



**UNIVERSITI TEKNOLOGI MARA**

**Analysis of Gray Hole attack On MANETs Using  
different MANET Routing Protocols**

**Yashar AzabDaftari**

Dissertation submitted in fulfillment of the requirements

For the degree of

**Master of Science in Computer Network (Course Work)**

**FACULTY OF INFORMATION TECHNOLOGY AND  
QUANTITATIVE SCIENCES**

**April 2011**

## **ABSTRACT**

According to recent technological advance in the electronic and wireless telecommunications, the performance and use of wireless technologies has increased tremendously. One such field, concerns mobile ad hoc networks (MANETs) in which mobile nodes organize themselves in a network without the help of any predefined infrastructure.

The dynamic topology of MANETs allows nodes to join and leave the network at any point of time. This generic characteristic of MANET has rendered it vulnerable to security attacks.

Securing MANETs is an important part of deploying and utilizing them, since they are often used in critical applications where data and communications integrity is important.

However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes.

This study tries to compare of gray hole attack with two different routing protocols which called Ad-hoc on-demand Distance Vector (AODV) and Optimized Link State Routing Protocol (OLSR). Moreover simulate the behavior of these two protocols to show end to end delay packet loss and performance of the routings.

## **ACKNOWLEDGEMENT**

In the name of ALLAH who has always blessed me, support and help me during my studying Master.

Words are inadequate to dedicate my thanks to my supervisor, Dr. Adnan, his breadth of knowledge, vision for the future, and his enthusiasm towards research has been an inspiration to me and his encouragement that cause me work in this field.

I would like to express my gratitude and heartiest thanks to my beloved parents for their blessings, affection, understanding, and support me.

Finally, yet importantly, I would like to thank to my lovely wife for their help and supports for the successful completion of this project.

# Table of Contents

Declaration	i
Abstract	ii
Acknowledgement	iii
Table of Contents	iv
List of Tables	vii
List of Figures	viii
CHAPTER 1 Introduction	1
1.1 Research Background	1
1.2 Problem statement	3
1.3 Objective	3
1.4 Scope of Study	4
1.5 Research Question	4
1.6 Significant of Study	4
1.7 Overview of Thesis	4
CHAPTER 2 Literature Review	6
2.1 Introduction	6
2.2 Routing In MANETs	7
2.2.1 Table-Driven routing protocols (Proactive)	8
2.2.2 On Demand routing protocols (Reactive)	9
2.3 Ad hoc On-Demand Distance Vector Routing (AODV)	10
2.3.1 Technical description	10
2.4 Optimized Link State Routing Protocol (OLSR)	11
2.4.1 Multi Point Relaying (MPR)	12
2.4.2 Message	13
2.5 Security Issues for MANETs	14
2.5.1 Classification of attacks	14
2.5.1.1 External and Internal Attack	14
2.5.1.2 Active and Passive Attack	15
2.5.2 Attack Types	16
2.5.2.1 Passive Eavesdropping	16
2.5.2.2 Selective Existence (Selfish Nodes)	17

# CHAPTER 1

## INTRODUCTION

This chapter begins with a research background that gives an overview of the study. It is based on the problem statement, research question, objectives, scope, significance of study and overview of thesis that are discussed in sections 1.2, 1.3, 1.4, 1.5, 1.6, 1.7. This chapter also represents its scope as well as the structure of the thesis, chapter by chapter. It also explains the MANET network and gray hole attack. Eventually, this chapter concludes with an organization of the thesis.

### 1.1 Research Background

A MANET, sometimes called a mobile mesh network, is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.

The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

Control of the way of routing packet between devices in a network could be divided in some types pro-active which called a table-driven routing or reactive which called on-demand routing protocols.

The proactive protocols are keep the information of routing and update the routing tables to all possible destinations upon periodic exchanges, even if no traffic goes through. And the reactive protocols update routing tables only for the destination that has traffic going through in order to on-demand route finds (Hamma and Eddy, 2006).