COMPARATIVE STUDY OF MULTIPLE BLACK HOLE ATTACKS
SOLUTION METHODS IN MANET USING AODV ROUTING PROTOCOL

ELAHE FAZELDEHKORDI

A thesis submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JANUARY 2014
This thesis is dedicated to my beloved parents for their endless support and encouragement.
ACKNOWLEDGEMENT

First and foremost, I would like to sincerely thank my lovely parents, Behjat Kazemi and Manouchehr Fazel, my lovely brothers Peyman Fazel, Amin Fazel and Pouya Fazel, my best friend Akanbi Oluwatobi Ayodeji and all friends for their endless love, support and encouragement. I could not have done it without you! There is no word I can find to thank you.

Next, I would like to express my heartfelt gratitude to my supervisor Prof. Dr. Abdul Hanan Abdullah and Mr. Adnan Ahmed for their constant support during this project. They inspired me greatly to work in this project. Their willingness to motivate me contributed tremendously to the success of this project. I have learned a lot from them and I could not have imagined having a better advisor and mentor for my Master study. Many thanks to all my lecturers, I will forever be grateful.

Besides, I would like to thank my examiners: Dr. Mohammad Abdur Razzaque, and Dr. Ismail Fauzi Bin Isnin for their patience and insightful comments.

Finally, I would like to thank Universiti Teknologi Malaysia for their kind cooperation.
ABSTRACT

Mobile Wireless Ad Hoc Networks (MANET) are non-centralized wireless networks that can be formulated without the need for any pre-existing infrastructure in which each node can act as a router. It must discover its local neighbours and through them it will communicate to nodes that are out of its transmission range. Various features like open medium, dynamic topology, lack of clear lines of defence, makes MANET vulnerable to security attacks. Ad hoc On-demand Distance Vector routing (AODV) is one of the best and popular routing algorithms. AODV is severely affected by well-known black hole attack in which a malicious node injects a faked route reply message that it has a fresh route to destination. In this thesis, MANET performance against single black hole attack has compared with its performance against multiple black hole attacks by using Intrusion Detection System (IDSAODV) routing protocol (Dokurer, 2006). The result are analysed using NS-2.35, through various network parameter bases: total drop packets, end to end delay, packet delivery ratio and routing request overhead. The results indicate IDSAODV solution method which is presented for single black hole attack before, can be used effectively for decreasing total drop packets and improving packet delivery ratio against multiple black hole attacks, also. But, the method doesn’t have significant effect for improving end to end delay and routing request overhead.
ABSTRAK

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEDICATION</td>
<td></td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td></td>
<td>iv</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td></td>
<td>vi</td>
</tr>
<tr>
<td>TABLE OF CONTENT</td>
<td></td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td></td>
<td>xi</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td></td>
<td>xii</td>
</tr>
<tr>
<td>LIST OF APPENDICES</td>
<td></td>
<td>xv</td>
</tr>
</tbody>
</table>

1 INTRODUCTION

1.1 Introduction 1
1.2 Problem Background 2
1.3 Problem Statement 4
1.4 Purpose of Study 4
1.5 Project Objectives 5
1.6 Scope of Study 5
1.7 The Significant of Study 6
1.8 Organization of Report 7

2 LITERATURE REVIEW

2.1 Introduction 8
2.2 Wireless Networks 9
2.2.1 Classification of Wireless Networks 10
  2.2.1.1 Infrastructure Networks 10
  2.2.1.2 Infrastructure-less Networks 11
  2.2.2 Advantages of Wireless Networks 11
  2.2.3 Disadvantages of Wireless Networks 12

2.3 Ad-Hoc Networks 12
  2.3.1 Static Ad-Hoc Networks 14
  2.3.2 Mobile Ad-Hoc Networks 15
    2.3.2.1 Characteristics of MANET 18
    2.3.2.2 Applications of MANET 19
    2.3.2.3 Advantages of MANET 20
    2.3.2.4 Limitation of MANET 20

2.4 Routing 21

2.5 Ad Hoc Network Routing Protocols 21
  2.5.1 Classification of Routing Protocols 22

2.6 AODV Routing Protocol 27
  2.6.1 Routing in AODV 28
    2.6.1.1 Route Discovery Mechanism in AODV 30
    2.6.1.2 Route Maintenance Mechanism in AODV 31
  2.6.2 Characteristics of AODV 31
  2.6.3 Advantage and Disadvantage of AODV 32

