"I declare that I have read this project, in my opinion this project report has satisfied the scope and quality for the award of the degree of Master of Computer Science (Information Security)."

Signature :

Name of Supervisor : DR. MAZDAK ZAMANI

Date : JUNE 2013

A SECURE METHOD TO DETECT WORMHOLE ATTACK

IN MOBILE ADHOC NETWORK

PARICHEHR MANOUCHEHRI ARDESTANI

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Advanced Informatics School (AIS)
Universiti Teknologi Malaysia

JUNE 2013

DECLARATION

I declare that this thesis entitled: “A SECURE METHOD TO DETECT WORMHOLE ATTACK IN MOBILE ADHOC NETWORK ” is the result of my own research except as cited in references. The thesis has not been accepted for any degree and is degree and is not concurrently submitted in candidature of any other degree.

Signature :

Name : PARICHEHR MANOUCHEHRI ARDESTANI

Date : JUNE 2013

DEDICATION

Special dedicated this thesis to my parents, sisters and my lovely niece that made this work possible through all their unlimited love, guidance, patience, generosity, understanding, unconditional support and encouragement. I am dedicating this thesis to them with love and respect.

ACKNOWLEDGEMENT

First, my deepest thankfulness goes to the most merciful **ALLAH** for all his blessings and bounties he gave me since I was born, without his blessings I would not be in this place at all. I would like to express my sincere gratitude to my thesis supervisor, Dr. Mazdak Zamani, for his professional guidance and critical comments throughout the work on my master thesis. Also, I would like to thank my examiners, Dr. Bharanidharan Shanmugam and Dr. M Shahidan Abdullah, who kindly agreed to take on the examination role right from the beginning of this project. Finally, i would like to thank all professors and lecturers, and members of Advanced Informatics School for their generous help in various ways for the completion of this thesis.

I am deeply in debt to my father and mentor who was and still behind everything I have learned and achieved in my life. I owe everything I have to him. I love to express my deepest gratitude to my Mother, for her care, patience, support, prayers and for the endless nights, she was looking after me. Without her, I am nothing. Also, I love to thank my lovely sisters for their love, concern and engorgement along the way. I am very grateful for all the supporting me and pushing me future when the work has gone slow.

ABSTRACT

According to recent advances in wireless telecommunications, the performance and use of wireless technologies has increased extremely. In this study concerned on the Mobile Ad-hoc Network (MANET) is a collection of self-configuring mobile node without any infrastructure. There are different security flaws and attacks on the routing protocols in the MANET. One of the critical threats is the wormhole attacks, which have attracted a great deal of attention over the years. The wormhole attack can affect the performance of different routing protocols. During this attack, a malicious node captures packets from one location in the network, and “tunnels” them to another malicious node at a distant point, which replays them locally. This study presents a review of the most important solutions for counteracting wormhole attacks, as well as presents proposed method on DSR routing protocol for detecting them. The performance of the proposed method was examined through ns-2 simulations. Hence, the results show that proposed method can detect this serious attack in a Mobile Adhoc Network.

ABSTRAK

Menurut kemajuan terkini dalam telekomunikasi tanpa wayar, pelaksanaan dan penggunaan teknologi tanpa wayar telah meningkat sangat. Dalam kajian ini berkenaan atas Mobile Rangkaian Ad-hoc (Manet) adalah koleksi diri mengkonfigurasi nod mudah alih tanpa apa-apa infrastruktur. Terdapat kelemahan keselamatan yang berbeza dan serangan ke atas protokol di Manet. Salah satu ancaman kritikal adalah serangan lubang ulat, yang telah menarik banyak perhatian sejak beberapa tahun. Serangan lubang ulat boleh menjejaskan prestasi protokol laluan yang berbeza. Dalam serangan ini, nod berniat jahat menangkap paket dari satu lokasi dalam rangkaian, dan "terowong" mereka yang lain nod berniat jahat di tempat yang jauh, yang ulang tayang mereka dalam negara. Kajian ini membentangkan kajian semula penyelesaian yang paling penting bagi mengimbangi serangan lubang ulat, serta membentangkan kaedah yang dicadangkan pada DSR routing protokol untuk mengesan mereka. Prestasi kaedah yang dicadangkan telah diperiksa melalui ns-2 simulasi. Oleh itu, keputusan menunjukkan bahawa kaedah yang dicadangkan boleh mengesan serangan ini serius dalam Adhoc Rangkaian Mobile.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

