

STATUS OF THESIS

Title of thesis

**SNR-Based OLSR Routing Protocol for Wireless Mesh
Networks**

I MOHAMED ELSHAIKH ELOBAID

hereby allow my thesis to be placed at the Information Resource Center (IRC) of Universiti Teknologi PETRONAS (UTP) with the following conditions:

1. The thesis becomes the property of UTP.
2. The IRC of UTP may make copies of the thesis for academic purposes only.
3. This thesis is classified as
 Confidential
 Non-confidential

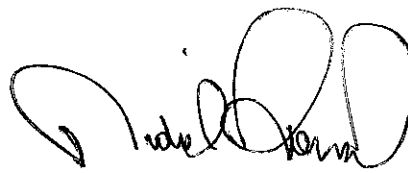
If this thesis is confidential, please state the reason:

The contents of the thesis will remain confidential for _____ years.

Remarks on disclosure:

Endorsed by


MOHAMED EL SHAIKH ELOBAID


Dr. NIDAL KAMEL

Universiti Teknologi PETRONAS
Bandar Seri Iskandar, Tronoh, 31750
Perak, Malaysia

Date: 17.03.09

Date: 17.03.09

The contents of the thesis will remain confidential for _____ years.

UNIVERSITI TEKNOLOGI PETRONAS

Approval by Supervisor

The undersigned certify that they have read, and recommend to The Postgraduate
Studies Programme for acceptance, a thesis entitled

“SNR-Based OLSR Routing Protocol for Wireless Mesh Networks”

submitted by

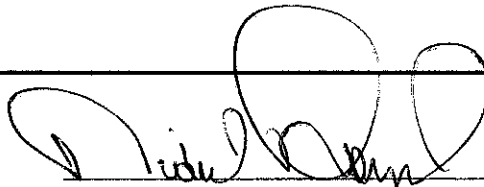
Mohamed Elshaikh Elobaid

for the fulfilment of the requirements for the degree of
Masters of Science in Electrical and Electronics Engineering

Date

Signature

:



Main Supervisor

:

Dr. Nidal Kamel

Date

:

17.03.09

Co-Supervisor

:

UNIVERSITI TEKNOLOGI PETRONAS

SNR-Based OLSR Routing Protocol for Wireless Mesh Networks

By

Mohamed Elshaikh Elobaid

A THESIS

SUBMITTED TO THE POSTGRADUATE STUDIES PROGRAMME

AS A REQUIREMENT FOR THE

DEGREE OF MASTERS OF SCIENCE IN ELECTRICAL AND ELECTRONICS

ENGINEERING

Electrical and Electronics Engineering

BANDAR SERI ISKANDAR,

PERAK

March, 2009

DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTP or other institutions.

Signature:  _____

Name : Mohamed Elshaikh Elobaid

Date : 17.03.09 _____

ACKNOWLEDGEMENT

I would like to thank *Dr.Nidal Kamel* for his supervision, advice and guidance throughout my graduate study. *Dr. Nidal Kamel* demanded the very best and pushed me to achieve it. This thesis in large owes to the concrete direction *Dr.Nidal Kamel* provided during my research work.

Thanks also go to my friends and colleagues for their emotional support during these years.

I would like to express my special gratitude to my parents for their unconditional support and particularly for the possibility to obtain this excellent education.

Finally, I would love to dedicate this work to my beloved wife "*ILA*".

Abstract

Wireless Mesh Networks (WMNs) consist of a collection of mobile and fixed nodes that form a network. Nodes are capable of communicating with each other either with infrastructure, or infrastructureless, or in a hybrid mode. The major advantages of WMNs over the other wireless networks are the low-cost, self organization, self configuration, last mile internet solution, scalability, and reliability. These advantages have attracted the researcher over the last five years. WMNs technology is gaining an increased attention from the Institute of Electrical and Electronics Engineers (IEEE) community. This led the IEEE organization to emerge a special working group (IEEE 802.11s) in charge of the issues deriving from a completely wireless distribution system used to interconnect different Basic Service Sets (BSSs) through secure and performing links.

In a multi-hop networks, like WMN, one of the main factors that influences the performance is the routing protocol. Generally speaking, routing protocols can be classified based-on the routing metric to 1) hop count-based routing protocols, like Ad-hoc on demand distance vector (AODV) where the optimum path is defined as the path that goes through the minimum number of nodes, 2) the link quality-based routing protocols, like OLSR where some metrics such as the bandwidth and the packet error rate are considered to define the optimum path to the destination.

In this work the performances of a three commonly used routing protocols are compared. The main goal of this stag is to study the influence of different routing protocols in WMNs. The comparison is conducted with two scenarios of networks; a high mobility

network and a low mobility network. (Open network) OPNET 11.5 modeler is used to build the WMNs. The performance of the network and the routing protocols has been studied in means of network throughput, End-to-End delay, routing protocol overhead and the mobility. The obtained results show that the Optimized link state routing protocol (OLSR) has the highest throughput over DSR and AODV routing protocols in WMNs.

The unpredictable behavior of the wireless medium in WMNs environment demands the need for a routing protocol that is aware of the link conditions. Unfortunately the routing protocols used such as AODV and Dynamic source routing (DSR) are hop count-based; where the routing algorithm uses the number of nodes to determine the optimum path to the destination.

In the second stage of this work a new routing technique for WMNs based-on Signal to noise ratio (SNR) as a new metric for OLSR routing protocol, is developed. The new metric has been implemented on the OLSR routing protocol module using OPNET simulator. The modified OLSR routing protocol is implemented in the comparison scenarios. The obtained results show that, when SNR is used as a routing metric in the OLSR routing protocol, the OLSR is getting the significantly higher network throughput over the DSR and AODV routing protocols. In the same time, the modified OLSR implemented with the SNR metric is showing a high improvement over the OLSR with the traditional hop-count metric. This thesis also studies the affect of different amounts of mobility in WMNs performance.

Abstrak

Rangkaian jejaring wayerless (WMNs) terdiri daripada satu pengumpulan nod-nod tetap dan bergerak yang membentuk rangkaian. Nod-nod mampu berhubung antara satu sama lain, sama ada dengan kemudahan atau tanpa kemudahan, atau dalam mod ragam. Ciri-ciri yang menjadikan WMN lebih menyerlah berbanding rangkaian-rangkaian tanpa wayar yang lain adalah: kosnya yang rendah, kemampuan beroperasi dan membentuk rangkaian sendiri, boleh menyelesaikan masalah 'last mile' pada Internet, keupayaan beroperasi di dalam populasi yang besar dan mampu beroperasi dengan baik pada kadar kegagalan yang minimum. Kelebihan-kelebihan ini telah menjadikan ia tumpuan dalam bidang penyelidikan semenjak 5 tahun kebelakangan ini. WMN boleh dijadikan sebagai tunjang utama kepada teknologi tanpa wayar berkapasiti tinggi seperti MANET. Selain daripada itu, WMN mudah untuk diselenggarakan dan mampu beroperasi sendiri serta sesuai diaplikasikan dengan pelbagai teknologi tanpa wayar (WiFi, WiMAX...dsb). Dewasa ini, WMNs semakin mendapat perhatian dari pihak persatuan IEEE. Berikutan itu, pihak pengurusan IEEE telah menubuhkan sebuah kumpulan kerja utama (IEEE 802.11s) yang menjaga isu-isu berkaitan daripada sistem pengagihan lengkap tanpa wayar untuk saling berhubung dengan Set Servis Asas (BSSs) yang pelbagai melalui pautan yang selamat dan berkesan. Dari segi pandangan sturukturnya, WMN ialah sekumpulan nod-nod wayerless yang menggunakan susunan jejaring. Nod-nod dalam WMN terdiri daripada penghala WMN (penghala jejaring) dan pelanggan wayerless. Penghala jejaring saling berhubung dengan wayerless membentuk tulang belakang rangkaian. WMN berkomunikasi dengan internet melalui satu get laluan atau lebih. Nod-

nod dalam WMN disusun dalam tiga senario; infrastruktur, tanpa infrastruktur dan rangkaian hybrid. Nod-nod WMNs menggunakan fasion hop berbilang untuk memindah data antara nod-nod; dalam teknik tersebut, bingkisan bergerak dari satu nod ke nod yang lain hingga ianya sampai destinasi terakhir. Teknik ini bergantung kepada protokol penghalaan untuk menentukan laluan dari punca ke destinasi. Dalam rangkaian berbilang hop, sebagai contoh WMN, salah satu faktor utama yang mempengaruhi prestasinya adalah protokol penghalaan. Secara umumnya, protokol penghalaan dibahagikan kepada dua kumpulan utama 1) protokol penghalaan reaktif, di mana halaan ke destinasi dibuat atas permintaan, 2) protokol penghalaan proaktif, dimana pertukaran jadual penghalaan nod-nod secara berkala dan pemeliharaan seluruh topologi terhadap rangkaian, dengan setiap nod mengetahui laluan terdekat ke setiap nod dalam rangkaian. Selain daripada itu, protokol penghalaan boleh diklasifikasi berdasarkan metrik penghalaan 1) protokol penghalaan hop berasaskan bilang, contohnya AODV dimana laluan optima didefinasikan sebagai laluan yang merentasi bilangan nod-nod yang minima, 2) protokol penghalaan pautan berasaskan kualiti, contohnya OLSR, di mana sesetengah metrik seperti lebar jalur dan kadar kesalahan bingkisan diambilkira untuk menentukan laluan optima ke destinasi. Dalam fasa pertama prestasi ini, di antara tiga yang biasanya digunakan, protokol-protokol penghalaan adalah dijadikan perbandingan. Matlamat utama pada fasa ini adalah untuk mengkaji perbezaan pengaruh protokol penghalaan dalam WMNs. Perbandingan ini dilakukan dalam dua rangkaian senario; rangkaian tinggi kebolehergerakan dan rangkaian rendah kebolehergerakan. Perisian OPNET 11.5 digunakan untuk membangunkan WMNs. Prestasi rangkaian dan protokol penghalaan telah dikaji berdasarkan rangkaian truput ,lengah hujung ke hujung, overhed protokol

penghalaan dan kebolehergerakan. Keputusan yang terhasil daripada fasa perbandingan dalam WMNs menunjukkan bahawa protokol penghalaan OLSR mempunyai truput tertinggi berbanding protokol penghalaan DSR dan AODV. Sifat luar jangkaan terhadap perantaraan wayerless dalam keperluan permintaan persekitaran WMNs untuk protokol penghalaan adalah prihatin dengan keadaan pautan. Malangnya, protokol penghalaan yang digunakan seperti AODV dan DSR adalah hop berasaskan bilang; dimana algoritma penghalaan menggunakan sebilangan nod-nod untuk menentukan laluan optima ke destinasi. Pada fasa kedua kajian ini, satu teknik penghalaan baru untuk WMNs yang berasaskan SNR sebagai metrik baru untuk protokol penghalaan OLSR dibangunkan. Metrik baru ini telah dilaksanakan pada modul protokol penghalaan OLSR dengan menggunakan penyelaku OLSR. Protokol penghalaan OLSR yang telah diubah dilaksanakan dalam senario perbandingan. Keputusan yang terhasil menunjukkan, apabila SNR digunakan sebagai metrik penghalaan dalam protokol penghalaan OLSR, OLSR mencapai ketinggian truput rangkaian yang bererti berbanding protokol penghalaan DSR dan AODV. Pada masa yang sama, OLSR yang telah diubah dan dilaksanakan dengan metrik SNR menunjukkan kemajuan 200% berbanding dengan tradisional metrik bilangan hop OLSR. Tesis ini juga turut mengkaji prestasi WMNs terhadap kesan pengaruh kebolehergerakan dalam kadar yang pelbagai.

TABLE OF CONTENTS

STATUS OF THESIS.....	I
DECLARATION.....	V
ACKNOWLEDGEMENT.....	VI
ABSTRACT.....	VII
ABSTRAK.....	IX
TABLE OF CONTENTS	XII
TABLE OF FIGURES.....	XV
1.CHAPTER ONE: INTRODUCTION.....	1
1.1 INTRODUCTION	1
1.2 PROBLEM STATEMENT	2
1.3 OBJECTIVES	4
1.4 METHODOLOGY	5
1.5 THESIS ORGANIZATION	6
2.CHAPTER TWO: BACKGROUND AND LITRATURE REVIEW	7
2.1 INTRODUCTION	7
2.2 WIRELESS NETWORKS.....	7
2.3 802.11 WLAN	9
2.3.1 <i>Infrastructure network</i>	10
2.3.2 <i>Infrastructureless network</i>	10
2.3.1 <i>Hybrid networks</i>	11
2.3.2 <i>802.11 Physical Layer</i>	12
2.3.3 <i>802.11 MAC Layer</i>	13
2.3.4 <i>Basic access method DCF</i>	13

2.3.6 802.11 MAC Frame Types	14
2.4 WIRELESS MESH NETWORKS	15
2.4.1 WMNs Definition and Benefit.....	16
2.4.2 WMN critical design factors.....	19
2.5 WMN ROUTING PROTOCOLS	20
2.5.1 OLSR Routing Protocol.....	21
2.5.2 DSR Routing Protocol	24
2.5.3 AODV Routing Protocol	25
2.6 RELATED WORKS.....	28
2.6.1 Hop count	28
2.6.2 Per hop Round Trip Time (RTT).....	29
2.6.3 Per Hop Packet pair Delay (PktPair)	29
2.6.4 Expected Transmission Count (ETX).....	30
2.7 SUMMARY	31
3.CHAPTER SNR-BASED OLSR	32
3.1 INTRODUCTION.....	32
3.2 OLSR (OPNET MODULE)	32
3.2.1 OLSR Packets.....	33
3.2.2 OLSR configuration on the OPNET	34
3.2.3 OLSR Routing Metric on the OPNET Model.....	35
3.3 MPR TECHNIQUE	36
3.4 SNR	37
3.5 SUMMARY	39
4.CHAPTER FOUR: SYSTEM DESIGN.....	40
4.1 INTRODUCTION.....	40
4.2 NETWORK MODELING USING OPNET	40
4.3 ROUTING PROTOCOLS DESIGN CONCEPTS.....	42

4.4 WMN SIMULATION DESIGN.....	43
4.4.1 The network level	44
4.4.2 The Node Level	45
4.4.3 The Process Level.....	50
4.4.4 Ad-Hoc Routing Protocols Configuration on the OPNET.....	52
4.5 SUMMARY	53
5.CHAPTER FIVE: RESULTS AND DISCUSSION.....	54
5.1 INTRODUCTION.....	54
5.2 PROTOCOL OVERHEAD.....	55
5.3 MOBILITY SCENARIOS	58
5.4 THROUGHPUT	59
5.5 END-TO-END DELAY	62
5.6 COMPARISON.....	65
5.7 SNR-BASED OLSR ROUTING PROTOCOL	66
5.7.1 SNR-based OLSR Throughput	66
5.7.2 SNR-based OLSR End-to-End Delay	68
5.7.3 Mobility scenario comparison	70
5.8 NODES SCENARIO	73
5.9 SUMMARY	76
6.CHAPTER SIX: CONCLUSION AND FUTURE WORK.....	77
REFERENCES.....	79
APPENDIXES.....	82
APPENDIX 1: THE SNR-BASED OLSR PROTOCOL CODE	82
APPENDIX 2: THE SNR-BASED OLSR PROTOCOL BLOCK DIAGRAM	95

Table of Figures

Figure 1.1	Wireless Mesh Networks.....	1
Figure 2.1	The 802.11 Layer architecture	9
Figure 2.2	The Infrastructure Wireless Networks.....	10
Figure 2.3	Infrastructureless Wireless networks.....	11
Figure 2.4	CSMA/CA	14
Figure 2.5	802.11 MAC Layer frame fields	15
Figure 2.6	Infrastructure WMNs	16
Figure 2.7	Infrastructureless WMNs	17
Figure 2.8	Hybrid WMNs	17
Figure 2.9	Neighborhood sensing	22
Figure 2.10	Multipoint Relay (MPR)	23
Figure 2.11	Counting to infinity scenario.....	26
Figure 3.1	OLSR packet format.....	33
Figure 3.2	OLSR packet header file.	34
Figure 3.4	OLSR Parameters Configuration.....	35
Figure 3.5	OPNET Pipeline Stages	38
Figure 3.6	SNR module.	39
Figure 4.1	Neighbor discovery example.....	43
Figure 4.2	Node Model.....	46
Figure 4.3	Receiver Attributes.....	46
Figure 4.4	Transmitter attributes.....	47

Figure 4.5	wireless_lan_mac attributes.....	48
Figure 4.6	MANET-rte-mgr attributes.....	50
Figure 4.7	MANET routing layer architecture in OPNET.	51
Figure 4.8	Ad-Hoc routing Protocol Parameters.	52
Figure 4.9	AODV Protocol Parameters.	52
Figure 4.10	DSR Protocol Parameters.	53
Figure 5.1	Sub-Network (Overhead scenario).....	55
Figure 5.2	Traffic Generation Parameters.	56
Figure 5.3	AODV protocol overhead.....	56
Figure 5.4	DSR Protocol Overhead.	57
Figure 5.5	OLSR Protocol Overhead.....	57
Figure 5.6	Main scenario.	58
Figure 5.7	AODV throughput (Non-mobility scenario).....	60
Figure 5.8	DSR Throughput (Non-mobility scenario).....	60
Figure 5.9	OLSR Throughput (Non-mobility scenario).....	61
Figure 5.10	Throughput comparison (Mobility Scenario).....	62
Figure 5.11	AODV End-to-End Delay	63
Figure 5.12	DSR End-to-End delay.....	64
Figure 5.13	OLSR End-to-End delay.....	64
Figure 5.14	Throughput comparison between SNR and hop-count metrics.....	67
Figure 5.15	Comparison between hop-count and SNR OLSR Delay.....	68
Figure 5.16	Delay Comparison OLSR, DSR, and AODV.....	69
Figure 5.17	Delay Comparison	69

Figure 5.18 SNR vs. hop-count OLSR throughput)	70
Figure 5.19 SNR vs. hop-count OLSR delay.....	71
Figure 5.20 Three routing protocols vs. SNR OLSR throughput).....	72
Figure 5.21 Three routing protocols vs. SNR OLSR delay	73
Figure 5.22 In AODV, DSR, OLSR, and SNR-OLSR protocols Throughput	74
Figure 5.23 The 1000 nodes scenario	74
Figure 5.24 SNR-OLSR vs. OLSR throughput (1000nodes scenario)	75

CHAPTER ONE: INTRODUCTION

1.1 Introduction

Wireless Mesh Networks (WMNs) technology is getting recently more interest, and several companies are introducing it as a solution for the last-mile internet access. The analysts expect that the WMN's market will jump from \$33.5 million to \$974.3 million between 2004 and 2009. WMN can be deployed as high bandwidth wireless backbone. Like ad-hoc networks, WMN enjoys the advantage of easy deployment and self configuration with the compatibility to different wireless technologies [1].

WMN is a group of wireless nodes that employ a mesh arrangement. Nodes in WMN comprise of WMN routers (Mesh routers) and wireless clients. Mesh routers interconnect wirelessly creating the network backbone. WMN communicates with the internet through one or more gateways as shown in Figure 1.1. Nodes in WMN arranged in three scenarios; Infrastructure, Infrastructureless and hybrid network [2].

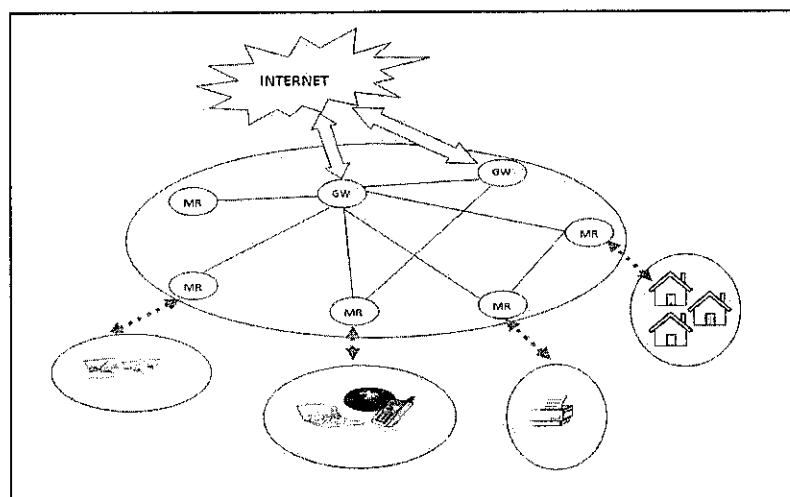


Figure 1.1: Wireless Mesh Networks.

WMN's nodes use a multi-hop fashion to transfer data between them; in such technique packet travels from one node to another until it reaches the last destination. This technique depends on the routing protocol to define the path from the source to the destination [1].

In this research we consider the problem of selecting optimum paths in networks made up of multiple wireless links, such as WMNs. By "optimum paths" we mean the paths that lead to a high aggregate network capacity. This problem is considerably harder in wireless networks than in traditional wired networks (where the routing problem is usually solved by running a distributed shortest-path algorithm on a graph) because the notion of a "link" between nodes is not well-defined. The properties of the radio channel between any pair of nodes vary with time, and radio communication range is often unpredictable. The communication quality of a radio channel depends on background noise, obstacles, and channel fading, as well as on other transmissions occurring simultaneously in the network [3].

