Route discovery mechanism has been implemented by disseminating route request packet RReq. RReq packet has the information of packet transferring, the nodes which are responsible for sending the information has special credential number. The route response or route reply is also generated when either the destination node or the middle node has the information for the target. So DSR is optimistic and reliable for routing, moreover nodes are actively participated in case of DSR [43].

3.8.2.2 Route Control Mechanism

Route control mechanism acts by detecting the movement of network topology. If the link is failed then it can adopt other route to reach the destination. By detecting the problem in route, a route error acknowledgement is conveyed back to the source node. To get rid of this error packet, it must be eliminated from its original host cache, and approximately all routes that contain hop are cut off at its original point. There is specialty of DSR, that it uses source routing. There is no need for intermediate nodes to be consistent in updating routing information. There is also necessary for periodic messages to limit the bandwidth. Battery power is less consumed while using DSR. There is a security threat to use the interfaces in abandoned modes, due to incorporations of interfaces causing address infiltration. So to overcome this issue scanning of useful information should be done by using security passwords or credit card numbers. Routing protocols may be the main targets and thus they should be encrypted properly. DSR has the ability to support one direction links by consulting with source route. This definitely improves the performance of DSR in unidirectional links. MAC layer should also work side by side with DSR for security and maintain the performance [43].

3.8.3 Optimized Link State Routing Protocol

There are lot of deployments and achievements of wireless networks in this age. With the passage of time, due to changing in wireless networks day by day. It is necessary to introduce new routing protocols to achieve stability and reliability. There are two prominent topologies in wireless networks, infrastructure and ad-hoc. To deploy the wireless networks in different scenarios, lot of crises and situations arise that have to overcome. Among new topologies ad-hoc topology is more likely to be reliable and scalable. Mobile ad-hoc networks has lot of applications in wireless network field, it is also helpful in military usage as well. The research in wireless networks proposed two kinds of protocols mainly, the reactive protocol and proactive protocols. Basically proactive protocols depend on periodically link state updates and control packets delivery. There is a large traffic which ultimately effects original traffic. Messages are being updated and disseminated by flooding. Optimized Link State Protocol is considered to be proactive protocol [44]. OLSR provides the best possible way to develop a link state protocol and reduced the size of information which is being delivered by the
messages. OLSR also controls the flood within network. The technique which is probably used in OLSR is multipoint relay technique. OLSR proved to be good agent to control the congestion traffic. OLSR is expedient for large and dense ad-hoc networks. It provides solidity to link state algorithm. The protocol has the capability to update the route for all the network targets. So it generates optimization for all sort of traffic where large subnet of nodes is communicating with each other. OLSR is appropriate for large networks and dense functions. The designing of this protocol is almost in the distribution form like peer to peer network, and do not depend on central point. Each node has the ability to send control messages in periodic form. The other advantage of OLSR is that it does not require sequence of messages. Hop by hop routing is being performed by OLSR. By critical analysis OLSR protocol is proactive protocol by inheritance, thus favorable in terms of networking, where we need update information and the route request for new targets are quick. Therefore by using OLSR protocol, delay process would be minimized and reliable communication between among dense and large number of nodes is delivered [45].

3.8.4 Destination Sequenced Distance Vector Routing

The idea for destination sequenced distance vector routing depends on Bellman-Ford Routing algorithm with some updates to make it efficient for wireless networks. In this scheme every node has to create a consistent path towards routing table to the destination, also maintains hops to reach target and the sequence numbers allocated to destination nodes. The function of sequence numbers is to create the difference between old and new routes. The function of nodes is to send routing table information to nearby nodes in the form of periods. Thus update in this case is in form of time driven and event driven. The routing table in this scheme adopts two methods for updates, one is full dump and other is progressive update. The dump shows the transmission of full routing table to neighbor nodes but progressive or incremental update indicates that those units from routing table are transmitted that has changing in metric. Incremental or progressive updates help to prevent traffic load whereas full dump is comparatively occasional. In fast changing environment incremental packets can develop more so full dumps can be more efficient to work. As DSDV is considered to be periodic in nature it takes some time to coincide before route can be used, which has no effect in case of static wired network, where topology does not change dynamically. But in case of Mobile Ad-hoc networks, the topology has been changed dynamically, so the convergence or coinciding factor of DSDV give rise to dropped packets. Moreover periodic broadcasts result into large number of overhead in the network [43].

3.8.5 Temporally Ordered Routing Algorithm

Basically TORA lies in the category of distributed routing protocol. The basic idea used in this algorithm is link reverse process. This routing algorithm is being developed by IETF to control the effects of topological changes. It makes it sure that loop free environment is developed and various routes should be created for source to the destination. Its specific quality is to develop routing mechanism and rely on Internet MANET Encapsulation Protocol (IMEP) for other different functions. The route mechanism defined by TORA has three preliminary key functions Route detection plus deletion, Route generation and route maintenance [43].

3.8.6 Zone Routing Protocol

It is prototype protocol by nature. It is comprised of two sub protocols i.e. Inter-zone and Intra-zone. Intra-zone is less capable proactive routing protocol which is helpful to improve the quality of global
reactive routing protocols. It depends on specific neighbor discovery protocol. Intra-zone can use scheme Time to Live TTL in IP packets to control range. On the other hand IERP is reactive routing component of zone routing protocol. This is helpful in determining global path. It keeps away from queries to target that could be transferred to neighbor R-hop nodes. ZRP has the specialty to get the benefits from reactive and proactive protocols [46].

3.9 Wireless Mesh Network Protocols

Wireless Mesh Networks are generally considered as the type of mobile ad-hoc networks. However there are some differences between them. Firstly in wireless mesh networks all most all the traffic starts from gateways and ends ups also on gateway. Secondly in wireless mesh networks, nodes are clearly separated from each other either they are in the form of stagnant nodes or mobile nodes. MANETs are linked with mobile ad-hoc networks, general MANETs routing protocols can be used in WMNs. Additionally WMNs are new technological networks which are similar to MANETs. One of the applications of WMNs is that, it provides connection to an infrastructure node. It plays vital role for providing broadband internet access. The other successful production of WMNs is Wireless local area network. Routing is basic attribute of WMNs. The protocols have the clear effect on the behavior of WMNs. Therefore selection of suitable routing protocol increases the efficiency of network. Some of the effects of routing protocols in WMNs are listed below.

1. They are responsible to strengthen the network.
2. They are helpful to make connection between nodes.
3. Creates synchronization between nodes.
4. Provides quality of service in terms of bandwidth utilization, delay, throughput, network load, and jitter.

As mentioned earlier general MANETs protocols can be implemented in WMNs, however the more efficient protocol which synchronizes with wireless mesh networks is mesh routing protocol (MRP). The protocol creates the continuity between routing paths and gateway destinations. It has also the ability to select the route, which is basic requirement to make better communication in WMNs. There are lots of relevant protocols in this context. Many of them have been authorized by IETF, some of them are reactive and some of them are proactive for example AODV and DSR are implemented for ad-hoc networks. Wireless mesh technology is the latest well developed technology which has vital role in the field of telecommunication as well as internet services; however there are still some challenges and problems which have been faced by trouble shooters. To fix up the problems in WMNs many projects have been launched such as MAC layer, internet mobility and transport layer efficiencies. Consequently for designing of routing protocols in WMNs, it must be considered that almost all the traffic is supposed to flow to and from gateway to internet systems. Thus routing protocol should be designed to avoid flooding for the discovery of route [47].

