DETECTION OF WORMHOLE ATTACK IN MOBILE AD-HOC NETWORKS

MOJTABA GHANAATPISHEH SANAEI

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

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013

Dedicated to my beloved mother,
my father and my kind sister

ACKNOWLEDGEMENT

I wish to express my deepest appreciation to all those who helped me in one way or another to complete this project. First and foremost I thank God almighty who provided me with strength, direction and purpose throughout the project. Special thanks to my project supervisor Dr. Ismail Fauzi Isnin for all his patience, guidance and support during the execution of this project. Through his expert guidance, I was able to overcome all the obstacles that I encountered in these enduring ten months of my project. In fact he always gave me immense hope every time I consulted with him over problems relating to my project. Even though my research area wormhole detection; was not his specialty, not once did he fail to provide me the duly needed assistance. Simply put his help was invaluable.

I take this opportunity to thank my friends for taking time out of their busy schedule to help me. Last, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as computer laboratory to complete this project with software which I need during process.

ABSTRACT

An ad-hoc network is a group of wireless mobile node that shapes a temporary network without any infrastructure and centralized management. Each mobile node functions are not only restricted to base station but also as router for forwarding packets to other mobile nodes in the network. One primary application of Mobile Ad-hoc Networks (MANETs) is for military purpose including the tactical operations where security is often the major concern. The different leaks that threaten the security of wireless network contain, selective forwarding, wormhole attack, Sybil attack, sinkhole attack and black hole attack. One of the dangerous attacks in mobile ad hoc network is named as wormhole attack in which two or more destructive nodes record the packets at one point and transmits them by a wired or wireless to another point in the network. Wormhole attack is so strong and detection of this attack is hard. Also, the wormhole attack may cause another type of attacks like Sinkhole or Select forwarding. The using a cryptographic technique is not enough to prevent wormhole attack. So, in this study, a new method is proposed based on modifying the forwarding packet process and also using a delay per hop and expiry time technique to detect wormhole. The performance evaluation of the proposed method is done using a mathematical modeling and simulation.

ABSTRAK

Rangkaian ‘ad-hoc’ adalah kumpulan nod mudah alih tanpa wayar yang membentuk rangkaian sementara tanpa sebarang infrastruktur dan pengurusan berpusat. Fungsi bagi setiap nod mudah alih bukan sahaja sebagai stesen pangkalan tetapi juga sebagai laluan penghantaran paket untuk nod mudah alih yang lain di dalam rangkaian. Satu kegunaan utama Rangkaian ad-hoc Mudah alih (Manet) adalah dalam ketenteraan termasuk operasi taktikal. Dalam persekitaran ini keselamatan sering membimbangkan. Pencerobohan yang berbeza telah mengancam keselamatan rangkaian tanpa wayar merangkumi: penghantaran terpilih, serangan ‘wormhole’, serangan ‘Sybil’, serangan ‘sinkhole’ dan serangan ‘black hole’. Salah satu serangan berbahaya dalam rangkaian ‘ad hoc’ mudah alih dinamakan serangan ‘wormhole’ yang mana dua atau lebih nod yang rosak merekodkan paket pada satu titik, dan menghantar mereka melalui wayar atau tanpa wayar ke titik yang lain dalam rangkaian. Serangan ‘worm hole’ begitu kuat dan untuk mengesan serangan ini juga sukar. Selain itu, serangan ‘wormhole’ boleh menyebabkan satu lagi jenis serangan seperti ‘Sinkhole’ atau Pilih penghantaran. Menggunakan teknik kriptografi tidak cukup untuk mencegah serangan ‘wormhole’. Dalam kajian ini, satu kaedah baru dicadangkan yang mana berdasarkan pengubahsuaian proses penghantaran paket dan menggunakan kelewatan setiap hop dan teknik masa tamat untuk mengesan ‘worm hole’. Penilaian prestasi kaedah yang dicadangkan dilakukan dengan menggunakan model matematik dan simulasi.