1.2 Problem Statement

Routing protocols designed for ad hoc networks are not well suited WMNs; where the design of a routing protocol requires considering some characteristics of the network. Unfortunately most of the routing protocols for WMNs are mainly designed for ad hoc network. Protocols developed so far do not make use of the characteristic of WMNs [3]. For example, nodes' mobility in WMNs is quite less than node's mobility in ad hoc networks. Thus the need for a routing protocol that considers the stationary nature of nodes in WMNs cannot be found in a protocol designed for ad hoc network. Hop count is

the most common used routing metric for ad hoc networks. Due to the unpredictable behavior of wireless link and the stationary nature of WMNs, hop count is expected to give a poor performance and low throughput, because it selects paths with minimum number of hops. Those paths could contain lossy and poor performance link. Thus, using hop count metric in WMNs is leading to poor performance and low throughput. Moreover the unique combination of static nodes with the shared behavior of the medium in WMNs needs a special design of the routing protocol. Thus, one can find that, WMNs special characteristics is the main factor that involved in designing a routing protocol for WMNs [4].

Before developing a new metric for WMNs, one can find it essential to understand the influence of different types of routing protocols on WMNs, and which routing protocol would be more suitable for WMNs. Routing protocols broadcast different type of topology information and control messages in the networks. Control messages are used for updating information about the link quality and topological change of the network. The broadcasting of control messages might result in protocol overhead, which is might affect in poor bandwidth utilization. Moreover most of the routing metrics are calculated by generating additional protocol overhead on the network. Therefore, designing a routing metric for WMNs should take into account bandwidth utilization; by not adding additional overhead on the network, and wireless link quality for path selection. Doing that would give high network performance, such as high network throughput, and low end-to-end delay.

1.3 Objectives

Routing protocols developed for Ad-hoc networks are not necessary suitable for WMNs because the design of a protocol needs to take advantage of some WMN's characteristics. Protocols developed so far do not completely make use of the characteristics of WMNs, such as node mobility factor. Most of these protocols are using hop-count as a routing protocol metric. Due to the static nature of nodes and unpredictable behavior of wireless link, hop-count based routing protocols are expected to decrease the overall network throughput, and increase the End-to-end delay which results in a low performance network. Moreover, hop count-based protocols prefers path with less number of hop, and does not account to link condition. Thus, it may select a poor link, while better paths are available with additional hops. All this can cause a degrading in the network performance.

In this thesis a new metric (Signal-to-Noise ratio (SNR)) is proposed to tackle the problem of wireless link condition awareness, without adding additional protocol overhead to the network. The calculated SNR in the physical layer is brought to the routing layer by using a network layers interaction approach. The use of the new metric is contributed to the following:

- Improving the wireless mesh network throughput.
- Decreasing the End-to-End delay in WMNs.
- Studying the influence of different routing protocols in WMNs.
- Mobility variation factor is important issue to deploy a proper routing protocol for WMNs.

1.4 Methodology

This thesis aims at improving the performance of WMN by modifying an existing routing protocol. The work in this thesis is divided into two main stages. In the first stage the three commonly used routing protocols are studied and their performances are compared. The main goal of this stage is to study the influence of different routing protocols on WMNs. The comparison is conducted with two network scenarios; a high mobility network and a low mobility network. In the second stage of this work a new routing technique for WMNs based-on SNR as a new metric for Optimized link stat routing protocol (OLSR) is developed. The new metric has been implemented with the OLSR routing protocol module using Open Network (OPNET) simulator.

The objective of these simulations is to measure the performance of Ad-hoc on demand distance vector (AODV), Dynamic source routing (DSR), Optimized link stat routing protocol (OLSR), and signal to noise ratio OLSR (SNR-OLSR) with certain performance metrics [5]. The metrics used by this thesis are given below:

Network throughput: is the average of successful received data in the destination per second.

End-to-end delay: is the average time to transfer a data packet from a source node to a destination.

Protocol overhead: The total number of routing packets transmitted per data packet delivered at destination. Each transmission (hop-wise) of a routing packet was counted as one transmission.

Mobility: is considered as a design metric in this work, it has been used to measure the affect of different amounts of mobility in a network,

1.5 Thesis Organization

The rest of this thesis is organized as follow:

Chapter 2: this chapter gives a background on the wireless networking architecture and standards. The 802.11 physical and MAC layer are described in this chapter. This chapter also gives the main idea behind the wireless mesh networks and the studies four routing protocols those are used for this work. As this work means on deploying SNR as a routing metric, the end of this chapter is focusing on the routing metrics those had been proposed on similar researches.

Chapter 3: this chapter focuses on the implementation of the SNR on the OLSR protocol. The idea behind the OLSR module in the OPNET could be found in this chapter, as well as the SNR estimation technique. The OLSR setup and configuration on the OPNET are also described in this chapter.

Chapter 5: this chapter shows the design of the wireless network simulation. It addresses the design steps in this research work. The OPNET simulator and its modules are described in this chapter. This chapter also shows the simulation scenarios, and the network configuration used for this research work.

Chapter 6: shows and discusses the simulation results in this research work. This chapter is divided into three sections, the first one is showing the result from the comparison stage of this research work, while the other section is comparing between the new metric and the original metric. The last part of this chapter is focusing on the results from the mobility scenarios.

Chapter 7 concludes the thesis and discusses the future research directions.

CHAPTER TWO: BACKGROUND AND LITRATURE REVIEW

2.1 Introduction

Over the last two decades, wireless networks have become increasingly popular in the communication industry. The main reason for their popularity is their significant benefits over wired networks, especially due to the mobility allowed in wireless networks. The basics of wireless networking in addition to the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard, Mobile Ad-Hoc Networks (MANET), and WMNs are reviewed. This chapter is concluded with a description of some variants of WMNs proposed to meet some real-world application requirements.

2.2 Wireless Networks

In WLANs, the connection between the client and the user is accomplished by the use of a wireless medium such as Radio frequency (RF) or Infrared (IR) communications instead of a cable. This allows a remote user to stay connected to the network while mobile or not physically attached to the network. The wireless connection is usually accomplished by the user having a hand-held terminal or laptop that has an RF interface card installed inside the terminal or through the Personal computer (PC) card slot of the laptop. The range of a Wireless local area network (WLAN) depends on the actual usage and environment of the system. An important feature of WLANs is that they can be used independently of wired networks. They can be used as stand-alone networks anywhere to link multiple computers together without having to build or extend wired networks. The following are a few advantages of deploying WLANs [6]:

-
- Mobility improves productivity with real-time access to information, regardless of worker location, for faster and more efficient decision making
 - Cost-effective network setup for hard-to-wire locations such as older buildings and solid wall structures
 - Reduced cost of ownership, particularly in a dynamic environment requiring frequent modification due to minimal wiring and installation costs per device and per user.

However, there are several issues that should be considered in deploying the WLAN including [7]:

- *Frequency allocation:* Operation of a wireless network requires that all users operate in a common frequency band. The frequency band must be approved in each country.
- *Interference and reliability:* In a wired LAN, one hears only the terminals connected to the network. In a WLAN, interference is caused by simultaneous transmission of information in the shared frequency band and by multipath fading. The reliability of a communication channel is measured by bit error rate (BER). Automatic repeat request (ARQ) and forward error correction (FEC) techniques are used to increase reliability.
- *Security:* Radio waves are not confined to the boundary of buildings or campuses. There exists the possibility of eavesdropping and intentional interference. Data privacy over a radio medium is usually accomplished by using encryption.

- *Power consumption:* WLANs are typically related to mobile applications. In these applications, battery power is a scarce resource. Therefore, the devices must be designed to be energy efficient.
- *Mobility:* One of the advantages of a WLAN is the freedom of mobility. The devices should accommodate handoff at transmission boundaries to route data calls to mobile users.
- *Throughput:* To support multiple transmissions simultaneously, spread spectrum techniques are often used.

2.3 802.11 WLAN

In 1997 the IEEE developed an international standard for WLANs: IEEE 802.11-1997. This standard was revised in 1999. Like other IEEE 802 standards, the 802.11 standard focuses on the bottom two layers of the OSI model, the physical layer (PHY) and data link layer (DLL). The objective of the IEEE 802.11 standard is to define a medium access control (MAC) sublayer, MAC management protocols and services figure 2.1, and three PHYs for wireless connectivity of fixed, portable, and moving devices within a local area.

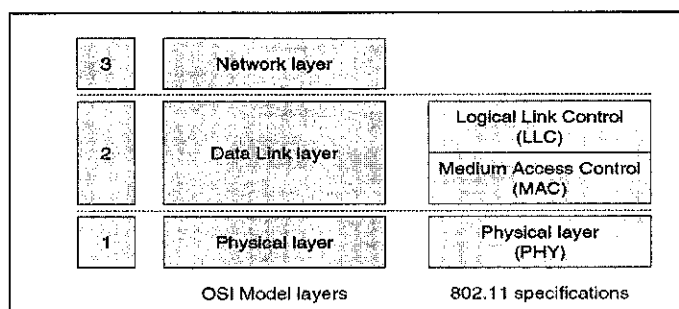


Figure 2.1: The 802.11 Layer architecture [5].

The architecture of the IEEE 802.11 WLAN is designed to support a network where most decision making is distributed to mobile stations. Three network architectures are defined in the IEEE 802.11 standard [8]:

2.3.1 Infrastructure network

An infrastructure network is the network architecture for providing communication between wireless clients and wired network resources. The transition of data from the wireless to wired medium occurs via an Access point (AP). An AP and its associated wireless clients define the coverage area. Together all the devices form a *basic service set*

Figure 2.3

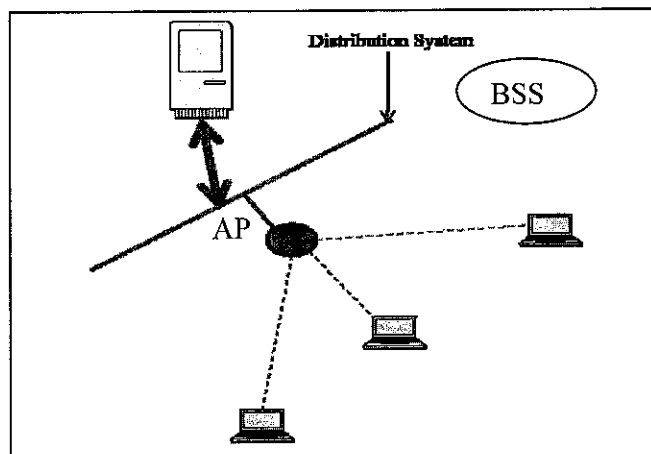


Figure 2.3: The Infrastructure Wireless Networks.

2.3.2 Infrastructureless network

An ad hoc network is the architecture that is used to support mutual communication between wireless clients. Typically, an ad hoc network is created spontaneously and does not support access to wired networks. An ad hoc network does not require an AP.

2.3.1 Hybrid networks

Hybrid network is a combination of infrastructure and infrastructureless modes. Like the infrastructureless networks nodes can work as routers and in the same time they can be a simple wireless workstation. Like the infrastructure network there are centre points to provide the gateway functionalities for the other nodes. Routers can form a wired backbone. It is simply gather the advantages of the two other types [6].

IEEE 802.11 supports three basic topologies for WLANs: the independent basic service set (IBSS), the basic service set, and the extended service set (ESS). The MAC layer supports implementations of IBSS, basic service set, and ESS configurations.

The IBSS configuration is referred to as an independent configuration or an ad hoc network. An IBSS configuration is equivalent to a peer-to-peer office network in which no single node is required to act as a server. IBSS WLANs include a number of nodes or wireless stations that communicate directly with one another on an ad hoc basis. In the other hand the basic service set configuration relies on an AP that acts as the logical server or a centre point. The third configuration is ESS. ESS configuration consists of multiple basic service set cells that can be linked by either wired or wireless backbones called a distributed system.

Figure 2.3 and Figure 2.4) sketch these three configuration modes.

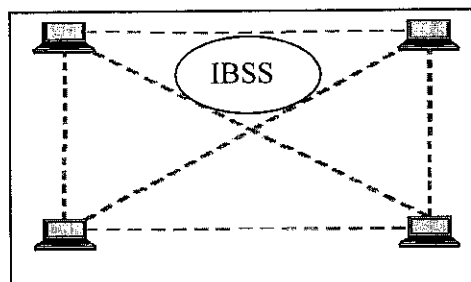


Figure 2.4: Infrastructureless Wireless networks.

2.3.2 802.11 Physical Layer

Physical layer is the first layer in the IEEE 802.11 standards. It provides three levels of functionality. These include: (1) frame exchange between the MAC and PHY under the control of the physical layer convergence procedure (PLCP) sublayer; (2) use of signal carrier and spread spectrum (SS) modulation to transmit data frames over the media under the control of the physical medium dependent (PMD) sublayer; and (3) providing a carrier sense indication back to the MAC to verify activity on the media.

Physical Layer convergence Procedure (PLCP):

This sub layer means by the capabilities of the physical medium dependent (PMD). It uses the associated PMD system to frame the MAC sub-layer Data unit (MPDUs) into a suitable format for transmission between two end nodes.

Physical Medium-dependent (PMD):

This sub-layer handles the transmission and reception characteristics.

The most common radio transmission technologies used by the IEEE 802.11 physical layer are Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). Both FHSS and DSSS support 1 and 2 Mbps data rates. The now a day technologies supports up to 45 Mbps data rate; in order to achieve higher data rates a new extension to DSSS called High Rate DSSS (HR/DSSS) has been developed. The physical layer also supports high data rate technologies such as Orthogonal Frequency Division Multiplexing (OFDM) [7].

2.3.3 802.11 MAC Layer

The MAC layer is implemented in every 802.11 station, and enables the station to establish a network or join a pre-existing network and to transmit data passed down by Logical Link Control (LLC). These functions are delivered using two classes of services, station services and distribution system services, which are implemented by the transmission of a variety of management, control and data frames between MAC layers in communicating station. 802.11 MAC layer provide the access method for stations. The fundamental access method of the IEEE 802.11 MAC is a distributed coordinate function (DCF) known as carrier-sense multiple access with collision avoidance (CSMA/CA). The DCF will be implemented in all stations, for use within both IBSS and infrastructure network configurations. The IEEE 802.11 MAC may also incorporate an optional access method called point coordinate function (PCF), which is only usable on infrastructure network configurations. PCF exhibits an extension of MAC functions and provides lower transfer delay variations to support time-bounded services [7].

2.3.4 Basic access method DCF

The Basic Medium Access Protocol is a DCF that allows for medium sharing between stations through the use of CSMA/CA. In this protocol, the station, before transmitting, senses the medium. If the medium is free for a specified time, called *distributed interframe space* (DIFS), the station executes the emission of its data. Otherwise, if the medium is busy because another station is transmitting, the station defers its transmission, and then it executes a backoff algorithm within a *contention window* (CW). Figure 2.5 sketches this method.

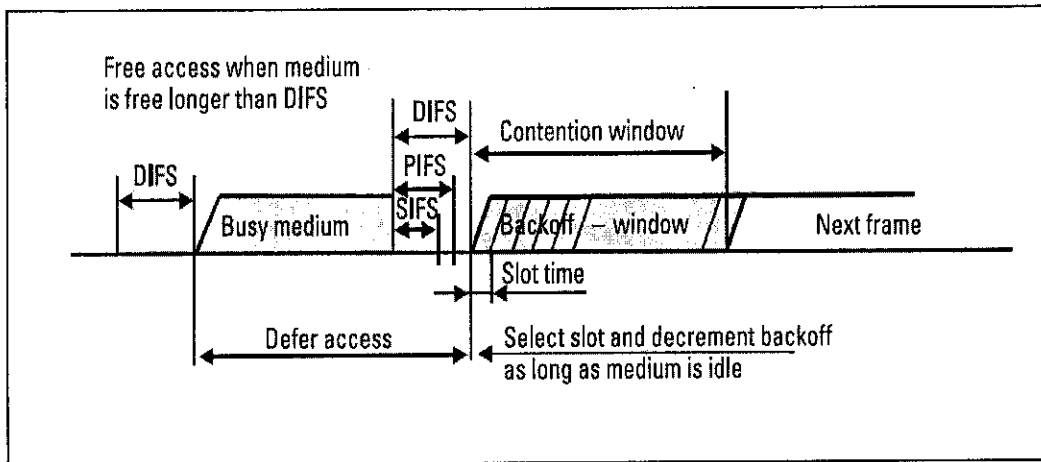


Figure 2.5: CSMA/CA [6].

The virtual carrier-sense mechanism is achieved by distributing reservation information announcing the impending use of the medium. The exchange of *request to send* (RTS) and *clear to send* (CTS) frames prior to the actual data frame is one means of distribution of this medium-reservation information.

2.3.5 PCF

The PCF option is implemented to provide contention-free frame transfer and to thus support time-bounded services as well as transmission of asynchronous data, voice, or mixed. It is based on a *point coordinator* (PC), which has higher priority than other STAs. If it wants to transmit, it must wait a PIFS time, which is shorter than DIFS. Other STAs have to obey medium access rules of the PCF by setting their NAV at the beginning of a *contention-free period* (CFP).

2.3.6 802.11 MAC Frame Types

802.11 MAC layer uses three types of frames: management frame, control frame, and data frame. All these types are using a predefined frame format for communication.

A MAC frame of IEEE 802.11 contains up to 9 fields as shown in Figure 2.6.

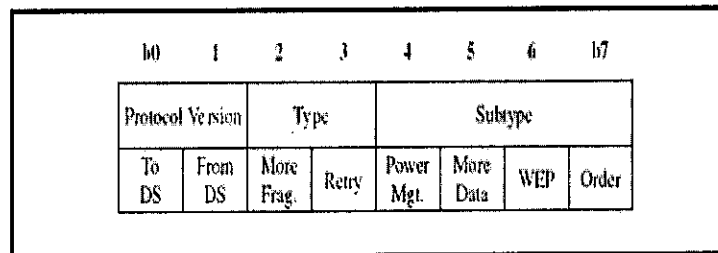


Figure 2.6: 802.11 MAC Layer frame fields [6].

Data frame: they used for data transmission.

Control frame: this type is used for the traffic control messages such as Request to send (RTS), Clear to Send (CTS), and Acknowledgment (ACK).

Management frame: such as beacon frames, are transmitted in the same manner as data frames to exchange management information, but are not forwarded to upper layers.

2.4 Wireless Mesh Networks

Generally speaking, wireless networks are either point-to-point, or a point-to-multi point configuration. In the point-to-point configuration each node needs its own dedicated connection. In the other side, point-to-multi point requires that all wireless nodes are within the same range of communication, which it may leads to a bottleneck problem. Another topology called WMN which is also known as a multi-hop network which is gaining more attention from the wireless community in the last decade.

WMNs are self healing, reliable, self configuration, and scalable. The next section introduces the idea behind WMNs; and shows some application could be applied to WMNs; and also discuss the current problems faces this type of network [9].

2.4.1 WMNs Definition and Benefit

WMN construction is quite similar to a smaller version of the internet. It consists of mesh routers, mesh nodes, and gateways. In WMN each computer or node are connected in a mesh topology. In this type of network each node is connected only to the nodes that are close to it. The network architecture of WMNs can be classified into three main groups based on the network infrastructure [1].

(1) *The infrastructure WMNs:* mesh routers act as centre points and bring connectivity for mesh clients. In other words mesh routers act as access points to mesh clients. Moreover, mesh routers create the wireless backbone, and also works as gateways to provide the internet connectivity to the network. Figure 2.7 depicts the infrastructure

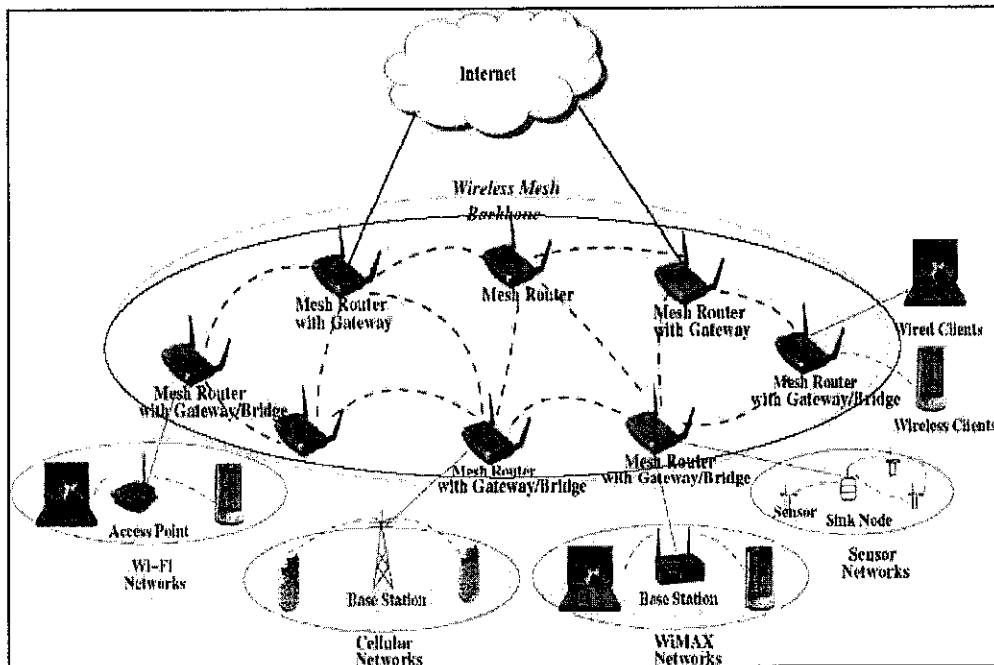


Figure 2.7: Infrastructure WMNs [2].

WMNs. (2) *In the infrastructureless network:* there is no concept of mesh router, thus they acts as mesh clients. In this type all the nodes are able to establish connection with any other node. This type of WMNs architecture is similar to Mobile ad hoc networks (MANET). Thus mesh clients have to forward or route each other nodes' packets. Figure 2.8 shows example of infrastructureless WMNs.