3.9.1 Pre-Requisite or General Prospective for WMNs Routing

To resolve the main issues like dynamic connectivity and guaranteed delivery for routing protocols in WMNs or MANETs following factors play vital role. There should be the clear path from source to destination, so that routing protocols can easily deliver data through that path. If there is variation due to change in connectivity between nodes, routing protocols should have the capability to recover by using alternate path. There are also some other issues and problems regarding routing wireless Ad-hoc networks, for instance overhead is very important in wireless networks with small bandwidth. One of the other issues is power consuming issue in MANETs. Moreover other vital issue is to maintain
quality of service. Routing protocols should have the ability to handle traffic balance on links. Protocols scalability should be updated regarding large networks. The implementation of security through routing protocols is also necessary to protect against different sort of attacks like sniffer, interruption, fabrication and denial of service etc. Routing protocols can also depend on other layers, for instance the implementation of Global position System in Wireless Ad-hoc networks. The determination or analysis of mobility can also play important role to give worth to routing in WMNs. Cross layer designing is another field of research in the field of MANET protocols [46].
Chapter 4- Introduction to Research Methodology

4.1 Introduction of Research

In almost every profession the research is undertaken. It is a way of thinking. The word “Research” can be defined in different ways [48].

- Gathering of useful data or information about a particular topic.
- An investigation with full of surprises on a chosen topic.
- A skill that can help in getting deep understanding about a topic.
- Way to know what has been done in past on a particular topic.
- Understanding the questions and obtain the answers of a topic.
- Dealing the topic with different angles.
- Struggle for getting the right thing related to a topic.

4.1.1 A way of Thinking

Research is actually a way of thinking. Suppose a person is working in the field of marketing and he can be a sales engineer, sales representative, sales executive or sales manager there. He has to take care of lot of things like administration and planning. There will be lot of questions in his mind on which he has to work and find an answer to these questions so that he might be able to perform his duties in an efficient manner. The answers to his questions can lead him to a valuable worker/asset in the organization. The type of questions and their answers differ organization to organization. May be the person who is working in a marketing field has to deal with questions on daily basis or may be on monthly basis, depending on requirement of organization. The questions that he may tackle while working in the marketing field are as follows.

- How a particular product can become valuable
- How many workers will be suitable responsible for advertising the product
- What percentage this advertising will gain
- Will the customers like the product
- What should be the packing of that product

Similarly if a person is having a professional education, he can face some professional questions and he has to find the answers to these questions. His questions need literature study and the experiment/testing. The kind of questions he might face is as follows

- What is the result if I do this
- How can I test particular thing
- What platform should I require for testing
- Are the results accurate
- What are the causes of this particular testing

4.2 Types of Research

The research is categorized into two types. These types are the most commonly used in every research.
1) Qualitative Research
2) Quantitative Research

4.2.1 Qualitative Research

Qualitative research focuses on the word “what” “why” rather than the “how” in the research topic. This kind of research requires literature review of a topic. It is mostly called as a soft science and requires research questions that may arise from the topic. Qualitative research is a kind of research in which gathering of data, analysis, and translation of data is being done. In qualitative research each and every process of phenomena is explored through an independent analysis of raw information like interviews, observations, documents, emails, news, photos and videos etc. This research enables the researchers to seek out the understanding of various functions through communication and research. Examples of qualitative research include meetings, face to face conversation with different people for the sake of useful data, group interview and observation of data by watching the behavior of data [49].

4.2.2 Quantitative Research

Quantitative research focuses on the word “how” in the research topic. This type of research is carried out by doing experiments and by simulations which are helpful in testing a theory. In quantitative research results are needed in the form of graphs which helps in observing the behavior of a topic accurately and easily. It lies under the category of hard science. As its word tells that it is a kind of research that emphasizes on quantity and for this experiments and simulations are the ways to define quantity. It is used to check whether the theory is true or false. Examples of quantitative research include experiments and surveys [50].

4.3 What is Research Methodology?

It is method of getting familiar with how to do research in the every field like professional education or professional work. Similarly it is a way of doing research by following the different logical steps. In simple words research methodology is a pre requisite to do research. It guides about the useful techniques how to do the research and makes us more familiar with the things that we have to keep in mind while doing research. Research methodology helps in making minds deal with topics more logically and efficiently. While doing researches it is a good idea to use information resources like internet, libraries, and old research papers. Research methodology helps in making aware how to use these information resources in a good manner.

4.3.1 Methods of Knowing

Robert B Burns in his book “Introduction to Research Methods” has written that according to Kerlinger in 1986, there are four methods of knowing which are as follows [51]. According to him, from these four methods one can get knowledge about a particular topic or issue. Once knowledge about a particular topic is achieved, it is easy to do research on it.

- Method of obstinacy
- Method of authority
- Method of perception
- Method of science
4.3.1.1 Method of Obstinacy

Here is a fact because one knows where it held to be true. The more this truth will repeat more chances of increasing the validity of a research. Method of obstinacy is also called as method of continuity. This means what the concept of a particular thing is coming from ancient times; it has to be taken forward like this.

4.3.1.2 Method of Authority

A thing is true if it is come from the Holy book, the president or from the teacher. These things must be followed by everyone. The thing that may come from the authority cannot be tested again and again as it comes from the authentication source. This type of method requires less individual efforts.

4.3.1.3 Method of Perception

The things must be perceive in this kind of method. People make perception about particular thing; it may be like this. Example; people can make a perception that education can give wealth in future, but actually it is not hundred percent sure.

4.3.1.4 Method of Science

This method has a plus point i.e. self correction. Neither of all methods gives this advantage. By doing experiments on a particular topic/thing, if the results are not satisfied, it can be corrected. Experiment can be verified and validate according to the requirement, by checking again and again. In this method a hypothesis is made in the beginning of the topic. Science is a mixture of knowledge, inquiry and correcting knowledge.

4.4 Combination of both research types

As both of the research methods have their own plus points, combining all the positive aspects of both these research methods automatically yields a great benefit to carry out a research for a particular topic. It is becoming very common nowadays that research is being carried out by using both the research methods together. The benefits of combining qualitative and quantitative researches are [52].

- Research maturation ➔ mixture of both research methods make a research extremely mature
- Increased stiffness ➔ makes the research very much valid
- Addition of information ➔ lot of related information can be obtained
- More authenticated ➔ research with different methods make it more authenticated

4.4.1 Thesis Research Type

The research type that is being followed in this thesis topic is a mixture of both qualitative and quantitative methods. The reason to choose the mixture of both the methods is to increase the validity of this thesis topic. This thesis includes theoretical study as well as simulation in OPNET tool.

