SECURE ROUTING IN WIRELESS SENSOR NETWORKS

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Computer Science & Engineering

By:
Suman Bala
(80732024)

Under the supervision of:
Dr. A. K. Verma
Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

MAY 2009

Certificate

I hereby certify that the work which is being presented in the thesis entitled, **"Secure Routing in Wireless Sensor Networks"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in Computer Science and Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. A. K. Verma* and refers other researcher's works which are duly listed in the reference section.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

(***Suman Bala)***

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(**Dr. A. K. Verma)**
Assistant Professor
Computer Science & Engineering Department
Thapar University
Patiala.

Countersigned by:

(SEEMA BAWA)
Professor & Head
Computer Science & Engineering Department,
Thapar University,
Patiala.

(R.K.SHARMA)
Dean (Academic Affairs)
Thapar University,
Patiala.

Acknowledgement

No volume of words is enough to express my gratitude towards my guide, ***Dr. A. K. Verma****, Assistant. Professor, Computer Science and Engineering Department, Thapar University, who has been very concerned and has aided for all the material essential for the preparation of this thesis report. He has helped me to explore this vast topic in an organized manner and provided me with all the ideas on how to work towards a research-oriented venture.*

I am also thankful to ***Mrs. Seema Bawa****, Head of Department, CSED and* ***Mrs. Inderveer Channa****, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.*

I would also like to thank the staff members and my colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis.

Most importantly, I would like to thank my parents and the Almighty for showing me the right direction out of the blue, to help me stay calm in the oddest of the times and keep moving even at times when there was no hope.

Suman Bala

80732024

Abstract

Wireless Sensor Networks is the new concept in the field of networks consists of small, large number of sensing nodes which is having the sensing, computational and transmission power. Due to the lack of tamper-resistant packaging and the insecure nature of wireless communication channels, these networks are vulnerable to internal and external attacks. Moreover, routing protocols are designed, taking the consideration of power consumption not security as a goal. As security plays an important role in the ability to deploy and retrieve trustworthy data from a wireless sensor network. The proper operations of many WSNs rely on the knowledge of routing algorithms. However, most existing routing algorithms developed for WSNs are vulnerable to attacks in hostile environments.

Current routing protocols assume the networks to be benevolent and cannot cope with misbehaviour of nodes. The misbehaviour may be due to node being malicious to save the battery power. Whenever any device comes within the frequency range can get the access to the transmitting data and may affect the transmission. Thus, this work has significant importance, to build a highly secure system through frequency hopping.

Keywords: Security, Wireless Sensor Networks, Frequency hopping.