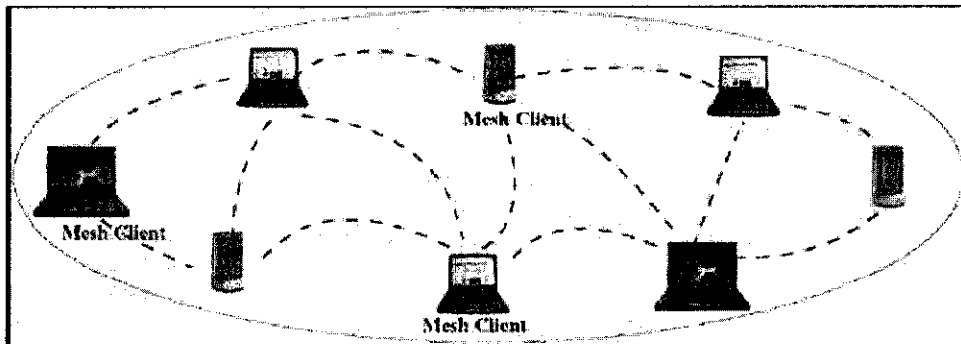


Figure 2.8: Infrastructureless WMNs [2].

(3) *The hybrid architecture* of WMNs is a combination between the two types of WMNs. In this architecture mesh clients can access the network through mesh routers as well as directly communicate with other mesh clients. And mesh routers create the wireless backbone of the network. Figure 2.9 shows an example of the hybrid architecture of WMNs.

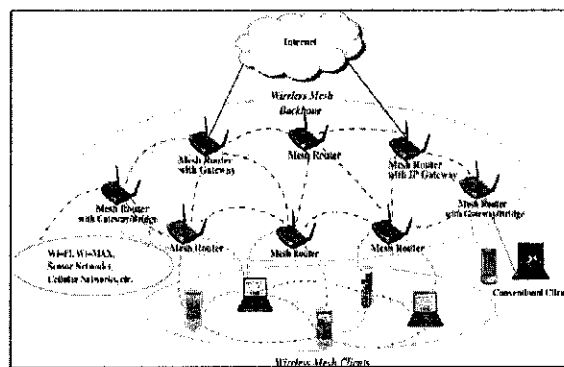


Figure 2.9: Hybrid WMNs [2].

Nodes in WMNs act as routers to forward packets to nearby nodes. For example, each node could be placed in a home and transmits to its closest neighbors. By doing this one can achieve a high reliability, and the distance between nodes become smaller, it also increases the bandwidth and decreases the transmission power needed for communication. For instance, if the distance between two nodes is less by factor of two, the signal between them is approximately four times stronger [10].

Furthermore, as the distance between two nodes is decreased the probability of the noise error decreases since more noise is presented in the long distance transmissions. Thus, nodes can transmit at much lower power in WMNs, which may save frequencies to be reused in different areas of the network. Reusing frequencies, allow multiple devices to transmit simultaneously without interference[3].

Much like the internet, WMNs allow multiple paths that can be taken between nodes, by including more nodes in the network, which leads to more reliable network since if one node is down, alternate path can be found always. WMNs are reliable and it is also can be expanded easily by simply add more nodes. The last considered benefit of WMNs solved the problem of the last mile internet access. For example, if two nodes that are far apart need to be connected, intermediate nodes (repeater nodes) can be inserted into the network to connect the two nodes. Another situation where this is beneficial occurs when bypassing large obstacles such as buildings or trees [6]. A single mesh network can handle up to thousands of nodes. Since there is no central control point that is present in point-to-multipoint networks [11].

2.4.2 WMN critical design factors

WMN is a new wireless network technology. As a new technology it faces many critical design factors. The coming sections explore the design factor that faces WMNs technology, and it gives a spot of light on the challenges that faces WMNs.

Scalability

WMN as a community network; Therefore, the number of nodes in such a network is unpredictable. For the last reason, scalability is a critical design factor for WMNs. Without support of this feature, the network performance degrades significantly as the network size increases. To ensure the scalability in WMNs, all protocols from the MAC layer to the application layer need to be scalable.

Security

Due to the distributed architecture of WMNs, and the non-centralized behavior of WMNs, one can find it difficult to distribute a public key in WMNs. Although many security schemes have been proposed for wireless LAN in recent years, they are still not fully applicable for WMNs. Due to similarity between ad-hoc networks and WMNs; one can find it possible to adopt ad-hoc security schemes for WMNs. However, most of the security solutions for ad hoc networks are still not mature enough to be implemented practically. Moreover, the dissimilar network architectures between WMNs and ad hoc networks usually make a solution for ad hoc networks ineffective in WMNs.

Ease of Use

The need to design Protocols that must enable the network to be as autonomous as possible is a necessity for WMNs. Also, the network management tools must be

implemented to efficiently monitor the performance, maintain the operation, and configure the parameters of WMNs. The ease of use in WMNs, enable rapid deployment of WMNs.

Routing Protocol

Due to the unpredictable behavior of the wireless medium in WMNs, the need for a routing protocol that aware to the link conditions appears as a necessity. Unfortunately the routing protocols used such as AODV and DSR are hop count-based; where the routing algorithm uses the number of nodes to determine the optimum path to the destination. Moreover, the scalability is one of the design factors that affect the performance of routing protocols; the scalability is one of the critical factors in WMNs. Unfortunately the routing protocols used are mainly designed for ad-hoc networks, where the network scalability is not considered. Thus it is critical to have a scalable routing protocol for WMNs. Also, WMNs routing protocol must be robust to link failure, so it can avoid service disruption. The mobility in WMNs is less than ad-hoc network, which is due to user's behavior of this network. Thus WMNs needs a routing protocol that cops well with this amount of mobility.

2.5 WMN Routing Protocols

In this section we will discuss the available WMN's routing protocols and show the major differences among them. Practically, there is no reliable list for WMN's routing protocols and currently the [16] is listing more than 90 of them. So the question of which one of the available routing protocols best fits the WMN, remains without answer.

In this chapter the most commonly used routing protocols are introduced and fully described in order to give better understanding of the wide range of requirements that are imposed.

Generally speaking, WMN's routing protocols can be classified into three groups:

- *The reactive routing protocols.*
- *The proactive routing protocols.*
- *The hybrid routing protocols.*

In reactive routing protocols a route to a destination is created only on demand. This means that when a node needs to send its packet to a certain destination, a routing request is sent in the network. The protocols that belong to this category are the "AODV", the "DSR" and the "TORA". These three protocols have been proposed to the IETF MANET workgroup. On the other hand, the proactive protocols are periodically sending control packets in order to maintain the knowledge of the network topology. Among the protocols of this group one can find the "OLSR", the "FSR" and the "TBRPF". The hybrid routing protocols such as (Temporary Order Routing Protocol (TORA)) are a combination of the above two groups [7].

Due to the limitation in the thesis space, in the next section we fully describe one protocol from each of the three aforementioned groups.

2.5.1 OLSR Routing Protocol

The "OLSR" Optimized Link State Routing protocol is described in RFC 4782 (3). It is a proactive routing protocol and also a link state protocol. "OLSR" defines two types of

control packets: “hello” packets and “TC” packets (TC for Topology Control). “Hello” packets are used to build the neighborhood of a node and at the same time “hello” packets is used to compute the “multipoint” relays of a node (the concept of multipoint relay will be explained latter) “hello” packets are sent in broadcast at one hop. “TC” packets are broadcasted in the whole network. “TC” packets broadcasted by a node contain the list of its neighbors. Actually this list does not contain all its neighbors but a subset, which will be explained latter. A “hello” sent by a packet contains the list of neighbor. OLSR uses periodic broadcast of hello packets to sense the neighborhood of a node and to verify the symmetry of radio links. Hello packets sent by a node contain the status of its links with the other nodes in its neighborhood. This status can be: asymmetric, symmetric, or multipoint relay. During the initialization phase, when a node A receives a hello packet from a neighbor, say node B, this station sets in its neighbor table station A with a status “Asymmetric”. Then, when node B send its next hello packet, B will send in its hello packet that A is its neighbor table with status “Asymmetric”. At the reception of the hello packet from B, A will put in its neighbor table B with the status “Symmetric”. A will then send a hello packet in which B will appear with the status “Symmetric” and B will update the status of A in its neighbor table and will register it as “Asymmetric”. See Figure 2.10.

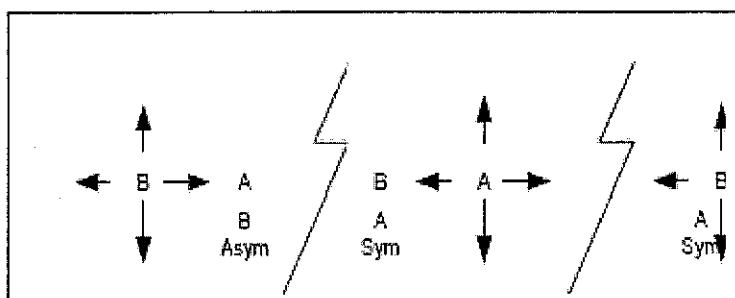


Figure 2.10: Neighborhood sensing [19].

Multipoint relay is a special status that will permit optimization of broadcast. Let us consider figure 2.11.

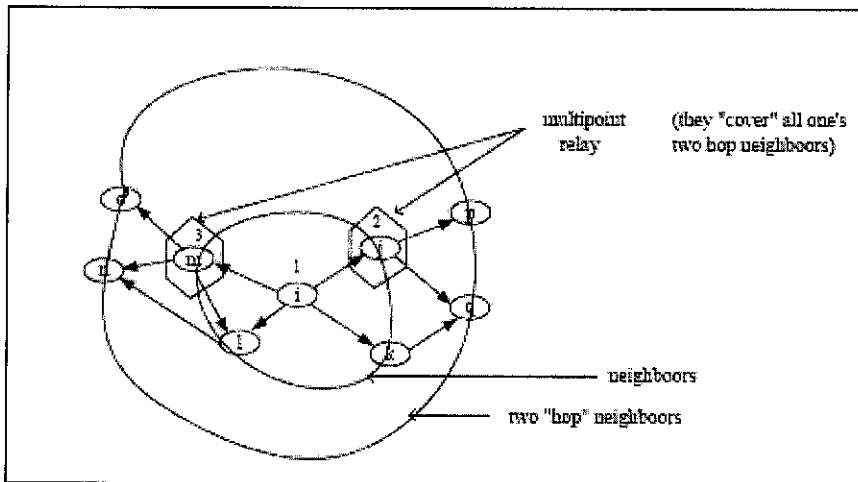


Figure 2.11: Multipoint Relay (MPR) [4].

In this figure 2.11, we have shown a node with its neighbors and its two hop neighbors. A two hop neighbor of a node is a neighbor of its neighbors which is not already a neighbor. To obtain a complete broadcast, it is sufficient that the packet be repeated by a convenient subset of its neighbor. This subset must be computed in such a way that the entire two hop neighbor receive the packet. If this requirement is achieved, it can be shown by induction that a complete broadcast is obtained. Actually, this technique provides a way to locally compute a spanning tree. For a given node the computation of the subset of its neighbor that satisfies the two hop coverage is an NP hard problem. However one can find simple heuristics, a very natural heuristic is derived from the greedy algorithm and selects at each step the neighbor which covers the maximum number of two hop neighbors. The "TC" packets are sent periodically by a node. This

packet contains the list of its multipoint relay i.e. the subset of nodes which make it possible to cover all its two hop nodes. The “TC” packets are sent in broadcast and with the multipoint relay rule only the multipoint relay nodes will retransmit the packet.

A sequence number is used to avoid loops due to infinite retransmission of the packet. Another field is used to allow knowing which of two “TC” packets is the more up to date. Although a node does not send its entire neighborhood in the “TC” packet, it can be shown that this information is sufficient to build a topology of the network giving the shortest path, this was shown for the first time in [19].

2.5.2 DSR Routing Protocol

The Dynamic source routing (DSR) is described in request for comments (RFC 4782) [23]. Like AODV it is a reactive routing and a hop-count-based routing protocol. It is based on source routing, where the source specifies the complete path to the destination in the packet header and each node along this path simply forwards the packet to the next hop indicated in the path. It utilizes a route cache where routes it has learned so far are cached. Therefore, a source first checks its route cache to determine the route to the destination. If a route is found, the source uses this route. Otherwise, the source uses a route discovery protocol to discover a route. In route discovery, the source floods a query packet through the ad hoc network, and the reply is returned by either the destination or another host, which can complete the query from its route cache. Each query packet has a unique ID and an initially empty list. When receiving a query packet, if a node has already seen this ID (i.e., duplicate) or it finds its own address already recorded in the list, it discards the copy and stops flooding; otherwise, it appends its own address in the list and broadcasts the query to its neighbors. If a node can complete the query from its route

cache, it may send a reply packet to the source without propagating the query packet further. Furthermore, any node participating in route discovery can learn routes from passing data packets and gather this routing information into its route cache. A route failure can be detected by the link-level protocol (i.e., hop-by-hop acknowledgments), or it may be inferred when no broadcasts have been received for a while from a former neighbor. When a route failure is detected, the node detecting the failure sends an error packet to the source, which then uses route discovery protocol again to discover a new route. Note that in DSR, no periodic control messages are used for route maintenance. The major advantage of DSR is that there is little or no routing overhead when a single or few sources communicate with infrequently accessed destinations. In such situation, it does not make sense to maintain routes from all sources to such destinations. Furthermore, since communication is assumed to be infrequent, a lot of topological changes may occur without triggering new route discoveries. Even though DSR is suitable for the environment where only a few source communicate with infrequently accessed destinations, it may result in large delay and large communication overhead in highly dynamic environment with frequent communication requirement. Furthermore, DSR may have scalability problem. As the network becomes larger, control packets and message packets also become larger since they need to carry addresses for every node in the path. This may be a problem since ad hoc networks have limited available bandwidth [24].

2.5.3 AODV Routing Protocol

The Ad-Hoc On-Demand Distance Vector routing protocol is described in RFC 3561[25]. It is a reactive routing protocol, and it is also a hop-count based routing protocol. The

philosophy in AODV, like all reactive protocols, is that topology information is only transmitted by nodes when there is a request for route (on-demand). When a node wishes to transmit traffic to a host to which it has no route, it will generate a route request (RREQ) message that will be flooded in a limited way to other nodes. This causes control traffic overhead to be dynamic and it will result in an initial delay when initiating such communication.

A route is considered exist when the RREQ message reaches either the last end point itself, or an intermediate node with a valid route entry for the destination. For as long as a route exists between two endpoints, AODV remains passive. When the route becomes invalid or lost, AODV will again issue a request [24].

AODV avoids the “counting to infinity” problem from the classical distance vector algorithm by using sequence numbers for every route. The counting to infinity problem is the situation where nodes update each other in a loop. Consider nodes A, B, C and D making up a MANET as illustrated in Figure 2.12.

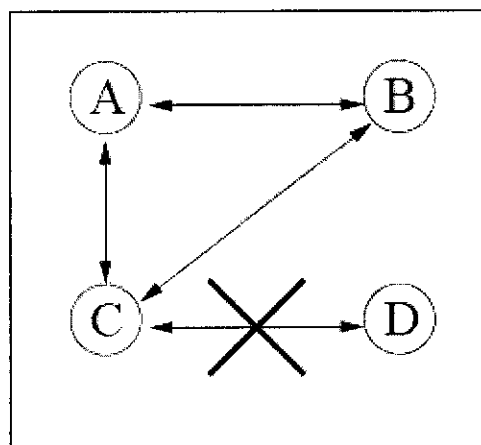


Figure 2.12: Counting to infinity scenario.

A is not updated on the fact that its route to D via C is broken. This means that A has a registered route, with a metric of 2, to D. C has registered that the link to D is down, so once node B is updated on the link breakage between C and D, it will calculate the shortest path to D to be via A using a metric of 3. C receives information that B can reach D in 3 hops and updates its metric to 4 hops. A then registers an update in hop-count for its route to D via C and updates the metric to 5. And so they continue to increment the metric in a loop. The way this is avoided in AODV, for the example described, is by B noticing that A's route to D is old based on a sequence number. B will then discard the route and C will be the node with the most recent routing information by which will update its routing table. AODV has three types of message for route maintenance (5):

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

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

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

2.6 Related works

Most of the current researches in routing protocols for wireless Mesh networks [4],[12] and [13] are focused on finding the suitable routing metric. Different routing metrics are proposed and simulated in ad hoc network such as round trip time (RTT), and expected transmission counts (ETX). The coming sections give an overview of some of these routing metrics.

2.6.1 Hop count

Hop count is the most widely used routing metric in existing protocols, such as ad-hoc on demand distance vector (AODV) routing protocol. This metric considers either the link exists or not. Thus it does not account for the link quality. The major advantage of this metric is its simplicity. Moreover, one can find it easy to calculate the path with the minimum number of hops, whenever the network topology is known. In a wireless communication the behavior of the link is unpredictable. Thus in order to define the optimum path, it needs to account for the link quality. In hop count metric the link is either exists or not, which is expected to have a poor network performance in wireless network. For example, over fast and reliable links, a two hop path can show better

performance rather than a one hop path over a lossy or slow link. Hence, using a hop-count metric may not result in a good performance [2].

2.6.2 Per hop Round Trip Time (RTT)

Round Trip Time is proposed by [14]. RTT calculates the round trip delay of a probe between two nodes. To calculate RTT, a node sends a probe packet with a timestamp for all its neighbors every half a second. Once this probe is received; the node must immediately reply by a probe acknowledgement message. When the sender receives the probe acknowledgement, the sender node calculates the difference between its time and the timestamp time. By doing this, sender knows the required RTT time of its neighbors. The source node then calculates the average of all received RTTs. In order to determine the optimum path, the sender calculates the sum of least average RTTs. This metric considers any delay that could happen to the packet within its journey to the destination. Example: if any node is busy, then queuing delay would increase the RTT. It is also affected by the delay could occur by the channel contention. Moreover slow and lossy links may result on sending the probe several times, thus the RTT will increase. Although this metric accounts for different link quality aspects, also it has disadvantages as well. The protocol overhead caused by sending probes may result in poor bandwidth utilization, which is unpleasant in wireless networks [10].

2.6.3 Per Hop Packet pair Delay (PktPair)

Per hop packet pair delay (PktPair) metric calculates the delay between two back-to-back probes. This first probe is small and the second one is large. When these probes are received by the neighbor, the neighbor calculates the delay between the two probes. The

calculated delay is to be sent back to the source node. The overall objective of this metric is to minimize the sum of these delays for the entire path to the destination.

Like RTT this metric considered different link quality aspects. The main different is, when there is a high loss rate in the network, the second probe has to be retransmitted several times according to ARQ. Thus the delay measured by the neighbor will increase. It also increases when the neighbor has a low bandwidth. Like RTT this metric generates a big amount of protocol overhead. Even more than RTT generated overhead, due to the big size of the second probe [4].

2.6.4 Expected Transmission Count (ETX)

ETX which is proposed by [15], is a metric that calculates the retransmission tries that are made by the node to send a unicast packets, by measuring the loss rate of broadcast packets between two nodes. Every node broadcasts a probe every second (Hello packet). Then each node counts the received probes of a certain neighbor within the last ten seconds. Then each node calculates the loss rate of probe on every link with a neighbor. For example, suppose there are two nodes A and B. assuming that node B receives 7 probes from A within the last ten seconds. While node A receives 6 probes from node B in the same ten seconds. The loss rate then is calculated as flow:

The loss rate from A to B = 0.3

The loss rate from B to A = 0.4

The probability of successful delivery of packets on the link between A and B =

$$(1-0.3) \times (1-0.4) = 0.42$$

The calculated ETX = $1/0.42$

The calculated value of ETX is assigned to the dedicated link as a metric. The routing protocol will look for a path with the least calculated ETX. ETX is recalculated each time a node received a probe from a neighbor.

This metric generates an unwanted overhead over the link by sending probes. Moreover, the broadcasted probe are small, and if the probes are sent at low rate (802.11 a / 6Mbps), it may not face the same data loss rate if it happen in a high data rate links (6).

2.7 Summary

Wireless network is increasingly attracting mobile users due to its benefits in providing a wireless connectivity. WMNs provide attractive benefits in comparison to other types of wireless networks. As a new technology, WMNs faces several challenges. One of these challenges is the routing problem. Practically, there is no reliable list for WMN's routing protocols. WMN's routing protocols are classified into three groups reactive, proactive, and hybrid routing protocols. In this chapter three of the most commonly used routing protocols (AODV, DSR, and OLSR) are introduced and fully described. Though the many routing protocols that have been proposed over the last few years, the routing protocol problem is still an open issue for research in WMNs.

CHAPTER SNR-BASED OLSR

3.1 Introduction

OLSR routing protocol is one of the existing routing protocols in the OPNET model library. It has been implemented according to the RFC 3626 reference model. In OPNET it has been implemented as a manager for the MANET-rte-mgr. The first sections describes the OLSR model operations, specification and the message used in this model as it has been implemented in the OPNET model library [26]. The MBR is the technique used by the OLSR to reduce the routing control traffic broadcasting. The next section describes this technique in details and shows how it works in the OPNET model. The standard OLSR model uses the hop-count as a metric to define the optimum route. In this chapter a cross layer optimization is proposed. Modified OLSR is also presented and the modifications that have been done in the OPNET model are described later in the last section of this chapter.

3.2 OLSR (OPNET module)

OLSR is designed to work as a manager for the MANET routing protocols suit in the OPNET model. It is constructed from three main mechanisms, neighbor sensing, MPR flooding, and Topology discovery mechanism. These mechanisms are implemented as functions of code inside the main process model. The OLSR process model controls all of the incoming and the outgoing traffic from other parts of the simulation [26].

As OPNET allows the data exchange between different modes; OLSR model uses the IP common routing table model to build its own table. OLSR uses two types of control

packets TC and Hello Message to update the topological changes and to build the MPR table respectively. The OLSR model supports multiple interfaces. OLSR can be configured on a router and workstation. Routers connect more than one network; which make it necessary for the routing protocol that runs on the router to support multiple interfaces. The model also supports memory efficient topology table entries and both IPv4 and IPv6.