MANET	Mobile Adhoc Network
AODV	Ad Hoc On Demand Distance Vector
OLSR	Optimized Link State Routing
OPNET	Optimized Network Engineering Tool
DSR	Dynamic Source Routing
MAC	Medium Access Control
RREQ	Rout Request
RREP	Rout Replay
RERR	Rout Error
UDP	User Datagram Protocol
ZRP	Zone Routing Protocol
NS	Network Simulator
IETF	Internet Engineering Task Force
MNs	Mobile Nodes

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

A network is a set of connected nodes. Networks can be wired, wireless or wired cum wireless (Suganya and Palaniammal, 2012). Network technology is developing quickly, particularly in wireless communications. Therefore, fixed networks cannot satisfy enormous demands on the network connectivity, data storage and information exchange any longer (Fan, 2010).

Two wireless network models that have been developed for the wireless communication systems. The fixed backbone wireless model consists of a large number of Mobile Nodes (MNs) and relatively fewer fix nodes; but fixed nodes are more powerful. The communication between a fixed node and a MN within its range happens via the wireless medium. However, this needs a fixed stable infrastructure (Junhai *et al.*, 2009). Another system model, a Mobile Ad-hoc NETwork (MANET) is based on wireless and multi-hop communication have emerged to provide efficient solutions for the growing number of mobile wireless applications and services (Fan, 2010). It is a

self-organizing collection of MNs that form a temporary and dynamic wireless network on a shared wireless channel without fixed network infrastructure or centralized administration (Junhai et al., 2009).

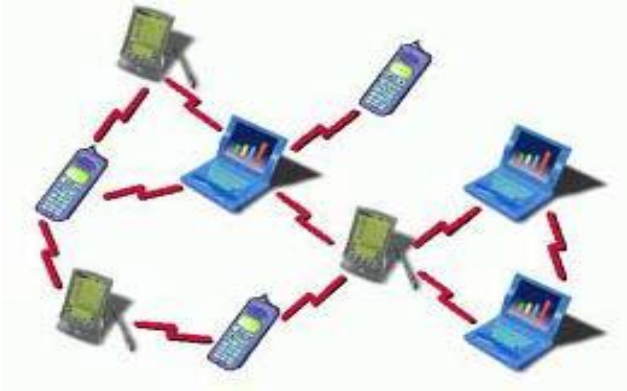

Figure 1.1: Wireless Network (Suganya and Palaniammal, 2012)

1.1.1 Mobile Adhoc Network

The Mobile Adhoc Network (MANET) are a group of mobile nodes collaborate and send packets to each other (Sen *et al.*, 2007a). Each node operates as an end-system, also as a router to send packets. The nodes are self- organization and free to move into a network (Yi *et al.*, 2005). Such networks extend the limited wireless transmission range of each node by multi-hop packets forwarding (Sen *et al.*, 2007a).

According to the IETF (Internet Engineering Task Force), a MANET is an independent system of mobile routers connected by wireless links. The network's wireless topology may change rapidly and unpredictably. Nodes can be different wireless devices such as PCs, mobile phones, printers, scanners, fax machines, MP3 players, key boards, joysticks, robots etc (Ben Othman and Mokdad, 2010).

In a MANET, a source node must rely on other nodes to forward its packets on multi-hop routes to the destination (Wang *et al.,* 2011) and thus, they are ideally suited for scenarios in which pre-deployed infrastructure support is not available. MANETs have some special characteristics such as constantly changing network topologies, infrastructure less, limited bandwidth, limited resources, low power, high cost etc. While these characteristics are essential for the flexibility of MANETs, they introduce specific security concerns that are either absent or less severe in wired networks (Sen *et al.*, 2007b).

1.2 Background of the Problem

Security issues in the MANET are main threat to the operation of it. Due to mobility and open media nature, MANET are much more prone to all kind of security threats, such as intrusion, information disclosure, or even denial of service (Jawandhiya *et al.,* 2010). However, with the convenience the MANET have brought to us, there are also increasing security threats for the MANET, which need to gain enough attention (Rai and Singh, 2010).

