SECURITY IN WIRELESS SENSOR NETWORK ENHANCED AODV ROUTING

RAZATULSHIMA BINTI GHAZALI

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Engineering (Electrical – Electronics & Telecommunication)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

NOVEMBER 2006

To my beloved family… my faithful husband Sabaahul Ahmad, for all your support and encourages and all my sons Ammar Syafiq, Aiman Syakir and Amir Safwan.

ACKNOWLEDGEMENT

I wish to express my sincere appreciation to my beloved and respectful supervisor, Professor Dr. Norsheila Fisal, for encouragement, guidance, critics and friendship. There are so much precious knowledge I get under her guidance and friendship.

I am also thankful to Mr.Adel and Professor Madya Puan Liza Abd Latif, Phd students for their guidance, advices and motivation. Their continued support and time has made the completion of the thesis possible.

I would never have been able to make this accomplishment without my loving support of my husband, family and friends who have provided assistance at various occasions.

ABSTRACT

An ad-hoc network comprises mobile nodes that cooperate with each other using wireless connections to route both data and control packets within the network. They are characterized by the used of wireless links, dynamically changing topology, multi-hop connectivity and decentralized routing mechanism and decision-making. Previous studies have shown limitations of Ad-hoc On Demand Vector (AODV) protocols in certain network scenario. The performance of AODV has been modifying by including the source route accumulation feature define as AODV with path accumulation (AODV-PA). As low transmission power of each ad-hoc node limits its communication range, the nodes must assist and trust each other in forwarding packets from one node to another. However, this implied trust relationship can be threatened by malicious nodes that may fabricate, modify or disrupt the orderly exchange of packets. Security demands that all packets be authenticated before being used. A particularly hard problem is to provide efficient broadcast authentication, which is important mechanism for sensor networks. This project, proposed a solution; to include the authentication key along path accumulation to enhance the security of the data transferred. It is done by inserting the authentication key in the agent DYMOUM payload, which responsible for path accumulation process in AODV-PA. Network Simulator2(Ns2) has been used as the platform for the simulation environment and authentication key has programmed by using C.

ABSTRAK

Ad-hoc merupakan rangkaian nod-nod yang bekerjasama antara satu sama lain menggunakan hubungan tanpa wayar bagi penghantaran data dan mengawal paket di dalam rangkaian. Ia di kategorikan mengikut sambungan tanpa wayar, topologi yang berubah secara dinamik, hubungan pelbagai-lompatan dan mekanisme pengagihan laluan dan kuasa membuat keputusan. Kajian sebelum ini menunjukkan batas-batas di dalam protokol Ad-hoc On Demand Vector (AODV) di dalam senario rangkaian tertentu. Bagi membaiki mutu AODV, ia telah diubahsuai dengan memasukkan pengumpulan ciri-ciri sumber yang dipanggil *AODV with path accumulation* (AODV-PA). Kuasa penghantaran yang rendah antara nod ad-hoc membataskan julat komunikasi, dan nod hendaklah mempercayai antara satu sama lain pada masa penghantaran paket dari satu nod ke nod lain. Walaubagaimana pun, kebolehpercayaan dalam perhubungan ini boleh diancam oleh nod-nod liar yang berupaya mereka, menukar atau mengacau-bilaukan susunan pertukaran paket-paket. Keselamatan memerlukan kesemua paket diberikan pengesahan sebelum digunakan.. Bahagian yang paling sukar adalah untuk memastikan penyebaran pengesahan yang berkesan, yang mana merupakan mekanisma yang penting untuk rangkaian pengesan. Projek ini mencadangkan satu penyelesaian ; memasukkan kunci pengesahan bersama *path accumulation* untuk menambahkan lagi keselamatan dalam pemghantaran data. Ia dilakukan dengan menyelitkan kunci pengesahan di dalam *payload agent DYMOUM* yang bertanggungjawab dalam proses *path accumulation.Network Simulator (NS2)* digunakan sebagai platform dalam persekitaran simulasi dan kunci pemgesahan diprogramkan menggunakan bahasa program C.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

m^2	-	meter square
s	-	second
Mb/s	-	Megabyte per second
µ	-	micro
m	-	meter
pkt	-	packet