3.2.1 OLSR Packets

The OPNET uses objects to transfer data between models. These objects are defined as packets. OLSR model defines three types of packets which are Data Packets, TC (Topology Control), and Hello Message. OPNET defines a packet format for the OLSR packet. OLSR packet composes of three fields which are Message, packet length, and packet sequences number. Figure .1 shows the OLSR packet format.

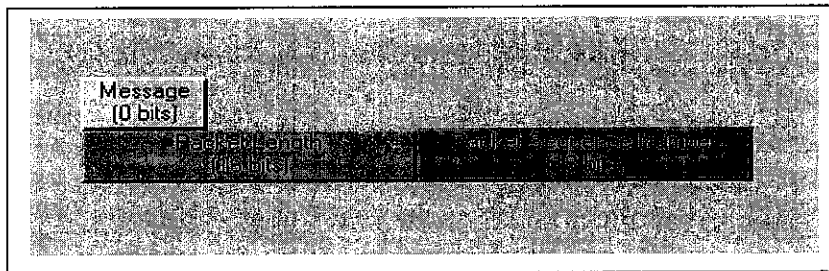


Figure 3.1: OLSR packet format.

Hello Message: Hello message are used to detect new neighbors. Each node broadcasts a hello message periodically with the channel information. The channel information can be piggybacked in the hello message to reduce the routing traffic overhead.

Hello message is also used to compute the multipoint relay for the node. The multipoint relays are a set of neighbors those are authorized to broadcast a packet from this node. Further information about the MPR (Multi Point Relay) could be found later in this chapter.

TC Message: it is use by the OLSR node to update the topological state information. TC packet is broadcasted for the whole network, but not all the neighbors are broadcasting it. Only the MPR nodes are broadcasting this packet due to the use of MPR technique.

Data packet: this type of packet only contains the OLSR header. The rest of the fields are for the information data. OLSR uses this type of message for application data transfer.

3.2.2 OLSR configuration on the OPNET

OLSR routing protocol on the OPNET model can be configured on these types of nodes: routers, MANET node, Mobile MANET nodes, wireless workstations, and servers. To configure OLSR routing protocol parameters on the node it must be selected as the running routing protocol on the ad-hoc routing protocol parameters. Figures (3.2 and 3.4) show how to configure the OLSR parameters on the node model.

```

/**** Data Structures ****/

/* OLSR Message */
/* Contents of OLSR messages are shared between copies of a
/* However, the header is not shared as it can be modified by
/* node. Header is represented by OlsrT_Message OS.
typedef struct {
    Opt_uInt8      message_type;
    Opt_uInt8      vtime;          /* Valid time */
    Opt_uInt16     message_size;
    int            originator_addr;
    Opt_uInt8      ttl;
    Opt_uInt8      hop_count;
    Opt_uInt16     message_seq_num;
    Boolean        is_ipv6;
    void*          message;
} OlsrT_Message;

```

Figure 3.2: OLSR packet header file.

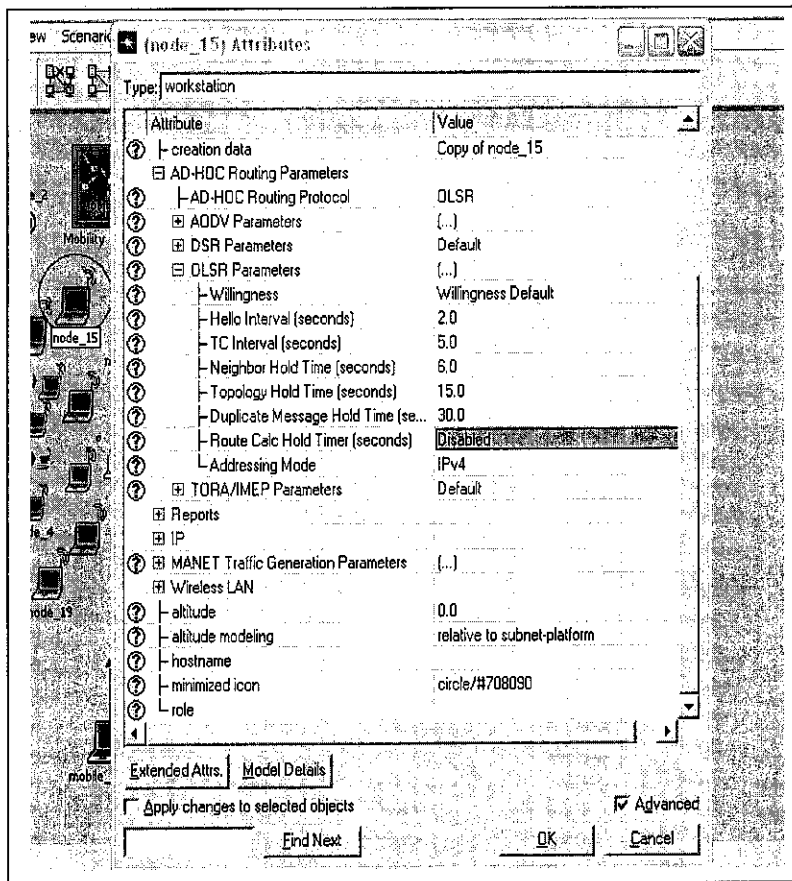


Figure 3.4: OLSR Parameters Configuration.

3.2.3 OLSR Routing Metric on the OPNET Model

The OLSR protocol on the OPNET uses the traditional hop-count metric to define the optimum path to the destination. There is a special field on the OLSR routing table that contains the number of hop-count for any reachable destination. This field is used to be updated periodically as one of the topological information. When a node tends to transmit a packet to any destination it goes to calculate the optimum path (the path with minimum hop-count number) by using algorithm which is designed for this reason.

In this thesis the SNR metric is proposed and implemented in the OLSR model as a routing algorithm metric. The SNR in the model is calculated in the physical layer as one of the receiver's models. Once the SNR need to be used in the network layer; the need for a collaborative future is required. OPNET provides an especial kind of message (ICI) which is used to exchange any type of information within the node model. The ICI has been used to get the SNR information from the physical layer of the model to the OLSR process model. New functions are implemented in the OLSR function block to support the SNR. The modification that has been done to the OLSR mode code can be found in appendix A.

3.3 MPR Technique

The Multi Point Relays (MPR) is the main idea behind the OLSR routing protocol. OLSR uses the MPR technique to reduce the routing information broadcasting. Moreover, instead of flooding the information through the network, MPR technique selects number of one hop neighbors (MPRs) to broadcast the information. Each node in the network selects a set of its one hop neighbors (MPRs). This list of MPRs must cover all two hop neighbors. Also, each node must have MPR selector list. This list contains a list of all nodes that have selected this node as the MPR [19].

The set of MPR list is kept small in order for the protocol to be efficient. In OLSR only the MPRs are allowed to forward the data of the origin node through the network. In order to calculate the MPRs, node must have the information about the symmetric one hop and two hop neighbors. Hello message is used to extract this information about the neighborhood of each node. Each hello message contains a list of one hop neighbors.

MPR technique uses this list of one hop neighbors in the hello message to minimize its MPRs list.

MPR selector list is a list that contains all nodes which have selected this node as the MPR. When a broadcast message is received from a host that exists in the MPR selector node, then this node must forward this message to its neighbors. MPR Selectors sets are updated continuously using Hello messages.

3.4 SNR

Signal to noise ratio is an engineering term for the power ratio between the signal (information) and the background noise. Which it could be expressed as:

$$\text{SNR} = P_{\text{signal}} / P_{\text{noise}} = (A_{\text{signal}} / A_{\text{noise}})^2 \quad (1)$$

In equation (1) P is the average power, and A is the RMS amplitude. Both power elements in equation (1) must be measured at the same time in a system. Which means: signal and noise power (or amplitude) must be measured at equivalent points in a system, and within the same system bandwidth. Since signals have a wide dynamic range, SNR is used to express in terms of logarithmic decibel scale.

$$\text{SNR (dB)} = 20 \log_{10} (A_{\text{signal}} / A_{\text{noise}}) = 10 \log_{10} (P_{\text{signal}} / P_{\text{noise}}) \quad (2)$$

SNR has been long used as the standard measure of quality of analog signals in noisy environment. It has been also proposed that measurement of effective SNR to be used in evaluating the quality of the received signals, which is corrupted by both noise and

distortion, in communication systems [7]. In the real world SNR is calculated in the network interface card (NIC) when data is received. NICs are using estimation technique to measure the SNR value of the received data. In this research work the SNR value is calculated in the receiver pipeline stage on the OPNET module as in equation (3).

$$\text{SNR} = \frac{r_s(0)}{\sigma^2} \quad (3)$$

OPNET is using a series of software blocks that perform all the wireless physical layer operation. These block diagrams are called the pipeline stages. Pipeline stages could be divided to transmitter and receiver pipeline stages. The first 5 stages are dedicated to the transmitter operation, while the rest of the 14 stages are for the receiver operations (Figure 3.4). Each stage is simply a piece of software that can be substituted or modified as desired. SNR is defined in the OPNET as one of the pipeline stages modules on the receiver group [21].

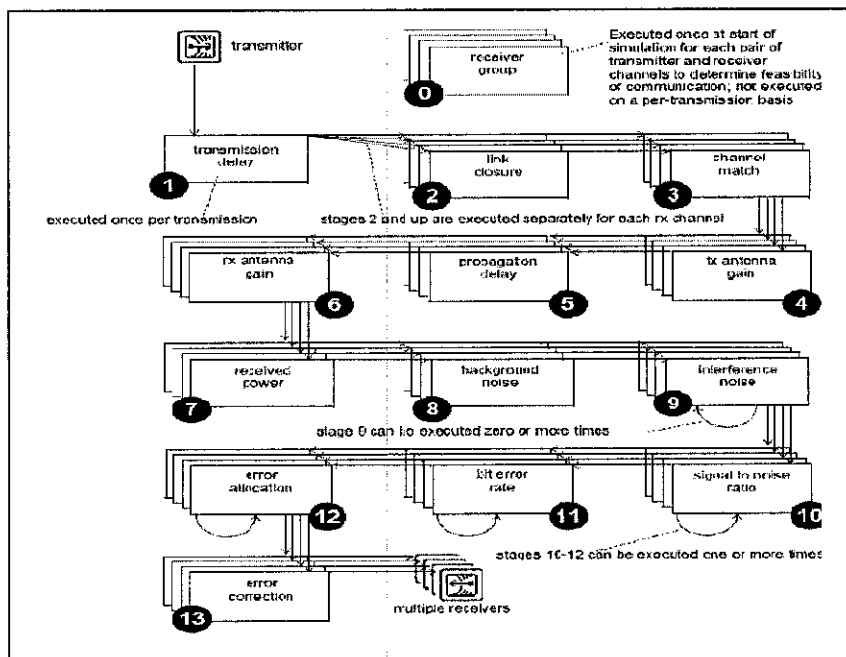


Figure 3.4: OPNET Pipeline Stages [7].

SNR is calculated in the pipeline stage according to two modules of noise the background noise and the accumulated noise modules. The module is using equation (2) to calculate the SNR value. Figure 3.5 depicts this module.

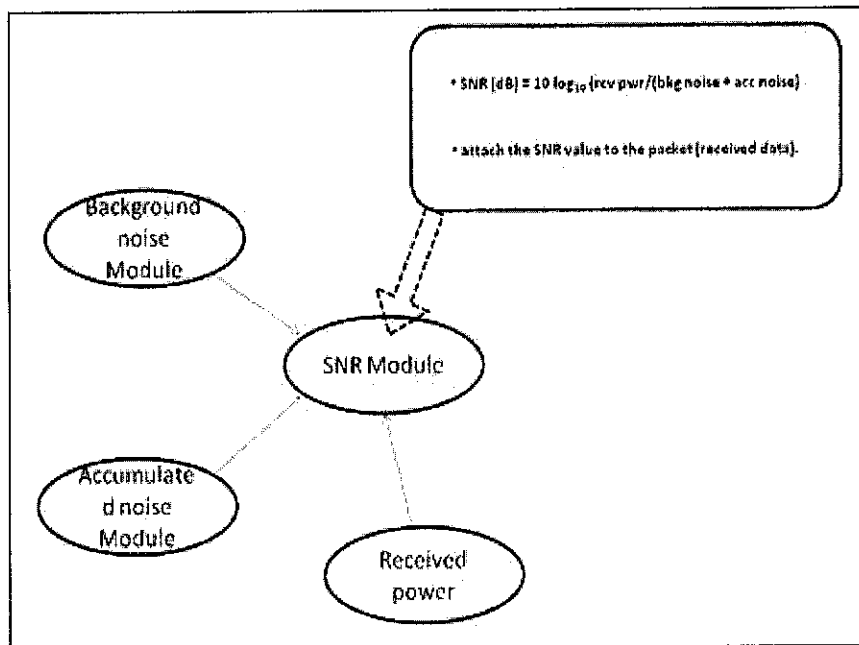


Figure 3.5: SNR module.

3.5 Summary

In this chapter the SNR is implemented in the OLSR routing protocol. The OLSR module in the OPNET simulator is explored. The linear prediction SNR estimation technique is described and implemented in the OPNET pipeline stages.

CHAPTER FOUR: SYSTEM DESIGN

4.1 Introduction

In developing wireless communication protocols, simulation is widely used as an evaluation mechanism. There are many simulation tools specially developed for this purposes, like OPNET and NS2 simulators. In this work the OPNET 11.5 modeler has been used.

The main objective of this chapter is to test the use of SNR as a routing metric for OLSR routing protocol in a WMN. Accordingly, this chapter has been divided into two parts:

- *Designing the simulation test bed of WMN.*
- *Running the standard routing protocols (DSR, AODV, and OLSR) modules.*

4.2 Network Modeling Using OPNET

OPNET provides a wide-ranging framework for modeling wired as well as wireless network scenarios. It is among the top discrete event network simulators used both by the commercial and research communities. The OPNET 11.5 simulator is used in our simulation for analysis and comparison between OLSR, AODV, DSR, and SNR-based OLSR protocols. The simulation network is composed of three levels of design (Network, node, and process model). The first level is to implement the main network scenarios. In this level user can define the number of nodes, the environmental parameters, communication scheme, and the simulation area. The second level is the node design level. It concerns of node parameters such as the traffic generation module used by this node. The third level of design is the process model. In this design level the user can

build, implement or modifies a communication protocol. Process modules are used to build the nodes. Moreover, users can design or modify any protocol and attach it to the node modules. Routing protocols modules are implemented using Visual C++ language [26].

The simulation network: This refers to the simulation scenario and network. At this level of design one can defines the network layout, the nodes and the configuration of node's attributes among the scenario.

Node model: This level of design is based on process models. It consists of a set of modules describing the various functions of the node.

Process model: At this level of design one can implement or modify the main functionality of the modules. It consists of a finite state machines, definitions of model functions, and a process interface that state the parameters for interfacing with other process models and configuring attributes. The process models are implemented using Proto C, which is a discrete event library based on C functions.

OPNET ModelerTM uses an object-oriented approach for the development of models and simulation scenarios. The models can be recognized as a *CLASS*, which can be reused any number of times in the simulation by creating its different instantiations, just like the creation of objects in any object-oriented programming language. Besides allowing the creation of multiple instances, OPNET allows the user to extend the functionality of the basic models already available as part of the model library. Thus, by defining the value of the attributes of the basic model, the user can develop customized models following particular standards or vendor specifications [26].

4.3 Routing Protocols Design Concepts

The widely used wireless routing protocols like AODV and DSR are designed based on protocols and mainly developed for wired networks, so they assume a packet delivery, which is correct in the wired medium, but NOT in wireless. However, the critical assumptions about them are:

- Links are either perfectly usable or not at all. If we can transmit a packet to a node once, then we will be able to repeat it later as long as the topology does not change.
- Links are bidirectional. If a station can receive packets from a neighbor node, it can be sure that the neighbor will receive its packets, too.

Several studies showed that these assumptions are unrealistic in wireless environments [24]. Nevertheless, many wireless protocols still, either explicitly or implicitly, rely on them. And here is a summary of the problems that may arise because of that:

Neighbor Discovery: Most protocols use *HELLO* messages in discovering the neighboring stations. Each node transmits periodically a broadcast packet, including at least its identification number. Other nodes located within the transmission range will receive the transmitted packets and inform back so each node will know its direct neighbors. This information is used later in calculating the best routes to distant nodes. However, in wireless networks the quality of transmitted signals at the boarder areas is deteriorating. This may cause the working nodes at the border of transmission not to receive all the transmitted HELLO messages from the neighboring nodes.

To make the problem of neighbor discovery clearer, let's look into the simple example that is shown in Figure . The links between A, and C and between C and B are of a good

quality, represented by their high packet delivery ratio of about 98 %. On the other hand, the link between A and B has a weak connectivity with packet delivery ratio of about 10 %. Such scenarios are common in wireless multi-hop networks [8].

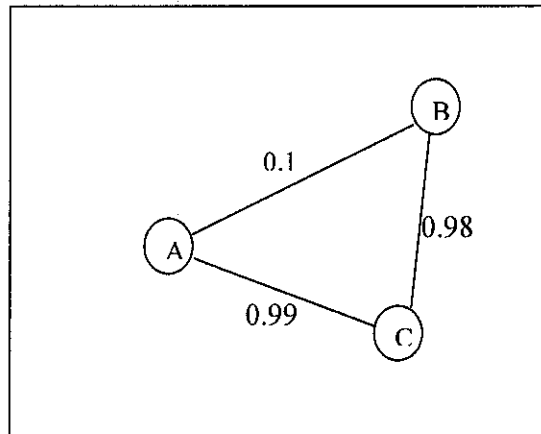


Figure 4.1: Neighbor discovery example.

The neighbor discovery of station A will detect B and C as one-hop neighbors and usable for routing, though the low value for the packet delivery ratio for the HELLO packet of B. However, when this link is used for transmitting packets, most of them will be lost because of the low delivery ratio. This problem is further amplified by routing protocols that use shortest path routing and thus choose relatively long (and thus lossy) links. In our example it would also be possible to forward packets from A to B via (A, C, B) with a better delivery ratio. However, the shortest path algorithms prefer the one-hop path.

4.4 WMN Simulation Design

According to OPNET architecture there are three levels of design: 1) network level, 2) node level and 3) process model level. These levels of design are explained in the remainder of this chapter.

4.4.1 The network level

Main Network Scenario

Since the hybrid architecture is the preferred architecture for WMN [6], we select it for the simulation as a fundamental network. The OPNET version 11.5 simulator is used for the simulation.

The simulation network consists of four subnets; each with 20 stationary nodes and 5 mobile nodes; spread randomly in an area of 20x80 m². Each station generates exponential amount of traffic with 1 Kbit packet size and selects a random destination. We use the MANET workstation model as a node, which is designed to fulfill the IEEE 802.11 standards. The workstation bit rate is 2 Mbps with transmitted power of 0.005 watts and (-85%) dBm receiver sensitivity. The workstation MAC layer runs Carrier Sense Multiple Access, with Collision Avoidance (CSMA/CA); to fulfill the IEEE 802.11 standards. RTS/CTS feature is set to disable. The routing layer, which is the main issue for this work is done through three different scenarios; each scenario deploys one of the selected routing protocols.

To measure the influence of the different amount of mobility on the network, two scenarios of high and low mobility have been built.

High Mobility Network Scenario

In the high mobility scenario we assume 100 MANET nodes spread randomly as the main scenario above. Each group of nodes has 80% of their nodes as mobile nodes and each mobile node applies a different mobility module. The applied mobility modules

such as random movement model and the power down model are created in the OPNET trajectory creator.

Low Mobility Network Scenario

In the low mobility scenario we assume 100 nodes spread randomly as the main scenario above. Each fixed node runs the MANET model from the Opnet 11.5 standard modules. The mobile nodes are running the mobile MANET node model. In this scenario only 20% of the nodes are considered as mobile nodes.

4.4.2 The Node Level

This level of design focuses on the nodes characteristics. In order to simplify the programming all nodes are defined as either Mobile or Fixed MANET nodes. The only difference between these two types is that the mobile node has additional process model to define the mobility trajectory. Each node can transmit and receive traffic from other nodes. Each node supports 802.11 standards. The OPNET MANET node model is used for this level of design. The models of the mobile and fixed nodes are shown in Figure. The node model is composed of the following four layers:

concerns certain function in the receiver. The receiver model is shown in the receiver attributes group as in Figure 4.3.

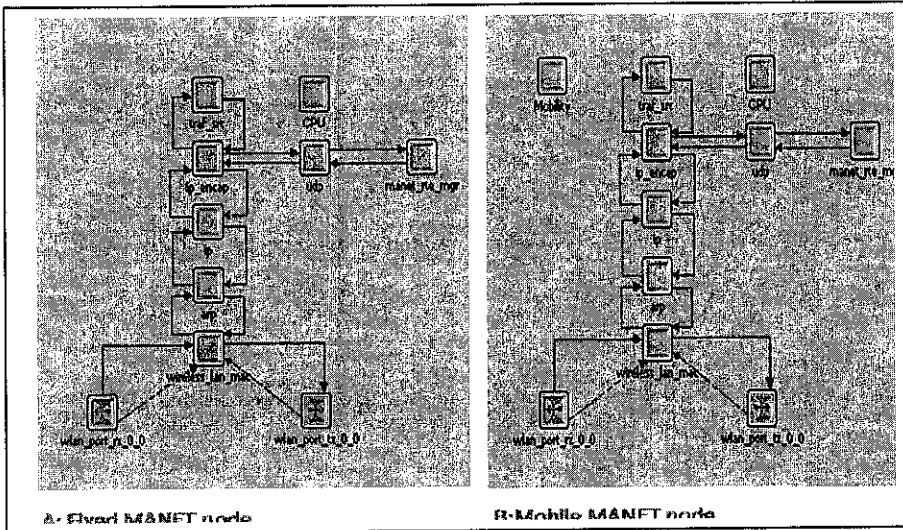


Figure 4.2: Node Model.