2.7 Classifications of MANET Attacks 33

2.8 Black Hole Attack 40

2.9 Related Studies 41

2.10 Studied Solutions 45

2.11 IDSAODV 45

2.12 Evaluation Metrics 46

2.13 Summary 47
### 3 RESEARCH METHODOLOGY

3.1 Introduction 48

3.2 Research Framework 48

3.2.1 Phase 1: Investigating the Existing Solutions 51

3.2.2 Phase 2 51

3.2.2.1 Phase 2a: Determining Efficient Solution 51

3.2.2.2 Phase 2b: Implementing the Existed Solution 51

3.2.2.2.1 Simulation: The Formal Definition 52

3.2.2.2.2 NS (Network Simulator) 52

3.2.2.2.3 Tcl Language in NS 54

3.2.3 Phase 3: Comparing the Effects of Proposed Solution on MANET Performance 55

3.3 Summary 55

### 4 INVESTIGATION AND SELECTION PROCEDURE

4.1 Introduction 56

4.2 Implementing a New Routing Protocol in NS to Simulate Black Hole Behavior 56

4.3 Testing the Black Hole AODV 61

4.3.1 Simulation Parameters and Measured Metrics 61

4.3.2 Evaluation of the Simulation 62

4.4 Simulation of Black Hole Attack 66

4.4.1 Simulation Parameters and Measured Metrics 66

4.4.2 Examining the Trace File and Getting the Results 71

4.4.3 Evaluation of Results 72

4.5 Summary 77

### 5 SOLUTION IMPLEMENTATION AND RESULT
5.1 Introduction 78
5.2 An Overview of Investigation 78
5.3 Implementing the Solution in NS-2 79
5.4 Testing the IDSAODV 82
5.5 Simulation of IDSAODV and Evaluation of Results 83
5.6 Summary 91