Table of Contents

Certificate.....i

Acknowledgement.....ii

Abstract.....iii

Table of Contents.....iv

List of Figures and Tables.....viii

Chapter 1: INTRODUCTION.....1

1.1. Motivation.....1

1.2. State of the Art.....2

1.3. Importance of the Study.....3

1.4. Thesis Outline.....3

Chapter 2: BACKGROUND INFORMATION.....5

2.1. Wireless Sensor Networks.....5

2.1.1. Wireless Sensor Network Model.....6

2.1.2. The Sensor Node.....7

2.1.3. Wireless Sensor Node Communication Architecture: Protocol Stack.....8

2.1.4. Routing Techniques in Wireless Sensor Networks……..9

2.2. Security in Wireless Sensor Networks……10

2.2.1. Security Goals for Sensor Networks……10

2.2.2. Security Challenges……11

2.2.3. Threat Models……11

2.2.4. Secure Routing in Wireless Sensor Networks……13

Chapter 3: LITERATURE REVIEW……14

3.1. Routing Protocol……14

3.1.1. Ad-hoc On-demand Distance Vector (AODV)……14

3.1.2. Security Issues in AODV……17

3.2. The Frequency Hopping……18

3.3. IEEE 802.15.4 Standard: LR-WPAN……19

3.3.1. Network Topologies……19

3.3.2. The Physical Layer……19

3.3.3. The MAC Sub-Layer……21

3.3.4. The Superframe Structure……22

3.3.5. Carrier Sense Multiple Access – Collision Avoidance……23

3.3.6. Data Transfer Model…….. ...26

Chapter 4: PROBLEM STATEMENT & OBJECTIVE..... …27

4.1. Problem Statement..... …27

4.2. Objective and Sub-Tasks..... …28

Chapter 5: INSTALLATION, SIMULATION & DESIGN..... …29

5.1. Fedora Core 4..... …29

5.2. The Network Simulator (NS2)..... …29

5.2.1. NS2 Overview..... …29

5.2.2. Tool Command Language (Tcl)..... …30

5.2.3. The Network Animation (NAM)..... ...31

5.2.4. The Trace File..... ...31

5.2.5. The Tracegraph..... ...32

5.2.6. Low Rate WPAN Function Modules..... ...32

5.3 Frequency Hopping..... ...33

5.4. Simulation..... ...35

Chapter 6: RESULTS, PERFORMANCE EVALUATION & ANALYSIS..... ...36

6.1. AODV Simulation..... ...36

6.2. AODV with Frequency Hopping....38

6.3. AODV with Malicious Node....39

6.4. AODV with Malicious Node and Frequency Hopping....41

Chapter 7: CONCLUSION & FUTURE SCOPE....42

ANNEXURES

I REFERENCES....44

II ABBREVIATIONS....48

III LIST OF PUBLICATIONS....50

List of Figures and Tables

Fig.2.1. Components of Wireless Sensor Networks..……...6

Fig.2.2. Components of a wireless sensor node .....…….....7

Fig.2.3. Protocol stack .....….....…….....9

Fig.3.1. AODV; (a) Timing diagram, (b) Broadcasts a HELLO packet.....14

Fig.3.2. Structure of a RREQ packet ...…….15

Fig.3.3. Path discovery of AODV.....……...16

Fig.3.4. Network topologies: (a) Star, (b) Tree, (c) Mesh .....….....19

Fig.3.5. Layer approach of IEEE 802.15.4....……..……..…....21

Fig.3.6. A superframe structure .....….....…….23

Fig.3.7. Timing diagram for CSMA-CA .....……....23

Fig.3.8. Un-slotted CSMA/CA flow chart..…….…….....25

Fig.5.1. Running NS2 program.....30

Fig.5.2. Fields of trace file.....31

Fig.5.3. LR-WPAN (IEEE 802.15.4) function modules.....33

Fig.5.4. Frequency hopping at transmitting side……...34

Fig.5.5. Frequency hopping at receiving side…...……...…..34

Fig.6.1. Source node broadcasts RREQ……..37

Fig.6.2. Transmission of data packets from source node to destination node……. .37

Fig.6.3. No packet dropping……..38

Fig.6.4. Malicious node broadcasts a RREQ……..39

Fig.6.5. Malicious node attacks the network…….40

Fig.6.6. Throughput of dropping packets with malicious node……..40

Fig.6.7. Throughput of dropping packets with malicious node and frequency hopping…… 41

Table 3.1. Comparison between Wireless Personal Area Networks (IEEE 802.15)....20

Table 5.1. Network Parameter Definition.....35

Table 6.1. Percentage of received packets at the destination node.....38

Table 6.2. Percentage of received packets at the destination node.....41

CHAPTER 1

INTRODUCTION

1.1. Motivation

Due to the recent advancement in micro-electro-mechanical systems (MEMS), wireless communication like Bluetooth [1], IEEE 802.11 [2], or MANETs [3], a new concept of networking has emerged known as Wireless Sensor Networks (WSNs). Wireless Sensor Network, consists of large number of sensor nodes having the capability of wireless communication, limited computation and sensing. WSN was initially developed for military and disaster rescue purposes but because of the availability of ISM band (2.4 GHz), the technology is now emerging in public applications. The salient features in Wireless Sensor Network makes it different from other network; self-organize, low power, low memory, low bandwidth for communication, large-scale nodes, self-configurable, wireless, infrastructure-less. Therefore, WSN design must encounter these features in order to provide a reliable network. However each sensor node is equipped with its own sensor, processor and radio transceiver, so it has the ability of sensing, data processing and communicating with each other.

Wireless Sensor Networks (WSN) relies on collaborative work of large number of sensors. For this reason, they are deployed densely throughout the area where they monitor specific phenomena and communicate with each other and with one or more sink nodes that interact with a remote user. The user can inject commands into the sensor network via the sink to assign data collection; data processing and data transfer tasks to the sensors in order to receive the data sensed by the network. However, due to the lack of tamper-resistant packaging and the insecure nature of wireless communication channels, these networks are vulnerable to internal and external attacks.

WSN are prone to failure and malicious user attack because it is physically weak, a normal node is very easy to be captured to become a malicious node or by inserting a malicious node in the network. The malicious nodes try to disrupt the network operation by modifying, fabricating, or injecting extra packets; they may mislead the

operation of packet forwarding or will try to consume the resources of the nodes by making them believe that the packets are legitimate. The malicious node will not cooperate in the network operation resulting in the malfunction of the network operation. This happens 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.

1.2. State of the Art

Many security mechanisms have been proposed for the security of the WSN. Most of the mechanisms for the detection of the malicious nodes are based on the cryptography. The technique requires security keys in the algorithm that consume the memory storage space inside the device. There are different challenges in providing security to a WSN deployment. These are:

- There is a conflicting interest between minimization of resource consumption and maximization of security level. A better solution actually gives a good compromise between the two of them. During the design of any security solution we need to take care of following node resource limitations like memory and energy, sensor network constraints like unreliable communication, collisions and latency and physical limitation like unattended after deployment and remotely managed.
- The type of security mechanism that can be hosted on a sensor node platform is dependent on the capabilities and limitations or constraints of sensor node hardware.
- Ad-hoc networking topology of WSN facilitates attackers for different types of link attacks ranging from passive eavesdropping to active interfering. Attacks on a WSN can come from all directions and target at any node leading to leaking of secret information, interfering message, impersonating nodes, etc.
- The communication in WSN is through wireless media, mainly radio. This characteristic of WSN makes wire-based security schemes impractical for WSNs.
- The topology of WSN is always dynamic. The sensor nodes can come and go in an arbitrary fashion. Node failures may be permanent or intermittent and this gives a higher level of system dynamics. Again very often large numbers of nodes are expected in sensor network deployments and the nature of it is unpredictable.