CHAPTER 1

INTRODUCTION

1.1 Ad Hoc Networks

Mobile ad hoc networks are a new paradigm of wireless communication for mobile hosts. Hosts are always represented as different nodes in the mobile ad hoc networks. There are a number of differences between mobile ad hoc networks and traditional networks. Ad hoc networks do not rely on any fixed infrastructure. It relies on each other to keep the network connected. Also, the topology of ad hoc networks is dynamically changing and its communication is based on wireless links. Due to the above characteristics, the main challenge in the design of mobile ad hoc networks is their vulnerability to security attacks. Securing mobile ad hoc networks is particularly difficult with its characteristics. The problem is so broad that there is no way to devise a general solution. It is also clear that different applications will have different security requirements

In future, the increasing miniaturization of electronic components and advances in modern communication technology make the development of powerful spontaneously networked and mobile systems possible. In the next 15 years, wireless sensor networks have an enormous economical potential. Sensor networks consist of a huge number of small sensor nodes, which communicate wirelessly. These sensor nodes can be spread out in hard accessible areas by what new applications fields can be pointed out. A sensor node combines the abilities to compute, communicate and sense.

The aim is to fit all mentioned features in a single chip solution. In principle, controlling of an actuator is possible, too. The development of sensor nodes is influenced by:

- ✓ increasing device complexity on microchips,
- ✓ high performance, wireless networking technologies,
- ✓ a combination of digital signal processing and sensor data acquisition,
- ✓ advances in the development of micro electromechanical systems (MEMS), and
- ✓ Availability of high performance development tools.

1.2 AODV with Path Accumulation (AODV-PA)

An ad hoc network is collection of mobile nodes that are capable of communicating with each other without the aid of any established infrastructure or centralized administration. They are self-organized, dynamically changing multi-hop networks. Each node in an ad hoc network performs the dual task of being a possible source/destination of some packets while at the same time acting as a router for other packets to their final destination.

Two of the leading ad-hoc network routing protocols are the Ad hoc On-Demand Distance Vector Routing protocol (AODV) and the Dynamic Distance Vector Routing protocol (DSR). Previous work has studied the performance of AODV and DSR in a variety of scenarios. This work showed that both AODV and DSR drop in performance at high velocities or when the number of connections is high. The AODV and DSR performance can be improved by include the source route accumulation feature that called AODV with path accumulation. This is the accumulation of the source route in request and reply packets during the route discovery process in AODV. By accumulating this information, nodes can learn an increased amount of routing information to different destinations. Because of the resulting decrease in the number of route discoveries, the proposed modification should lead to a reduction in the routing load of AODV.

1.3 Security in Wireless ad-hoc sensor network

Security is not easy; compared with conventional desktop computers. Severe challenges exist due to sensors having limited processing power, storage, bandwidth, and energy. We need to surmount these challenges, because security is so important. Sensor networks are used in a number of domains that handle sensitive information. Due to this, there are many considerations that should be investigated related to protecting sensitive information traveling between nodes (which are either sensor nodes or the base station) from being disclosures to unauthorized third parties.

In Mobile Ad-hoc Networks (MANET), each mobile node functions as both a host and a router. Mobile nodes are typically powered by batteries, and have less powerful computing resources than desktop computers. Moreover, the network topology is highly dynamic due to the movements of the nodes. These features introduce unique problems that do not appear in traditional, wired networks. To ensure the security of the network, it is critical to develop security mechanisms that can survive malicious attacks. The protection of routing from adversaries is necessary for any wireless ad hoc network to be adopted for a critical mission. Such necessity is exacerbated by the fact that the criteria for admitting routers in an ad hoc network may not be strict. An adversary can meet his objective to disrupt the packet delivery service by attacking either route discovery or data packet forwarding.

Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. All these mean that a wireless ad-hoc network will not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly. Another characteristic is that there is dynamic changing topology. Mobile nodes are autonomous units that are capable of roaming independently. Nodes roaming in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Therefore, not just external attacks should be considered, but attacks launched inside the network by compromised nodes should also be dealt with. It means that nodes with inadequate physical protection are receptive to being captured, compromised, and hijacked. It is easy to attach and hard to detect, so any node in a wireless ad-hoc network must be prepared to operate in a mode that trusts no peer.

1.4 Problem Statement

The most popular routing protocol in ad-hoc networks are the AODV and the DSR protocols. They are often been used for research on securing routing protocols. The most significant difference between the AODV and the DSR protocols is their route reply message. In AODV protocol, the route attribute in the route reply message only contains the next hop address. However, the route attribute in the route reply message contains the addresses of all the intermediate nodes on the route in DSR. Therefore, the route reply message of DSR is longer and less scalable. Due to the above reason, AODV may be the more favorable routing protocol in the future. This project is developing a new secure routing protocol in ad hoc network based on the AODV-PA protocol.

AODV and DSR are having an efficient in terms of networks performance. However AODV and DSR also allow attackers to easily advertise falsified route information, to redirect routes, and to launch denial-of-service attacks. AODV can be modified to enable path accumulation during the route discovery cycle. This should decrease the number of route discovery cycles as compared to basic AODV. AODV-

PA increases the efficiency of AODV. In order to avoid the attacker, the authentication key is distributed along the path accumulation to enhance the security of the AODV-PA thus only the nodes in the accumulated path will get the key and source will validate the destination node.

1.5 Objective

Unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks, those functions are carried out by all active nodes. This very difference is at the core of the increased sensitivity to nodes misbehavior in ad hoc networks. If a priori trust relationship exists between the nodes of an ad hoc network, entity authentication can be sufficient to assure the correct execution of critical network functions. A priori trust can only exist in a few special scenarios.

A secured route discovery protocol will not suffice to protect against a determined adversary; such an adversary can, for example, instruct its routers to announce fictitious links so as to attract traffic and then drop the packets they receive, or known as Man In The Middle (MAIM) attacks. The objectives of this project are:-

- To develop on authentication mechanism
- To distribute the authentication key along path accumulation
- To ensure only authenticated destination will get the data.

1.6 Scope

Security protocols in network normally require cryptographic operations. In this project, the authentication key has not encrypted and it was distributed to nodes through the path accumulation established in AODV, make it easier and simple. This means only the nodes in path accumulation are authenticated in the network to send the packet/data. A key management scheme keeps track of bindings between keys and nodes, and assisting the establishment of mutual trust and secure communication between nodes. The 802.15.4 Network Simulator-2 (NS-2) is used to simulate the AODV-PA by capturing the traffic and passed it through the simulated network. The authentication key is programmed using C that inserted in the DYMOUM Routing Element (RE) programming from MASIMUM. The operating system environment need is Linux Fedora Core 3.

1.7 Thesis outline

This thesis consists of 5 chapters. Each chapter elaborates different stage development of this project until to the conclusions. First chapter of this thesis describes the background of the project, problem statements, objectives and the scope of the project.

Second chapter is about the literature reviews that have been made in order to complete the tasks of the project. Most of the literature reviews are taken from IEEE and the journals that have been made by the researcher in the wireless sensor networks areas.

The development of AODV-PA is quite new in wireless sensor networks and also the implementation of security data transfer in AODV-PA, still in progress. Literature reviews in area connected in AODV-PA are very helpful since it is still instead of other routing protocols.

Third chapter explain the methodology parts of this project. In this chapter, elaborate the path accumulation process more details. It also describes the network model use in the project. The simulations to compares effectiveness between AODV and AODV-PA are simulating using NS-2 and visualize it by NAM also have been show in this chapter.

The fourth chapter is describes more details the process of the authentication keys development, the programming codes and the distribution of the authentication keys. In this chapter also show the graphical pictures of the whole process. The process of key distribution is also explained in this part. The results of using AODV-PA with correct authentication keys and fake authentication keys are show using NS-2 simulator. AWK program is also used to compare the average delay and round trip time of the AODV-PA with keys and without the keys.

