UNIVERSITI PUTRA MALAYSIA

PERFORMANCE ANALYSIS ON DETECTION AND PREVENTION OF WORMHOLE ATTACK IN WIRELESS NETWORK

MOHAMAD AIMAN HANIF APANDI

FSKTM 2019 10

PERFORMANCE ANALYSIS ON DETECTION AND PREVENTION OF WORMHOLE ATTACK IN WIRELESS NETWORK

By

MOHAMAD AIMAN HANIF APANDI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia,
in Fulfilment of the Requirement of Master of Computer Science

JUNE 2019

COPYRIGHT

ABSTRACT

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Computer Science (Computer Network)

PERFORMANCE ANALYSIS ON DETECTION AND PREVENTION OF WORMHOLE ATTACK IN WIRELESS NETWORK

By

MOHAMAD AIMAN HANIF APANDI

JUNE 2019

Chair: Fahrul Hakim Ayob, PhD.
Faculty: Faculty of Computer Science and Information Technology

In the wireless network, there is an attack called Wormhole attack that capable in confusing the route of packets during packet transmission and causing data loss. Ad hoc On-Demand Distance Vector (AODV) is routing protocol is usually where the Wormhole attacks happen. This routing protocol is designed for Mobile Ad hoc Network (MANET) and wireless. Ad hoc is a decentralised wireless network which not rely to another device such as router. Due to the use of AODV protocol with limited security during packet delivery, wireless network often suffers from Wormhole attack which causes significant performance restrictions such as low throughput, high end-to-end packet delay and low packet delivery ratio. This project explained the performance analysis on detect and prevent of Wormhole attack in MANET by using tunnelling method among neighbour nodes in AODV protocol environment to ensure the packets safely delivered to destination. The system will prevent Wormhole node remain in the network, which surely improves the performance of wireless network. The simulation experiments using Network Simulator 2 (NS2) have been carried out to analyse the performance of the proposed work. The simulation results show that the proposed work outperforms because the increase numbers of throughput about 36 percent and packet delivery ratio increase 90 percent compared to when Wormhole node in the network. In addition, the proposed work also reduces the end-to-end packet delay about 64 percent compared to before proposed work being implemented. As a result, wireless network communication using AODV protocol now more safe and secure due to malicious attack cannot enter into the system.

Abstraktesis yang dikemukakan kepada Senat Universiti Putra Malaysia
Sebagai memenuhi keperluan untuk ijazah Sains Komputer (Pengkhususan Rangkaian Komputer)

ANALISIS PRESTASI DALAM MENGESAN DAN MENCEGAH SERANGAN WORMHOLE DALAM RANGKAIAN TANPA WAYAR

Oleh

MOHAMAD AIMAN HANIF APANDI

JUNE 2019

Pengerusi: Fahrul Hakim Ayob, PhD
Fakulti: Fakulti Sains Komputer dan Teknologi Maklumat

Dalam rangkaian tanpa wayar, terdapat satu serangan dipanggil serangan Wormhole yang berupaya mengelirukan laluan paket-paket semasa proses penghantaran dan menyebabkan data hilang. “Ad hoc On-Demand Distance Vector (AODV)” adalah protokol laluan dimana selalunya serangan Wormhole berlaku. Protokol laluan ini dibuat untuk “Mobile Ad hoc Network (MANET)” dan rangkaian tanpa wayar. Adhoc adalah rangkaian tanpa wayar yang tidak memusatkan yang mana tidak bergantung kepada peranti yang lain seperti penghala. Disebabkan penggunaan protocol AODV dengan sekuriti dengan had tertentu semasa penghantaran paket, rangkaian tanpa wayar kerap terkena serangan Wormhole yang menyebabkan sekatan prestasi seperti rendah jumlah paket yang dihantar, tinggi masa kelewatan satu ke satu paket dan rendah ratio penghantaran paket. Projek ini menerangkan analisis prestasi dalam mengesan dan menghalang serangan Wormhole ke atas Manet dengan menggunakan kaedah “tunnelling” antara nod-nod jiran menggunakan protokol AODV untuk memastikan paket-paket selamat dihantar ke destinasi. Sistem ini akan menghalang nod Wormhole berada dalam rangkaian, yang mana akan meningkatkan prestasi rangkaian tanpa wayar. Simulasi kajian mengunakan “Network Simulator 2 (NS2)” untuk menganalisa prestasi kerja yang dicadangkan. Hasil simulasi menunjukkan bahawa kerja yang dicadangkan ini bagus kerana peningkatan jumlah paket yang dihantar sebanyak 36 peratus dan nisbah paket dihantar meningkat sebanyak 90 peratus berbanding apabila nod Wormhole dalam rangkaian. Tambahan lagi, kerja yang dicadangkan ini juga mengurangkan

