SECURE ROUTING USING FREQUENCY HOPPING
IN WIRELESS SENSOR NETWORK

RAJA ZAHILAH BINTI RAJA MOHD. RADZI

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

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

MAY 2007

For Mak and Ayah.
For Anata and our little Princesses.

ACKNOWLEDGEMENT

In preparing this master project, I was in contact with many people, researchers, and academicians. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my thesis supervisor, Professor Dr. Hjh. Norsheila Fisal, for encouragement, guidance, critics and friendship. Without her continued support and interest, this project report would not have been the same as presented here.

I am also indebted to Universiti Teknologi Malaysia (UTM) for funding my Ms. study. Librarians at UTM also deserve special thanks for their assistance in supplying the relevant literatures.

My fellow postgraduate students (especially Mr. Adel and Mrs. Razatulshima) should also be recognized for their support. My sincere appreciation also extends to all my colleagues at Department of Computer System and Communication, Faculty of Computer Science and Information System, UTM and others who have provided assistance at various occasions. Their views, comments and tips are very helpful. Finally, I am also very grateful to all my family members for their continuous encouragement and support.

ABSTRACT

Wireless ad hoc sensor networks (WSN) operate in the absence of a pre-deployed infrastructure, are self-configurable, low cost and can be rapidly deployed. Hence, such networks enable a variety of consumer applications, such as emergency rescue, disaster relief, smart homes and patient monitoring, industrial applications, such as structural health monitoring and environmental control, and military applications, such as target identification and tracking. WSN are prone to failure and malicious user attack because any device within the frequency range can get access to the data being transmitted. Thus, the project aims to provide a secure WSN through frequency hopping at the network layer. In this work, Ad hoc On Demand Distance Vector Routing algorithm is used to determine the route and un-Slotted Carrier Sense Multiple Access / Collision Avoidance (slotted CSMA/CA) algorithm is used to access the medium. The frequency hopping algorithm was tested in WSN environment with and without malicious node. The results show tremendous decreased of throughput from malicious node when the number of frequency hop is increased. Therefore, WSN's security is improved even though the throughput from source is slightly decreased. Proposed future works are addition of frequency synchronization with beacon using slotted CSMA-CA and addition of multiple interfaces support for IEEE 802.15.4 standard.

ABSTRAK

Rangkaian Sensor Tanpa Wayar (WSN) beroperasi dalam infrastruktur yang segera, boleh mengkonfigurasi sendiri, kos yang rendah dan sangat mudah dirangkaikan. Oleh itu, rangkaian ini berupaya menyokong pelbagai aplikasi pengguna seperti operasi menyelamat, bencana alam, pemantauan pesakit, pemantauan rumah pintar, aplikasi industri seperti pemantauan keselamatan struktur, pengawalan alam sekitar dan aplikasi ketenteraan seperti mengenalpasti dan mengesan target. WSN sangat mudah menghadapi ketidakfungsian dan serangan pengguna kerana sebarang peralatan yang berada di dalam julat frekuensi boleh mencapai data yang sedang dihantar. Oleh itu, projek ini bertujuan untuk menyediakan WSN yang selamat dengan menggunakan *frequency hopping* di aras Rangkaian. Dalam projek ini, algoritma *Ad hoc On Demand Distance Vector Routing* digunakan untuk mengenalpasti perjalanan data dan algoritma *un-Slotted Carrier Sense Multiple Access / Collision Avoidance* (*slotted CSMA/CA*) digunakan untuk mencapai medium penghantaran. Algoritma *frequency hopping* telah diuji dalam WSN dengan dan tanpa kehadiran nod asing. Keputusan menunjukkan penurunan truput yang sangat ketara daripada nod asing apabila bilangan frekuensi ditambah. Oleh itu, keselamatan WSN telah dapat dipertingkatkan walaupun truput daripada sumber juga mengalami sedikit penurunan. Cadangan sambungan kerja penyelidikan ialah penambahan frekuensi segerak dengan *beacon* menggunakan *slotted CSMA/CA* dan penambahan sokongan antaramuka yang banyak untuk standard IEEE 802.15.4.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACK	-	Acknowledgement
AODV	-	Ad hoc On-demand Distance Vector
AWK	-	derived from surname of its author (Alfred **A**ho, Peter **W**einberger, and Brian **K**ernighan)
BE	-	Backoff Exponent
BP	-	Backoff Period
CAP	-	Contention Access Period
CBR	-	Continuous Bit Rate
CCA	-	Clear Channel Assessment
CFP	-	Contention Free Period
CTS	-	Clear-To-Send
CSMA/CA	-	Carrier Sense Multiple Access/ Collision Avoidance
CSMA/CD	-	Carrier Sense Multiple Access/ Collision Detection
CW	-	Contention Window
DARPA	-	Defense Advanced Research Project Agency
FC6	-	Fedora Core 6
FTP	-	File Transfer Protocol
GENOME	-	GNU Network Object Model Environment
GTS	-	Guaranteed Time Scale
GUI	-	Graphical User Interface
IEEE	-	Institute of Electrical and Electronic Engineering