The problem of detecting the malicious nodes has been addressed separately in different protocols, which are either extensions or based on secure routing protocols. There are various ways for providing security to networks [4]. These are encryption, steganography, and securing access to the physical layer; frequency hopping can provide this service to sensor networks. So, in WSN that 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 packets to the same destination. First examine the throughput without using frequency hopping, and then compare it with throughput by using frequency hopping. After that, throughput from source and from malicious node is compared. So, the objective is to develop security in Wireless Sensor Network using frequency-hopping method, and to analyze the throughput before and after the implementation of frequency hopping.

1.3. Importance of the Study

Wireless Sensor Network is categorized in IEEE 802.15.4 task group that is in Low Rate Wireless Personal Area Network. The standard was released in 2003 and the upgraded version was released in 2006. Since it 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.

1.4. Thesis Outline

We have organized the thesis into 7 chapters which include Introduction; Background Information; Literature Review; Problem Statement; Installation, Simulation and Design; Results, Performance Evaluation and Analysis and finally Conclusion and Future Scope.

Chapter 1 describes the Wireless Sensor Network in general in terms of motivation and then follows by state of art, the importance of the study and finally the whole thesis outline. Chapter 2, describes the background information relating to the WSN

and secure routing. Chapter 3 describes the state of the art of secure routing in WSN, namely mechanisms based on the spread spectrum. AODV protocol in detail has been discussed covering the description of protocol modes and working, structure of various packets being transferred; procedures followed by the nodes in the particular modes. Chapter 4 discusses the problem statement. Chapter 5 discusses the installation of tools and the simulation environment. Chapter 6 describes the results, evaluates the performance, and analysis done based on the results and finally Chapter 7 summarizes the conclusions drawn in the thesis along with future research directions.

CHAPTER 2

BACKGROUND INFORMATION

2.1. Wireless Sensor Networks

Wireless Sensor Network is a heterogeneous network composed of a large number of small low-cost devices called nodes and few general-purpose computing devices referred to as base stations. The definition from SmartDust program of DARPA is:

"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" [5].

The definition from National Research Council of USA is:

"Sensor networks are massive numbers of small, inexpensive, self-powered devices pervasive throughout electrical and mechanical systems and ubiquitous throughout the environment that monitor (i.e., sense) and control (i.e., effect) most aspects of our physical world" [5].

A sensor node is able to observe condition values of a certain area like temperature, sound, vibration, pressure, motion or pollutants. The measured values are then forwarded to a data collection point that is in charge of their further processing. Wireless Sensor Network (WSN) applications are suite with IEEE 802.15.4 standards [6]. IEEE 802.15.4 standard is for low rate Wireless Personal Area Network (WPAN) [7, 8] and the standard was defined for wireless Medium Access Control layer and the Physical layer.

The characteristics of WSN are wireless medium, low power consumption, low cost and low data rate. Other characteristics of WSN are large numbers of sensors, collaborative signal processing, easily deployed, self-configurable and self-organize, and infrastructure-less. Whereas, the characteristics of IEEE 802.15.4 (Low Rate Wireless Personal Area Network – LR WPAN) are data rates of 250 kb/s, 40 kb/s, and 20 kb/s, star or peer-to-peer operation, allocated 16 bit short or 64 bit extended

addresses, allocation of guaranteed time slots (GTSs), carrier sense multiple access with collision avoidance (CSMA-CA) [9, 10] channel access, fully acknowledged protocol for transfer reliability, low power consumption, energy detection (ED), link quality indication (LQI) and 16 channels in the 2450 MHz band, 10 channels in the 915 MHz band, and channel in the 868 MHz band.

2.1.1. Wireless Sensor Network Model

Unlike their ancestor ad-hoc networks, WSNs are resource limited, they are deployed densely, they are prone to failures, the number of nodes in WSNs is several orders higher than that of ad hoc networks, WSN network topology is constantly changing, WSNs use broadcast communication mediums and finally sensor nodes don't have a global identification tags [11]. The major components of a typical sensor network are:

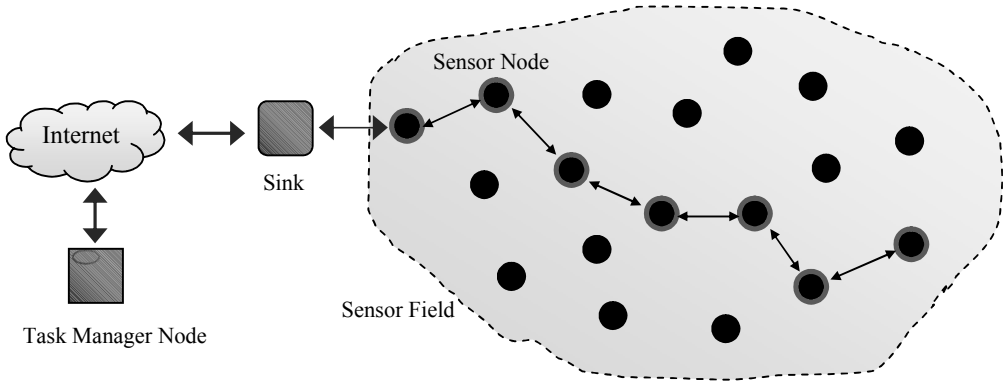

Fig. 2.1. Components of Wireless Sensor Networks

- *Sensor Field:* A sensor field can be considered as the area in which the nodes are placed.
- *Sensor Nodes:* Sensors nodes are the heart of the network. They are in charge of collecting data and routing this information back to a sink.
- *Sink:* A sink is a sensor node with the specific task of receiving, processing and storing data from the other sensor nodes. They serve to reduce the total number of messages that need to be sent, hence reducing the overall energy requirements of the network. The network usually assigns such points dynamically. Regular nodes can also be considered as sinks if they delay outgoing messages until they have aggregated enough sensed information. Sinks are also known as data aggregation points.

- *Task Manager:* The task manager also known as base station is a centralised point of control within the network, which extracts information from the network and disseminates control information back into the network. It also serves as a gateway to other networks, a powerful data processing and storage centre and an access point for a human interface. The base station is either a laptop or a workstation. Data is streamed to these workstations either via the internet, wireless channels, satellite etc. So hundreds to several thousand nodes are deployed throughout a sensor field to create a wireless multi-hop network. Nodes can use wireless communication media such as infrared, radio, optical media or Bluetooth for their communications. The transmission range of the nodes varies according to the communication protocol is use.

2.1.2. The Sensor Node

A sensor is a small device that has a micro-sensor technology, low power signal processing, low power computation and a short-range communications capability. Sensor nodes are conventionally made up of four basic components as shown in Figure 2.2: a sensor, a processor, a radio transceiver and a power supply/battery [11]. Additional components may include Analog-to-Digital Convertor (ADC), location finding systems, mobilizers that are required to move the node in specific applications and power generators. The analog signals are measured by the sensors are digitized via an ADC and in turn fed into the processor. The processor and its associated memory commonly RAM is used to manage the procedures that make the sensor node carry out its assigned sensing and collaboration tasks. The radio transceiver connects the node with the network and serves as the communication medium of the node.

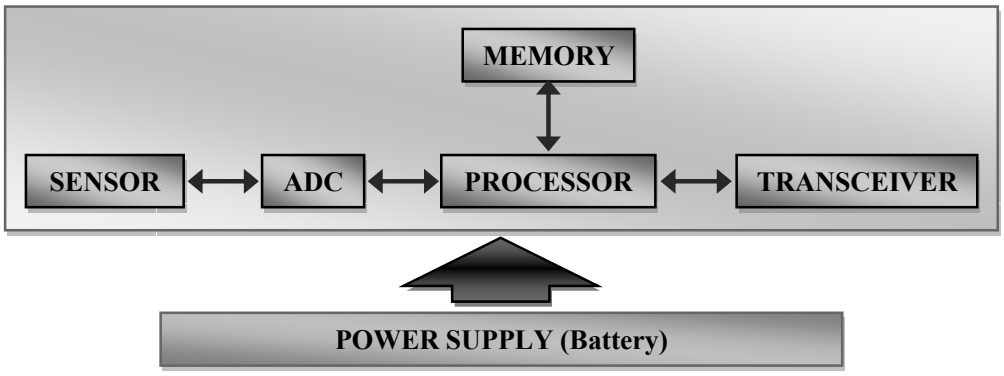

Fig. 2.2. Components of a wireless sensor node

Memories like EEPROM or flash are used to store the program code. The power supply/battery is the most important component of the sensor node because it implicitly determines the lifetime of the entire network. Due to size limitations of AA batteries or quartz, cells are used as the primary sources of power. To give an indication of the energy consumption involved, the average sensor node will expend approximately 4.8mA receiving a message, 12mA transmits a packet and 5μA sleeping [11]. In addition the CPU uses on average 5.5mA when in active mode.

2.1.3. Wireless Sensor Node Communication Architecture: Protocol Stack

The protocol stack used by the base station and sensor nodes is shown in Figure. 2.3. This protocol stack combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes. The protocol stack consists of the physical layer, data link layer, network layer, transport layer, application layer, power management plane, mobility management plane and task management plane.

The physical layer should meet requirements like carrier frequency generation, frequency selection, signal detection, modulation and data encryption, transmission and receiving mechanisms.

The Data Link Layer should meet the requirements for medium access, error control, multiplexing of data streams and data frame detection. It also ensures reliable point to point and point to multi-hop connections in the network. The MAC layer in the data link layer should be capable of collision detection and use minimal power.

The network layer is responsible for routing the information received from the transport layer i.e. finding the most efficient path for the packet to travel on its way to a destination.