In ad-hoc routing protocols, due to nodes are also routers, they exchange information about the network topology with each other. This is an important weakness because a compromised node could give bad information to forward traffic or simply stop it (Deshpande, 2007). Moreover, the existing Adhoc routing protocols such as Adhoc on Demand distance vector (AODV), Dynamic Source Routing (DSR) do not provide a trusted environment; therefore, a attacker can become a router and disturb network operations by disobeying the specific protocol (Rai and Singh, 2010). Due to diverse features of MANET, security is an important subject in wireless. Also, there are different types of challenges in MANET which are given below (Ali and Sarwar, 2011).

1.2.1 Lack of Centralized Management

Lack of centralized management in MANET makes it hard to recognize whether the attack is created by adversaries or because of benign failures. Observing the traffic of a extremely dynamic large MANET is a hard task and is even more complex when adversaries regularly change their pattern and targets for attack (Mandhata *et al.*, 2012).

In MANET, all network nodes are required to work together in the network, although no security organization can be assumed for all nodes in the network. And a correct operation between trusted and un-trusted nodes cannot be obtained (Mandhata *et al.*, 2012).

1.2.2 Non-Predetermined Infrastructure

This feature removes the opportunity to establish a central authority to control the network characteristics. Due to lack of authority, traditional techniques of network management and security are hardly appropriate to MANETs (Agrawal, Jain *et al.*, 2011).

1.2.3 Dynamic Topology

In MANET, nodes are free to join, leave and move arbitrarily; as a result, the network topology, which is typically multi hop and consisting of both bidirectional and unidirectional links, may change randomly and rapidly (Mandhata *et al.*, 2012).

1.2.4 Resource Constraints

MANETs are a group of mobile devices, which are limited in power capacity, computational capacity, memory, bandwidth etc. by default. Thus, in order to accomplish a secure and reliable communication between nodes, these resource constraints make the task more enduring (Agrawal, Jain *et al.*, 2011).

1.3 Problem Statement

Wormhole attack is a sever attack on MANET routing protocol where two or more malicious nodes make tunnel in the network that transport packets between the tunnel endpoints. The tunnel can establish in many different ways such as out - of - band channel, packet encapsulation, high power transmission, packet relay and using protocol deviations. This route via wormhole tunnel is attractive for legitimate nodes because it provides less number of hops and latency than normal channel multi-hop routes. However, these malicious nodes act as neighbors to other nodes whereas they are several hops away. Therefore, such attack results a false route. So, if wormhole attack lunched in the network and source node chooses this false route as least hop count to the destination, then malicious nodes have the option of delivering the packets or dropping them (Choi *et al.*, 2008). In this project uses some techniques that are used to propose the possibility of method that detects false route created by malicious nodes.

1.4 Research Questions

The main questions this research motivates to answer are as follows

- How do current methods detect wormhole attack in the MANET?
- How can detect wormhole attack in the MANET?

- How can measure the performance of the proposed method?

1.5 Project Objectives

The objectives of this study are

- To investigate the current methods to detect wormhole attacks in the MANET
- To propose and develop an enhance method to detect wormhole attack in the MANET
- To evaluate the effectiveness of the proposed method against wormhole attack

1.6 Project Aim

Due to the mobility and open media nature, the MANETs are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. MANET is susceptible to many attacks, including an attack known as the wormhole attack. The wormhole attack is very powerful and detecting wormhole attack has proven to be very difficult. The aim of this study is to investigate the possibility of improving method to make a reliable and secure MANET against wormhole Attack.

1.7 Scope

Security in MANET is hard because of dynamic topology, infrastructure less, limited bandwidth, etc. Hence, this study has focused on security issues and threats of

MANET and we investigate vulnerability of MANET against Active attacks specially wormhole attacks. Wormhole attack is a sever attack on the MANET leads to create false route. Therefore, there are several types of protocol that vulnerable to this attack. In this project will investigate the possibility of method to make a reliable and secure MANET (Mobile Adhoc Network) on the DSR protocol (Dynamic Source Routing) against wormhole attack. This study implements wormhole attack by using out of band channel also, it will detect both Exposed and Hidden Wormhole attack without use any special hardware requirements. Ns2 network simulator software will use for implementing this project.

1.8 Significance of the Study

Due to the mobility and open nature of the MANET, they are much more prone to all kind of security threats. Therefore, increasing security threats for the MANET needs to gain enough attention. As a result, the aim of this project is increasing security in MANET and tries to reduce drawbacks in previous methods and investigate the possibility of method to make a reliable and secure MANET against wormhole Attack.