Physical Layer: This layer consists of receiver and transmitter. The receiver receives data from all transmitters within its range and passes it to the upper layer (wireless_lan_mac). The receiver model is designed as a combination of different models. Each model

The second element in the physical layer is the transmitter. Transmitter receives data from the upper layer (wireless_lan_mac), and sends it to all nodes in its transmission range. Figure and 4.4) show the receiver transmitter attributes.

Attribute	Value
? name	wlan_port_rx_0_0
? channel	(...)
? modulation	dpsk
? noise figure	1.0
? ecc threshold	0.0
? ragaain model	NONE
? power model	wlan_power
? bkgnoise model	dra_bkgnoise
? inoise model	dra_inoise
? snr model	dra_snr
? ber model	wlan_ber
? error model	wlan_error
? enc model	wlan_enc

Figure 4.3: Receiver Attributes.

Attribute	Value
name	wlan_popt tx 0 0
channel	(...)
modulation	dpsk
rxgroup model	wlan_rxgroup
txdel model	wlan_txdel
closure model	dra_closure
chanmatch model	wlan_chanmatch
tagain model	NONE
propdel model	wlan_propdel
icon name	ra_tx

Figure 4.4: Transmitter attributes.

5.4.2.2 MAC Layer: This layer is composed of two processors, which are the `wireless_lan_mac` and the `arp`. The main functions of this layer are:

Receive packets from upper and lower layer and send them to the desired process handle.

- *Defines the wireless LAN parameters.*
- *Declares the MAC layer protocol.*

Figure shows the `wireless_lan_mac` model attributes.

5.4.2.3 MAC Layer Process: The received packet by this layer is either coming from the upper layer or from the receiver. In case, it is coming from the receiver then the `MAC_Protocol` will check whether it is addressed to this node or not. If it is addressed to this node then the protocol will handle the packet; otherwise the `mac_protocol` will discard the packet.

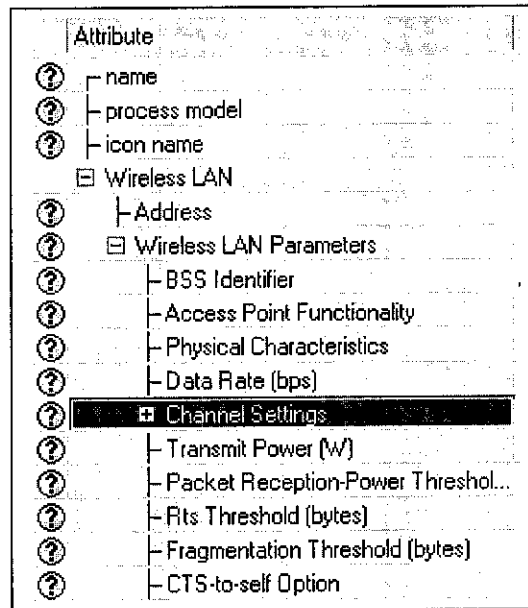


Figure 4.5: wireless_lan_mac attributes.

The other case is when a packet is received from the upper layer. In this case the `mac_protocol` has to add to its header the necessary information that is needed for the packet to reach the next hop. The `mac_protocol` uses a cache table with all the needed information about the node neighbors. The `mac_protocol` updates its information table by exchanging a special type of messages between the neighbors. After the header is added, the `wireless_lan_mac` model sends the packet to the transmitter.

5.4.2.4 Network Layer: This layer focuses on the routing mechanism for the packets and it is composed of four processing models:

IP Process Model: This model handles the packets from the IP-ecap and the MAC layer. In this model, the IP address of the node is saved and used later to build up the IP routing table. When a packet is received and has to be handled by this model, the model checks firstly where it came from. If the packet came from the MAC layer, the IP model checks the destination address of the packet; if it is addressed to this node or not. In case the

packet is addressed to this node, the model updates its routing table and sends it to the upper model for further processing. On the other hand, if the packet is not addressed to this node then the IP model will discard it. If the packet came from the upper layer, the IP model has to pass it to the MAC layer models. It also exchanges the IP routing table information with other models in this layer.

IP_encap Model: This process model is operating as a dispatcher. When a packet is received from a higher layer then it should be encapsulated into an IP frame. The next step is to send the IP frame for the IP process. On the other hand, when a packet is received from the lower layer, the IP_encap model reads the frame header to decide the next processing form of the data.

UDP Model: This model has the same functionality as the IP_encap model. The only difference is the uses of the UDP frame format.

MANET_rte_mgr Model: The MANET_rte_mgr handles all the MANET routing protocols operation. It receives the packets from the data generation layer and from the IP-dispatcher. When data is received from the upper layer then this model sends the received data to the running routing protocol in this node.

The OLSR routing protocol is used to be the default protocol in the MANET-rte-mgr. In case the node uses another routing protocol, the MANET-rte-mgr handles the data to the running routing protocol.

More details about how the routing operation is running in the OPNET can be found in section 4.4.3.1. Figure shows the MANET-rte-mgr attributes.

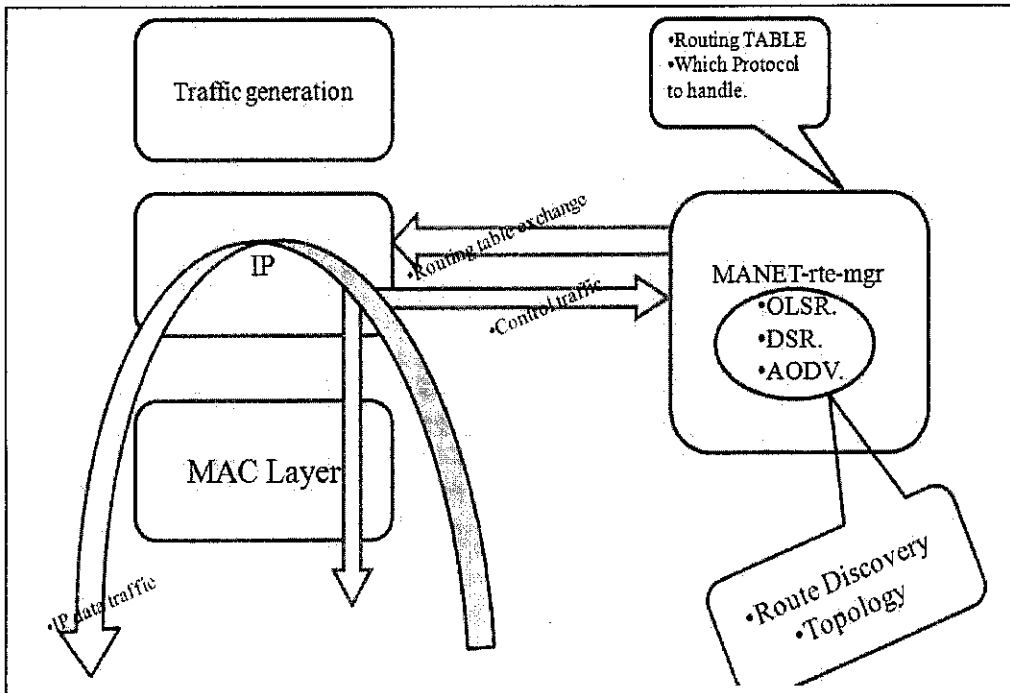


Figure 4.7: MANET routing layer architecture in OPNET.

packet to one of its child processes (routing protocols process models). When data is received from the upper layer, the MANET-rte-mgr sends it to the running child process in this node.

There are three routing protocols running under the MANET-rte-mgr as a child process which are: DSR, AODV, and TORA.

The OLSR routing protocol is included inside the MANET-rte-mgr; which means if the node runs the OLSR routing protocol the MANET-rte-mgr doesn't need to send the data to a child process, it runs it directly from the process model functions.

4.4.4 Ad-Hoc Routing Protocols Configuration on the OPNET

OPNET supports four of the ad-hoc common routing protocols which are: OLSR, AODV, DSR, and TORA. These routing protocols can be configured on the MANET node model. Each protocol has configurable parameters to fit the research requirements. On the node model attributes one can apply one of the considered routing protocols by configuring it on the ad-hoc routing parameters option. Each routing protocol has parameters that can be configured on the model.

Figure shows how to configure the routing protocol on the node attributes.

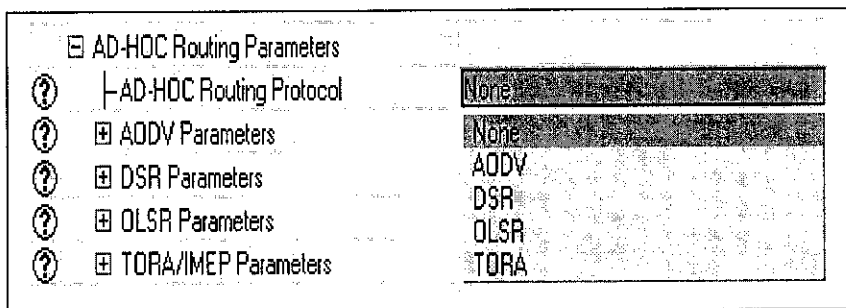


Figure 4.8: Ad-Hoc routing Protocol Parameters.

Figure shows how to configure the AODV routing protocol parameters.

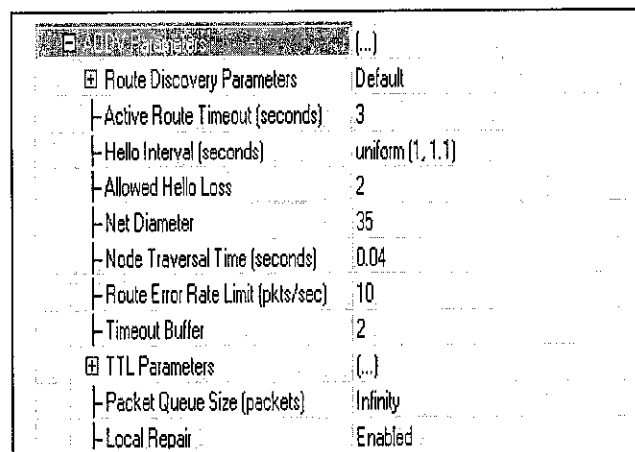


Figure 4.9: AODV Protocol Parameters.

Figure shows how to configure the DSR routing protocol parameters.

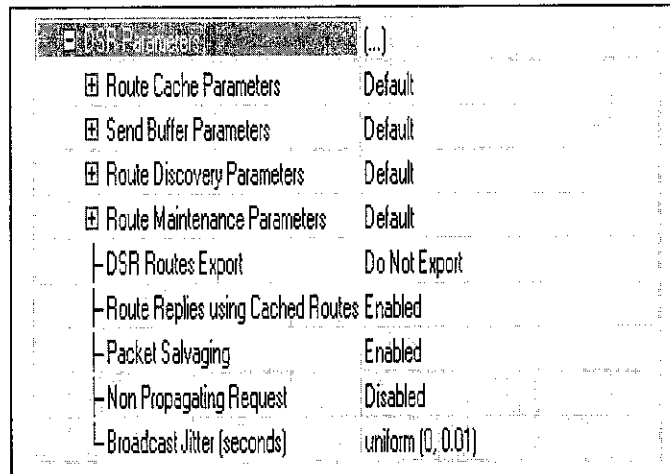


Figure 4.10: DSR Protocol Parameters.

4.5 Summary

This chapter addresses the implementation of the network scenarios. OPNET simulator software is used to simulate the nodes, protocols and networks in this research work. OPNET simulator is representing a good platform for designing and testing networks. OPNET uses three level of design (network, node, and process modules) for building and implementing network components. This chapter gives a wide preview on the OPNET design levels. In this research work two network scenarios (low and high mobility scenario) are designed. In the first scenario 25% of the nodes are engaged with a high mobility trajectory and the second one with 75% of its nodes are mobile nodes. The main purpose of these scenarios is to test the influence of the mobility on WMNs. Making use of the OPNET features we were able to manipulate and change the network parameters in the three levels of design. This chapter gives in depth details on how the configuration and setup is performed.

CHAPTER FIVE: RESULTS AND DISCUSSION

5.1 Introduction

In this research work the SNR is proposed as a routing metric, and implemented in the OLSR routing protocol. To achieving this goal the work is divided into three parts. The first part is focused on making a performance comparison between three of the common used routing protocols for WMNs. These routing protocols are implemented in different WMNs scenarios, and the network performance is calculated in terms of three performance metrics (Throughput, End-to-End Delay, and protocols overhead), The protocols are simulated in the OPNET simulator. The second part of this research is to implement the SNR in the most suited routing protocol for WMNs. The first part of this research shows that, the OLSR is getting the highest performance among the compared routing protocols. Thus, the OLSR is chosen to be adapted with the proposed metric (SNR). The modifications are done on the OLSR module on the OPNET simulator, and the new protocol performance metric are collected and showed in this chapter. The last part of this research work is to study the influence of the mobility on the routing protocol performance. This part is accomplished by building two network scenarios with different mobility. The rest of this chapter is organized as follow. Firstly we started by the comparison scenarios. Secondly, a comparison between the original and SNR metric result is shown. The last sections are dedicated for the mobility scenarios results.

5.2 Protocol Overhead

The routing protocol overhead presented here is the total number of routing packets transmitted per data delivery. To measure the protocol overhead for each of (DSR, AODV, and OLSR) routing protocol the following scenario is adopted [17].

Network: Four sub networks are created. Each network consists of nine nodes. The nodes can transmitted and receive data from all the nodes, as long as the distance between the two nodes is less than 300m, for each sub-network there is a node with a higher data rate than other nodes. Each sub-network is created in area of $300 \times 300 \text{m}^2$. Nodes in the network are spread randomly in the dedicated area. Figure 5.1 shows a snapshot of a sub-network.

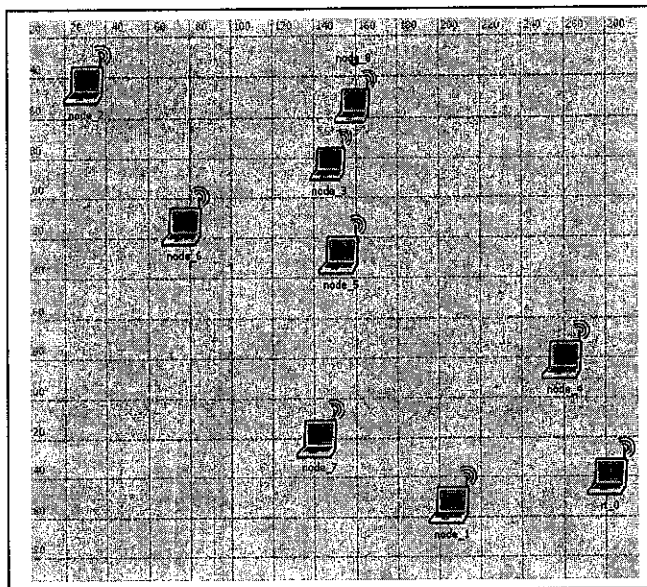


Figure 5.1: Sub-Network (Overhead scenario).

Node: Nodes' physical layer and MAC layer characteristics are designed according to IEEE 802.11 standard nodes. Each node generates two packets per second. Packet size used here is 512 bits. The traffic generation model parameters are presented in Figure .

- Start Time (seconds)	100.0
- Packet Inter-Arrival Time (seconds)	exponential (1)
- Packet Size (bits)	exponential (1024)
- Destination IP Address	Random
- Stop Time (seconds)	End of Simulation

Figure 5.2: Traffic Generation Parameters.

Protocols: The overhead of three routing protocols is presented here. (Figures 5.4, 5.5, and 5.6) show the AODV, DSR, OLSR routing traffic that are generated by these routing protocols respectively; which is considered as the routing protocol traffic overhead.

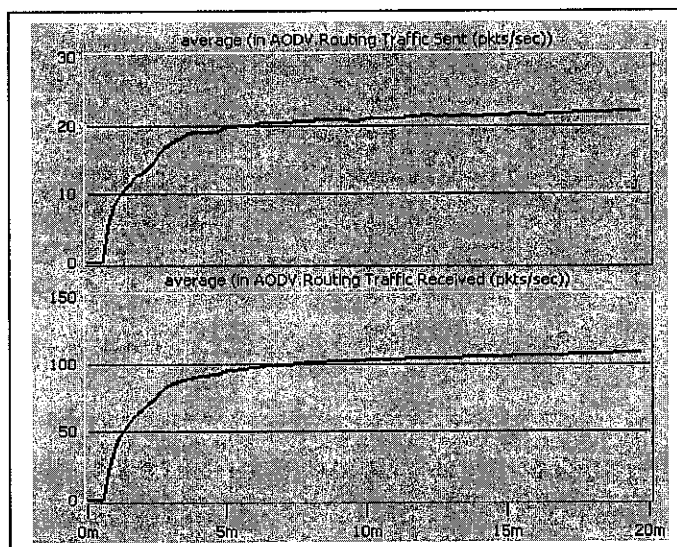


Figure 5.4: AODV protocol overhead (x-axis shows the simulation time in minutes, and y-axis shows the received routing traffic in packets)

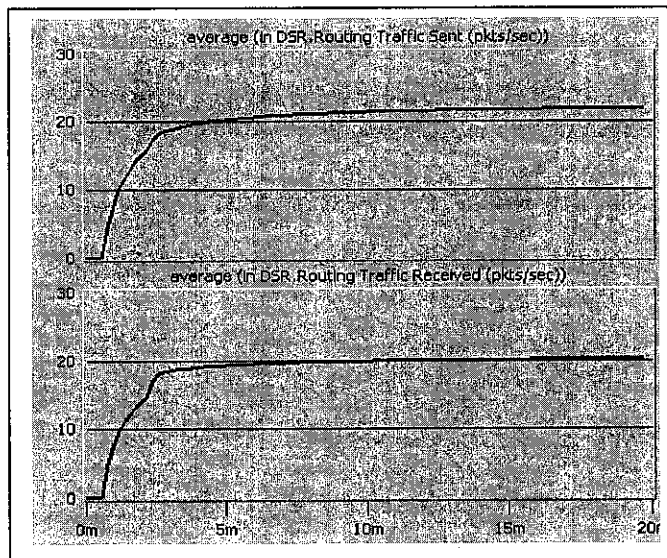


Figure 5.5: DSR Protocol Overhead (x-axis shows the simulation time in minutes, and y-axis shows the received routing traffic in packets).

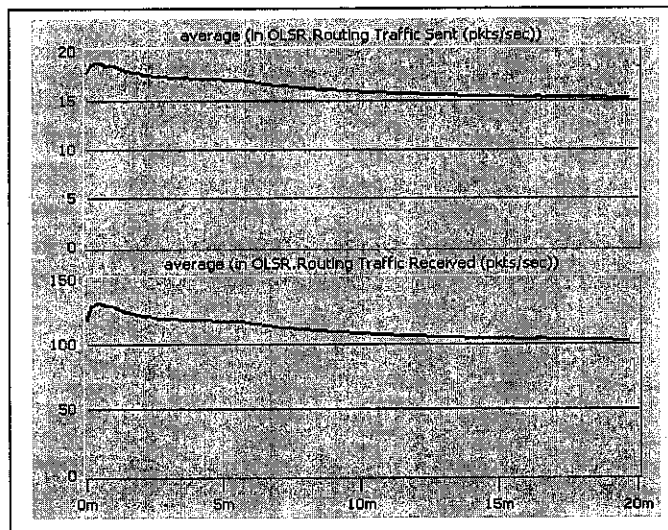


Figure 5.6: OLSR Protocol Overhead (x-axis shows the simulation time in minutes, and y-axis shows the received routing traffic in packets)

The obtained results show that the routing traffic that generated by the OLSR protocol is less than the DSR and AODV in the simulated scenario. Thus OLSR has the highest

performance in WMNs in terms of routing traffic generation (It produces less protocol overhead).

5.3 Mobility Scenarios

To observe the mobility influence in WMNs, two scenarios are created. The first scenario has a low amount of mobility and the second one has a high amount of mobility. The main scenario consists of 100 nodes spread into four sub-networks. Each sub-network consists of 25 nodes spread randomly in $20 \times 80 \text{ m}^2$ area. The sub-networks are placed in a way similar to Universiti Teknologi PETRONAS main Campus.

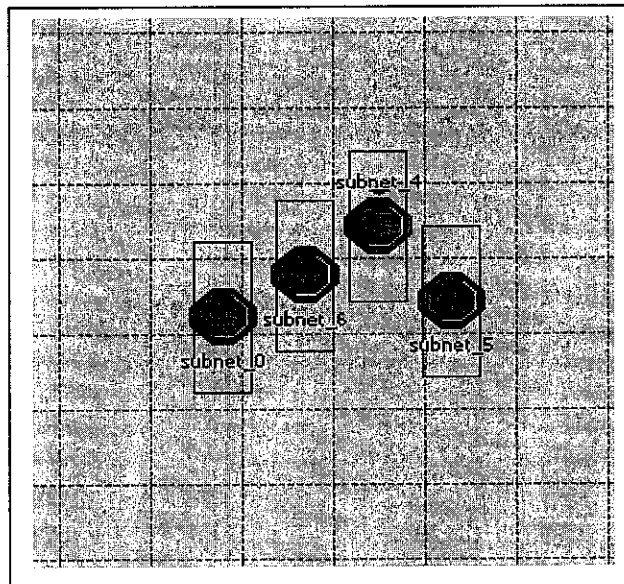


Figure 5.6: Main scenario.

