

LIGHTWEIGHT SECURITY MECHANISM TO MITIGATE NETWORK LAYER BASED ACTIVE ATTACKS IN A MOBILE ADHOC NETWORK

DEAN'S OFFICE

15 AUG 2022

Faculty of Applied
Sciences

By

UTHUMANSA AHAMED

A thesis submitted to the **Faculty of Applied Sciences, Rajarata University of Sri Lanka** in partial fulfillment of the requirements for the award of the degree of
MASTER OF PHILOSOPHY in Computer Sciences

ACC NO.	PGT0003
CALL NO.	005-82AHA

Faculty of Applied Sciences
Rajarata University of Sri Lanka
Mihintale – Sri Lanka
May 2021

ABSTRACT

Mobile Ad hoc Network (MANET) is one type of an Ad hoc network. General properties of a MANET are self-configuration capability, open network boundary, infrastructure-less network nature, and limited resources. This nature of MANET opens the network to different security threats. Network layer-based Active attacks are widespread. Available security solutions for Active attacks contain complex calculations. Therefore, the objective of this research is to propose a lightweight security mechanism to enhance and strengthen the security of the data communications between source and destination nodes in a MANET. This research consists of three different experiments. Experiment I was designed to investigate the behaviours and impacts of malicious nodes on network performance. Experiment II was designed to identify the impacts and validity based on node mobility when designing security countermeasures in MANET. Experiment III was designed to propose a widely deployed lightweight security mechanism based on the results of experiments I and II. Ad-hoc On-Demand Vector is used as the routing protocol to detect network layer attacks. Blackhole and Grayhole attacks are used as network layer-based Active attacks. Packet Delivery Ratio (PDR), Average End to End Delay (AEED), Throughput, Average Data Dropping Rate (ADDR), and Simulation Processing Time at Intermediate Nodes (SPTIN) are measured by changing the number of connected nodes in the network and by changing the speed of the nodes. A network without attack is used to compare the performances of each network. In experiment I, due to the impact of the blackhole attack, compared to the network without attack, the PDR was found to be 0.28%, AEED was infinity and Throughput was 0.33%. In experiment II, PDR and Throughput values are increased by twice in higher node mobility than in lower node mobility. The network that is affected by a grayhole attack shows higher performance than the network that was affected by a blackhole attack and lower performance than the network without attack. In experiment III, the performances of the proposed security mechanism were compared with the network without attack, and the values of PDR, AEED, Throughput, and SPTIN were found to be 98.0825%, 100.9346%, 99.9988%, and 96.5660% respectively. The data packet delivery ratio was 100.00% compared to the network without attack. The network which was affected by a blackhole attack showed a higher amount of ADDR than the network without the attack and the lowest amount of PDR. The network that was affected by a blackhole or a grayhole attack showed underperformance than the network without the attack. It was also found that the blackhole attack degraded the network performance more than the grayhole attack. The mobility of nodes degraded the network performance. Node mobility either led to the breaking of the links between nodes or the creation of new links. Therefore, node mobility created an opportunity to break the link between malicious and other nodes in the network. Active attacks degraded the MANET performance. The main similarity of most Active attacks was the abnormal amount of packet dropping. Therefore, node mobility is a favourable factor for network security. Furthermore, this implied that the security mechanism should be flexible enough to handle security attacks amidst node mobility. Therefore, initial screening to detect malicious nodes was found to be effective in the presence of mobile nodes. The proposed security mechanism performs well in the presence of a blackhole attack. Moreover, it performs well in PDR, AEED, and Throughput compared to the network without attack. The performance of the AEED and SPTIN proves that the proposed solution is free from complex calculations. The scope of the proposed security mechanism can be expanded into a lightweight Intruder Detection System to handle different types of security attacks.