The Transport Layer is needed when the sensor network intends to be accessed through the internet. It helps in maintaining the flow of data whenever the application requires it.

The application layer is responsible for presenting all required information to the application and propagating requests from the application layer down to the lower layers.

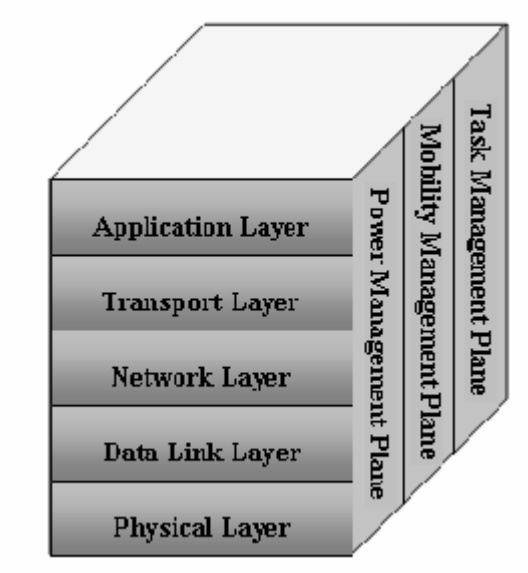

Fig. 2.3. Protocol stack

The power management plane manages power utilization by the nodes. Mobility management plane is responsible for the movement pattern of the sensor nodes, if they are mobile. The task management plane schedules the sensing and forwarding responsibilities of the sensor nodes. Designing a network protocol for such wireless devices should meet the limitations like limited channel bandwidth, limited energy, electromagnetic wave propagation, error-prone channel, time varying conditions and mobility.

There are general ideas that can be used to overcome these limitations. Low-energy protocols help extend the limited node energy. Power control can be used to combat the radio wave attenuation. A transmitter can set the power of the radio wave, such that it will be received with an acceptable power level. Link-layer protocols and MAC protocols can be used to combat channel errors. Adaptive routing, MAC and link-layer protocols can be used to overcome the time-varying conditions of the wireless channel and node mobility.

2.1.4. Routing Techniques in Wireless Sensor Networks

Due to WSNs differing from one network to another, many new algorithms have been proposed for the routing problem in WSNs. These routing mechanisms have considered the characteristics of sensor nodes depending on the type of application and underlying architecture requirements. Almost all of the routing protocols can be classified according to the network structure as flat, hierarchical or location-based.

2.2. Security in Wireless Sensor Networks

Due to inherent limitations in wireless sensor networks, security is a crucial issue and a sensor network is highly vulnerable against any external or internal attack, thus the infrastructure and protocols of the network must be prepared to manage these kinds of situations. This section examines the security problems that sensor networks face due to node resource limitations like memory and energy, sensor network constraints like unreliable communication, collisions and latency and physical limitation like unattended after deployment and remotely managed.

2.2.1. Security Goals for Sensor Networks

The security goals encompass both those of the traditional networks and goals suited to the unique constraints of sensor networks. The four security goals for sensor networks are:

- *Confidentiality*: The ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.
- *Integrity*: It ensures the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while on the network. Even if the network has confidentiality measures in place, there is still a possibility that the data's integrity has been compromised by alterations.
- *Authentication*: It ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional bogus packets. Therefore, the receiving node needs to be able to confirm that a packet received does in fact stem from the node claiming to have sent it. Data authentication verifies the identity of senders. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys to compute the Message Authentication Code (MAC).
- *Availability*: The ability to use the resources and whether the network is available for the messages to communicate.

2.2.2. Security Challenges

WSNs have many characteristics that make them very vulnerable to malicious attacks. Some of these are:

- A wireless channel is open to everyone. With a radio interface configured at the same frequency band, anyone can monitor or participate in communications. This provides a convenient way for attackers to break into WSNs.
- Due to standard activity, Most routing protocols for WSNs are known publicly and do not include potential security considerations at the design stage. Therefore, attackers can easily launch attacks by exploiting security holes in those protocols.
- Due to the complexity of the algorithms, the constrained resources make it very difficult to implement strong security algorithms on a sensor platform. To design such security protocols is not an easy task. A stronger security protocol costs more resources on sensor nodes, which can lead to the performance degradation of applications. In most cases, a trade-off must be made between security and performance. However, attackers can break weak security protocols easily.
- A WSN is usually deployed in hostile areas without any fixed infrastructure. It is difficult to perform continuous surveillance after network deployment.

2.2.3. Threat Models

As discussed in [11], Security threat in a WSN can be divided into various categories. These are:

- *External threats versus internal threats*: An external threat occurs from outside the sensor network and may amount to mere passive eavesdropping on data transmissions, but can extend to injecting bogus data into the network to consume network resources and rage Denial of Service (DoS) attacks. An internal threat occurs from compromised nodes running malicious data or from attackers who have stolen the cryptographic contents from legitimate nodes.
- *Mote-class attacker versus laptop-class attacker*: A mote-class attacker has access to a few motes with the same capabilities as other motes in the network. However a laptop-class attacker has access to more powerful devices, such as laptops.
- *Insider attack versus outsider attack*: An outside attacker has no special access to the sensor network, such as passive eavesdropping. On the other hand an inside attacker has access to the encryption keys or other codes used by the network.