Mobility scenario: In the mobility scenario 80% of the nodes are mobile nodes. Each mobile node has a mobility trajectory. Thus, it can move freely in the overall area. The mobility trajectories are created using OPNET 11.5 new trajectory define tool. Four trajectories are used for this purpose. The node module used is the Mobile-MANET module that exists in the OPNET 11.5. In the node one can define the mobility trajectory,

traffic generation criteria, wireless LAN parameters, and specifies the routing protocol module. Results are collected and demonstrated using the datasheet. Figure shows the general parameters for the mobile-MANET node module.

Non-mobility scenario: it is similar to the mobility scenario, except the number of mobile nodes. In this scenario 20% of the nodes are mobile node, and the rest are fixed MANET nodes. For the fixed MANET nodes the MANET node module is used. This module is similar to mobile-MANET node module except in the mobility trajectory.

The above scenarios are used with different routing protocols to measure the network throughput and End-to-End delay. The coming sections are using these scenarios to collect the dedicated results. .

5.4 Throughput

The OPNET traffic generator module is used to generate a random traffic in the nodes. Each node generates traffic with a 512 and 1024 bytes packets size. Each node generates two packets per second to a random destination. The obtained throughput is the number of successful received data in the destination. For each routing protocol two scenarios are deployed.

To determine the suitable routing protocol for WMNs, a comparison between the throughput of three routing protocols (AODV, DSR, and OLSR) is done. Figures (5.8, 5.9 and 5.10) demonstrate the obtained results of the collected throughput in the non-mobility scenario. The same comparison is also done for the mobility scenario. The throughput is collected and demonstrated in Figure).

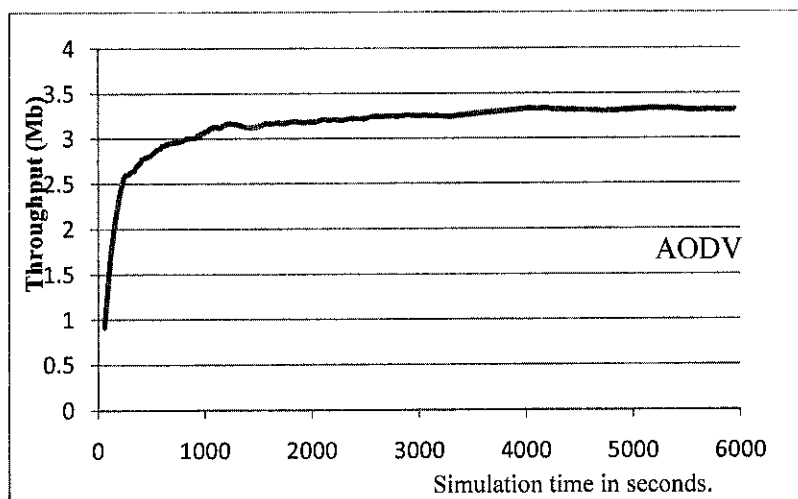


Figure 5.7: AODV throughput (Non-mobility scenario) x-axis represents the real time in seconds and the y-axis represents the throughput in (Mb).

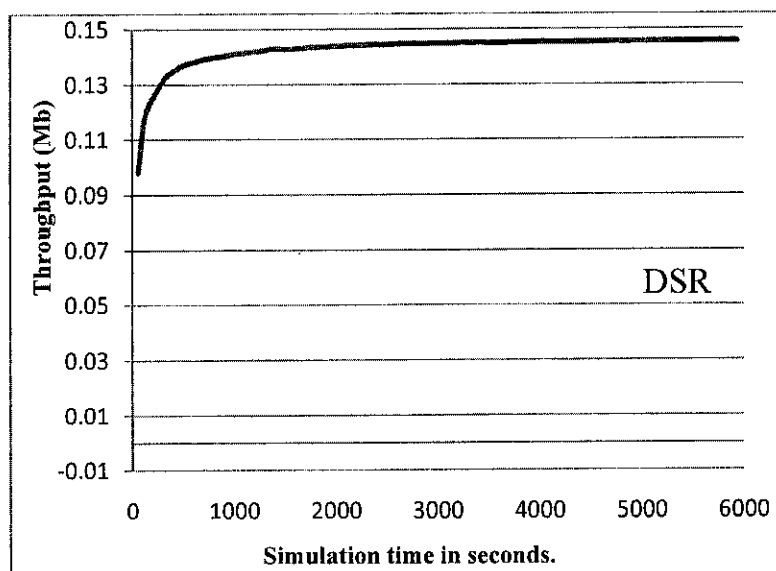


Figure 5.8: DSR Throughput (Non-mobility scenario) x-axis represents the real time in seconds and the y-axis represents the throughput in (Mb).

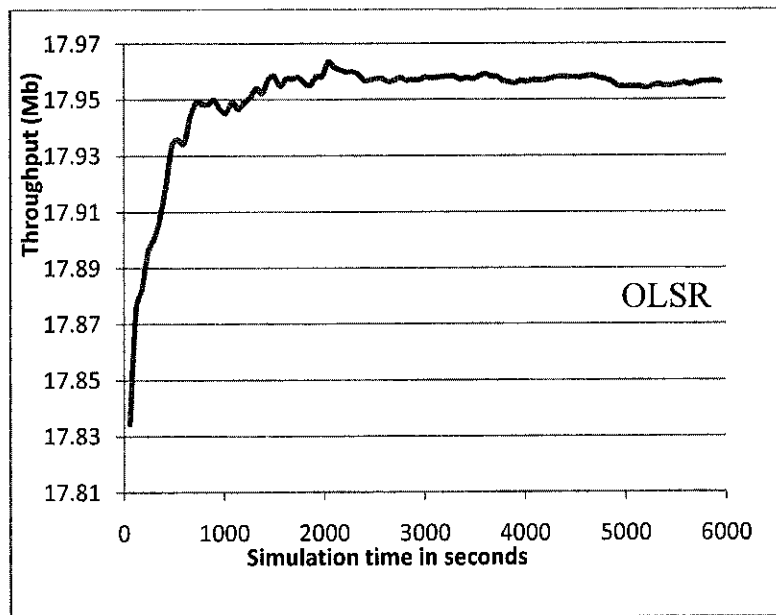


Figure 5.9: OLSR Throughput (Non-mobility scenario) x-axis represents the real time in seconds and the y-axis represents the throughput in (Mb).

Figures (5.8, 5.9 and 5.10) show the obtained throughput for each routing protocol in the non-mobility scenario. The x-axis represents the simulation time in seconds, and the y-axis represents the collected throughput in Mega bits. From the obtained result, it appears clearly that DSR has the lowest throughput among the other routing protocols, and OLSR has the highest throughput in this scenario. The low performance of DSR is due to the big number of nodes in the simulated network. However, when the mobility scenario is applied, the DSR has the highest throughput among the other protocols. This demonstrates that, AODV and OLSR routing protocols acts poor in the high mobility networks.

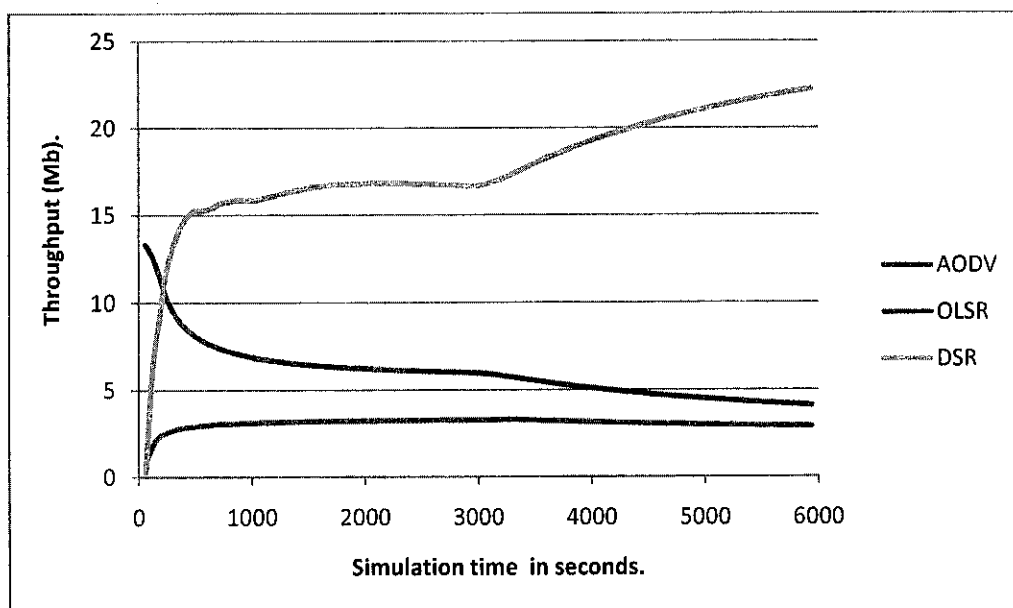


Figure 5.10: Throughput comparison (Mobility Scenario) x-axis represents the real time in seconds and the y-axis represents the throughput in (Mb) x-axis represents the real time in seconds and the y-axis represents the throughput in (Mb).

This thesis aims at improving the throughput of WMNs. Unlike ad-hoc network, the routers in WMNs are stationary nodes, which decrease the amount of mobility in WMNs. Thus, OLSR is expected to gain the highest throughput in WMNs.

5.5 End-to-End Delay

End-to-End delay is the average time to transfer a data packet from a source node to a destination. A network with 100 nodes spread in four sub-networks is used for this simulation. Each sub-network contains 25 nodes within $20 \times 80 \text{m}^2$ area. Different data rates (1, 2, 11, and 45 Mb/s) are applied for nodes. The traffic generation module used here is the OPNET traffic generator module. Nodes generate two packets per second and

packet size used here are 512, and 1024 bytes. Two scenarios are applied per each routing protocol, and three routing protocols are deployed. The network scenarios used are the scenarios from chapter 4. The simulation runs 100 minutes real time per routing protocol scenario. Each routing protocol scenario is simulated two times separately. The first run is for the non-mobility scenario and the second run is for the mobility scenario. The results are collected and demonstrated using the OPNET individual statistic tools. Figures (5.12, 5.13, and 5.14) represent the average End-to-end delay for each routing protocol.

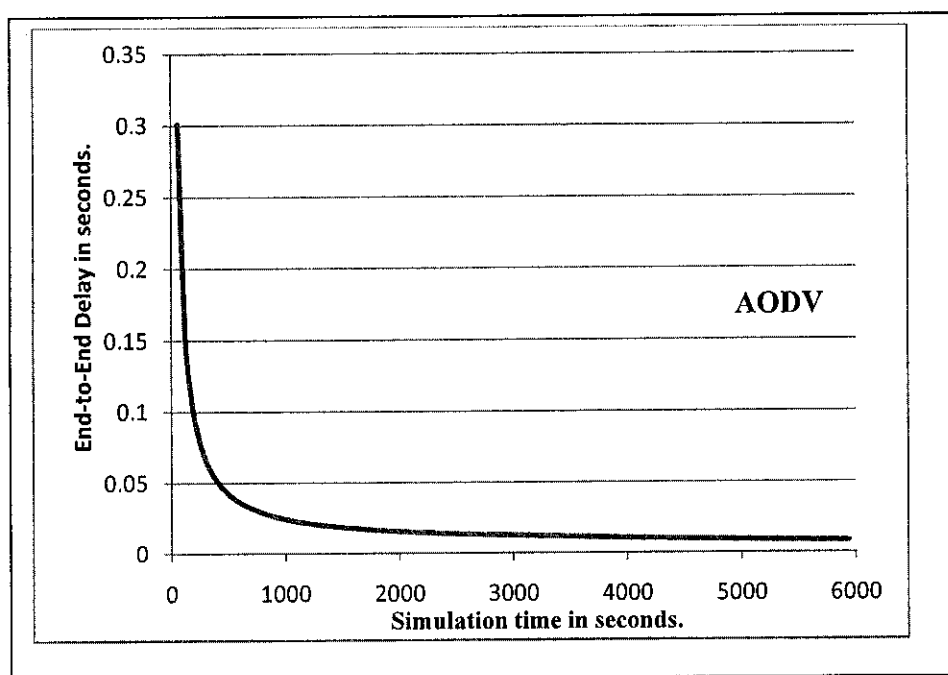


Figure 5.11: AODV End-to-End Delay, x-axis represents the real time in second and y-axis represents the End-to-End delay in second.

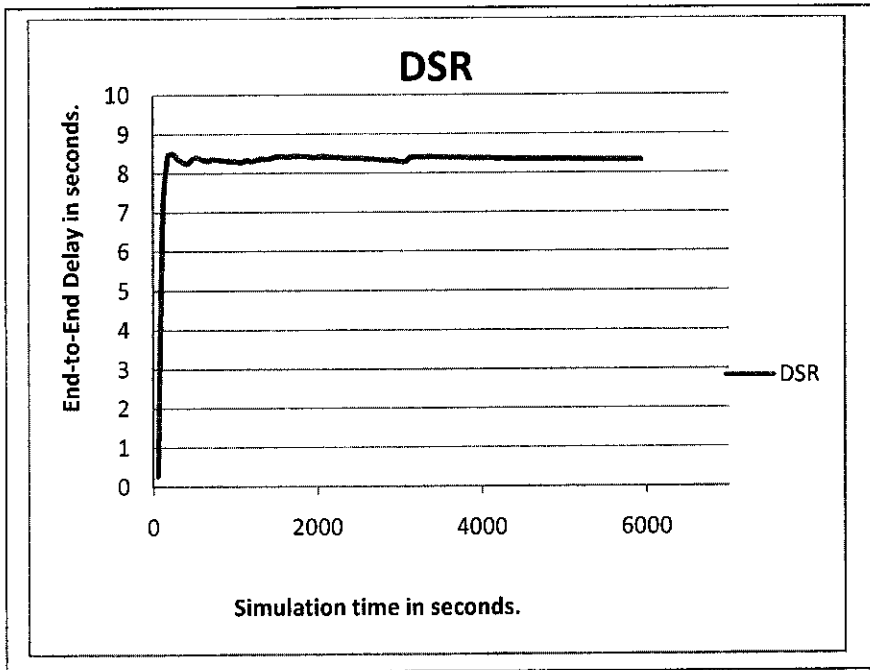


Figure 5.12: DSR End-to-End delay, x-axis represents the real time in second and y-axis represents the End-to-End delay in second.

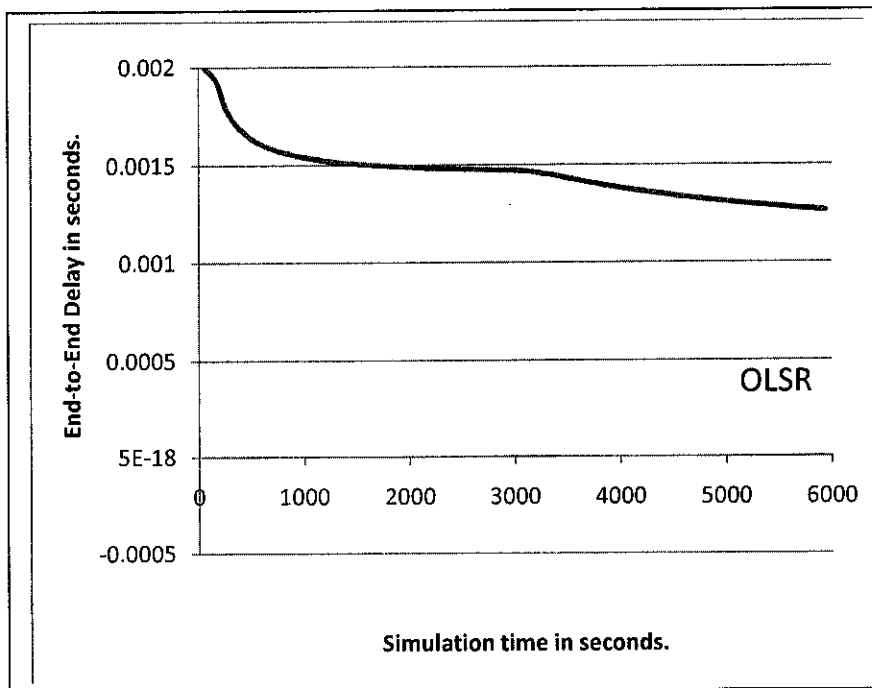


Figure 5.13: OLSR End-to-End delay, x-axis represents the real time in second and y-axis represents the End-to-End delay in second.

The results show that, by using DSR the packet may need more than one second to reach its destination. AODV can deliver a packet in hundreds of millisecond, but OLSR needs only few milliseconds to deliver its data packet. This is mainly because DSR and AODV are reactive routing protocols, and in reactive protocols there is no exiting route for the destination when it is needed. Thus reactive protocols need to create a request a find a path to the desired destination when there is a demand for it. Reactive protocols use this technique to reduce the generated routing protocol overhead, which might result in a bad delivery time. This technique shows a significant improvement in the high mobility networks (ad hoc, and MANET), but in WMNs where the nodes are stationary; it can be found that, reactive routing protocols are not well suited for WMNs.

5.6 Comparison

OLSR generates the highest protocol overhead among the other protocols; this is because OLSR periodically exchanges topology information. Although OLSR generates the highest amount of protocol overhead, still it records the lowest End-to-End delay, and the highest network throughput in WMNs.

DSR generates the lowest protocol overhead, and in the mobility scenario it gets the highest throughput among the other protocols. But in the low mobility scenario its performance degrades gradually when the number of nodes increases. DSR also records the lowest throughput and the highest End-to-end delay when deployed in the low

mobility scenario. Thus, it can be said that, DSR degrades the performance of WMNs. The lack of scalability in DSR degrades the WMNs throughput when DSR is used. From the aforementioned discussion it is clear that OLSR routing protocol is performing best among the considered routing protocol.

5.7 SNR-Based OLSR routing protocol

In this section a comparison between the hop count and SNR as a routing metric is done. End-to-End delay and throughput are used as performance metrics for the comparison. A network with 100 nodes spread in four sub-networks is used for this simulation. Each sub-network contains 25 nodes within 20X80m² area. Different data rates (1, 2, 11, and 45 Mb/s) are applied for the nodes. The traffic generation module used here is the OPNET traffic generator module. Nodes generate two packets per second and packets size used here are 512, and 1024 bytes.

5.7.1 SNR-based OLSR Throughput

Two scenarios are used to obtain the throughput. In the first scenario the original OLSR with the hop-count metric is used. In the second scenario the new metric is deployed in all the nodes. Figure 5.14 shows the obtained throughput among the comparison scenarios.

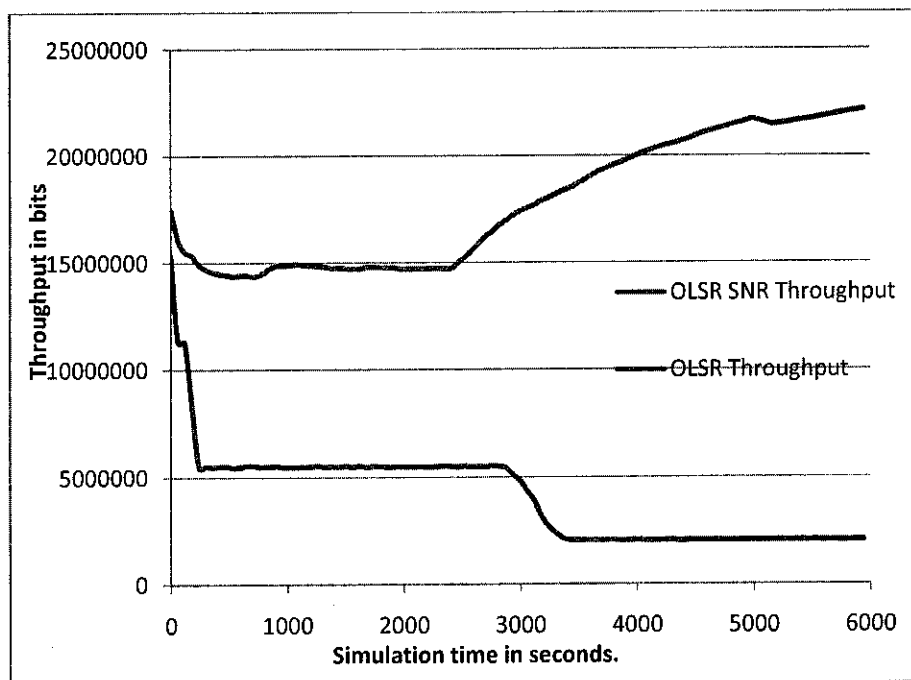


Figure 5.14: Throughput comparison between SNR and hop-count metrics x-axis represents the real time in seconds and the y-axis represents the throughput in (Mb) x-axis represents the real time in seconds and the y-axis represents the throughput in (Mb).

In figure 5.15 the results show that the throughput is increasing with the simulation time in the OLSR-SNR case. While in the original hop-count metric the average throughput is decreasing with the simulation time. In both scenarios the mobility of the nodes is starting after a certain time where the throughput starts to change. The hop-count metric does not cope with the network changes as it is the case in the SNR metric. Also it can be found that by using the SNR the nodes are able to deal with the network change. Moreover, the awareness of the link quality in the routing protocol might result in a good network throughput.

5.7.2 SNR-based OLSR End-to-End Delay

Four scenarios are used for this comparison. In each scenario a different routing protocol is deployed. The general network that is used here is similar to that one in the main scenario in section 5.3. The result are collected and presented in spreadsheet file. As it is shown in Figure , 5.15, and 5.16.