CONTENTS

LIST OF ABBREVIATIONS	XI
LIST OF TABLES	XIII
LIST OF FIGURES	XIV
CHAPTER 1	
INTRODUCTION	1
1.1 Mobile Ad-hoc Network	1
1.2 Problem statement	2
1.3 Research objective and question	4
1.3.1 Research objective	4
1.3.2 Research question	4
1.4 Research inspiration	6
1.5 Research methodology	7
1.6 Research outcome	7
1.7 Thesis organization	8
CHAPTER 2	
LITERATURE REVIEW	9
2.1 Introduction	9
2.2 General security of MANET	9
2.2.1 Mobility	9
2.2.2 Infrastructure-less network	10
2.2.3 Limited resources	10
2.2.4 Open network boundary	11
2.3 Routing protocols	11
2.3.1 Proactive routing protocols	12
2.3.2 Reactive routing protocols	13
2.4 AODV overview	14
2.4.1 Path discovery	15
2.4.2 Routing table management	16
2.4.2 Path maintenance	16
2.4.2 Local connectivity management	16
2.5 Security attacks	17
2.5.1 Active attacks	18
2.5.2 Passive attacks	20
2.6 Network Performance Metrics (NPM)	21
2.6.1 PDR	21
2.6.2 AEED	22
2.6.3 Throughput	22
2.6.4 ADDR	23
2.6.5 SPTIN	23
2.7 Taxonomy of available security mechanisms	24
2.7.1 Trust-based mechanisms	24
2.7.2 Sequence number validation-based mechanisms	24
2.7.3 Threshold value-based mechanisms	25

2.7.4	Anomaly detection-based mechanisms	25
2.7.5	Logical inference-based mechanisms	25
2.7.6	Surveillance-based mechanisms	25
2.7.7	Cross-layer collaboration-based mechanism	26
2.7.8	Clustering-based mechanisms	26
2.7.9	Node collaboration-based mechanisms	26
2.7.10	Acknowledgment-based mechanisms	27
2.7.11	Routing packets-based mechanisms	27
2.7.12	IDS-based mechanism	27
2.7.13	Hardware-based mechanisms	27
2.7.14	Cryptography-based mechanisms	28
2.7.15	Collective mechanisms	28
2.8	Lightweight nature	36
2.9	Computer simulation	39
2.10	Experimental validation	41
2.11	Summary	41

CHAPTER 3

RESEARCH METHODOLOGY

		43
3.1	Introduction	43
3.2	Research strategy	43
3.3	Research sub-questions and objectives	44
3.4	Network simulator	45
3.5	Blackhole attack simulation	46
3.5.1	Modification on aadv.h	47
3.5.2	Modification on aadv.cc	47
3.5.3	Finalizing the changes	50
3.5.4	Applying the blackhole attack	51
3.5.5	Grayhole and wormhole attack simulation	51
3.6	Experimental setup	51
3.6.1	Experiment I	52
3.6.2	Simulator configurations	53
3.6.3	Assumptions and considerations	53
3.6.4	Experiment II	54
3.6.5	Simulator configurations	56
3.6.6	Assumptions and considerations	57
3.6.7	Experiment III	57
3.6.8	Simulator configurations	58
3.6.9	Assumptions and considerations	59
3.7	Simulation outputs	59
3.8	Experimental best practices	60
3.9	Summary	61

CHAPTER 4

PROPOSED SOLUTION

		62
4.1	Introduction	62
4.2	Proposed solution	62
4.2.1	Protection	63
4.2.2	Pinpoint	68
4.2.3	Prevention	70

4.3	Summary	71
CHAPTER 5		
RESULTS AND DISCUSSION		72
5.1	Introduction	72
5.2	Results	72
5.2.1	Experiment I	72
5.2.2	Experiment II	79
5.2.3	Experiment III	91
5.3	Summary	95
CHAPTER 6		
CONCLUSION AND FUTURE WORKS		97
6.1	Introduction	97
6.2	Research findings	97
6.3	Achievement of the research objective	97
6.4	Efficiency of the proposed security mechanism	102
6.5.	Limitations	103
6.6.	Future work	103
6.6.1	Network performance evaluation	104
6.6.2	Extending available service	104
6.6.3	Component for complex security systems	104
6.6.4	Expansion on different network structures	105
6.6.5	Compatibility for green networking	105
6.6.6	Arise research question	105
6.7	Summary	105
REFERENCES		107
APPENDIX A		
Basic Parameters of the Simulator		122
APPENDIX B		
Sample NAM Visualizations		124
APPENDIX C		
Routing Table Content Display Function		125
APPENDIX D		
A Sample TCL Program Used in the Experiment		126
APPENDIX E		
Random Movement Details of Nodes in Experiment		132
APPENDIX F		
Explanation of Trace File Format		134
APPENDIX G		
Defining Malicious Node List		140

APPENDIX H	
Grayhole Attack Simulation	147
APPENDIX I	
Wormhole Attack Simulation	148
APPENDIX J	
List of Publications	150