4.5 Steps in Research Methodology

While doing a research on a particular topic following steps are necessary to be implemented. These steps help in carrying out the research in a very efficient and smooth way.
• Identify the problem
• Build the questions
• Literature study of topic
• Start Writing New Research
• Getting Started with Simulation Environment
• Implement the Simulation
• Simulation Results

4.5.1 Identify the Problem

First of all it is necessary to identify the main thing in the thesis topic i.e. what we are going to do in this research. Everything should be crystal clear that what is the problem and what we should do to cope with it. The problem process cannot be solved without identifying the problem which means that identifying the problem in the very beginning is really very necessary. Moreover identifying the problem also proves beneficial to the researcher because it can save time as the time is limited in the research. The most important problem should be given priority if there are lots of questions in the research because it is not necessary that all the problems are solved.

4.5.2 Build the Questions

Once the problem is identified, the second step is to build the research questions i.e. on which thing our research will focus. These questions are of any type. It can include “what” “why” and “how”. Building the questions initially help in carrying the research topic in a right direction.

4.5.3 Literature Study of Topic

After building and setting up the questions, the one of the important tasks come i.e. study of all the important things that a thesis contains. Our thesis is on routing protocols in WMNs under certain parameters. So this thesis contains the literature study of routing protocols, WMNs, parameters (delay, throughput and network load), routing protocols in WMN and the traffic that is injected into WMNs. This stage requires deep literature study of all relevant materials including study of old research papers.

4.5.4 Start Writing New Research

After all the relevant literature study has been done, writing thesis is the next step. This includes what you have observed must be written and expressed in your own words.

4.5.5 Getting Started with Simulation Environment

After all the research and detail has been completed, the next step is to get familiar with a simulation environment. Start reading the simulation environment handbook or other relevant material. Our simulation is on OPNET Modeler 14.5, this section includes getting familiarize with OPNET Modeler 14.5, reading their commands, getting familiar with its tools etc. Every simulation environment requires that it should be read before doing simulation in it.
4.5.6 Implement the Simulation

After getting familiar with simulation environment, it’s time to implement the simulation in it i.e. testing/experiment is being done. The testing produces results in the form of graphs that explains the behavior of the research issue. These graphs should be displayed in the thesis report. Implementing the simulation is the most critical part of the thesis report.

4.5.7 Simulation Results

The graphs show behavior of the research issue which can be explainable. The simulation graphs also exhibit some results which can be written in the research report. These results can be well defined from each and every angle so that one must understand them easily.

![Figure 4.1 Steps in Research Methodology](image)

4.6 Research Strategies

According to Robert K. Yin in his book “Research Design and Methods” there are five kinds of strategies of research. According to him a research can be carried out in five different ways. Each of them has their own form of questions which are best described in the following table [53].

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Form of Question</th>
<th>Control of Behavioral Events</th>
<th>Focuses-on Contemporary Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Study</td>
<td>How, Why?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>History</td>
<td>How, Why?</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Survey</td>
<td>Who, What, Where, How many, How much?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Archival Analysis</td>
<td>Who, What, Where</td>
<td>No</td>
<td>Yes/No</td>
</tr>
<tr>
<td>Experiment</td>
<td>How, Why?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Table 4.1 Situations of Different Research Strategies [53]*
Chapter 5- Design Parameters; Guide to Simulation Environment

5.1 Design Parameters

There are various parameters that are available in WMNs and they are also termed as performance metrics or design parameters. Every parameter has its own importance. These parameters are named and described below. These design parameters/performance metrics are used for the evaluation of routing protocols. These design parameters have a great impact on overall performance of a communication network. This thesis has dealt with the first three performance metrics of a network i.e. delay, throughput and network load. These three performance metrics are evaluated with respect to routing protocols to see the performance. The descriptions of all the design parameters that are useful in WMNs are as follows.

- Delay
- Throughput
- Network Load
- Jitter
- Packet Loss
- Routing overhead
- Packet Delivery Ratio

5.1.1 Delay/End to End Delay

Time taken by a bit of data in a network to flow from one to another node is known as delay or end to end delay. The unit of delay is second. In different kinds of networks delay is a major concern, every network has some kind of delay in it, but it is always practiced to reduce the delay in a network as low as possible. Delay in a network is a mixture of several kinds of delays which are Processing Delay (PDe), Queuing Delay (QD), Transmission Delay (TD) and Propagation Delay (PD). The end to end network delay does not include the queuing delay [54] as network delay has no concern with it and mathematically it is written as follows

\[ d_{\text{end-end}} = N [ d_{\text{trans}} + d_{\text{prop}} + d_{\text{proc}}] \]

Where

- \( d_{\text{end-end}} \) = end to end delay
- \( d_{\text{trans}} \) = transmission delay
- \( d_{\text{prop}} \) = propagation delay
- \( d_{\text{proc}} \) = processing delay

If there are \( n \) nodes in a network, the average delay [54] is calculated by taking the average of all packets, source-destination pairs and network configurations. Another name for delay/end to end delay
is latency, both have similar meaning. There is some level of delay that certain applications need, some applications are very sensitive to delay and some can bear the delay to some extent.

5.1.2 Throughput

The rate at which the data is transferred from one node to another node in a communication network is known as throughput. The unit of throughput is bits/sec. Throughput is usually referred with a symbol \( \lambda \). It is acceptable [54] if all the nodes in a network send data at a rate of \( \lambda > 0 \) bits/sec to the destination node.

5.1.3 Network Load

When there is lot of traffic going on in a network and it is becoming difficult for a network to handle the traffic it is said that network is having a load on it and is known as network load. For efficient network the requirement is that it avoids load on it, and for this purpose lot of techniques have been introduced.

5.1.4 Jitter

Variation in time of a periodic signal or the shifting of a signal in time domain is known as jitter. It is among the unwanted problems in a communication network that should be avoided by any means. To avoid jitter in network different preventive measures can be taken. It includes anti-jitter circuits, jitter buffers and dejitterizer. Jitter can cause loss of data transmitted between different nodes in a wireless network.
5.1.5 Packet Loss

It is term which occurs when a data packet does not reach to its destination node in a communication network. Definitely when a source node sends data packet towards its destination node and when node does not get that data packet, it is called a packet loss. If QOS is ensured in a communication network, there is less chances of packet loss in a network. There can be various reasons of packet loss in a network like hardware problems, corrupted information etc. In some cases network by its own also discard the packet which includes reason like router or switch is too much overloaded that it cannot treat another incoming data packet easily. This packet loss can cause noise in a network which is due to natural interference or by human fault.

5.1.6 Routing Overhead

As the network size increases the flow of traffic shows increase which is also called routing traffic. WMNs are scalable networks, to measure how much network is scalable it is necessary to measure the routing overhead of that network. When total numbers of routing packets are transmitted over a network, it is known as routing overhead. This is expressed in bits/sec.