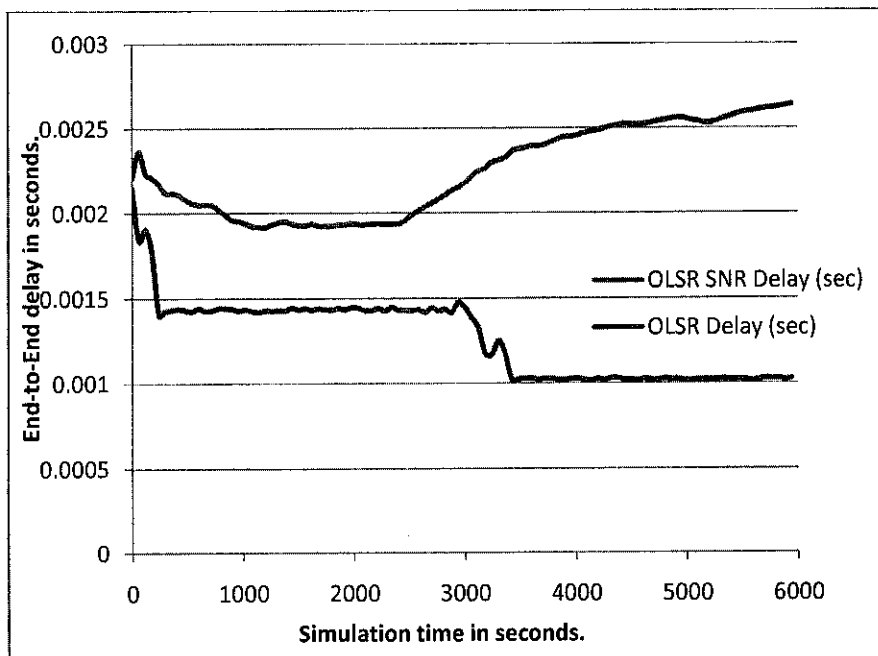


Figure 5.15: Comparison between hop-count and SNR OLSR Delay, x-axis represents the real time in second and y-axis represents the End-to-End delay in second.

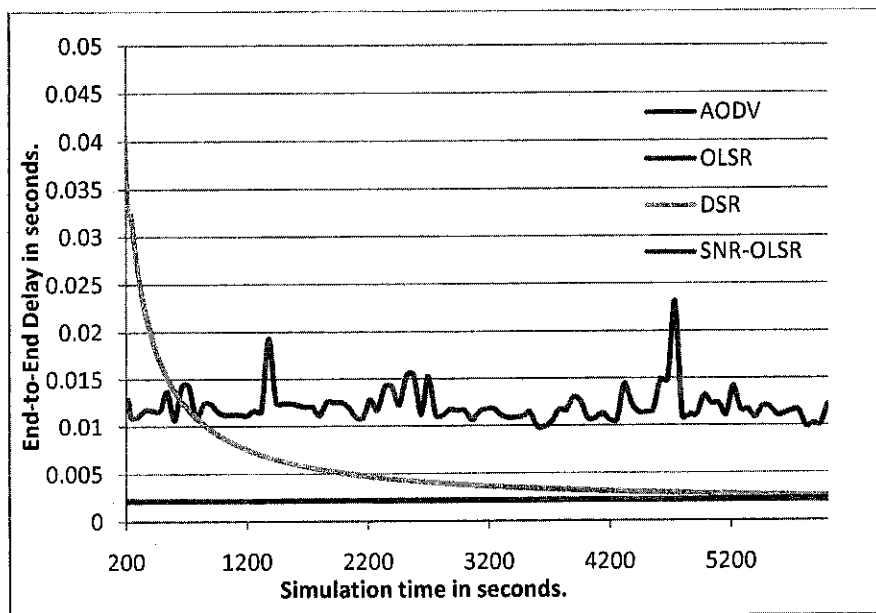


Figure 5.16: Delay Comparison OLSR, DSR, and AODV, x-axis represents the real time in second and y-axis represents the End-to-End delay in second.

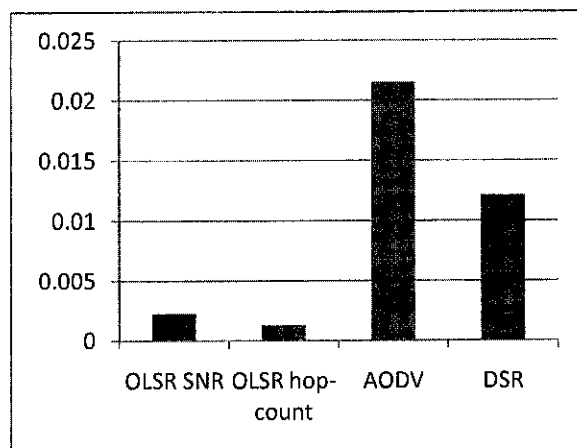


Figure 5.17: Delay Comparison, x-axis represents the routing protocols and y-axis represents the delay in seconds.

The obtained results show that, by using SNR metric, the OLSR suffers from a small amount of delay. The reason for this delay might be because of the use of different path to deliver a packet. Moreover, it can be said that, SNR prefer a path with certain delay and a low packet loss ratio, than a path with small delay and a high packet loss ratio. This

makes users face a certain amount of delay, and in the same time improves the overall network throughput. A routing protocol with a big amount of delay is not good for a network; unless this delay is in the range of few milliseconds. A comparison between three routing protocols and the OLSR with the new metric is done, by considering the End-to-End delay as the performance metric. The results show that the delay caused by the new metric is tolerable in comparison to the one caused by other routing protocols.

5.7.3 Mobility scenario comparison

This experiment shows the performance of the new metric in a mobility scenario. It also compares between the hop-count OLSR and SNR OLSR in term of throughput and delay. For this experiment the scenarios from section 5.3 are used to collect the results. SNR OLSR model from chapter 3 is used here for the comparison. The simulation is run for 100 minutes in real time.

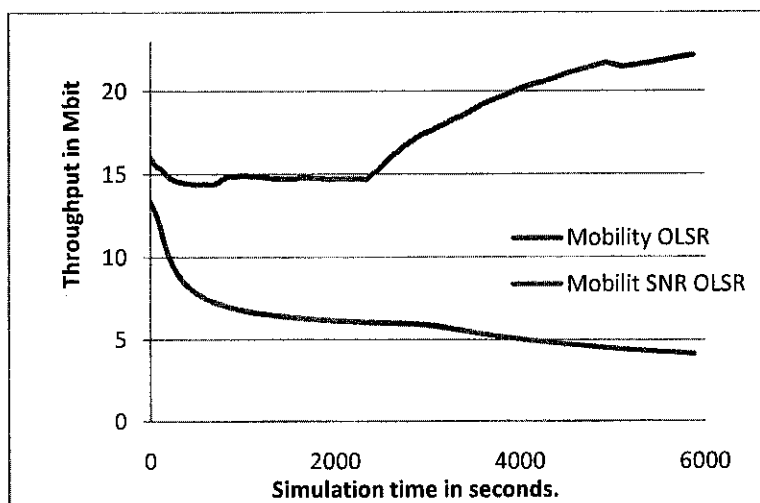


Figure 5.18: SNR vs. hop-count OLSR throughput) x-axis represents the real time in seconds and the y-axis represents the throughput in (Mb).

In Figure , it appears clearly that the SNR OLSR protocol improves the network throughput. In the original OLSR scenario the network throughput is decreased with both time and mobility. In contrast, the network is recording higher performance when the SNR OLSR protocol is used.

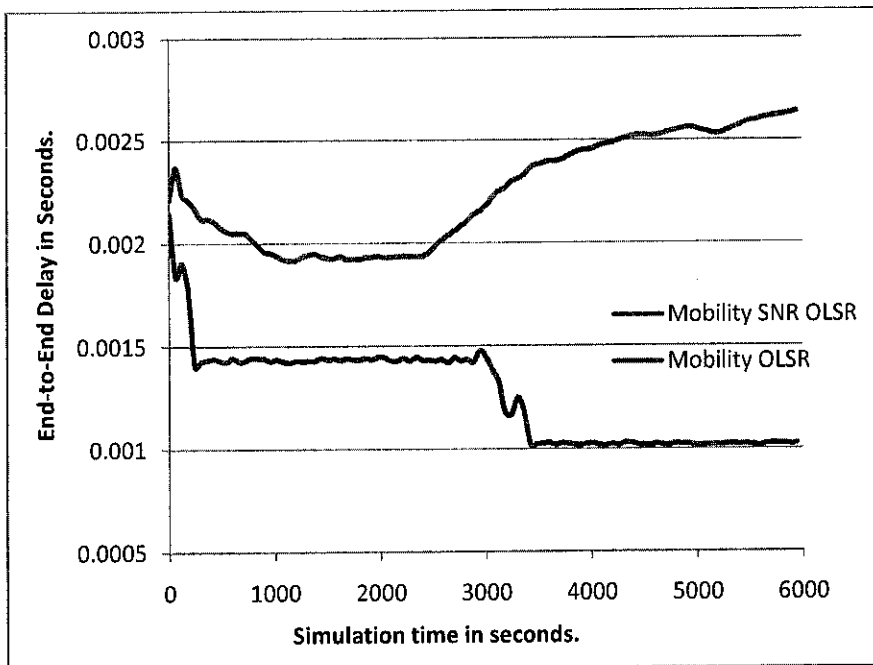


Figure 5.19: SNR vs. hop-count OLSR delay, x-axis represents the real time in second and y-axis represents the End-to-End delay in second.

In Figure , in contrast to the recorded delay in the low mobility scenarios, the SNR OLSR records the lowest End-to-End delay. The increase of mobility in the network causes the instability of the wireless link; this results in rapidly change in the transmission quality of nodes. Moreover, in the high mobility network a routing protocol that considers the link condition is expected to gain better performance than the traditional hop-count protocols. Figure depicts the obtained end-to-End delay for both the original and the modified

OLSR protocol in a high mobility scenario. Considering the collected results it can be said that, the SNR OLSR is suitable for the high mobility scenarios. Moreover, the OLSR performance is improved in both high and low mobility networks when SNR is used as a metric.

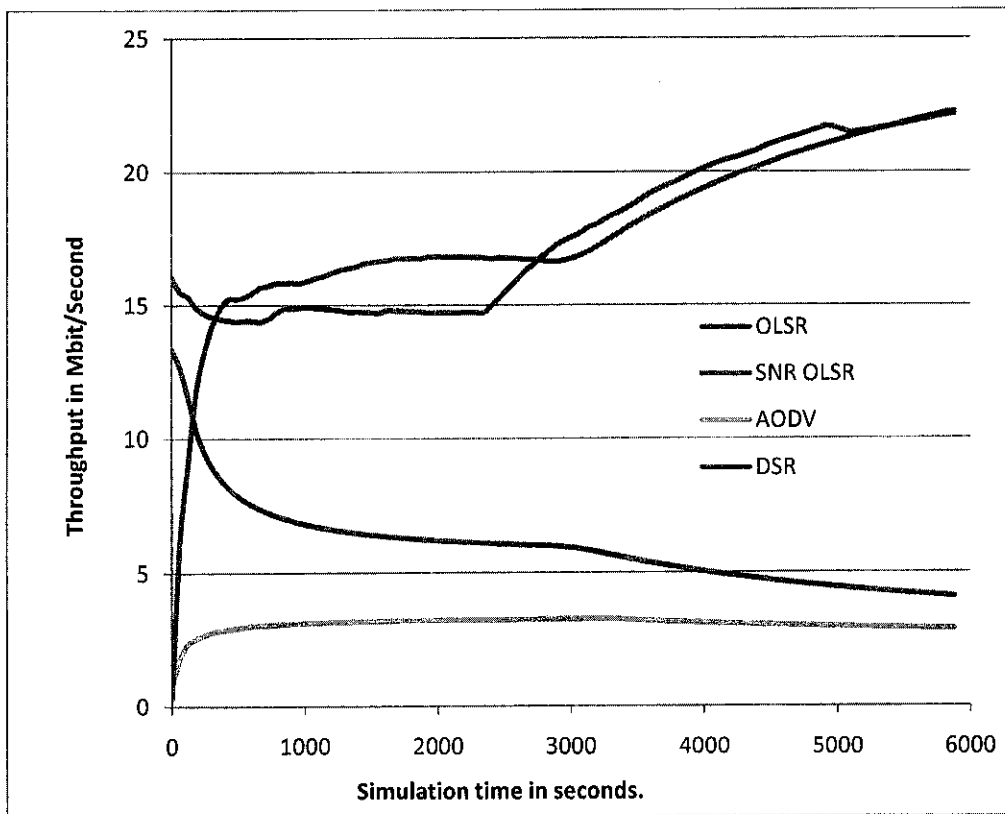


Figure 5.20: Three routing protocols vs. SNR OLSR throughput) x-axis represents the real time in seconds and the y-axis represents the throughput in (Mb).

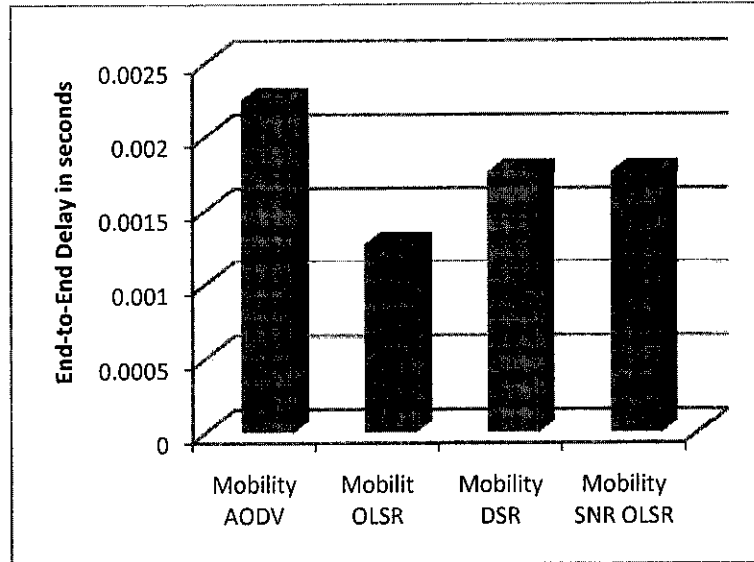


Figure 5.21: Three routing protocols vs. SNR OLSR delay, x-axis represents the routing protocols and y-axis represents the delay in seconds.

5.8 Nodes scenario

The nodes number is considered as a design parameter in the coming section, which is to study the effect of the new metric when it is applied to a large network. Two scenarios are applied per each routing protocol, and four routing protocols are deployed. The first scenario is deployed with 100 nodes while the second one with 1000 nodes. The simulation is run for 100 minutes. The results are collected and demonstrated in figures (5.22, 5.23, and 5.24).

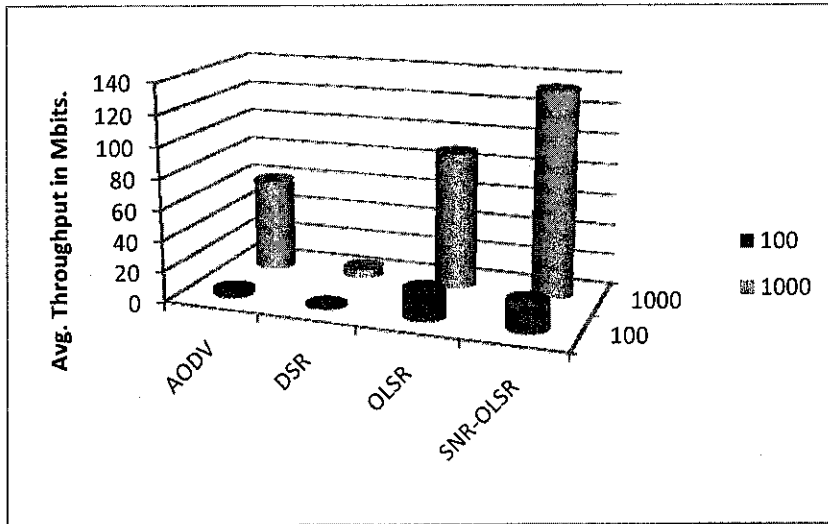


Figure 5.22: In the x-axis AODV, DSR, OLSR, and SNR-OLSR protocols are presented, y-axis represents the average throughput in Mbits, and the z-axis represents the number of nodes per simulation.

In figure 5.22 the results are presented in a three dimensions graph; the x dimension presents the routing protocols, and y dimension presents the average throughput in Mbits, while the z dimension presents the number of nodes.

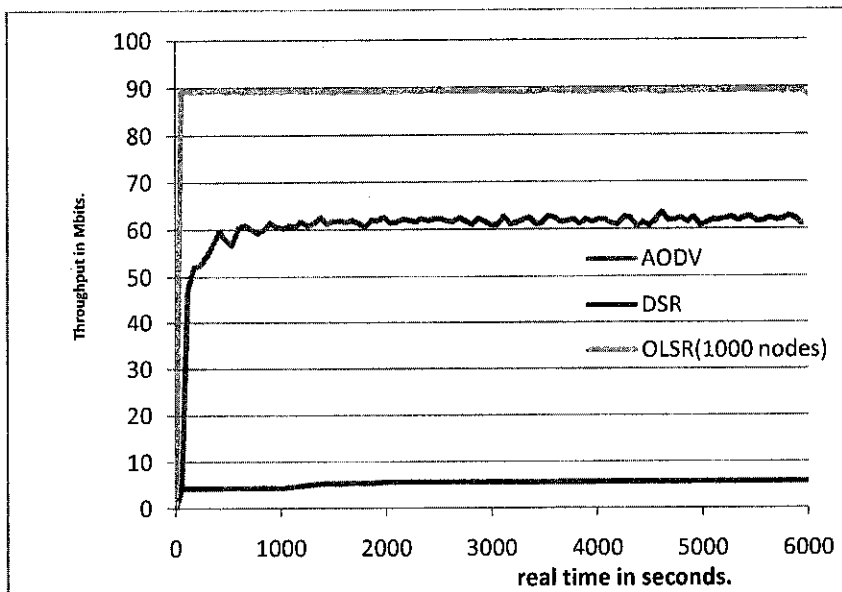


Figure 5.23: The 1000 nodes scenario, x-axis presents the real time in second, y-axis presents the throughput in Mbits.

In Figure 5.23 the x-axis represents the simulation time in seconds, and the y-axis represents the collected throughput for AODV, DSR, and OLSR routing protocols in the nodes scenario in Mbits. From the obtained result, it appears clearly that DSR has the lowest throughput among the other routing protocols, and OLSR has the highest throughput in this scenario. The low performance of DSR is due to the big number of nodes in the simulated network.

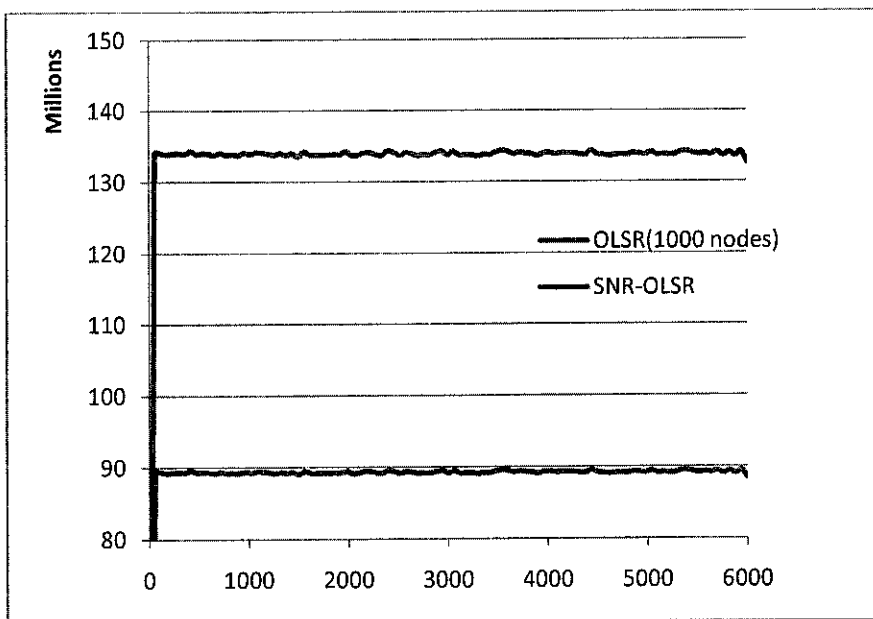


Figure 2.24: SNR-OLSR vs. OLSR throughput (1000nodes scenario), x-axis presents the real time in seconds, y-axis presents the throughput in Mbits.

In Figure 2.24 the new metric is presented against the original hop-count metric in term of throughput, in this figure the x-axis represents the real time in seconds and the y-axis presents the throughput in Mbits. The obtained results show a significant network throughput improvement when the SNR metric is used.

5.9 Summary

In this chapter the results of the simulation are presented. The first part of this chapter is giving the results of a simulation comparison between the performances of AODV, DSR, and OLSR protocols on WMNs. The performance is tested in two scenarios with different mobility. In this stage the results show that, OLSR protocol is getting the highest throughput and the lowest End-to-End delay among the selected protocols. Thus, we come with the fact that OLSR is the well suited protocol for the simulated scenarios (WMNs). However, OLSR is getting the highest performance among the selected protocols, but its still in need for a metric that consider the link condition. In the second part of this chapter SNR is proposed and implemented in the OLSR protocol. SNR is usually calculated in the physical layer of wireless node with no need for additional protocol overhead. In this part the new metric is deployed in the OLSR protocol, and the performance of the modified protocol is examined in two scenarios. Afterwards, the modified protocol is conducted in performance comparisons against the original protocol. The simulation results show that, the modified protocol is getting better performance than the original protocol, and the highest performance among the selected protocols. The last part of this chapter is giving the results from the mobility scenarios. The results show that, the amount of mobility is important factor to select the routing protocol in a network.