kelewatan satu ke satu paket sebanyak 64 peratus berbanding sebelum kerja yang dicadangkan ini diimplementasikan. Hasilnya, komunikasi rangkaian tanpa wayar menggunakan protokol AODV sekarang semakin selamat dan kukuh daripada serangan berbahaya yang tidak lagi boleh masuk ke dalam sistem.

ACKNOWLEDGEMENT

Assalamualaikum w.b.t and Warm Greetings,

I would like to express my sincere gratitude to my supervisor, Fahrul Hakim Ayob (PhD.), Department of Computer Network and Communication, Universiti Putra Malaysia, for his valuable guidance, critics and suggestions during throughout my project. Without his continue support and encouragement, this project would not have been possible to complete. I am extremely obliged to the faculty members and staff of Faculty of Computer Science and Information Technology, for their tremendous guidance and generous attitude. Without them, it would have been very difficult for me to finish this project. Also, I am greatly indebted to Universiti Putra Malaysia for their assistance in supplying the relevant literatures and facilities for my research. My fellow friends should also be acknowledged for being there with me though ups and downs. Last but not least, I am grateful to all my family members in giving me all the love and motivation that I need in order to complete this project successfully. Their contributions are extraordinary and indeed beyond words.

APPROVAL

I certify that a Thesis Examination Committee has met on 1st January 2017 to conduct the final examination of Mohamad Aiman Hanif Bin Apandi on his thesis entitled Robust Internet Connection based on Redundancy Protocols in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Bachelor Degree of Computer Science (Major Network)

Members of the Thesis Examination Committee were as follows:

Fahrul Hakim Ayob, PhD.
Doctor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Muhammad Daniel Hafiz Abdullah, PhD.
Doctor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Examiner)

Rohaya Latip, Assoc. Prof.
Head of Department
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Examiner)

Norwati Mustapha, Assoc. Prof
Deputy Dean
Faculty of Computer Science and
Information Technology
Universiti Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Computer Science (Major Network). The members of the Supervisory Committee were as follows:

Fahrul Hakim Ayob, PhD.
Doctor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Abu Bakar Md.Sultan, Prof.
Professor and Dean
Faculty of Computer Science and
Information Technology
Universiti Putra Malaysia

DECLARATION

Declaration by student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: 24/6/2019

Name and Matric No.: MOHAMAD AIMAN HANIF APANDI GS49836

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- Supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature:	
Name of Chairman of Supervisory Committee:	Fahrul Hakim Ayob,PhD. Doctor Faculty of Computer Science and Information Technology Universiti Putra Malaysia (Chairman)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figures **Pages**

LIST OF ABBREVIATIONS

Symbols

AODV	Ad hoc On-Demand Distance Vector
DSR	Dynamic Source Routing
IoT	Internet of Things
MANET	Mobile Ad Hoc Network
M/S	Millimetre per Second
NS2	Network Simulation 2
PDR	Packet Delivery Ratio
RREQ	Route Request
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WiMAX	Worldwide Interoperability for Microwave Access

CHAPTER 1

INTRODUCTION

1.1 Background

This project is one of the academic purposes which are SSK 5980. The project proposed is Performance Analysis on Detection and Prevention of Wormhole Attack in Wireless Network. Wireless Network have broad type of area such as satellite, internet of things (IoT) and many more. This project will be focus on mobile ad hoc network (MANET). MANET consist of mobile nodes that can stand on its own without need to rely to another device. They use wireless as a communication between each node. Devices such as laptop, computer, mobile phone and sensors can be the mobile nodes because these devices can provide functions of a network. Network functionality means they can act as a router to deliver packets or server where data is store. Moreover, these devices are portable which make MANET very dynamic network compare to another networks. That is the reason why MANET is used by the military, missionary, rescuers and educators when they go to remote area. Besides that, MANET is easy to setup and cheaper than infrastructure network. The idea to create this project due to people need a stable internet connection even though they are in remote area. But because MANET is dynamic, it become highly exposed to the possibility of being attack by malicious threats. The threats can cause communication failure or delay in delivery. Security is become an issue in MANET where threats can penetrate the security and attack the network. This project will focus on to detect and prevent a threat called Wormhole attack.