5.1.7 Packet Delivery Ratio

It is a ratio between numbers of packets transmitted by the source to the number of packets received by the destination. For an efficient network Packet Delivery Ratio (PDR) should be larger. Since it is ratio, it has no unit. From PDR we can see how much is the network throughput. The characteristics of PDR include the precision and competence of routing protocols.

5.2 What is Simulation?

To make a model of an existing or proposed system and to understand the aspects that controls the system so that it becomes easy to foretell the future behavior of the system. Simulation is a testing of system to see what response the system gives how it behaves. It is a method of exploring new processes. Simulation of a system is mostly in graphical representation as graphs are easy to read and it can well describe the behavior of a system in all aspects. In the following figure simulation has been done. This figure tells what simulation is and how it looks like.

![Figure 5.3 Graphs showing behavior after simulation [55]](image-url)
5.2.1 Why Simulation

Simulation is important for checking the results of a system and to understand the system in a better way. Simulation functions at packet level. A simulation tool like OPNET is useful for analyzing the behavior of network systems. To evaluate the performance of large networks, simulation is one of the used methods. But simulation is preferred because it gives more and accurate detail about the behavior of network, useful for larger networks; it can study dynamic behavior of a system and involves little approximations.

5.2.2 Simulation Environment Used

Simulation environment used in this master's thesis is OPNET. It stands for Optimized Network Evaluation Tool. It is a very sophisticated tool and gives very user friendly Graphical User Interface (GUI). It is used especially for network simulations which includes the research and development of the networks. OPNET is among the leading simulators these days. Most of the other networking tools do not have so much vast library like this OPNET has. In this tool we can have a deep understanding of routing protocols, network devices and network scenarios in a very efficient manner. The good thing about OPNET is that it has the ability to simulate each and every happening of a system. There are various useful tools inside OPNET such as the tools made for programming our own packet formats in the routing protocols. As it is a dominant tool, that is why it is complex also, but for users it is very easy to operate. In OPNET we can easily make a network model of any type by introducing the nodes in that network model and having a connection of these nodes with each other and with a network model as well [56].

5.2.3 What can be learnt from OPNET?

It is a very user friendly tool for network designing. While working on OPNET it can give various benefits, and these benefits help in future with great deal. OPNET teaches us how to make and design networks of any size and of any type. A network is designed in a very easy way and in a cheap way in terms of cost. It can make us a very good network designer which helps in getting good professional jobs in lot of organizations. These days many organizations are working on this efficient network tool and every now and then they require network designers who know how to build and design a network in less time. A network design in OPNET looks like a real network which is another plus point of this sophisticated tool [56].

5.3 Division of Simulation Work

While a project or work is carried out in a simulation tool like OPNET, the whole work is divided into three parts/levels. The three levels are

- Highest Level
- Middle Level
- Low Level

5.3.1 Highest Level

The highest level includes the making of a network in the simulation tool. When we build or design any network in a simulation tool, it lies under the highest level. Example if we build a Local Area
Network (LAN) in the simulation tool this work comes in a highest level. This highest level is also called as a network level. The below figure is showing a design of a network and this work has been done in a highest level [57].

![Figure 5.4 Highest Level; Designing of Network [57]](image)

### 5.3.2 Middle Level

In this level, the placing of devices, nodes like routers, switches, bridges and servers are done. Any network without the nodes is useless, as nodes are the major items in a network. Without the nodes the communication cannot be processed. The placing of these nodes/devices is categorized in this middle level. This middle level is also called as node level. The figure below is showing a simple server node.

![Figure 5.5 Middle Level; Simple server node [57]](image)

### 5.3.3 Low Level

In this level, the placing of individual protocols like MAC, TCP/IP, reactive and proactive protocols are done. For communication purpose nodes require some protocols which help nodes to carry their information from one end to another. Routing protocols have key importance in the field of
networking. Without these protocols the communication between networks is not possible. This low level is also known as process level, which means to process something. This level uses huge amount of functions for gripping various attributes, packets and events etc.

![Figure 5.6: Low Level; Making of finite state machine [57]](image)

### 5.4 Diagram showing Divisions

![Figure 5.7: Levels of simulation project [34]](image)

### 5.5 Flow of work in OPNET

The work in OPNET has to stream through some steps. The work is executed step by step in OPNET. If the work is assigned to build a local area network with hundred nodes in OPNET, then the first step will be making and setting up a LAN using a project window of OPNET modeler. Once the LAN is set, place hundred nodes within that LAN and connect those nodes with each other and definitely with LAN also. For connecting nodes with each other, OPNET offers many attributes. In this master’s thesis we have to create a WMN with some nodes that will easily show the WMN and couple of
Routing protocols will be executed on this WMN under certain parameters i.e. delay, throughput and network load. The making of WMN and the testing of routing protocols in WMN are described in next chapter. The general flow of work in OPNET can be described by drawing a simple flow chart which is shown as below.

*Figure 5.8 Flow Chart of work in OPNET*

### 5.6 Application Areas of OPNET

There are some application areas where this OPNET is very useful and can give better results. These include [58].

- Evaluation of Routing algorithms
- Protocol Management
- Wireless and Satellite Communication Protocols
- Network Management
- Network Planning

#### 5.6.1 Evaluation of Routing Algorithms

OPNET can be used for the evaluation of routing algorithms for devices like routers, switches, bridges, servers and other communication devices. Every device uses protocols that are compatible with them and give best performance. So OPNET has the tendency to evaluate routing protocols whatever the devices are. As it is user friendly tool, evaluation of routing algorithms can be done in an easy way.
5.6.2 Protocol Management

OPNET gives a facility to develop and manage the protocol. A self made protocol can be managed in OPNET modeler tool.

5.6.3 Wireless and Satellite Communication Protocols

Wireless and satellite communication protocols and schemes can be tested in OPNET in a very sophisticated way. As wireless and satellite communication is progressing day by day, the protocols in these fields are tested every now and then for future enhancements. So there is always a need of an efficient tool or software that can give us to test the protocols and new schemes. OPNET has this feature inside.

5.6.4 Network Management

Microwave and fiber optic are one of the latest technologies in the field of networks. There exists microwave and fiber optic networks whose management is the essential part. To do the network management of microwave and fiber optic networks, OPNET Modeler tool is a very good option.

5.6.5 Network Planning

Network planning of local area networks (LANs) and wide area networks (*WANs) can be done in this tool. It gives us the facility to analyze the behavior of the networks and facilitate us to find the problems occurring in the network. Through OPNET we can have a better look on the performance of our networks. The problems in an actual network can be studied if that network is built in OPNET.

5.7 Tabs in OPNET

While working with OPNET, it is recommended to have familiarity with all the buttons, tabs and the functionalities of these tabs. Without getting familiar with OPNET, becomes difficult to do work. Here is some of detail of tabs that may be used while performing the project in OPNET [58].

- Scenario
- Topology
- Traffic
- Protocols
- Simulation
- Result
- DES

5.7.1 Scenario Tab

This tab is used for creating, deleting and editing the scenarios in OPNET. Scenario can be of any kind, it may be WMN, LAN or WAN.