- *Passive attacker versus active attacker*: Passive attackers are only interested in collecting sensitive data from the sensor network, which compromises the privacy and confidentiality requirements. These are attempts to reach the owner data and make use of it without the owner realizes it. It is hard to detect this kind of attack because it does not modify the data. So, the prevention of the attack is more useful rather than struggle for detection. The types of passive attacks are:

  - *Release of message contents*: Any information transferred through telephone conversation or electronic mail can be release to opponent which data may contains confidential information.
  - *Traffic Analysis*: Opponent can observe the frequency and length of data being transmitted and this information can be analyzed to get the nature of communication taking place. The attacker also may know the location of base stations, and the type of protocol being used in the transmission.

  An example of passive attack is - Eavesdropping. An attacker that monitors traffic can read the data transmitted and gather information by examining the source of a packet, its destination, size, number, and time of transmission. The active attackers' goal is to disrupt the function of the network and degrade its performance. These are involving alteration of information that may be disastrous to the organization. Oppose to passive attack, active attack is more likely to be detected rather than to prevent. Furthermore, the detection has a preventive effect that may contribute to prevention as well. There are four types of active attacks:

  - *Masquerade*: Impersonation of an identity that pretends to be an authorized identity.
  - *Replay:* A passive capture of information to produce an unauthorized effect.
  - *Modification of Message*: The sequence of message has been jumble-up or the message has been delayed or even worst the meaning of message has been modified.
  - *Denial of Service (DoS)*: DoS may disrupt the network and degrade its performance. This type of attack can be grouped into three categories: disabling of service (e.g., sinkhole, HELLO flood attack), exhaustion, and service degradation (e.g., selective forwarding attack)

An example of active attack can be - Man-in-the-middle attack, in which a rogue establishes an intermediary, pretending to be a valid sensor.

2.2.4. Secure Routing in Wireless Sensor Networks

A wireless sensor network is only as good as the information it produces. In this respect, the most important concern is information security. Indeed; in most application domains sensor networks will constitute a mission critical component requiring commensurate security protection. Sensor network communications must prevent disclosure and undetected modification of exchanged messages.

Due to the fact that individual sensor nodes are anonymous and that communication among sensors is via wireless links, sensor networks are highly vulnerable to security attacks. If an adversary can thwart the work of the network by perturbing the information produced, stopping production, or pilfering information, then the perceived usefulness of sensor networks will be drastically curtailed. Thus, security is a major issue that must be resolved in order for the potential of wireless sensor networks to be fully exploited.

CHAPTER 3

LITERATURE REVIEW

3.1. Routing Protocol

Routing is a process of determining a path between source and destination upon request of data transmission. In WSNs the network layer is mostly used to implement the routing of the incoming data. It is known that generally in multi-hop networks the source node cannot reach the sink directly. So, intermediate sensor nodes have to relay their packets. The implementation of routing tables gives the solution. This contains the lists of node option for any given packet destination. Routing table is the task of the routing algorithm along with the help of the routing protocol for their construction and maintenance.

3.1.1. Ad-hoc On-demand Distance Vector (AODV)

AODV [16] is the simplest and widely used algorithm either for wired or wireless networks. It is one of the most efficient routing protocols in terms of establishing the shortest path and lowest power consumption. It is an algorithm use for finding a route for peer-to-peer connection between sensors. It is mainly used for ad-hoc networks but also in wireless sensor networks. It uses the concepts of Path Discovery and Maintenance.

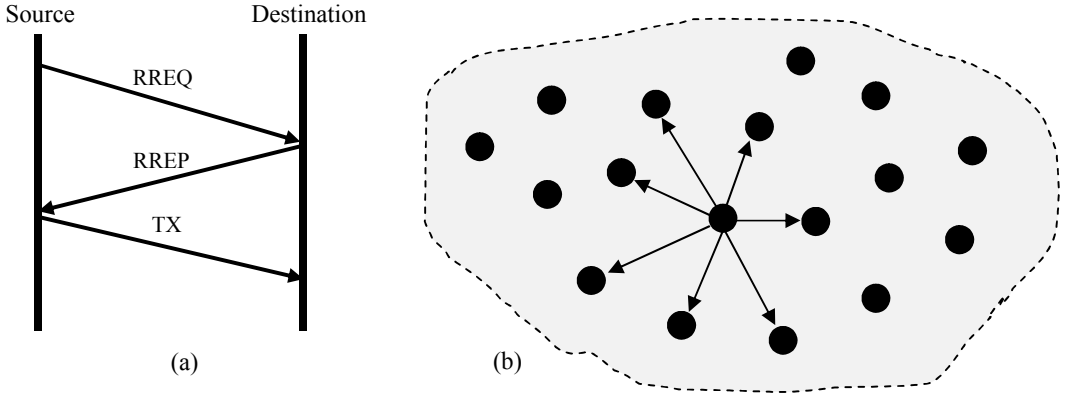

Fig. 3.1. AODV; (a) Timing diagram, (b) Broadcasts a HELLO packet to the neighbours

However, AODV builds routes between nodes on-demand i.e. only as needed. So, AODVs' primary objectives are:

- To broadcast discovery packets only when necessary,
- To distinguish between local connectivity management (neighborhood detection) and general topology maintenance,
- To disseminate information about changes in local connectivity to those neighboring mobiles nodes that is likely to need the information.