IP	-	Internet Protocol
ISM	-	Industrial, Scientific and Medical
Kbps	-	Kilobits per Second
KDE	-	K Desktop Environment
LOS	-	Line of Sight
LQI	-	Link Quality Indication
LR-WPAN	-	Low Rate Wireless Personal Area Network
Mbps	-	Megabits per Second
MHz	-	Mega Hertz
NAM	-	Network Animation
NB	-	Number of Backoffs
NS	-	Network Simulator
OSI	-	Open System Interconnection
PTYPE	-	Packet Type
RREP	-	Route Reply
RREQ	-	Route Request
RTP	-	Real-time Transport Protocol
RTS	-	Request-To-Send
TCL	-	Tool Command Language
TCP	-	Transmission Control Protocol
TS_	-	Time Stamp
UDP	-	User Datagram Protocol
UID	-	Unique Identity
VINT	-	Virtual InterNetwork Test-bed
WPAN	-	Wireless Personal Area Network

WSN	-	Wireless Sensor Network

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 A Review of Wireless Sensor Network

Wireless Sensor Network is a set of large number of sensors which provide a smart environment surrounding us, the sensors respond to its particular sensing characteristic changes around them and send the information to centre of processing unit. SmartDust program which is sponsored by DARPA defined sensor networks as:

> *"A sensor network is a deployment of massive numbers of small, inexpensive, self-powered devices that can sense, compute and communicate with other devices for the purpose of gathering local information to make global decisions about a physical environment."* (Olariu, 2006)

Sensor is a device which is very small, using low power to process or compute, use within short range of distance, got energy budget (battery) and got micro-sensor technology. Usually, it is link by wireless medium such as radio, infrared, ultrasound, laser and many more but the most popular medium is radio because it can operate without line of sight (LOS). Types of sensor are pressure sensor, temperature sensor, humidity sensor, seismic sensor, light sensor, chemical sensor and many more.

WSN was initially developed for military and disaster rescue purposes but because the availability of ISM band (2.4 GHz), the technology are now emerging in public applications.

The salient features in Wireless Sensor Network makes it different from other network (self-organize, low power, self configure, wireless, infrastructure-less).

Therefore, WSN design must encounter these features in order to provide a reliable network. One more thing to be considered is the fact that WSN are prone to failure and malicious user attack. This is because any device within the frequency range can get access to the data. So, we need a secure way to protect the network. Wireless communication only affects the physical, data link and network layers of the OSI layer.