5.7.2 Topology Tab

This tab helps in creating different kind of objects in a project window. Objects may be routers, hub or computers etc.
5.7.3 Traffic Tab

This tab is used to control the traffic of a network. The traffic can be brought in and out of a network by the user.

5.7.4 Protocols Tab

This tab is used to edit and shape the protocols that are going to use in the simulation.

5.7.5 Simulation Tab

This tab is used to start the simulation of the project/work that is done in the OPNET. The simulation tab also gives the constraints to set like time of simulation, speed of simulation and samples for simulation.

5.7.6 Result Tab

This tab is used to see the result of the simulation. There are various options in a result tab for viewing the result of a simulation. The result can be seen in multiple windows separately, multiple results can be seen in one window also.

5.7.7 DES Tab

This tab helps in choosing the statistics that is one of the mandatory parts of a simulation procedure. DES statistics include Global Statistics, Link Statistics and Node Statistics. The selection of statistics depends upon what kind of simulation is carrying out or what kind of statistics the simulation procedure requires.
6.1 Introduction

In this chapter we have discussed the simulation results plus the analysis that we have obtained after doing the simulation in OPNET Modeler 14.5. As Mobile Adhoc Networks are the subset of Wireless Mesh Networks, we simulated MANETs as our networking scenario and run three protocols (AODV, DSR and OLSR) on this network and checked the performance of these protocols according to three parameters i.e. Delay, Throughput and Network load. All these parameters and the simulation environment’s guide have been discussed in detail in chapter number 5 of our thesis report. The important concept of these parameters and the important tabs used in OPNET also has been discussed in the previous chapter. During our simulation we have used Global Statistics by choosing individual DES statistics in a workspace window of OPNET and the results are displayed in the form of graphs, where all the graphs are displayed as average. The FTP was used as traffic in our simulation for all kinds of scenarios in equal amount. There were three scenarios used in our simulation i.e. 15 nodes, 30 nodes and the third one was 60 nodes. All scenarios were tested separately against three protocols and the different graphs were obtained which are shown in next articles.

6.2 First Scenario

We made first scenario in which we used 15 mobile nodes from the object palette window of OPNET Modeler 14.5 and pasted all of them in the workspace window. For these 15 mobiles there had to be one server, so we took one fixed wlan_server from the object palette. These nodes were being pasted in the campus network size of 1000 x 1000 meters. Once all the mobile nodes and fixed node server have been pasted on a workspace window, IPv4 addressing was assigned automatically to all nodes. After this we drag application config and profile config from object palette to workspace window. All the attributes of these two config(s) contain mostly the number of rows, speed in meters/seconds and pause time in seconds. So these settings must be done according to the requirement. The FTP was selected as traffic and FTP was set to High Load FTP traffic. After doing all the configurations to a network now it’s time to deploy the configured profile which can be done by clicking Protocol tab in OPNET workspace window and selecting the Deploy Defined Application. Mobility Config was also dragged into workspace window, all its necessary attributes had been set and then random mobility was set to MANET as a profile. Before running simulation, individual statistics had been selected from where we can choose protocols and wireless LAN etc. The figure of this first scenario is shown as follows in which all the three protocols (AODV, DSR and OLSR) were tested against the three parameters (Delay, Throughput and Network Load). The steps of making this scenario and all the necessary attributes can be found which are written in [APPENDIX].
6.2.1 Second Scenario

Similarly we made our second scenario in which have increased the number of mobile nodes from 15 to 30. This scenario was made by clicking scenario → new scenario option when all the necessary steps of scenario 1 have been completed. All the settings in this scenario remained same like it had in the first scenario, only the number of nodes was increased. In this scenario also, the protocols are tested against the three parameters. The figure of our second scenario in simulation environment is shown as follows. The steps relating to this scenario can be found which are written in [APPENDIX].
6.2.2 Third Scenario

Similarly we made our third scenario when the number of mobile nodes in a workspace window was 60. This scenario was made by clicking scenario → new scenario option when all the necessary steps of second scenario have been completed. All the steps remained same in this scenario also just the number of mobile nodes was increased so that we can have a deep look on the behavior of all the routing protocols. To know how we have done the simulation, all the necessary steps are written in [APPENDIX].

![Simulation Scenario with 60 nodes](image)

**Figure 6.3 Thesis Simulation Scenario with 60 nodes**

6.3 Simulation Results

After making all three scenarios in OPNET Modeler 14.5, we run the simulation and compared the results of these three scenarios. Initially simulation time was set to 50 minutes and graphs were taken, but for statistical calculation we found those graphs very difficult as the graphs are showing very little variations in it. That is why we then performed the simulation for 3 minutes (180 seconds) and graphs were taken and saved in bitmap image. These graphs were found very helpful for statistical analysis as they are showing reasonable variations in the graphs. Hence we preferred those graphs that were obtained during 3 minutes simulation. Results in the form of graphs were taken from every possibility so that the results can become more defined and satisfactory. The results of delay, throughput and network load were saved in different kinds of figures which will be shown in the next articles. The DES execution manager window for both the simulation periods clearly shows that simulation has been performed for 50 minutes and 30 minutes also.
6.3.1 When Nodes=15, AODV Performance

This figure was taken when we were working in our scenario 1 when we have 15 mobile nodes and 1 fixed node server. The protocol run in this case was Ad-hoc On-Demand Vector (AODV) against all three parameters. In this figure delay, throughput and network load are being shown when AODV protocol is used in MANETs. The graphs are showing in time average form. The upper small window is showing the delay when AODV protocol was used, the x-axis denotes time which is in minutes and y-axis is also in time but in seconds. According to the upper figure the average peak value of delay is almost 0.027 seconds, and it gradually drops and attains a constant value of approximately 0.001 seconds, after 3 minutes the value of delay is almost 0.001 seconds. Similarly the middle graph is for network load when protocol was AODV and nodes were 15. The x-axis of this graph denotes time...
which is in minutes and y-axis denotes data rate which is in bits/seconds. According to this graph the peak value of network load is 500,000 bits/sec and it gradually drops as time progresses and reaches to almost 80,000 bits/sec after 3 minutes. The third graph is for throughput when AODV protocol was used and numbers of nodes were 15. The x-axis denotes time which is in minutes and y-axis denotes data rate which is in bits/seconds. According to this graph the peak value of throughput is almost 510,000 bits/sec and after this it gradually decreases and reaches to almost 100,000 bits/sec at time 3 minutes.