TABLE OF CONTENTS

LIST OF ABBREVIATION

ANS	Authentication of Node Scheme
AODV	Ad hoc On-Demand Distance Vector
Aridane	A Secure On-Demand Routing Protocol for Ad-hoc Network
BS	Base Station
BSR	Boundary State Routing
CBR	Constant Bit Rate
DaW	Defense against Wormhole
DelPHI	Delay per hop indication
DoS	Denial of Service
DPH	Delay per Hop
DREP	DelPHI Reply
DREQ	DelPHI Request
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HMAC	Hash-based Message Authentication Code
HMTIs	HELLO Message Timing Intervals
IP	Internet Protocol
LEACH	Low Energy Adaptive Clustering Hierarchy
MANET	Mobile Ad-hoc Network
MEMS	Micro Electro Mechanical Systems
NoN	Number of Node
NS2	Network Simulation 2
OLSR	Optimized Link State Routing Protocol
QoS	Quality of Service
RREP	Route Reply Packets

RREQ	Route Request Packets
RRS	Reverse Routing Scheme
RRT	Round Trip Time
RWP	Random Waypoint Model
SEAD	Secure Ad-hoc Distance Vector
UDP	User Datagram Protocol
VANET	Vehicular Ad Hoc Network
WAP	Wormhole Attack Prevention
WMN	Wireless Mesh Network
WPT	Wormhole Prevention Timer
WSN	Wireless Sensor Network

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Overview

Nowadays, by the development of new technologies in the field of science, especially in Micro Electro Mechanical Systems (MEMS), the applications of wireless sensors are increasing rapidly. This application is widely used in militarily monitoring, health monitoring and also for various other purposes.

Generally, the wireless sensor nodes are developed in an untrusted environment. For this reason security becomes one of the important major concerns in these small devices. Wireless mobile nodes usually suffers from security issues such as leakage of secret information, eavesdropping, active interfering, data tampering, message replay, message contamination and denial of service; also the most secure algorithms that are proposed for this issue is not perfect. This study will focuses on the aspects of wormhole attack and the ways to improve WAP (Wormhole Attack Prevention) method as to find the hidden and exposed wormhole attack in the mobile ad-hoc network. A wormhole is a kind of attack that typically happens with two or more malicious nodes in which the first malicious node eavesdrop or listen in packets at one location and then send them by tunnel to the second malicious node in another area by direct link such as cable or strong wireless communication like antenna or cellular broadcasting.

The main goal of this project is to consider these characteristics and behaviors of wormhole attack in MANETs, and the ways to improve the WAP method in order to find the wormhole nodes.

1.2 Background of study

Due to the nature of wireless communications in MANETs, the security problems are more than wired environments. Among the many attacks in wireless network attack, a wormhole is one of the dangerous and specific attacks, that the attacker does not require to exploit nodes in the network, and it can be done via the route foundation method. Without any special environment assumptions, we can use the MHA technique to analysis hop-count from the viewpoint of users. (Jen, Laih et al. 2009) provided a new model to prevent wormhole attack in MANETs that called Multipath wormhole attack analysis. In MHA three steps are needed: first, the hop-count values of all routes should be considered. Then choose a reliable set of paths for data transmission. Finally, send randomly packets through reliable routers, according to decreasing the level of packet that is sent by wormhole. Even if the wormhole is not avoided in some extreme situations, this method can still minimize the level of using the route path through the wormhole. The best property of this technique is no need a special hardware to well-done, it uses RFC3561, the AODV routing protocol, to control packets and modify them to satisfy the requirements.

The primary goal in MOBIWORP technique was to provide primitives that mitigate the wormhole attack in mobile ad hoc networks (Khalil, Bagchi et al. 2008). Mitigation involves detection of the attack, diagnosis of the adversary nodes, and nullifying their capability for further damage. Previous approaches to handling the wormhole attack have concentrated on detection using specialized hardware (Hu and Evans 2004) highly accurate time measurement, specialized trusted nodes and clock synchronization. However, these may not be feasible for many large scale ad hoc or sensor networks due to the hardware complexity or cost. Also importantly, all of these approaches focus only on detecting and avoiding the attack but do not identify

and neutralize malicious nodes. More recent work in a protocol called LITEWORP (Khalil, Bagchi et al. 2005) has provided both detection and local isolation of wormhole nodes. However, it breaks down in mobile scenarios. The limitation arises from the inability to securely determine neighbors at arbitrary points in the lifetime of the network.

A novel trusted-base scheme to detect wormhole node is presented by (Jain and Jain 2010), where a trust model in the form of dynamic source routing (DSR) was used to detect wormhole attack in the network. In DSR protocol the packet contains the address list of each node that has to traverse. In this method the wormhole attack is identified by using effort-return based trust model, which applies DSR protocol to derive and calculate respective trust levels in other nodes.

Delay per hop indication method is presented by (Chiu and Lui 2006), and called as (DelPHI). This method used the delay and hop count information to find disjoint path between sender and receiver when wormhole attack is subjected to these disjoint paths. The benefits are that DelPHI does not need any extra devices, hardware and clock synchronization.

