An Improved Adhoc On Demand Distance Vector Protocol for Mobile Adhoc Networks

M.M.Razmy

(169344 J)

Faculty of Information Technology

University of Moratuwa

April 2019

An Improved Adhoc On Demand Distance Vector Protocol for Mobile Adhoc Networks

M.M.Razmy

(169344 J)

Dissertation submitted to the Faculty of Information Technology, University of Moratuwa, Sri Lanka for the partial fulfillment of the requirement of the Degree of Master of Science in Information Technology

April 2019

Declaration

I do hereby declare that this work has been originally carried out by me under the guidance of and supervisor of Dr.M.F.M.Firdhous Director of Post Graduate Studies, Faculty of Information Technology, University of Moratuwa and this work has not been submitted elsewhere for any other degree.

I certify that this dissertation does not incorporate without due acknowledgement any material submitted for a Master Degree or any Degree in any university and to the best of my knowledge and belief, it does not contain any material previously published or written by any other person except where due reference is the text.

M.M.Razmy Signature of Student

Date: 2019/04/10

Supervised by

Dr.M.F.M.Firdhous Signature of Supervisor

Date: 2019/04/10

Dedicated to

My loving father, late Mr. Pakeer Mohamed

Acknowledgement

First of all I want to thank Al mighty Allah to help me to complete this work. Then I express deep gratitude to my loving parents who helped me financially and making me interest to do my work.

I particularly want to thank Dr.M.F.M.Firdhous, Director of Postgraduate Studies, Faculty of Information Technology, University of Moratuwa, who helped me to decide the topic and giving the explanation about the work. Also would like to thank for the all the lecturers taught us in the Master Program who gave their full support to complete this dissertation.

Furthermore, I deeply indebted to my loving wife and a son who have helped me in several ways. Finally, I express deep gratitude to my friends and all, who despite having had to cope with my tendency to become to absorbed in my work gave me all their support.

Abstract

Mobile Adhoc Network is a kind of adhoc network it can change the locations and configure by itself. The Mobile Adhoc Network uses the wireless connections to connect to various networks like standard WiFi connection, cellular or satellite communication. The mobile Adhoc network does not use any static infrastructure due to multipath broadcasting and high flexibility of nodes. Because of the availability of free license in wireless communication, the use of MANET Application has been increased. MANETs Applications are implemented in disaster-management, business meetings, military operations and rescue operations. There are many different protocols are implemented in MANET while sending data packet source node to the destination node. These protocols can be classified as Proactive, Reactive and hybrid Protocols. Reactive is a very popular routing protocol used in wireless communication that provide the accessible solution for large network. Ad-hoc on Demand Distance Vector Protocol is a kind of Reactive routing protocol. There are many issues in MANET. Security issue is one of the main issue in MANET. With the aim of this research, researcher interesting to find to Detect and Prevent the Cooperative Black hole attack for AODV Protocol.

Previous Authors were introduced Dynamic Learning System against Black hole attack Adhoc On Demand Distance Protocol for Mobile Ad-hoc Network. However the introduced method has only support for a single Black hole attack and its routing overhead is very high. This thesis presents the improved further implemented method Detect, Prevent and Reactive of AODV which will reduce the routing overhead and increasing the packet delivery ratio of AODV Protocol. For the implementation of the research, researcher use Network Simulator 3.24, which is new simulator written from scratch. It is supported C++ and Python language. It will depend on the ongoing contributions of the community to develop new models, debug or maintain existing ones, and share results.

Keyword : MANET, AODV, Black hole, Protocol, Cooperative

Table of Contents

	Page
Abstract	vi
List of Figure	xi
List of Table	xiv
Abbreviations	xv
Chapter 01	
1.0 Introduction	01
1.1 Background and Motivation	01
1.2 Problem Definition	02
1.3 Objective	02
1.4 Resource Required	03
1.5 Chapter organization of Dissertation	03
1.6 Chapter Summary	03
Chapter 02	
2.0 Introduction	04
2.1 Literature Review	04
2.2 Summarization of Literature Review	12
2.3 Chapter Summary	14
Chapter 03	
3.0 Introduction	15
3.1 Methodology	15
3.2 Improved AODV Protocol	16
3.3 Summary	17
Chapter 04	
4.0 Introduction	18
4.1 MANET	18
4.2 MANET Characteristics	18
4.2 MANET Applications	19
4.3 MANET Limitations	19
4.4 MANET Routing Protocol	20

4.5.1 Proactive Routing Protocol 20
4.5.1.1 Distance Sequence Distance Vector Routing Protocol 21
4.5.1.2 Fisheye State Routing Protocol 22
4.5.1.3 Optimized Link State Routing Protocol 22
4.5.2 Hybrid Protocol 23
4.5.2.1Temporary Ordered Routing Protocol 23
4.5.2.2Zone Routing Protocol 24
4.5.3 Reactive Routing Protocol 25
4.5.3.1Ad-hoc On Demand Distance Vector Protocol 26
4.5.4 Route Request Message 26
4.5.5 Route Reply Message 27
4.5.6 Route Error 28
4.5.7 Route Discovery Process 28
4.5.8 Route Maintenance Process 28
4.5.9 Merits and Limitations of AODV Protocol 29
4.6 Summary 29
Chapter 05
5.0 Introduction 30
5.1Security Attack 30
5.2 Active Attack 30
5.2.1Rushing attack 31
5.2.2Flooding Attack 31
5.2.3. Gray-hole attack 32
5.2.4. Denial of Service attack 32
5.2.5.Man-in-the-middle attack 33
5.2.6.Wormhole attack 34
5.2.7. Black hole attack 34
5.3 Passive Attack 36
5.3.1Traffic Monitoring 36
5.3.2 Eavesdropping 37