6.3.2 When Nodes=15, DSR Performance

This figure was taken when the numbers of nodes were 15 and the protocol was Dynamic Source Routing (DSR) in MANETs. This below figure is also showing the delay, network load and throughput of DSR protocol. The upper small figure is showing delay, in which x-axis denotes time which is in minutes and the y-axis also denotes time which is in seconds. The middle figure is for network load in which x-axis denotes time which is in minutes and the y-axis denotes data rate which is in bits/seconds. The third figure is for throughput in which x-axis denotes time which is in minutes and the y-axis denotes data rate which is in bits/sec. The peak value of delay in DSR is approx 0.030 seconds and after 3 minutes it reaches to almost 0.010 seconds. The peak value of network load in DSR is almost attaining a value of 400,000 bits/sec and then gradually decreases and reaches to approx 50,000 bits/sec at 3 minutes time. The behavior of throughput in DSR protocol is showing that after 3 minutes the value of throughput is approximately equal to 50,000 bits/sec when the numbers of nodes are 15.
6.3.3 When Nodes=15, OLSR Performance

Like above two criteria the figure for OLSR is also collected and saved when there are 15 mobile nodes in a scenario. The x-axis denotes time in minutes and y-axis denotes time in seconds for the upper window in this below figure. While the second middle figure has x-axis in minutes and y-axis in bits/sec because y-axis shows data rate. In the third small window the x-axis denotes time in minutes and y-axis denotes data rate in bits/sec. The average delay of OLSR after 3 minutes is approximately 0.0009 seconds which is very low as compared to first two routing protocols. OLSR is giving less delay as compared to previous two routing protocols. The network load in OLSR is approximately 50,000 bits/sec after 3 minutes and its peak value 450,000 bits/sec. The peak value of throughput of OLSR in 15 nodes scenario is almost equal to 580,000 bits/sec.
6.4 Increasing the nodes

As we have created three scenarios and run all the protocols in all the scenarios. Previous three figures contain graphs of individual protocol corresponding to all the parameters when there were 15 mobile nodes in a workspace. Similarly we will have a look on individual protocols corresponding to all parameters when there were 30 and 60 nodes in a workspace window of OPNET Modeler 14.5.

6.4.1 When Nodes=30, AODV Performance

When we have increased the number of nodes from 15 to 30, the protocols are checked individually on all parameters. First of all we have chosen AODV to see its performance on delay, throughput and network load. On increasing the number of nodes it made a slight difference on the graph of AODV delay, the delay’s peak value is starting from almost 0.048 seconds and reaches to almost 0.001 seconds after 3 minutes time. Similarly the load on network is also showing a different behavior than the one that was in 15 nodes. The peak value of network load is 790,000 bits/sec. Throughput of DSR in this scenario has also increased as the number of nodes was also increased. ADOV protocol gives throughput almost equal to 250,000 bits/sec when number of nodes is 30. This is shown in figure below.

Figure 6.9 Showing Graphs of all parameters when nodes=30 (AODV)

6.4.2 When Nodes=30, DSR Performance

When we have number of mobile nodes equal to 30, we checked the behavior of DSR protocol when run on MANETs. The design of this figure is also the same like the previous figures. If we have a deep look on this figure we can observe easily that while increasing the numbers of nodes, definitely the delay of all protocols increase but their delays vary in numeric values. Like in this figure the delay in 30 nodes scenario is almost equal to 0.02 sec exactly after 3 minutes. And if we see the delay in 15 nodes scenario it was 0.010 sec. Because number of nodes is increased the delay has also increased because when data has to pass more nodes while reaching to its destination node, definitely the delay will be introduced in it. And in the middle figure the network load is also increased and reaches up to 125,000 bits/sec in 3 minutes, but in 15 nodes scenario under DSR it was almost 50,000 bits/sec in 3
minutes. Similarly the throughput has also increased to 125,000 bits/sec in 3 minutes. But in 15 nodes it was 50,000 bits/sec. The figure is as below.

![Figure 6.10 Showing Graphs of all Parameters when nodes=30 (DSR)](image)

**6.4.3 When Nodes=30, OLSR Performance**

The figure of 30 nodes scenario with OLSR protocol is also showing that on increasing the number of nodes the delay generating by OLSR is also increasing but when we compared the delay of this figure with 15 nodes OLSR it is observable that the delay has the same value equal to 0.009 seconds after 3 minutes and the graph of delay also looks like same as in 15 nodes scenario. The peak value of network load in this scenario for OLSR protocol is approx 750,000 bits/sec and after 3 minutes the value is 150,000 bits/sec. Similarly we can measure and observe the value of throughput and can see the changing behavior of this graph.

![Figure 6.11 Showing Graphs of all Parameters with nodes=30 (OLSR)](image)
6.4.4 When Nodes=60, AODV Performance

If we have a very deep look on this scenario we can observe very easily that the delay in numeric values is almost equal to the one that was in 30 nodes scenario. Only the graph is changed in a sense from the previous one that is fluctuating a bit from the very beginning. But when we see network load in this scenario, the network load peak value is very low then the peak value in 30 nodes scenario. It means that it is showing a bit better result in terms of network load. Similarly we can find the difference of behavior between two scenarios in terms of throughput.

![Figure 6.12 Showing Graphs of all Parameters with nodes=60 (AODV)](image)

6.4.5 When Nodes=60, DSR Performance

The figure is clearly showing the change of behavior of graphs in terms of delay, network load and throughput.

![Figure 6.13 Showing Graphs of all Parameters with nodes=60 (DSR)](image)
6.4.6 When Nodes=60, OLSR Performance

All the graphs clearly are clearly showing the change in behaviors regarding the previous figures. In this scenario the peak value of delay is approx 0.0072 seconds. The peak value of network load is 1,010,000 bits/sec. And the peak value of throughput is 5,000,000 bits/sec.

![Graph](image)

*Figure 6.14 Showing Graphs of all Parameters with nodes=60 (OLSR)*

6.5 All Parameters-All Scenarios

Now we will show our results from a different angle, we saved these figures by marking tick on all parameters, all scenarios and on single routing protocol one by one in a Result Browser window of our simulation. We have saved the screen shots in this manner also for the sake of better understanding and comparison. The figures will clearly indicate the difference between the behaviors of routing protocols when run in three different scenarios.

6.5.1 AODV Performance

This figure was taken when we selected AODV as a protocol, all parameters and AODV in all three scenarios in a result browser. The different colors show the different graphs for different parameters in three different scenarios altogether. This is another angle of our results. From this figure it can be seen that the network load and throughput for AODV in 60 nodes scenario is greater than the previous two scenarios while delay is showing a constant behavior in all scenarios.
6.5.2 DSR Performance

From this figure we can say that network load and throughput in 60 nodes scenario is greater as compared to 15 and 30 nodes scenario. While delay, in all the scenarios is showing a constant behavior.

6.5.3 OLSR Performance

This figure is also showing the same thing that has been discussed in previous two articles. Network load and throughput of 60 node scenarios is greater than 30 and 15 node scenarios.
6.6 Performance Comparison

These figures are specially taken for the sake of comparison and for making the statistical calculation more easy and precise. However these figures are another view of our simulation results. These figures include all protocols in one scenario and for one parameter. The figures for all three nodes scenario with all protocols for delay, network load and throughput separately are as under.