6 CONCLUSION AND FUTURE WORK
6.1 Overview 92
6.2 Contribution 93
6.3 Future Work 93

REFERENCES 94
Appendices A - C 99-110
# LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Layered attacks</td>
<td>37</td>
</tr>
<tr>
<td>2.2</td>
<td>Related studies</td>
<td>42</td>
</tr>
<tr>
<td>4.1</td>
<td>Total drop packets comparison</td>
<td>73</td>
</tr>
<tr>
<td>4.2</td>
<td>End to end delay comparison</td>
<td>74</td>
</tr>
<tr>
<td>4.3</td>
<td>Routing overhead comparison</td>
<td>75</td>
</tr>
<tr>
<td>4.4</td>
<td>Packet delivery ratio comparison</td>
<td>76</td>
</tr>
<tr>
<td>5.1</td>
<td>Total drop packets comparison</td>
<td>83</td>
</tr>
<tr>
<td>5.2</td>
<td>Total drop packets comparison</td>
<td>84</td>
</tr>
<tr>
<td>5.3</td>
<td>End to end delay comparison</td>
<td>85</td>
</tr>
<tr>
<td>5.4</td>
<td>End to end delay comparison</td>
<td>86</td>
</tr>
<tr>
<td>5.5</td>
<td>Routing overhead comparison</td>
<td>87</td>
</tr>
<tr>
<td>5.6</td>
<td>Routing overhead comparison</td>
<td>88</td>
</tr>
<tr>
<td>5.7</td>
<td>Packet delivery ratio comparison</td>
<td>89</td>
</tr>
<tr>
<td>5.8</td>
<td>Packet delivery ratio comparison</td>
<td>90</td>
</tr>
</tbody>
</table>
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Infrastructure based network</td>
<td>10</td>
</tr>
<tr>
<td>2.2</td>
<td>Infrastructure-less network</td>
<td>11</td>
</tr>
<tr>
<td>2.3</td>
<td>Simple ad hoc network</td>
<td>13</td>
</tr>
<tr>
<td>2.4</td>
<td>Mobile ad-hoc network</td>
<td>16</td>
</tr>
<tr>
<td>2.5</td>
<td>MANET routing protocols</td>
<td>23</td>
</tr>
<tr>
<td>2.6</td>
<td>Another classification of MANET routing protocols</td>
<td>27</td>
</tr>
<tr>
<td>2.7</td>
<td>AODV mechanisms</td>
<td>29</td>
</tr>
<tr>
<td>2.8</td>
<td>Flooding RREQ in AODV</td>
<td>29</td>
</tr>
<tr>
<td>2.9</td>
<td>Route reply in AODV</td>
<td>29</td>
</tr>
<tr>
<td>2.10</td>
<td>Classification of MANET attacks</td>
<td>34</td>
</tr>
<tr>
<td>2.11</td>
<td>Different types of attacks on MANET</td>
<td>40</td>
</tr>
<tr>
<td>2.12</td>
<td>Black hole attack</td>
<td>41</td>
</tr>
<tr>
<td>3.1</td>
<td>Research framework</td>
<td>50</td>
</tr>
<tr>
<td>3.2</td>
<td>NS-2 schema</td>
<td>54</td>
</tr>
<tr>
<td>4.1</td>
<td>“blackholeaodv” protocol agent is added in “tcl\lib\ns-lib.tcl”</td>
<td>58</td>
</tr>
<tr>
<td>4.2</td>
<td>Addition to the “\makefile”</td>
<td>58</td>
</tr>
<tr>
<td>4.3</td>
<td>“If” statement for dropping or accepting the packets</td>
<td>59</td>
</tr>
<tr>
<td>4.4</td>
<td>Case statement for choosing the AODV control message types</td>
<td>60</td>
</tr>
<tr>
<td>4.5</td>
<td>False RREP message of black hole attack</td>
<td>61</td>
</tr>
<tr>
<td>4.6</td>
<td>Data flow between node 0 and node 4 via node 1 with 6 mobility nodes</td>
<td>63</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>4.7</td>
<td>Data flow between node 0 and node 4 via node 3 after mobility</td>
<td></td>
</tr>
<tr>
<td>4.8</td>
<td>Data flow between node 0 and node 4 via nodes 13, 12 and 6 with 20 mobility nodes</td>
<td></td>
</tr>
<tr>
<td>4.9</td>
<td>Data flow between node 0 and node 4 via nodes 8, 17, 11 and 2 after mobility</td>
<td></td>
</tr>
<tr>
<td>4.10</td>
<td>Data flow between node 0 and node 4 via nodes 18, 2 and 12 with 30 mobility nodes</td>
<td></td>
</tr>
<tr>
<td>4.11</td>
<td>Data flow between node 0 and node 4 via nodes 5, 28 and 10 after mobility</td>
<td></td>
</tr>
<tr>
<td>4.12</td>
<td>The statements for creating mobile nodes</td>
<td></td>
</tr>
<tr>
<td>4.13</td>
<td>Mobile node configurations</td>
<td></td>
</tr>
<tr>
<td>4.14</td>
<td>Node 5 (black hole node) attracts the connection between nodes 0 and 3</td>
<td></td>
</tr>
<tr>
<td>4.15</td>
<td>Node 19 (black hole node) attracts the connection between nodes 0 and 4</td>
<td></td>
</tr>
<tr>
<td>4.16</td>
<td>Node 29 (black hole node) attracts the connection between nodes 0 and 4</td>
<td></td>
</tr>
<tr>
<td>4.17</td>
<td>Total drop packets comparison</td>
<td></td>
</tr>
<tr>
<td>4.18</td>
<td>End to end delay comparison</td>
<td></td>
</tr>
<tr>
<td>4.19</td>
<td>Routing overhead comparison</td>
<td></td>
</tr>
<tr>
<td>4.20</td>
<td>Packet delivery ratio comparison</td>
<td></td>
</tr>
<tr>
<td>5.1</td>
<td>RREP caching mechanism</td>
<td></td>
</tr>
<tr>
<td>5.2</td>
<td>Receive RREP function of the IDSAODV</td>
<td></td>
</tr>
<tr>
<td>5.3</td>
<td>CBR packet are reached to destination node properly</td>
<td></td>
</tr>
<tr>
<td>5.4</td>
<td>Total drop packets comparison</td>
<td></td>
</tr>
<tr>
<td>5.5</td>
<td>Total drop packets comparison</td>
<td></td>
</tr>
<tr>
<td>5.6</td>
<td>End to end delay comparison</td>
<td></td>
</tr>
<tr>
<td>5.7</td>
<td>End to end delay comparison</td>
<td></td>
</tr>
<tr>
<td>5.8</td>
<td>Routing overhead comparison</td>
<td></td>
</tr>
<tr>
<td>5.9</td>
<td>Routing overhead comparison</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Value</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>5.10</td>
<td>Packet delivery ratio comparison</td>
<td>90</td>
</tr>
<tr>
<td>5.11</td>
<td>Packet delivery ratio comparison</td>
<td>91</td>
</tr>
</tbody>
</table>
# LIST OF APPENDICES