The last chapter of the thesis is the conclusion of the project. This chapter explains briefly the processes have been done in the project as well the results. Future recommendations are also include in this chapter to improve this project for future works.

REFERENCES

1. Samir R. Das, Charles E. Perkins, and Elizabeth M. Royer . Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks. *Proceedings of the IEEE Conference on Computer Communications (INFOCOM).* March 2000, Tel Aviv, Israel: IEEE. 2000. 1-3.

2. B. Warneke, M. Last, B. Leibowitz, and K. Pister. Smart dust: Communicating with a cubic-millimeter computer. *IEEE Computer Magazine.* January 2001.

3. Peng Ning, Kun Sun. How To Misuse AODV: A Case of Insider Attacks against Mobile Ad-Hoc Routing Protocol, *IEEE Systems, Information Assurance Workshop, West Point, New York,* May 2002. *USA*. IEEE 2003. 1-38.

4. Qifeng Lu (2002). *Vulnerability of Wireless Routing Protocols*, University of Massachusetts Amherst. Unpublished.

5. Panagiotis Papadimitratos and Zygmunt J. Haas. Secure Routing for Mobile Ad hoc Networks. *In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, TX,* January, 2002. CNDS 2002. 1-13.

6. Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz, Elizabeth M. Belding : A Secure Routing Protocol for Ad Hoc Networks, *Proceedings of the 10th IEEE International Conference on Network Protocols.* IEEE Computer Society 2002. 1-3.

7. Sumit Gwalani, Elizabeth M. Belding-Royer and Charles E. Perkins: AODV-PA: AODV with Path Accumulation, *IEEE International Conference on Communications*. 15 May 2003. IEEE 2003. 1-5.

8. Jan Blumenthal, Matthias Handy, Frank Golatowski, Marc Haase, Dirk Timmermann. Wireless Sensor Networks - New Challenges in Software Engineering. *Proceeding EIFA '03, IEEE Conference Emerging Technologies and factory Automation 2003*, 16-19 Sept. IEEE 2003.1-6.

9. C. Buschmann, S. Fischer, N. Luttenberger, and F. Reuter. Middleware for swarm-like collections of devices. *IEEE Pervasive Computing Magazine*, 2003.

10. Ian D. Chakeres and Elizabeth M. Belding-Royer. AODV Routing Protocol Implementation Design. *Proceedings of the International Workshop on Wireless Ad Hoc Networking (WWAN), Tokyo, Japan*, March 2004. DBLP 2004. 1-6.

11. Asad Amir Pirzada and Chris McDonald. Kerberos Assisted Authentication in Mobile Ad-hoc Networks. *Proceedings of the 27th Australasian conference on Computer science, Dunedin, New Zealand.* Australian Computer Society, Inc 2004. 4-6.

12. Xuefei Li, Lurie Cuthbert. On-Demand Node – Disjoint Multipath Routing in Wireless Ad Hoc Networks. *Proceeding of the 29th Annual IEEE International Conference on Local Computer Networks*, 2004. IEEE 2004. 1-3.

13. Elaine shi, Adrian Perrig. Designing secure sensor networks, *IEEE Wireless Communications*, December 2004. IEEE 2004. 1-6.

14. André Weimerskirch (2004). *Authentication in Ad-hoc and Sensor Networks.* University of Ruhr Bochum: Ph.D. Thesis.

15. Chris Karlof, Naveen Sastry, David Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. *Proceedings of the Second ACM*

Conference on Embedded Networked Sensor Systems, South Charles St., Baltimore. November 2004. SenSys 2004. 1-15.

16. I.Chakeres Boeing, E Belding-Royer. Dynamic MANET On-demand (DYMO) Routing. *Proceeding of Mobile Ad hoc Networks, UC Santa Barbara.* Oktober 2005. IETF. 2006.1-9.

17. Jianliang Zheng, Myung J. Lee. A Comprehensive Performance Study of IEEE 802.15.4. *Sensor Network Operations Wiley Interscience*, IEEE Press 2006. 1-14.