This WAP model introduced by (Choi et al. 2008), called as wormhole attack prevention (WAP) is for preventing the wormhole attack. In this technique when nodes send the request packets to destination, all nodes should monitor the neighbor's behavior, by using a special list called as neighbor list. After the respond packet if received from source node, it can detect the path under wormhole attack between all paths. "Once wormhole node is detected, source node records them in the Wormhole List. Even though malicious nodes have been excluded from routing in the past, the nodes have a good chance to attack once more." So the WAP model stores the information of the malicious nodes at the source node to avoid them taking part in routing again. Furthermore, the WAP method can detect both hidden and exposed attack without any extra devices.

1.3 Statement of problem

Wormhole attack prevention (WAP) method is a detection method that works on DSR routing protocol to identify the wormhole attack in the mobile ad hoc network. The WAP model uses the neighbors monitoring to detect the wormhole. The detection of wormhole in hidden mode is too easy but in exposed mode the nodes play a role of legitimate nodes. Therefore if neighbor nodes of a route are considered as malicious nodes, therefore it can be difficult to identify. The problem statement in this project is to find the route under wormhole attack, while the attacker node will play the legitimate nodes in one route to the destination. (Chiu and Lui 2006; Choi et al. 2008).

The different leaks that threaten the security of sensor network are containing: selective forwarding, wormhole attack, Sybil attack, sinkhole attack and black hole attack. Sinkhole attack occurs when the malicious node announces to node in the network that have low distance to transmit the packets to the destination, so the other node send the packets to malicious node and the traffic goes to the attacker side. Sybil attack is like sinkhole attack, if the attacker is able to illustrate the fake identification of other nodes. In selective forwarding the attacker, first attempts to be reliable by the sender for forwarding the packets to malicious node and finally the attacker select an optional dropping of the packets.

One of the important issues in wireless security is sensor nodes that have been extended in an untrusted environment. In a wireless network if we do not have any security, certainly the attackers can manipulate and compromise the security (Cayirci and Rong 2008). “According to the sensor nodes they are faced with some limitations such as limited memory, short power radios, almost complicated security algorithms are not suitable and applicable for a long time to create a solution and to provide a security unavoidable” (Sookhak et al. 2011).

1.4 Project objectives

The objectives of this study include:

i. To review various methods on the detection of wormhole attack in ad-hoc.
ii. To implement the WAP model and analyze the performance.
iii. To propose a new method and compare the performance with original WAP.

1.5 Research questions

The research questions of this study are:

i. What are the issues for detecting wormhole attack in an Ad-hoc network?
ii. How to implement the wormhole attack detection and analyze the parameter?

1.6 Project scope

This study focuses on detecting the wormhole attack in the DSR routing protocol of the MANET. The network of this study contains the malicious nodes that play the role of route for sending the information from source node to the destination node. Based on the WAP model when all the nodes on one route be a malicious one; then the source node cannot identify, which routes are under wormhole attack.

1.7 Significance of the study

In order to avoid wormhole attack, the nodes participating in the mobile ad hoc network communication have to be registered in the network. Each node is provided with unique ID which would help in maintaining the record of each and every node participating in the network, but this situation enables the attacker to compromise the network easily. Some prevention method exists to avoid this problem but they often cannot be successful to avoid and prevent the attack, for this reason the detection is offered to be collaborate with prevention, when the attacker penetrates the network and prevention method could not avoid to influence the attacker, so here the detection can identify and find the malicious person/node (Choi et al. 2008).

1.8 Summary

In Chapter 1, the overview of the project along with problem backgrounds, problem statements, objectives, research questions and scope of the study are explained. The remaining parts of this study are prepared as follows: In chapter 2, the literature review describes an overview of wormhole attack and several detection methods in wormhole attack. In chapter 3, the proposed method against wormhole attack is explained and finally in chapter 4 the design of the proposed method and simulation method of the proposed method are explained.

REFERENCES

Akyildiz, I. F., et al. (2005). "Wireless mesh networks: a survey." Computer networks 47(4): 445-487.

Altman, E. and T. Jimenez (2003). "NS Simulator for beginners." Lecture notes. Univ. de Los Andes, Merida, Venezuela and ESSI. Sophia-Antipolis, France.

Awerbuch, B., et al. (2008). "ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks." ACM Transactions on Information and System Security (TISSEC) 10(4): 6.

Awerbuch, B., et al. (2002). An on-demand secure routing protocol resilient to byzantine failures. Proceedings of the 1st ACM workshop on Wireless security, ACM.