6.6.1 All Protocols, 15 Nodes

These figures are showing delay, network load and throughput respectively in 15 nodes scenario with all three routing protocols AOD, DSR and OLSR. The color scheme above the graphs are clearly showing, which graph belongs to which protocol.
6.6.2 All Protocols, 30 Nodes

Figure 6.19 Showing Delay, Network load and Throughput (30 nodes)

6.6.3 All Protocols, 60 Nodes

Figure 6.20 Showing Delay, Network Load and Throughput (60 nodes)
6.7 Final Comparison and Statistical Information

According to figure 6.18, which is showing the behavior of routing protocols in 15 nodes scenario, it is concluded that OLSR outperforms the other two routing protocols in terms of delay and throughput while in network load it looks like that OLSR is attaining greater numeric value as compared to AODV and DSR. For network load, it looks like DSR is showing better result than other two routing protocols, as it is putting low load on a network. However this will be confirmed from the statistical information/calculation which is shown in table 6.1. From these graphs we can also observe that OLSR, in terms of delay and throughput has outstanding good results.

According to figure 6.19, which is showing the behavior of routing protocols in 30 nodes scenario, it is again concluded that OLSR is outperforming the other two routing protocols in terms of delay and throughput, but it seems from the graph that it might be possible that again OLSR is putting greater load on network as compared to other two routing protocols. However statistical information will tell this thing in a more accurate way.

Similarly when we see figure 6.20, which is showing behavior of routing protocols in 60 nodes scenario, it can be said that OLSR is outperforming the other two routing protocols in terms of all parameters i.e. delay, network load and throughput. Because this time OLSR graph for network load graph is under the graphs of AODV and DSR which means that OLSR has a better result in terms of network load also. However this can be confirmed from the statistical table 6.1 below. Similarly if we only compare AODV and DSR, keeping in mind the figures (6.18→6.20), we can say that AODV is better than DSR in terms of delay, network load and throughput. There is only one scenario i.e. 15 nodes where AODV is showing large network load than DSR.

So from the graphical study it is observed that we can easily say that if we need better performance in MANETs or in WMNs among these three routing protocols, OLSR is best to use. Moreover the behavior of the figures (6.18→6.20) is also collected in the form of statistics so that one can better understand why OLSR is recommended to use from among these three routing protocols. This statistical information is calculated in the mean value and is shown in the form of table as below.

<table>
<thead>
<tr>
<th>Nodes</th>
<th>Parameters</th>
<th>AODV</th>
<th>DSR</th>
<th>OLSR</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Delay (sec)</td>
<td>0.001625</td>
<td>0.0105</td>
<td>0.001</td>
</tr>
<tr>
<td></td>
<td>Network Load (bits/sec)</td>
<td>63750</td>
<td>56500</td>
<td>66250</td>
</tr>
<tr>
<td></td>
<td>Throughput (bits/sec)</td>
<td>93500</td>
<td>57750</td>
<td>166250</td>
</tr>
<tr>
<td>30</td>
<td>Delay (sec)</td>
<td>0.00225</td>
<td>0.01425</td>
<td>0.00075</td>
</tr>
<tr>
<td></td>
<td>Network Load (bits/Sec)</td>
<td>108500</td>
<td>133250</td>
<td>122250</td>
</tr>
<tr>
<td></td>
<td>Throughput (bits/sec)</td>
<td>252500</td>
<td>142500</td>
<td>715000</td>
</tr>
<tr>
<td></td>
<td>Delay (sec)</td>
<td>0.007</td>
<td>0.0575</td>
<td>0.00025</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-------</td>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Load (bits/sec)</td>
<td>285000</td>
<td>333000</td>
<td>282500</td>
</tr>
<tr>
<td></td>
<td>Throughput (bits/sec)</td>
<td>1077500</td>
<td>377500</td>
<td>4037500</td>
</tr>
</tbody>
</table>

*Table 6.1 Statistical Information (Mean Calculation)*
Conclusion

The analytical study of this thesis demonstrates that WMN technology proved to be a revolutionary and modern technology which has remarkable impacts in the field of Telecommunications and Internet Systems. Routing protocols play vital role to increase the credibility of WMNs. The selection of appropriate routing protocol with respect to network improves the efficiency and reliability of network. There are some suggestions regarding analytical study, routing protocols should not be centralized. These should be distributed in nature. Routing protocols used in ad-hoc networks should develop loop free routes; due to loop free environment bandwidth consumption becomes low. Routing protocols should have capability to maintain QoS in terms of different parameters such as delay, load, jitter and throughput etc. Mainly there are two categories of protocols used in WMNs or MANETs i.e. reactive and proactive. Both types of protocols have different utilization in MANETs; both categories have advantages and disadvantages discussed in this thesis. Thus to achieve good results and efficiency in communication according to scenarios and parameters, selection of suitable category of protocol is very important. The simulation study of this thesis reveals that, Optimized Link State Routing (OLSR) protocol works better than Ad-hoc on-demand Vector (AODV) and Dynamic Source Routing (DSR) protocols regarding end to end delay and throughput in all three scenarios (15, 30 and 60 nodes), while regarding network load it was observed that OLSR had better result in 60 nodes scenario only, in 15 and 30 nodes scenario OLSR network load was high which can be seen from table 6.1. For network load, there is no consistent performance shown by any of the three routing protocols. When there are 15 mobile nodes in a network, DSR is performing well regarding network load, when there are 30 mobile nodes in a network, AODV is outperforming the other two routing protocols regarding network load and when there are 60 nodes scenario OLSR is outperforming regarding network load. Two out of three routing protocols are reactive (AODV and DSR) while OLSR is proactive protocol. The traffic we used in our simulation was FTP. Traffic is distributed to all nodes in each scenario in equal amount. From our simulation we can conclude that DSR is a very slow routing protocol as it has taken lot of time while simulating each scenario (15, 30 and 60), OLSR does not take so much time. The feature of OLSR pace is its less delay due to its pre determined route quality, it can process data from node to node without taking much time. On the other hand DSR has large delay, which means it takes so much time in processing the data from one node to another. Throughput is the rate at which data is processed from node to node which has a great importance in any network, so that routing protocol is always needed which gives best throughput and in our simulation OLSR is providing best throughput. Moreover it cannot be said that DSR should not be used because every routing protocol has its own attributes on which it performs well. Some routing protocols perform well in larger network while some perform well in smaller network. But in our situation, OLSR has an edge on two parameters out of three. Finally we conclude that OLSR gives better results in terms of delay and throughput due to its proactive behavior. OLSR has the quality to reduce size of information that is why it gives less delay, controls flood within a network therefore throughput is better than other protocols. So we can easily recommend that in these kinds of networks and parameters that we have created in this thesis, OLSR is a good option to use as compared to AODV and DSR.