Wormhole attack is a threat that confusing the packet routing during packet delivery. Wormhole attack is started when attacker send Wormhole nodes as fake

nodes. A pair of Wormhole node then form a Wormhole tunnel that is shorter than another path in the network. This can attract source node to send data using the Wormhole tunnel. After that, Wormhole nodes capture the packets and send them to another located node. The consequences of Wormhole attack are data loss, data leakage, modified data, routing disruption, denial of service and network congestion. For additional information, the attacker can easily enter the network using Wormhole attack without need to have knowledge of the network's topology, security and structures. There are several ways how Wormhole attack. First is by packet encapsulation, Wormhole node sends the packet to another Wormhole node using legitimate path. When arrive, the packet will get encapsulate to avoid other nodes from discovering another legitimate path. Seconds, out-of-band is a Wormhole link created by using out-of-band high bandwidth placed between two end points. Third is high power transmission, it attracts the packets to use Wormhole path by only using one high transmission Wormhole node. Lastly, packet relay is when two Wormhole nodes relay packets between two far nodes to create fake neighbours. Wormhole attack have different types, each type has their own functions. First type is open Wormhole attack, the attackers modify the packet header in a route discovery to make sure other nodes think they are part of neighbour nodes. Second type is half open Wormhole attack, this type only uses one Wormhole node to modify the packet while the other one does not modify. The last type is closed Wormhole attack, in this type the attackers do not modify any packet. It is only sending the packet through Wormhole tunnel and rebroadcasts the packet.

The problem in MANET is the current Ad hoc On-Demand Distance Vector (AODV) routing protocol have a weak security and cannot defence against Wormhole attack. AODV is routing protocol commonly used in MANET. The

purpose of this protocol is to make a route path between sender and receiver. However, this protocol cannot detect Wormhole attack from enter the network. It also confuses when Wormhole tunnel and uses the path instead original path. To solve the problems AODV need to be improved using method like tunnelling method.

In this project, it contains problem statements, objectives, scope of project, literature review, methodology, implementation, results and reference of proposed work.

1.2 Problem Statements

One of the problems in wireless network is the current AODV protocol used in MANET has a weak security. The network always suffers from performance restrictions during packet transmission when being attacked by Wormhole. This malicious attack causes the low of throughput, high end-to-end packet delay and low packet delivery ratio. Wormhole attack confuses the route path of the packets during packet transmission so that it can intercept the data then interrupt the network by causing data loss, data modification and denial of service.

1.3 Objectives

Every project must have objectives that need to achieve. This is very important to see the level of achievement of the project. In addition, the objective is use to provide an initial understanding to readers about the project. The objective of this project is to detect and prevent Wormhole attack in mobile ad hoc network (MANET) by improving AODV protocol using tunnelling method among neighbour nodes for secure the packets during delivery. The improved AODV protocol will be send messages to network nodes and report number of hops to sender nodes during

packet delivery. Each neighbour nodes in the MANET must report number of hops. In the initial state of packet delivery, the sender node will send "hello message" to neighbour nodes. Then, sender will compare the hops report with sensitivity parameter to determine which node is Wormhole and the shortest path to target. Approved neighbour nodes only can receive the packets from the sender. This process continues until the packet arrive to the destination. It will prevent Wormhole nodes receive any packet and discard from the network. Thus, network problems such as data loss, denial of service and data modification can be avoided.