Baras, J. S., et al. (2007). Intrusion detection system resiliency to byzantine attacks: The case study of wormholes in OLSR. Military Communications Conference, 2007. MILCOM 2007. IEEE, IEEE.

Biswas, K. and M. L. Ali (2007). "Security threats in mobile ad hoc network." Department of Interaction and System Design School of Engineering, march2007: 9-26.

Cayirci, E. and C. Rong (2008). Security in wireless ad hoc and sensor networks, Wiley.

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

Choi, S., et al. (2008). WAP: Wormhole attack prevention algorithm in mobile ad hoc networks. Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC'08. IEEE International Conference on, IEEE.

Dananjayan, P., et al. "Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks."

Das, R., et al. (2012). "Security Measures for Black Hole Attack in MANET: An Approach." arXiv preprint arXiv:1206.3764.

Deng, H., et al. (2002). "Routing security in wireless ad hoc networks." Communications Magazine, IEEE 40(10): 70-75.

Djenouri, D., et al. (2005). "A survey of security issues in mobile ad hoc networks." IEEE communications surveys 7(4).

Giordano, S. (2002). "Mobile ad hoc networks." Handbook of wireless networks and mobile computing: 325-346.

Gorlatova, M. A., et al. (2006). Detecting wormhole attacks in mobile ad hoc networks through protocol breaking and packet timing analysis. Military Communications Conference, 2006. MILCOM 2006. IEEE, IEEE.

Hartenstein, H. and K. P. Laberteaux (2008). "A tutorial survey on vehicular ad hoc networks." Communications Magazine, IEEE 46(6): 164-171.

Hu, L. and D. Evans (2004). Using directional antennas to prevent wormhole attacks. Network and Distributed System Security Symposium (NDSS), San Diego.

Hu, Y.-C., et al. (2003). "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks." Ad hoc networks 1(1): 175-192.

Hu, Y.-C., et al. (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, IEEE.

Hu, Y.-C., et al. (2005). "Ariadne: A secure on-demand routing protocol for ad hoc networks." Wireless Networks 11(1-2): 21-38.

Ilyas, M. (2010). The handbook of ad hoc wireless networks, CRC press.

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

Jen, S.-M., et al. (2009). "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET." Sensors 9(6): 5022-5039.

Kannhavong, B., et al. (2007). "A survey of routing attacks in mobile ad hoc networks." Wireless Communications, IEEE 14(5): 85-91.

Karlof, C. and D. Wagner (2003). "Secure routing in wireless sensor networks: Attacks and countermeasures." Ad hoc networks 1(2): 293-315.

Khalil, I., et al. (2005). LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks. Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on, IEEE.

Khalil, I., et al. (2008). "MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks." Ad hoc networks 6(3): 344-362.

Marti, S., et al. (2000). Mitigating routing misbehavior in mobile ad hoc networks. International Conference on Mobile Computing and Networking: Proceedings of the 6 th annual international conference on Mobile computing and networking.

Naït-Abdesselam, F. (2008). "Detecting and avoiding wormhole attacks in wireless ad hoc networks." Communications Magazine, IEEE 46(4): 127-133.

Ngadi, M., et al. (2008). "A review current routing attacks in mobile ad-hoc networks." International Journal of Computer Science and Security 2(3): 18-29.

Papadimitratos, P. and Z. J. Haas (2002). Secure routing for mobile ad hoc networks. Proceedings of the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS).

Roy, D. B., et al. (2010). "A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks." arXiv preprint arXiv:1004.0587.

Sanzgiri, K., et al. (2002). A secure routing protocol for ad hoc networks. Network Protocols, 2002. Proceedings. 10th IEEE International Conference on, IEEE.

Slijepcevic, S., et al. (2002). On communication security in wireless ad-hoc sensor networks. Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on, IEEE.

Sookhak, M., et al. (2011). "Detection Wormhole in Wireless Ad-hoc Networks." International Journal of Computer Science and telecommunication 2(7): 7.

Vivian, D., et al. (2006). Evaluation of QoS Metrics in Ad Hoc Networks with the use of Secure Routing Protocols. Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP, IEEE.

Wang, X. and J. Wong (2007). An end-to-end detection of wormhole attack in wireless ad-hoc networks. Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International, IEEE.

Wu, B., et al. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. Wireless Network Security, Springer: 103-135.

Yang, H., et al. (2004). "Security in mobile ad hoc networks: challenges and solutions." Wireless Communications, IEEE 11(1): 38-47.