1.9 Summary

In this chapter introduced the mobile adhoc network (MANET), described about its problem and focused on problem of wormhole attack, and followed by objectives. The project's aims were then discussed. Afterwards, research scope, significance of the study, and the summary of this chapter explained respectively. The next chapter presents the overview of literature of methods in MANET against wormhole attack.

REFERENCES

Agrawal, R., Tripathi, R., and Tiwari, S. (2011). Performance Evaluation and Comparison of AODV and DSR Under Adversarial Environment. *Computational Intelligence and Communication Networks (CICN), 2011 International Conference on*. 596-600.

Agrawal, S., Jain, S., and Sharma, S. (2011). A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks. *arXiv preprint arXiv:1105.5623*.

Ali, M. A., and Sarwar, Y. (2011). *Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions.* Master Thesis Computer Science.

Azer, M., El-Kassas, S., and El-Soudani, M. (2009). A Full Image of the Wormhole Attacks-Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks. *International Journal of Computer Science and Information Security (IJCSIS).* 1(1).

Beijar, N. (2002). Zone routing protocol (ZRP). *Networking Laboratory, Helsinki University of Technology, Finland*.

Ben Othman, J., and Mokdad, L. (2010). Enhancing data security in ad hoc networks based on multipath routing. *Journal of Parallel and Distributed Computing.* 70(3), 309-316.

Chiu, H. S., and Lui, K. S. (2006). DelPHI: wormhole detection mechanism for ad hoc wireless networks. *Wireless Pervasive Computing, 2006 1st International Symposium on*. 6 pp.

Choi, S., Kim, D., Lee, D., and Jung, J. (2008). WAP: Wormhole attack prevention algorithm in mobile ad hoc networks. *Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC'08. IEEE International Conference on*. 343-348.

Deshpande, V. S. (2007). Security in Ad-Hoc Routing Protocols.

Fan, X. (2010). *Efficient Cryptographic Algorithms and Protocols for Mobile Ad Hoc Networks.* University of Waterloo.

Gupta, S., Kar, S., and Dharmaraja, S. (2011). WHOP: Wormhole attack detection protocol using hound packet. *Innovations in Information Technology (IIT), 2011 International Conference on*. 226-231.

Haas, Z. J., Deng, J., Liang, B., Papadimitratos, P., and Sajama, S. (2003). Wireless ad hoc networks. *Encyclopedia of Telecommunications*.

Hu, Y. C., Perrig, A., and Johnson, D. B. (2003). Packet leashes: a defense against wormhole attacks in wireless networks. *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*. 1976-1986.

Hu, Y. C., Perrig, A., and Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless Networks.* 11(1-2), 21-38.

Jain, S. (2010). Detection and prevention of wormhole attack in mobile adhoc networks. *networks.* 1793, 8201.

Jawandhiya, P. M., Ghonge, M. M., Ali, M., and Deshpande, J. (2010). A Survey of Mobile Ad Hoc Network Attacks. *International Journal of Engineering Science and Technology.* 2(9), 4063-4071.

Junhai, L., Danxia, Y., Liu, X., and Mingyu, F. (2009). A survey of multicast routing protocols for mobile ad-hoc networks. *Communications Surveys & Tutorials, IEEE.* 11(1), 78-91.

Kandah, F., Singh, Y., and Wang, C. (2011). Colluding injected attack in mobile ad-hoc networks 235-240.

Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., and Jamalipour, A. (2007). A survey of routing attacks in mobile ad hoc networks. *Wireless Communications, IEEE.* 14(5), 85-91.

Karlsson, J., Dooley, L. S., and Pulkkis, G. (2012). Routing Security in Mobile Ad-hoc Networks. *Issues in Informing Science & Information Technology, Volume 9 (2012).* 9, 369.

Kayarkar, H. (2012). A Survey on Security Issues in Ad Hoc Routing Protocols and their Mitigation Techniques. *arXiv preprint arXiv:1203.3729*.

Khan, Z. A., and Islam, M. H. (2012). Wormhole attack: A new detection technique. *Emerging Technologies (ICET), 2012 International Conference on*. 1-6.

Kumar, K., Kumar, Y., and Munjal, R. (2012). Mobile Ad-Hoc Networks-Various Attacks. *IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011*. 12-15.

Kumar, M. S., Pahal, V., and Garg, S. (2012). Wormhole attack in Mobile Ad Hoc Networks: A.