1.4 Scope

This project will consist of creating an improved security in Mobile Ad hoc Network (MANET) on Wormhole attack. Wormhole attack harms the MANET by modifying the packets, confusing the routing path and increase network traffic. To detect and prevent Wormhole attack in MANET's security, the packets in the network are send with message. The message is to ask all neighbours to find route to destination and report number of hops to sender. Then, the sender will compare the hops report with sensitivity parameter to determine which node is Wormhole and the shortest path to target. To make this happen, Ad hoc On-Demand Vector (AODV) protocol is used as suitable routing protocol. This project involves simulation tools which is Network Simulation 2 (NS2). C/C++ and Tcl language is used throughout the experiment. The performance parameters used in this project are throughput, packet delivery ration and end-to-end delay. 36 number of nodes with the boundary

area of 800m X 800m are created in the mobile ad hoc network. The project will be finished by June ,2019.

.

1.5 Thesis Structure

The structure of the thesis contains a total of six chapters. The chapter are Introduction, Literature Review, Methodology, Configuration, Testing and Results and Conclusion.

In Chapter 1, this is the chapter for introduction of the project. It started with background of project, problem statements, objectives, scope of project and thesis structure.

REFERENCES

[1] Choudhary, N., and Agrawal, S., (2014) Analysis of Worm-Hole Attack in MANET using AODV Routing Protocol, In International Journal of Electronics and Communication Engineering, Vol. 1, Issue 10, December 2014.

[2] Ghormare, N., Dorle, S., and Swati, S., (2018) Detection and Prevention of Wormhole Attack in WiMAX Based Mobile Adhoc Network, Proceedings of the 2nd International Conference on Electronics, Communications and Aerospace Technology 2018

[3] Imran, M., et. al. (2015) Analysis of Detection Features for Wormhole Attacks in MANETs, In International Workshop on Cyber Security and Digital Investigation 2015

[4] Jhaveri, H., et. al. (2010) MANET Routing Protocols and Wormhole Attack against AODV. In International Journal of Computer Science and Network Security, Vol.10 No.4, April 2010

[5] Manju, O., and Kushwah, S., (2014) Impact and Performance Analysis of Wormhole Attack on AODV in MANET using NS2, In International Journal of Science and Reseach, Vol. 3, Issue 6, June 2014

[6] Marcus, O.J., Arish, S., and Amin, K., (2017) A Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks, In International Journal of Computer Applications, Vol. 174, No. 4, September 2017

[7] Neelima, S., and Ramanjeet, S., (2010) Wormhole Attack Prevention and Detection in MANETs Using HRL Method. In International Journal of Advance Research, Ideas and Innovations in Technology, Vol.3, Issue 2

[8] Otmani, M., and Ezzati, A., (2014) Effects of Wormhole Attack on AODV And DSR Routing Protocol Through the Using NS2 Simulator, In Journal of Computer Engineering, Vol. 16, Issue 2, March-April 2014

[9] Sharma, G., and Fatima, M., (2013) An Energy Efficient Approach for Wormhole Detection and Prevention, In International Journal of Computer Applications, Vol. 76, No.17, August 2013

[10] Sharma, P., Sinha, H.P., and Bindal, A., (2014) Detection and Prevention against Wormhole Attack in AODV for Mobile Ad-hoc Networks, In International Journal of Computer Applications, Vol. 95, No.13, June 2014

[11] Zaw, T., and Maw, A.H., (2008) Wormhole Attack Detection in Wireless Network, In International Journal of Electrical, Computer, Energetic, Electronic and Communcation Engineering, Vol. 2, No.10, June 2008

BIODATA OF STUDENT

Mohamad Aiman Hanif Bin Apandi was born in Kota Bharu, Kelantan; on 12th April, 1995. The first place where he studied is a school named SK Bechah Durian. Then, he received an education at one of Boarding School, which is SMS Tg. Muhammad Faris Petra.

After that, he further his studies in Foundation of Science Agriculture (Fast Track) at University Putra Malaysia (UPM). Next, he continues studies in the degree of Computer Science (Major Network) in the same university at Faculty Computer Science and Information Technology. The final year project done by this student at degree level is Robust Internet Connection based on Redundancy Protocols. Now, he pursues studies in Master of Computer Science in same university. The final year project done at Master level is Performance Analysis on Detection and Prevention of Wormhole Attack in Wireless Network.