Type	Reserved	Hop Count
Broadcast ID		
Destination IP Address		
Destination Sequence Number		
Source IP Address		
Source Sequence Number		
Request Time		

Fig. 3.2. Structure of a RREQ packet [18]

AODV does not depend on network-wide periodic advertisements of identification messages to other nodes in the network. It periodically broadcasts “HELLO” messages to the neighbouring nodes. It then uses these neighbours in routing. Whenever any node needs to send a message to some node that is not its neighbour, the source node initiates a Path Discovery, by sending a Route REQuest (RREQ) message to its neighbours. Nodes receiving the RREQ update their information about the source.

They also set up a backward link to the source in their routing tables. Each RREQ contains the source node’s address (IP address) and a Broadcast ID that uniquely identifies it. It also has a current sequence number that determines the freshness of the message. Thus, a message number with a higher sequence number is considered to be fresher or more recent than that with a lower sequence number. The RREQ also contains a hop count variable that keeps track of the number of hops from the source. On receipt of the RREQ, the node checks whether it has already received the same RREQ earlier. If it has received the same RREQ earlier, it drops the RREQ. Otherwise, if it is an intermediate node without any record of a route to the final destination, the node increases the hop count and rebroadcasts the RREQ to its neighbours. If the node is the final destination, or an intermediate node that knows the

route to the final destination, it sends back the Route REPly (RREP). This RREP is sent back via the same route traversing which the node had received the message from the source. As the RREP propagates back to the source node, the intermediate nodes setup forward pointers to the actual destination.

When the source node receives the RREP, it checks whether it has an entry for the route. If it did not have any entry in its routing table, the node creates a new entry in the routing table. Otherwise it checks the sequence number of the RREP. If the RREP arrives with the same sequence number as in its tables but with a smaller hop count, or a greater sequence number (indicating fresher route), it updates its routing table and starts using this better route. Once an entry for the new route has been created in the table, the node can start communication with the destination.

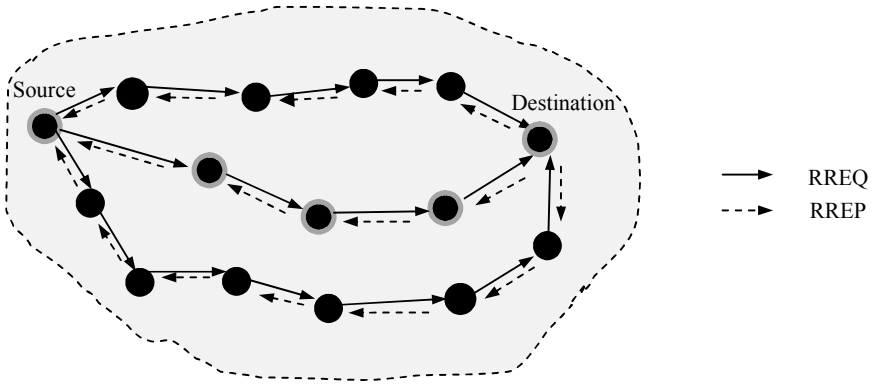

Fig. 3.3. Path discovery of AODV

Every time a node receives subsequent RREPs, it updates its routing table information, and only forwards those that are fresher or contain a smaller hop count. Each routing table entry contains information for the destination, the next node, number of hops to the destination, sequence number for that destination, active neighbours for the route and expiration time of the table entry. The expiration time frame is reset every time the source routes a packet to the destination. The advantage of AODV is that, it is bandwidth efficient; it has loop-free routing and acts as a reactive protocol that makes it worthy to be considered.

3.1.2. Security Issues in AODV

A node is *malicious* if it is an attacker that cannot authenticate itself as a legitimate node due to the lack of valid cryptographic information. A node is *compromised* if it is an inside attacker who is behaving maliciously but can be authenticated by the network as a legitimate node and is being trusted by other nodes. A node is *selfish* when it tends to deny providing services for the benefit of other nodes in order to save its own resources. AODV implemented networks are subjected to two main kinds of attacks, passive attacks and active attacks. There are several attacks can be launched against the AODV routing protocol. These are:

- *Message tampering attack*: An attacker can alter the content of routing messages and forward them with false information. For example, by reducing the hop-count field in either an RREQ or RREP packet, an attacker can increase its chance to be an intermediate node of the route.
- *Message dropping attack*: Both attackers and selfish nodes can intentionally drop some (or all) routing and data messages. This attack can paralyze the network completely as the number of message dropping increases.
- *Message replay (or wormhole) attack*: Attackers can retransmit eavesdropped messages again later in a different place. One type of replay attacks is the wormhole attack. A wormhole attacker can tunnel an RREQ directly to a destination node. Since a wormhole attacker may not increase the hop-count field value, it prevents any other routes from being discovered. The wormhole attack can be combined with the message dropping attack to prevent the destination node from receiving packets.