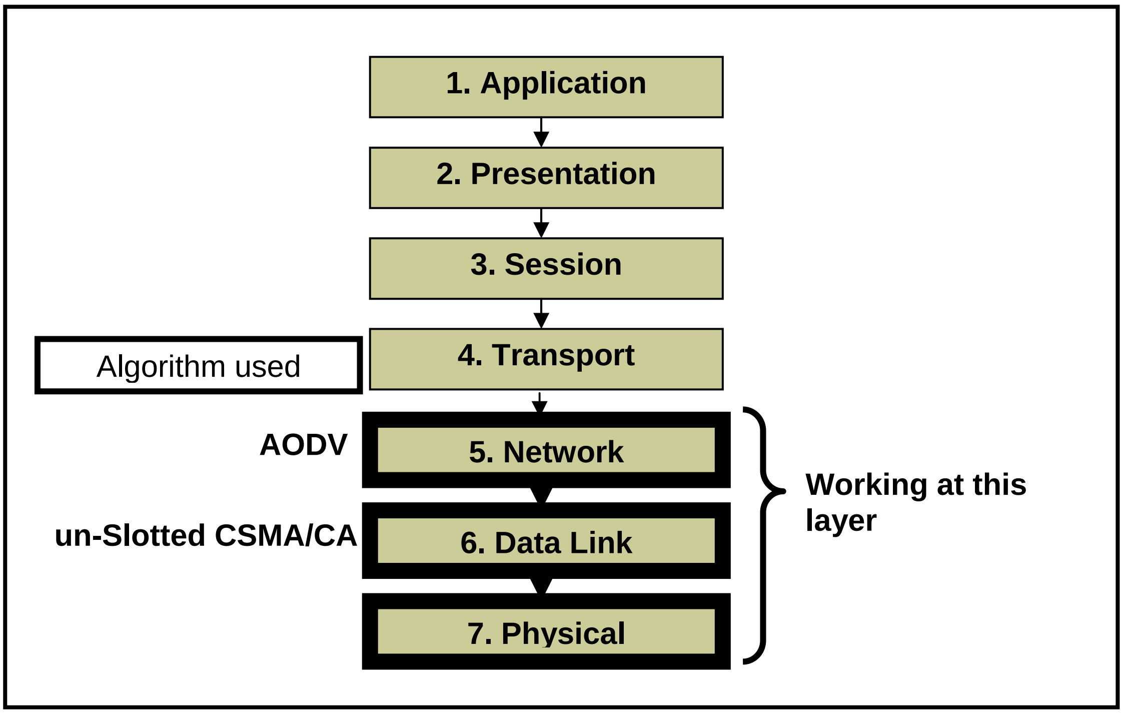

Figure 1.1: Open System Interconnection Layer

1.2 Statement of the Problems

Security attacks are consists of passive attacks and active attacks (William, 2003). When there is an observer who trying to obtain any information being transmitted, it is considered passive attack. Eavesdropping or monitoring of transmission is an example of passive attacks. When there is an attack to modify the data stream, it is considered an active attack such as denial of services.

In order to achieve secure routing in WSN, the frequencies used need to be change within a short period of time. If there is any malicious node trying to send information or retrieve information inside the WSN, the attempt can be prevent if the node can’t detect the frequencies that changes very quickly. Therefore, by using frequency hopping, we can prevent any intruder to reach the frequency. Thus, applying frequency hopping will secured the network.

1.3 Objectives

There are many kinds of security mechanism exists. The most common mechanism is encryption techniques (William, 2003). The techniques require security keys in the algorithm which consume the memory storage space inside the device. So, in wireless sensor network which aims to use as minimal space as they can in order to save energy, frequency hopping techniques was chosen.

In order to know the performance of the system, the throughput at destination was analyzed. Source and malicious node are sending the same amount of packets to the same destination. The throughput before the used of frequency hopping is examine first and then, the throughput after the used of frequency hopping is compared. After that, throughput from source and from malicious node is compared and the network performance can be seen.

In short, the objectives of this project are:

- To develop security in Wireless Sensor Network using frequency hopping method,
- To analyze the throughput before and after the implementation of frequency hopping.

1.4 Scopes

The simulation environment and testing parameter are based on Wireless Sensor Network according to IEEE 802.15.4 standard. 25 nodes are created in NS2 which runs on Linux Operating System. The nodes are assumed to be static and no hidden nodes between each other (all nodes within the signal range of the network). The security is base on frequency that hops randomly and the frequency is set during routing at Network layer. The frequency hopping algorithm was programmed using C++ and inserted into AODV functions, while the WSN environment was programmed using TCL. Then, analysis of the trace files were done by using AWK programming. Simulations of the nodes are automatically demonstrated using NAM which has been set inside the TCL programming.

1.5 Importance of the Study

Wireless Sensor Network is categorized in IEEE 802.15.4 task group which is in Low Rate Wireless Personal Area Network. The standard was just released in 2003 and the up grade version was released in 2006. Since this is a new research area, there are lots of arguments to be discussed and solved such as power consumption because the sensors depends on battery which only remains for a short period of time, topology because sensors can be static or mobile; and the topology is ever changing not only because of sensor mobility but also because of sleep-and-wake cycles of the sensors, bandwidth because usable bandwidth in WSN are limited compared to wired network, contribute by multi-path fading, noise and interference; and security because wireless is too vulnerable whether to insider user or outsider users attack. Therefore, one of topic of discussion (security) is chosen to be focused on this project.

1.6 Thesis Outline

The thesis consists of five chapters which include Introduction; Reviews of System; The Flow Process of Project; Results, Analysis and Discussion and finally Conclusion and Proposed Future Works. Besides these, there are preliminary pages which help the reader to understand the whole thesis outline such as table of contents and the listing of table, figures, abbreviations and appendices. There are also additional pages (appendices) at the end after the list of reference. The appendices show project planning and programming code listings.

Chapter 1 describes Wireless Sensor Network in general and then follows by problem statements, the project’s objectives, the scopes which guide the project boundary, the importance of the study and finally the whole thesis outline.

Chapter 2 elaborates the ideas from Chapter 1 in more details. This chapter was written based on various readings from IEEE website, journals, books and also the internet. All the references can be found at the list of References after the final chapter.

Chapter 3 explains the process of the whole project from installing the operating system until testing procedure and testing process.

Chapter 4 shows the results of simulation and testing in NS2 and NAM. There are animation captures in NAM and analysis results of the trace files.

The final chapter, Chapter 5 summarized the work that has been done and two proposals of future works that can be developed to enrich the test bed environment.