<table>
<thead>
<tr>
<th>APPENDIX</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Blackholeadv TCL file</td>
<td>99</td>
</tr>
<tr>
<td>B</td>
<td>Trace file example</td>
<td>104</td>
</tr>
<tr>
<td>C</td>
<td>Trace file field types</td>
<td>109</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Introduction

Mobile Ad-Hoc Networks are independent and non-centralized wireless techniques. MANETs involve mobile nodes which are free in shifting in and out in the network. Nodes are the techniques or gadgets i.e. cell phone, laptop computer, individual electronic support, MP3 gamer and pc that are playing the network and are mobile. These nodes can work like host/router or both at the similar time. They can type irrelevant topologies based on their connection with each other in the network. These nodes have the capability to set up them and because of their self-settings capability, they can be implemented quickly out of need to any infrastructure (Ullah and Rehman, 2010).

Security in Mobile Ad-Hoc Network is the most serious issue for the primary performance of network. The accessibility to network services, privacy and reliability of the details can be carried out by guaranteeing which protection problems have been met (Ullah and Rehman, 2010). MANETs generally is affected from protection attacks for the sake of its functions like open medium, modifying its topology dynamically, deficiency of main monitoring and control, cooperative methods and no obvious protection procedure (Ullah and Rehman, 2010). These aspects have modified the fight area scenario for the MANETs versus the protection risks.
Routing protocols have created that determine how routers communicate with each other and how to select routes between any two nodes on a computer network. In general, routing methods is one of the complicated and exciting analysis places. Many routing methods have been designed for MANETS, i.e. AODV, OLSR, DSR etc. (Ullah and Rehman, 2010).

AODV is one of the well-known On-Demand Routing techniques (Das et al., 2003). Some scientists (Deng et al., 2002, Ramaswamy et al., 2003) investigated on this routing protocol and discussed the weaknesses in Ad hoc routing protocols and the attacks which can be installed. Recording to a research carried out by (Usha and Bose, 2012) AODV technique is most unprotected versus the black hole attacks.

1.2 Problem Background

MANET is so much well-known due to the point which these networks are powerful, facilities less and scalable. Despite the truth of reputation of MANET, these networks are so much revealed to attacks (Lu et al., 2009, Ullah and Rehman, 2010). Wi-Fi hyperlinks also create the MANET more vulnerable to attacks which create it simpler for the enemy to go within the network and capture accessibility the continuous interaction. Different types of attacks have been examined in MANET and their impact on the network. Attack such as greyish opening, where the enemy node acts maliciously for enough time until the packages are decreased and then change to their regular actions. MANETs routing methods are also being utilized by the assailants by means of surging attack, which is done by the enemy either by using RREQ or details surging (Ullah and Rehman, 2010).

In any network, the sender wants its details to be sent as soon as possible in a protected and quick way, many assailants promote themselves to have the quickest and great data transfer usage available for the transmitting similarly in wormhole attack, and the enemy captures themselves in powerful ideal place in the network.
They create the use of their place i.e. they have quickest direction between the nodes (Mahajan et al., 2008, Shanthi et al., 2009). One of the most coming up problems in MANET is the restricted power supply, assailants take a benefit of this defect and attempts to keep the nodes conscious until all its power is missing and the node go into long lasting rest. Many other attacks MANET for instance jellyfish attack, modification attack, misrouting attack and Routing Table Overflow have been analyzed and revealed (Ullah and Rehman, 2010).

In black hole attack, a harmful node uses its routing technique to be able to promote itself for having the quickest direction to the place node or to the bundle it wants to identify. Furthermore, this aggressive node promotes its accessibility to clean tracks regardless of verifying its routing table. In this way enemy node regularly will have the provision in responding to the direction demand and thus identify the details bundle and maintain it (Ullah and Rehman, 2010).

Researchers have suggested alternatives to recognize and remove black hole nodes (Deng et al., 2002, Ramaswamy et al., 2003). Deng et al. (2002) suggested a remedy for personal dark gaps. But they have not regarded the supportive black hole attacks. As stated in their method, details about the next hop to place should be involved in the RREP bundle when any advanced node responses for RREQ. Then the resource node delivers a further demand (FREQ) to next hop of responded node and requests about the responded node and direction to the place. By using this technique we can recognize standing of the responded node only if the next hop is reliable. However, this remedy cannot avoid supportive black hole attacks on MANETs. For instance, if the next hop cooperates with the responded node, as well, the response for the FREQ will be basically “yes” for both concerns. Then the resource will believe in on next hop and deliver details through the responded node which is a black hole node.