Mamatha, G., and Sharma, D. S. C. (2010). Analyzing the MANET Variations, Challenges, Capacity and Protocol Issues. *International Journal of Computer Science & Engineering Survey (IJCSES) Vol.* 1.

Mandhata, S., Patro, S., and Mohanty, S. (2012). Exploration of security threats and its performance impact on Mobile Ad-Hoc Networks using NS-2. *International Journal of Computer Applications.* 45(8), 6-11.

Maulik, R., and Chaki, N. (2010). A comprehensive review on wormhole attacks in MANET. *Computer Information Systems and Industrial Management Applications (CISIM), 2010 International Conference on*. 233-238.

Maulik, R., and Chaki, N. (2011). A study on wormhole attacks in MANET. *International Journal of Computer Information Systems and Industrial Management Applications ISSN*, 2150-7988.

N.S.Raote, M., and Mr.K.N.Hande. (2011). Approaches towards Mitigating Wormhole Attack in Wireless Ad-hoc Network. *INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES.* 2(2), 172 - 175.

Rai, P., and Singh, S. (2010). A Review of 'MANET's Security Aspects and Challenges'. *International Journal of Computer Applications IJCA*(4), 162-166.

Roy, D. B., Chaki, R., and Chaki, N. (2010). A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks. *arXiv preprint arXiv:1004.0587*.

Sadeghi, M., and Yahya, S. (2012). Analysis of Wormhole attack on MANETs using different MANET routing protocols. *Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on*. 301-305.

Sen, J., Chandra, M. G., Harihara, S., Reddy, H., and Balamuralidhar, P. (2007a). A mechanism for detection of gray hole attack in mobile Ad Hoc networks 1-5.

Sen, J., Chandra, M. G., Harihara, S., Reddy, H., and Balamuralidhar, P. (2007b). A mechanism for detection of gray hole attack in mobile Ad Hoc networks. *Information, Communications & Signal Processing, 2007 6th International Conference on*. 1-5.

Singh, D., Dubey, V., Sharma, S., Mohapatra, A., Gulati, A., Luthra, R., et al. (2012). Performance Analysis of DSR and AODV in Manets: Using WLAN Parameters. *International Journal of Computer Applications.* 47(3), 1-6.

Song, N., Qian, L., and Li, X. (2005). Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach. *Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International*. 8 pp.

Suganya, S., and Palaniammal, S. (2012). A Dynamic Approach to Optimize Energy Consumption in Mobile Adhoc Network. *European Journal of Scientific Research.* 85(2), 225-232.

Ullah, I., and Rehman, S. U. (2010). Analysis of Black Hole attack on MANETs Using different MANET routing protocols. *Program Electrical Engineering with emphasis on Telecommunication, Type of thesis-Master Thesis, Electrical Engineering, Thesis no: MEE-2010-2698*.

Van Phuong, T., Canh, N. T., Lee, Y. K., Lee, S., and Lee, H. (2007). Transmission time-based mechanism to detect wormhole attacks. *Asia-Pacific Service Computing Conference, The 2nd IEEE*. 172-178.

Vani, A., and Rao, D. S. (2011). Providing of Secure Routing against Attacks in MANETs. *International Journal of Computer Applications (0975–8887) Volume*.

Vigna, G., Gwalani, S., Srinivasan, K., Belding-Royer, E. M., and Kemmerer, R. A. (2004). An intrusion detection tool for AODV-based ad hoc wireless networks. *Computer Security Applications Conference, 2004. 20th Annual*. 16-27.

Vu, H., Kulkarni, A., Sarac, K., and Mittal, N. (2008). Wormeros: A new framework for defending against wormhole attacks on wireless ad hoc networks. *Wireless Algorithms, Systems, and Applications*, 491-502.

Wang, J., Liu, Y., and Jiao, Y. (2011). Building a trusted route in a mobile ad hoc network considering communication reliability and path length. *Journal of Network and Computer Applications.* 34(4), 1138-1149.

Wazid, M., Singh, R. K., and Goudar, R. (2012). A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques. *IJCA Proceedings on International Conference on Computer Communication and Networks CSI-COMNET-2011*.

Win, K. S. (2008). Analysis of Detecting Wormhole Attack in Wireless Networks. *World Academy of Science, Engineering and Technology*. 48, 422-428.

Yi, P., Dai, Z., Zhang, S., and Zhong, Y. (2005). A new routing attack in mobile ad hoc networks. *International Journal of Information Technology*. 11(2), 83-94.