5.3.3Traffic Analysis 37
5.4.Chapter Summary 37

Chapter 06
6.0 Introduction 39
6.1 Software Requirement 39
6.2 Implementation 40
6.3 Simulation Environment 41
6.4 Installing Black hole Program 41
6.5 Compiling AODV Program 42
6.6 Output of AODV 43
6.7 Overall output of AODV 43
6.8 Compiling Modified AODV 44
6.9 Output of Modified AODV 45
6.10 Overall output of Modified AODV 46
6.11 Network Animator 46
6.11.1 Black-hole.xml 47
6.11.2 AODV.xml 47
6.11.3 MDPRAODV.xml 48
6.12 Summary 48
Chapter 07
7.0 Introduction 49
7.1Packet Delivery Ratio 49
7.2 Packet Loss Ratio 50
7.3 End-to-end delay 51
7.4 Throughput 51
7.5 Summary 52
Chapter 08
8.0 Introduction 53
8.1 Conclusion 53

8.2 Future Work 53
8.3 Summary 54

References 55
Appendix A Glossary of Terms 58
Appendix B Installation of NS3 60
Appendix C Flow Charts 62
Appendix D UML Diagrams 68
Appendix E Source Code 72

List of Figures

No	Description	Page
Figure 1	Mobile Adhoc Network	1
Figure 2	Research Methodology	15
Figure 3	MANETs Routing Protocols Classification	20
Figure 4	DSDV Routing Protocol Architecture	21
Figure 5	Fisheye Routing Protocol Architecture	22
Figure 6	Optimized Link State Routing Protocol Architecture	23
Figure 7	Temporary Ordered Routing Protocol Architecture	24
Figure 8	Zone Routing Protocol Architecture	25
Figure 9	AODV Routing Protocol Architecture	26
Figure 10	Route Request Message Format	26
Figure 11	Route Reply Message Format	27
Figure 12	Route Error Message Format	28
Figure 13	Route Discovery Process of AODV	28
Figure 14	Route Maintenance Process	29
Figure 15	Classification of Attack	30
Figure 16	Rushing Attack	31
Figure 17	Flooding Attack	32
Figure 18	Gray hole Attack	32
Figure 19	Denial of Service Attack	33
Figure 20	Man-in-middle attack	34
Figure 21	Wormhole attack	34
Figure 22	Single Black hole attack	35
Figure 23	Cooperative Black hole attack	36
Figure 24	Traffic Monitoring attack	36
Figure 25	Eavesdropping Attack	37
Figure 26	Traffic Analysis	37

Figure.27	Network Simulation Diagram	40
Figure 28	Ns3 over Ubuntu 14.04	40
Figure 29	Black hole Program installation	41
Figure 30	Compiling the Pure AODV Program	42
Figure 31	Output of AODV Program	43
Figure 32	Overall output of AODV Program	44
Figure 33	Compiling the Modified Ad-hoc on Demand Distance Program	45
Figure 34	Output of Modified AODV Program	45
Figure 35	Overall output of Modified AODV Program	46
Figure 36	Blackhole.xml	47
Figure 37	AODV.xml	47
Figure 38	MDPRAODV.xml	48
Figure 39	Packet Delivery Ratio	49
Figure 40	Packet Loss Ratio	50
Figure 41	End to end Delay	51
Figure 42	Throughput	52
Figure 43	NS3 installation	61
Figure 44	Route Discovery of AODV	62
Figure 45	Route Reply of AODV	63
Figure 46	AODV Protocol Flow Chart	64
Figure 47	Black hole attack Flow Chart	65
Figure 48	Cooperative Black hole Detection Flow Chart	66
Figure 49	Overall Diagram of Proposed Method	67
Figure 50	AODV Message parsing	68
Figure 51	AODV Protocol Class Diagram	69
Figure 52	AODV Protocol Message Parsing Sequence Diagram	70
Figure 53	AODV Message Passing for Route Discovery	71

List of Tables

No	Description	Page
Table 1.0	Summarization of the identified issues in Literature Review	12
Table 2.0	Simulation Setup Parameters	41

Abbreviations

AODV - Ad hoc On Demand Distance Vector

MDPRAODV - Method of Detecting Preventing Reactive AODV

WLAN- Wireless LAN

Wifi - Wireless Fidelity

DSDV -Distance Sequence Distance Vector Routing Protocol

FSR-Fisheye State Routing

OLSR- Optimized Link State Routing Protocol

WRP - Wireless Routing Protocol

DSR- Dynamic Source Routing

TORA-Temporary Ordered Routing Protocol

ZRP-Zone Routing Protocol

RREP - Route Reply

RREQ - Route Request

CAODV - Credit Based Ad hoc On Demand Distance Vector

DOS - Denial of Service Attack

HTTPS- Hyper Text Transfer Protocol Secure

SSL- Secure Socket Layer

WEP - Wired Equivalent Privacy

WAP - Wireless Protected Access

NS3 - Network Simulator 3