Ramaswamy et al. (2003) suggested a remedy to protecting versus supportive black hole attacks. Also, they claimed that no models or performance assessments
have been done. Therefore, this project focuses on assessment of the performance of the suggested plan in protecting versus the supportive black hole attack.

1.3 Problem Statement

Based on researches carried out by Sharma and Gupta (2009) shows that AODV greatly suffers from multiple black holes in terms of packet delivery ratio, drop packets, average end-to-end delay and route request overhead. Besides, the most common techniques used are inefficient in responding to multiple black hole attacks and just can prevent of single black hole attack (Lee et al., 2002, Deng et al., 2002, Sun et al., 2003). So little attention has been given examine and implementing existing methods for prevention of multiple black hole attacks. There is a need to analyze these methods on multiple black hole attacks. Therefore, this study will address the following questions:

i. How to detect single and multiple black hole attack?
ii. How to mitigate single black hole attack using the most efficient solution?
iii. How to mitigate multiple black hole attack using the methods in (ii)
iv. How to determine the efficiency of the solution used in black hole attack by comparing ids aodv with black hole aodv using the following metrics: packet delivery ratio, packet loss percentage, average end-to-end delay and route request overhead?

1.4 Purpose of Study

In this research, performance of one of the most efficient solutions for preventing single black hole attack in MANET using AODV routing protocol will be investigated in terms of packet delivery ratio, packet loss percentage, average end-to-end delay and route request overhead. Then will examine MANET performance
under multiple black hole attacks with proposed solution. At the end of this investigation, it will be highlighted if the solution which shows good performance in terms of high packet delivery ratio, low packet loss percentage, low average end-to-end delay and reduce route request overhead for single black hole attack can also be useful face with multiple black hole attacks.

1.5 Project Objectives

There are four objectives for this project. They are:

i. To investigate the existing solutions for preventing single black hole attack in MANET using AODV routing protocol.

ii. To determine one of the efficient existing solutions above using four metrics: packet delivery ratio, packet loss percentage, average end-to-end delay and route request overhead.

iii. To implement the existed solution (IDSAODV (Dokurer, 2006) which has presented for single black hole attack before), for multiple black hole attacks.

iv. To compare the effects of above solution on MANET performance with single black hole attack and multiple black hole attacks.

1.6 Scope of Study

The scopes of this research are as follow:

i. The project will study the effects of multiple black hole attacks in MANET using (AODV Ad-Hoc on Demand Distance Vector) routing protocol.
ii. Analysis of solutions for preventing single black hole attack is taken into account.

iii. The impact of solutions for preventing multiple black hole attacks on the performance of MANET is evaluated, finding out if solutions for single black hole attack are also useful for multiple black hole attacks.

iv. Simulation will be done in NS-2.35 (Network Simulator).

v. Simulation will examine on MANET without black hole attack, MANET with 1 black hole node, MANET with 2 black hole nodes and MANET with 3 black hole nodes. And in each scenario will work on networks with 6 nodes, 20 nodes and 30 nodes separately.

vi. Simulation parameters will be obtained from authors of proposed solution (Arya and Jain, 2011, Ahmad et al., 2012).

vii. The measurements will be obtained using packet delivery ratio, packet loss percentage, average end-to-end delay and route request overhead.

1.7 The Significance of Study

Nowadays, there is an increasing need to preventing multiple black hole attacks due to the adverse effect they can have on their victims. Lots of work has been done on single black hole prevention using several techniques to achieve the same goal, but the question is if these techniques can be useful for multiple black hole attacks? This study evaluates the performance one of the most efficient of these techniques as regards to packet delivery ratio, packet loss percentage, average end-to-end delay and route request overhead for preventing of single black hole attack and multiple black hole attacks on MANET using AODV routing protocol by studying each of those metrics individually and will carry out by MANET performance with multiple black hole attacks under single black hole attack prevention solutions.
1.8 Organization of Report

The thesis consists of six chapters. Chapter one describes the introduction, background of the study, research objectives and questions, the scope of the study and its primary objectives. The second chapter reviews available and related literature on black hole attack detection. Chapter three describes the study methodology along with the appropriate framework for the study. Chapter four describes the effects of the single black hole and multiple black hole attacks on MANT performance. Chapter 5 discusses the implementation, result and analysis based on research framework. Finally, Chapter 6 concludes the thesis with a closing remark, recap of objectives, contribution and future work.
REFERENCES