CHAPTER SIX: CONCLUSION AND FUTURE WORK

Designing a good routing protocol for Wireless Mesh Networks (WMNs) is an active research area. Currently researchers are considering the application of ad hoc network protocols for this new technology. However, most of these protocols find paths with minimum hop-count, which is not an efficient metric for WMNs. Most of the researches on WMNs are focused on finding the suitable metric that can cope well with the unpredictable behavior of wireless link in WMNs. In this thesis we have deployed a new metric signal to noise ratio (SNR) for WMNs which takes link quality into account for routing packets. This thesis presents the concepts of Wireless Networks followed by their characteristics. Considering these characteristics is important for designing a new protocol for WMNs. Afterwards we have given an overview of different routing metrics proposed for WMNs. We have also discussed three routing protocols (Ad-hoc on demand distant vector (AODV), Dynamic source routing (DSR) and optimized link state (OLSR)) with their major features such as route discovery and route maintenance. A comparison study of three routing protocols is also done, considering the result from this comparison, OLSR protocol is selected to deploy the new metric. The new metric is deployed in the OLSR protocol, and the performance of the modified protocol is examined in two scenarios. Afterwards, the modified protocol is conducted in performance comparisons against the original protocol.

The results show that, OLSR is gaining the highest throughput, and the lowest End-to-End delay among the compared protocols. However it does still need some modifications to cope well with the wireless link behavior. Many researches [6][9] are stated that, the

existing routing protocols are in need for a new metric which generates less protocol overhead and better defines the wireless link condition. The cross layer approach proposed here is to use the SNR that is generated in the physical layer in the routing protocol. The cross layer approach grants no additional protocol overhead is needed. Moreover, the SNR which is used as a routing metric is better describing the wireless link condition. The SNR is implemented in the OLSR routing protocol. A simulation comparison between the original OLSR with hop-count metric and the SNR metric is done. The obtained results show that, when SNR is used the OLSR gets the highest performance among the others routing protocols.

We have planned to enhance WMNs performance by using OLSR protocol with a new path selection metric (SNR). The simulation result shows that, using a link quality metric would improve the performance of OLSR on WMNs. After achieving this goal, The OLSR with the new metric will be fully functional for implementation in real world environments.

References

- [1] Y. Xiao and J. Rosdahl, "Throughput and Delay Limits of IEEE 802.11," in *IEEE Communications Letters*, Vol. 6, No. 8, August 2002.
- [2] M. Grossglauser and D. Tse, "Mobility Can Increase the Capacity of Ad-hoc Wireless Networks," in *proc. IEEE INFOCOM*, April 2001.
- [3] J. Li, C. Blake, D. S. J. Couto, H. I. Lee, R. Morris, "Capacity of Ad Hoc Wireless Networks," in *proc. ACM SIGMOBILE*, July 2001.
- [4] P. Gupta, and P. R. Kumar, "The Capacity of Wireless Networks," in *IEEE Transactions on Information Theory*, Vol. 46, No. 2, March 2000.
- [5] T. Ozugur, "Optimal MAC-Layer Fairness in 802.11 Networks," in *IEEE International Conference on Communications (ICC 2002)*, Vol. 2, 2002.
- [6] D. Qiao and K. G. Shin, "Achieving Efficient Channel Utilization and Weighted Fairness for Data Communications in IEEE 802.11 WLAN under the DCF," in *Tenth IEEE International Workshop on Quality of Service*, 2002.
- [7] C-K Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems*, Prentice Hall, 2002. ISBN 0-13-007817-4.
- [8] J. Schiller, *Mobile Communications*, Addison Wesley, 2000. ISBN 0-20-1398362
- [9] T. S. Rappaport, *Wireless Communications: Principles & Practice*, 2nd edition, Prentice Hall, 2001, ISBN 0-13-042232-0.
- [10] Y. C. Tay and K. C. Chua, "A Capacity Analysis for the IEEE 802.11 MAC Protocol," in *Wireless Networks 7*, Kluwer Academic Publishers, 2001.
- [11] Tanenbaum, *Computer Communications*, 4th edition, Prentice Hall, 2002. ISBN 0-13-066102-3.
- [12]
- [13] F. Cali, M. Conti and E. Gregori, "IEEE 802.11 wireless LAN: capacity analysis and protocol enhancement," in *Proc. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '98)*, Vol. 1, 1998
- [14] A. Banchs and X. Pérez, "Providing Throughput Guarantees in IEEE 802.11 Wireless LAN," in *IEEE Wireless Communications and Networking Conference (WCNC2002)*, Vol. 1, 2002.
- [15] A. Banchs, M. Radmirsch, and X. Pérez, "Assured and expedited forwarding extensions for IEEE 802.11 wireless LAN," in *Tenth IEEE International Workshop on Quality of Service*, 2002.
- [16] IEEE, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*. IEEE Std. 802.11, June, 1999.
- [17] IEEE, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification: High-Speed Physical Layer Extension in the 2.4 GHz Band*. IEEE Std. 802.11b, September 1999.
- [18] IEEE, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification: High-Speed Physical Layer in the 5 GHz Band*. IEEE Standard 802.11a, September 1999.
- [19] J. Jun, P. Peddabachagari and M. Sichertiu, "Theoretical Maximum Throughput of IEEE 802.11 and its Applications", submitted to *MOBISYS 2003*.

-
- [20] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," in *IEEE journal on selected areas in communications*, vol. 18, No.3, March 2000.
- [21] A. Banchs and X. Pérez, "Distributed weighted air queuing in 802.11 wireless LAN," in *IEEE International Conference on Communications (ICC)*, Vol. 5, 2002.
- [22] A. Banchs, X. Pérez, M. Radimirsch and H. J. Stuttgen, "Service differentiation extensions for elastic and real-time traffic in 802.11 wireless LAN," in *IEEE Workshop on High Performance Switching and Routing*, 2001.
- [23] [22] D. Beyer, "Fundamental Characteristics and Benefits of Wireless Routing ("Mesh") Networks," in *8th Annual WCA Technical Symposium*, January 2002.
- [24] J. C. Chen and J. M. Gilbert, "Measured Performance of 5-GHz 802.11a Wireless LAN Systems," <http://www.airvia.com/AtherosRangeCapacityPaper.pdf>.
- [25] M. Haenggi, "Probabilistic Analysis of a Simple MAC Scheme for Ad Hoc Wireless Networks (Short Paper)," in *IEEE Wireless Circuits and Systems Workshop, WCAS 2002*, Pasadena, CA, September 2002.
- [26] A. Woo, D. E. Culler, "A transmission control scheme for media access in sensor networks," in *proc. ACM MOBICOM*, July 2001.
- [27] M. Gastpar and M. Vetterli, "On the Capacity of Wireless Networks: The Relay Case," in *proc. IEEE INFOCOM*, 2002.
- [28] T. Nandagopal, T. Kim, X. Gao and V. Bharghavan, "Achieving MAC Layer Fairness in Wireless Packet Networks," in *proc. ACM MOBICOM*, 2000.
- [29] S. Mangold, S. Choi, P. May, O. Klein, G. Hiertz and L. Stibor, "IEEE 802.11e Wireless LAN for Quality of Service," in *proc. European Wireless*, 2002.
- [30] A. Lindgren, A. Almquist and O. Schelen, "Evaluation of Quality of Service Schemes for IEEE 802.11 Wireless LANs," in *proc. 26th Annual IEEE Conference on LCN*, 2001.
- [31] Y. Bejerano, "Efficient Integration of Multi-hop Wireless and Wired Networks with QoS Constraints," in *proc. ACM MOBICOM*, September 2002.
- [32] Y. Kishi, S. Konishi, S. Nanba and S. Nomoto, "A Proposal of Millimeter-wave Multi-hop Mesh Wireless Network Architecture with Adaptive Network Control Features for Broadband Fixed Wireless Access," in *proc. IEEE RAWCON*, 2001.
- [33] T. Shimomura, M. Iwanaga, K. Tsukamoto and S. Komaki, "Theoretical Capacity Investigation of Quasi-mm/mm Wave Mesh-type Wireless Entrance Network for FWA System," in *proc. Asia-Pacific Microwave Conference*, 2000.
- [34] [33] P. Whitehead, "Mesh networks: a new architecture for broadband wireless access systems," in *proc. IEEE RAWCON*, 2000.
- [35] [34] Nokia Corp., "Wireless Broadband Access: Nokia RoofTop," <http://www.nwr.nokia.com/>
- [36] MeshNetworks Inc., "Scalable Peer-to-Peer Networking Technology for Mobile Broadband Networks," <http://www.meshnetworks.com/>
- [37] Radiant Networks, "Meshworks," <http://www.radiantnetworks.com/>

-
- [38] Ricochet Networks Inc., “Micro Cellular Data Network,”
<http://www.ricochet.com/>
- [39] FHP Wireless Inc., “Intelligent Wi-Fi Infrastructure,”
<http://www.fhpwireless.com/>
- [40] Aerial Networks, “The 802.11b Mesh Access Point Network,”
<http://www.aerialbroadband.com/>

Appendixes

Appendix 1: The SNR-Based OLSR Protocol Code

```
static int
moh ()
{
    Packet*          pkptr;
    double          snr;
    int             snr_weight;
    FIN (moh(void));
    pkptr = (Packet*) op_pro_argmem_access ();
    snr=op_td_get_dbl(pkptr,OPC_TDA_RA_SNR);
    if(snr<20)
        snr_weight=0;
    else if(snr<30)
        snr_weight=1;
    else if(snr<40)
        snr_weight=2;
    else if(snr<50)
        snr_weight=3;
    else if(snr<60)
        snr_weight=4;
    else if(snr<70)
        snr_weight=5;
    else if(snr<80)
        snr_weight=6;
    else if(snr<100)
```

```
        snr_weight=7;

        FRET(snr_weight);
    }

static void
olsr_rte_pkt_arrival_handle (void)
{
    Packet*          pkptr;
    Ici*             ici_ptr = OPC_NIL;
    OlsrT_Message*  olsr_message_ptr;
    Boolean          do_not_process = OPC_FALSE;
    Boolean          discard_tc = OPC_FALSE;
    InetT_Address*  inet_local_intf_addr_ptr;
    InetT_Address*  inet_ip_src_addr_ptr;
    InetT_Address   inet_local_intf_addr;
    InetT_Address   inet_ip_src_addr;
    int             local_intf_addr, ip_src_addr;
    char            addr_str [256];
    OlsrT_Duplicate_Set_Entry*  dup_set_entry_ptr = OPC_NIL;
    OlsrT_Neighbor_Set_Entry*   nbr_set_entry_ptr = OPC_NIL;
    char            tmp_str [256];
    char            node_name [256];
    InetT_Address   inet_tmp_addr;
    IpT_Addr_Status is_local_ip_duplicate;
    IpT_Addr_Status is_remote_ip_duplicate;

    /** Whenever a control packet arrives at the**/
```

```

/** port where OLSR process is listening, **/

/** this process is invoked **/

/** A packet has arrived. Handle the packet **/

/** appropriately based on its type **/
FIN (olsr_rte_pkt_arrival_handle (void));

/* The process was invoked by the parent */
/* MANET_RTE_MGR process indicating the arrival*/
/* of a packet. The packet is OLSR control */
/* packet. Process depending upon the MESSAGE */
/* type. */

pkptr = (Packet*) op_pro_argmem_access ();

/* Obtain the interface address and ip source address from the installed ICI.*/
ici_ptr = op_intrpt_ici ();

op_ici_attr_get (ici_ptr, "interface received", &inet_local_intf_addr_ptr);
op_ici_attr_get (ici_ptr, "rem_addr", &inet_ip_src_addr_ptr);

/* Currently, we support only one message */
/* type in each OLSR control packet. */

/* Get the OLSR Message */
op_pk_nfd_access (pkptr, "Message", &olsr_message_ptr);

if ((LTRACE_ACTIVE) ||
    (op_prg_odb_ltrace_active ("trace_hello") == OPC_TRUE) ||

```

```

(op_prg_odb_ltrace_active ("trace_tc")== OPC_TRUE))
{
if (olsr_message_ptr->message_type == OLSRC_HELLO_MESSAGE)
    op_prg_odb_print_major (pid_string, "\nReceived HELLO message \n",
OPC_NIL);

else if (olsr_message_ptr->message_type == OLSRC_TC_MESSAGE)
    op_prg_odb_print_major (pid_string, "\nReceived TC message \n", OPC_NIL);
}

/* Update the statistics for the routing traffic received */
olsr_support_routing_traffic_received_stats_update (local_stat_handle_ptr,
global_stat_handle_ptr, pkptr);

/* Discard the packet if it carries an IP family different than */
/* the IP family of this OLSR process (e.g. if the packet is */
/* OLSR IPv6, when this process is OLSR IPv4.) */
if (is_ipv6_enabled != olsr_message_ptr->is_ipv6)
{
op_pk_destroy (pkptr);
inet_address_destroy_dynamic (inet_local_intf_addr_ptr);
inet_address_destroy_dynamic (inet_ip_src_addr_ptr);

if ((LTRACE_ACTIVE)||
(op_prg_odb_ltrace_active ("trace_hello")== OPC_TRUE) ||
(op_prg_odb_ltrace_active ("trace_tc")== OPC_TRUE))
{
printf ("Received a packet of different IP address family. Destroy it \n");
}
}

```

```
FOUT;
}

/* Discard the packet if its a loopback i.e. i received my own packet */
/* Discard the packet if TTL has reached zero */
if (olsr_message_ptr->originator_addr == own_main_address)
{
    op_pk_destroy (pkptr);
    inet_address_destroy_dynamic (inet_local_intf_addr_ptr);
    inet_address_destroy_dynamic (inet_ip_src_addr_ptr);

    if((LTRACE_ACTIVE)||
        (op_prg_odb_ltrace_active ("trace_hello")== OPC_TRUE) ||
        (op_prg_odb_ltrace_active ("trace_tc")== OPC_TRUE))
    {
        printf ("Received my own packet. Destroy it \n");
    }

    FOUT;
}

if (olsr_message_ptr->tll == 0)
{
    op_pk_destroy (pkptr);
    inet_address_destroy_dynamic (inet_local_intf_addr_ptr);
    inet_address_destroy_dynamic (inet_ip_src_addr_ptr);
```

```
if ((LTRACE_ACTIVE) ||
    (op_prg_oddb_ltrace_active ("trace_hello") == OPC_TRUE) ||
    (op_prg_oddb_ltrace_active ("trace_tc") == OPC_TRUE))
    {
        printf ("TTL reached zero. Destroy it \n");
    }

FOUT;
}

/* Check if this packet has been processed earlier */
/* Get the duplicate set entry, if it exists */
sprintf (addr_str, "%d %d", olsr_message_ptr->originator_addr, olsr_message_ptr-
>message_seq_num);
dup_set_entry_ptr = (OlsrT_Duplicate_Set_Entry*)
    prg_string_hash_table_item_get (duplicate_set_table, addr_str);

if (dup_set_entry_ptr != OPC_NIL)
    do_not_process = OPC_TRUE;

/* Get the InetT_Address from pointers */
inet_local_intf_addr = *inet_local_intf_addr_ptr;
inet_ip_src_addr = *inet_ip_src_addr_ptr;

/* Convert this InetT_Address to NATO index */
local_intf_addr = inet_rtab_unique_addr_convert (inet_local_intf_addr, &is_local_ip_duplicate);
ip_src_addr = inet_rtab_unique_addr_convert (inet_ip_src_addr, &is_remote_ip_duplicate);
```

```
/* Free the memory occupied by these addresses in the ICI */
inet_address_destroy_dynamic (inet_local_intf_addr_ptr);
inet_address_destroy_dynamic (inet_ip_src_addr_ptr);

/* If this Hello packet has the source or destination IP as duplicate */
/* addresses, do not process the packet. It will be discarded. By */
/* ignoring such hello packets, we are preventing link set entries */
/* with duplicate addresses from entering OLSR. This is not specified */
/* by the RFC, it is part of this OLSR implementation protection */
/* against misconfiguration.
    */
if ((is_local_ip_duplicate == IPC_ADDR_STATUS_DUPLICATE) ||
    (is_remote_ip_duplicate == IPC_ADDR_STATUS_DUPLICATE))
{
    op_pk_destroy (pkptr);

    if ((LTRACE_ACTIVE) ||
        (op_prg_odb_ltrace_active ("trace_hello") == OPC_TRUE) ||
        (op_prg_odb_ltrace_active ("trace_tc") == OPC_TRUE))
    {
        printf ("Check network for duplicate IP addresses. Destroying the packet\n");
    }

    FOUT;
}

/* This packet was not processed before */
if (do_not_process == OPC_FALSE)
```



```
{
/* Process the message according to msg_type */

switch (olsr_message_ptr->message_type)
{

case (OLSRC_HELLO_MESSAGE):
{
if (LTRACE_ACTIVE || (op_prg_oddb_ltrace_active ("trace_hello")==
OPC_TRUE))
{
inet_address_print (tmp_str, inet_ip_src_addr);
printf ("Processing HELLO received from: %s ", tmp_str);
inet_address_to_hname (inet_ip_src_addr, tmp_str);
printf ("%s\n", tmp_str);
}

/* Process the Hello Message */
olsr_rte_process_hello (olsr_message_ptr, ip_src_addr,
local_intf_addr);

/* Check if either neighborhood or topology has changed */
olsr_rte_neighborhood_topology_check ();

/* Hello message is not considered for forwarding */
/* Hence, destroy the message after processing */
op_pk_destroy (pkptr);
```

```
        /* Exit this function */
        FOUT;
    }

    case (OLSRC_TC_MESSAGE):
    {
        if (LTRACE_ACTIVE || (op_prg_odb_ltrace_active ("trace_tc")==
OPC_TRUE))
        {
            inet_address_print (tmp_str, inet_ip_src_addr);
            inet_address_to_hname (inet_ip_src_addr, node_name);
            printf ("Processing TC received from: %s (%s)\n", tmp_str,
node_name);

            inet_tmp_addr = inet_rtab_index_to_addr_convert
(olsr_message_ptr->originator_addr);
            inet_address_print (tmp_str, inet_tmp_addr);
            inet_address_to_hname (inet_tmp_addr, node_name);
            printf ("TC originator address %s (%s)\n", tmp_str,
node_name);
        }

        /* Process the TC message */
        discard_tc = olsr_rte_process_TC (olsr_message_ptr, ip_src_addr);

        /* Check if either neighborhood or topology has changed */
        olsr_rte_neighborhood_topology_check ();
    }
}
```

```
/* This TC is to be discarded */
/* It can be due to : */
/* 1. Heard from Non-Sym nbr */
/* 2. Out of order TC mesg */
if (discard_tc == OPC_TRUE)
{
    if ((op_prg_odb_ltrace_active ("trace_tc") == OPC_TRUE))
    {
        printf ("Discarding this TC \n");
    }

    /* This TC message will not be considered for */
    /* forwarding. Hence, destroy this TC packet */
    op_pk_destroy (pkptr);

    /* Exit the function */
    FOUT;
}

break;
}

default:
{
    /* Invalid message type */
    olsr_rte_error ("Invalid Message Type in OLSR packet", OPC_NIL,
OPC_NIL);
}
```

```

        }

    /*end if do_not_process*/

else

    {

    /* This else part just prints tracing information.

    */

    /* Only TC messages add duplicate set entries, hence for HELLO msg, */
    /* do_not_process will never be True. We'll reach here when this */
    /* TC message was already processed. Now consider it for forwarding.*/
    /* Do not destroy this packet yet as forwarding condition needs to */
    /* be checked.

    */

    if((LTRACE_ACTIVE)||
    (op_prg_odb_ltrace_active("trace_hello")== OPC_TRUE) ||
    (op_prg_odb_ltrace_active("trace_tc")== OPC_TRUE))
    {
        printf("Message has already been processed (or it involves duplicate IP
addresses). Do not process\n");
    }
    }

/* Check if this TC was already forwarded */
if(((dup_set_entry_ptr != OPC_NIL) &&
    (dup_set_entry_ptr->rexmitted == OPC_TRUE))
    {
    /* This TC has already been considered for forwarding */
    if(op_prg_odb_ltrace_active("trace_tc"))

```

```
        printf("This TC has already been considered for forwarding, Discarding TC
\n");

        /* Discard the packet */
        op_pk_destroy (pkptr);

        /* Exit the function */
        FOUT;
    }
else
    {
        /* Either no duplicate entry exists or this TC was not fwded*/
        /* Candidate for forwarding, check if the condition matches */
        /* Check if the source address is in my MPR selector list      */
        if (olsr_rte_forward_packet (olsr_message_ptr, ip_src_addr) == OPC_TRUE)
            {
                if (op_prg_oddb_ltrace_active ("trace_tc"))
                    printf ("Forwarding (Re-broadcasting) this TC message \n");

                /* Add entry in dup table set */
                olsr_rte_duplicate_set_entry_add
                    (olsr_message_ptr->originator_addr,olsr_message_ptr-
>message_seq_num, OPC_TRUE);

                /* Update the number of TC messages forwarded statistic      */
                op_stat_write (local_stat_handle_ptr->total_tc_forwarded_shandle, 1.0);
                op_stat_write (global_stat_handle_ptr->total_tc_forwarded_global_shandle,
1.0);
```

```
        /* Update the tc traffic sent in bits per second */
        op_stat_write (global_stat_handle_ptr->tc_traffic_sent_bps_global_handle,
op_pk_total_size_get (pkptr));
        op_stat_write (global_stat_handle_ptr->tc_traffic_sent_bps_global_handle, 0.0);

        /* Forward this TC Message */
        olsr_rte_pkt_send (pkptr, (is_ipv6_enabled?
InetI_Ipv6_All_Nodes_LL_Mcast_Addr: InetI_Broadcast_v4_Addr), OPC_TRUE);
    }
else
    {
        if (op_prg_odb_ltrace_active ("trace_tc"))
            printf ("The node is not an MPR to forward this TC, Discarding TC
\n");

        /* Update the duplicate set entry for this TC */

        op_pk_destroy (pkptr);
    }
}
FOUT;
}
```

Appendix 2: The SNR-Based OLSR Protocol Block Diagram