Future Work

As wireless mesh network technology is new emerging technology which has great applications in the new arena of Telecommunication, Internet Systems, and Internet mobility. Routing protocols has the great impact on wireless mesh networks and mobile ad-hoc networks as discussed in thesis report. Appropriate choosing of protocols according to network increases the credibility and scalability of network. To overcome congestion, traffic load and other restrictions in the network, synchronization
of protocols with the network is still challenge for researchers. We propose to overcome the drawbacks of proactive routing protocols as well as reactive routing protocols, such as in proactive routing, broadcast of information utilizes more bandwidth and energy in the form of control packets. On the other hand, in reactive routing latency should be overcome which is increased due to route discovery. There are also some other challenges in the form of increase in mobility rate. These kinds of researches should be performed in future to develop reliable and scalable communication in WMNs. Also further simulations and analytical study of protocols with respect to networks should be proceeding for future work.
Appendix – Simulation Steps

There are the simulation steps for our simulation. What we have done in our simulation is written in precise steps. One following these steps one can perform our simulation very easily, the only important thing that he/she should have familiarization with OPNET Modeler 14.5. In this simulation three routing protocols AODV, DSR and OLSR are investigated in WMNs/MANETs by making three scenarios i.e. when there are 15, 30 and 60 nodes in a workspace window of OPNET Modeler 14.5. All the procedure is explained in steps which are as follows.

**AODV in 15 nodes**

1) Choose Campus as network of size 1000 x 1000 meters.
2) Select MANET and click YES
3) In the workspace window, drag wlan_wkstn mobile node according to your need i.e. in first scenario we will drag 15 mobile nodes because we are creating 15 nodes scenario, then in second and third scenario we will choose 30 and 60 nodes respectively.
4) Drag wlan_server fixed node in a workspace window.
5) Click Edit Select all in subnet.
6) Protocols → IP → Addressing → Auto Assign IPv4 addresses
7) When all nodes are already selected, right click and edit attributes.
8) Choose appropriate protocol, say AODV for first time.
9) Tick Apply to selected objects and click OK.
10) Save the project.
11) Drag application_config from the object palette into the workspace window, set its name and then edit attributes.
12) Under application definitions, set number of rows equal to 1.
13) Enter application name as FTP.
14) Under description menu, choose FTP and apply high-load to it.
15) Tick Apply to selected objects and click OK.
16) Drag profile_config into workspace window, set its name and then edit attributes.
17) Under profile configuration menu, set number of rows equal to 1.
18) Under Enter profile name menu, set its name.
19) Under applications, set number of rows equal to 1.
20) Under application name, set its name to FTP.
21) Set Start time offset to constant=0.
22) Duration= End of profile.
23) Under repeatability option, set inter-repetition time (seconds) to uniform= (0,100).
24) Number of repetitions= Unlimited.
25) Start time (seconds) to constant= 0.
26) Duration= End of simulation.
27) Under repeatability option, set inter-repetition time (seconds) to constant = 300.
28) Set number of repetitions to constant =0.
29) Click Apply to selected objects and click OK.
30) Save the project.
31) Protocols → Applications → Deploy Defined.
32) Transfer all mobile nodes under the category of source on right hand side (RHS). And transfer server node under the category of “FTP-SERVER” on RHS.
33) Tick Apply and click Ok.
34) Drag mobility_config from object palette to workspace window set its name and edit attributes.
35) Under random mobility profile, set number of rows equal to 1.
36) Under default random waypoint and then under random waypoint parameters, set speed (meters/seconds) to constant = 10.
37) Set pause time to constant = 200.
38) Set start time (seconds) to constant = 0.
39) Leave all other options as default.
40) Tick Apply and click OK.
41) Save the project.
42) Topology → Random Mobility → Set Mobility Profile.
43) Right click in workspace window and choose individual statistics.
44) A window will appear, under global statistics, choose appropriate protocol, traffic pattern and Wireless Lan.
45) Click OK and Save the project.

**DSR in 15 nodes**

1) Scenario → Duplicate Scenario
2) Select all mobile nodes and one fixed server node, right click and edit attributes.
3) Under ad-hoc routing protocols choose DSR protocol this time.
4) Save the project.
5) Right click and choose individual statistics.
6) Under global statistics, choose DSR, traffic pattern and Wireless LAN.
7) Click OK and save the project.

**OLSR in 15 nodes**

1) Scenario → Duplicate Scenario.
2) Select all mobile nodes and one fixed server node, right click and edit attributes.
3) Under ad-hoc routing protocols choose OLSR this time.
4) Save the project.
5) Right click and choose individual statistics.
6) Under global statistics, choose OLSR, traffic pattern and Wireless LAN.
7) Click OK and save the project.

**AODV in 30 nodes**

1) Scenario → New Scenario.
2) Drag 30 mobile nodes in workspace window from the object palette this time and one fixed server node.
3) Repeat steps from 5 → 45.

**DSR in 30 nodes**

1) Scenario → Duplicate Scenario.
2) Select all mobile nodes and one fixed server node, right click and edit attributes.
3) Under ad-hoc routing protocols choose DSR this time.
4) Save the project.
5) Right click and choose individual statistics.
6) Under global statistics, choose DSR, traffic pattern and Wireless LAN.
7) Click OK and save the project.

**OLSR in 30 nodes**
1) Scenario → Duplicate Scenario.
2) Select all mobile nodes and one fixed server node, right click and edit attributes.
3) Under ad-hoc routing protocols, choose OLSR this time.
4) Save the project.
5) Under global statistics, choose OLSR, traffic pattern and Wireless LAN.
6) Click OK and save the project.

**AODV in 60 nodes**
1) Scenario → New Scenario
2) Drag 60 mobile nodes and one fixed server node from object palette into workspace window.
3) Repeat steps from 5 → 45.

**DSR in 60 nodes**
1) Scenario → Duplicate Scenario
2) Select all mobile nodes and one fixed server node, right click and edit attributes.
3) Under ad-hoc routing protocols, choose DSR this time.
4) Save the project.
5) Right click on workspace window and choose individual statistics.
6) Under global statistics, choose DSR, traffic pattern and Wireless LAN.
7) Click OK and save the project.

**OLSR in 60 nodes**
1) Scenario → Duplicate Scenario.
2) Select all mobile nodes and one fixed server node, right click and edit attributes.
3) Under ad-hoc routing protocols, choose OLSR this time.
4) Save the project.
5) Right click on workspace window and choose individual statistics.
6) Under global statistics, choose OLSR, traffic pattern and Wireless LAN.
7) Click OK and save the project.

**Managing the Scenarios**
1) Scenarios → Manage Scenarios
2) Click collect under the category of all the scenarios.
3) Enter the sim duration of your own choice.
4) Click OK to run the simulations.
Viewing of Results

1) DES → Results → Compare Results
2) Select the scenario of your own choice.
3) Select the statistics under global statistics option and view the results on RHS.
References


[19] Mihail L.Sichitiu, “Wireless Mesh Networks Challenges and Opportunities”, Electrical and Computer Engineering Department, NC State University, Raleigh, NC, USA.


[33] http://www.bgp4.as/
[38] Paper slides Telesystem Chapter10 “Protocols for QoS Support” Article 10.1 RSVP.
[40] Chapter 50 Simple Multicast Routing Protocol “Internetworking Technologies handbook”
[48] http://www.usg.edu/galileo/skills/unit01/infoage01_03.phtml
[49] Trisha Greenhalg, Rod Taylor, “How to read a paper: Papers that go beyond numbers (qualitative research)” university college London medical school, September 20


[55] www.opnet.com/

[56] Yi Pan, “Introduction to OPNET simulator”.