The security requirements for AODV routing protocol include:

- *Source authentication*: The receiver should be able to confirm that the identity of the source is indeed who or what it claims to be.
- *Neighbour authentication*: The receiver should be able to confirm that the identity of the sender (i.e., one hop previous node) is indeed who or what it claims to be.
- *Message integrity*: The receiver should be able to verify that the content of a message has not been altered either maliciously or accidentally in transit.

3.2. The Frequency Hopping

Frequency hopping is a method that provides security to the WSN. Frequency hopping in radio communication is not a new idea and was explored before [4, 17]. This solution is provided for the security of WSN. Their solution provides integrity, confidentiality and availability for the sensor networks that consist of anonymous nodes.

In Frequency hopping (FH) a radio signal communication is done between two or more nodes, by speedily changing the radio channels following a predetermined pseudorandom channel sequence known to both sender and receiver. Normally the procedure of FH is as follows:

- The transmitter sends a request via a predefined frequency channel (control channel).
- The receiver sends a number sequence, known as a seed. Or in many cases the sender has its own number sequence stored in which case this step in not executed.
- The transmitter uses the seed as one of the inputs in a random number algorithm, which then calculates the channel sequence i.e. the sequence of frequencies that is used for communication.
- The transmitter sends the channel sequence, channel stay time (same for all channels) and the time when it will start transmitting the data.
- The communication starts at the same point in time, and both the transmitter and the receiver change their frequencies according to the channel sequence.

In order to ensure the availability they use frequency-hopping scheme that is conventionally used for “implementing frequency diversity and interference averaging in a non-hostile environment. The frequency used within the environment/system will be hopped to different frequency/channel frequently. Therefore, it is hard for the attacker to track the data being transmitted. It provides anti-jamming capability and protection against interception are key priorities in wireless mobile ad hoc networks (MANETs) or sensor networks (WSNs) for military applications. There are number of drawbacks associated with Frequency Hopping such as:

- Due to the node anonymity their solutions does not provide access control and non-repudiation.

- They do not provide direct authentication mechanism but on the other hand it is very difficult for the external node that attempt to masquerade as a legitimate node.

3.3. IEEE 802.15.4 Standard: LR-WPAN

The IEEE 802.15.4 standard [6] defines the characteristics of the physical and MAC layers for Low-Rate Wireless Personal Area Networks (LR-WPAN). The advantages of an LR-WPAN are ease of installation, reliable data transfer, short-range operation, extremely low cost, use of unlicensed radio bands (ISM band), flexible and extendable networks, integrated intelligence for network set-up and message routing, and a reasonable battery life, while maintaining a simple and flexible protocol stack.

3.3.1. Network Topologies

- *Star Topology*: A Star network has a central node, which is linked to all other nodes in the network. All messages travel via the central node.

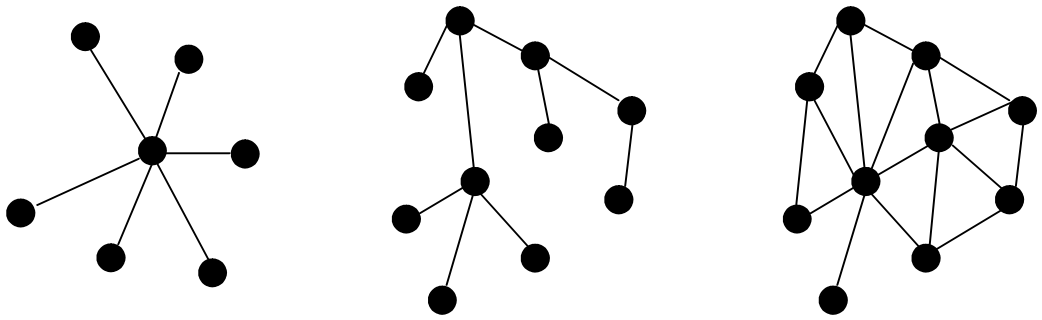

Fig. 3.4. Network topologies: (a) Star, (b) Tree, (c) Mesh

- *Tree Topology*: A Tree network has a top node with a branch/leaf structure below. To reach its destination, a message travels up the tree (as far as necessary) and then down the tree.
- *Mesh Topology*: A Mesh network has a tree-like structure in which some leaves are directly linked. Messages can travel across the tree, when a suitable route is available.

3.3.2. The Physical Layer

Physical layer of Low Rate Wireless Personal Area Network consists of 27 channel altogether. The channels available are divided in three different frequency bands: a

2450 MHz band (with 16 channels), a 915 MHz band (with 10 channels) and an 868 MHz band (1 channel), all using the Direct Sequence Spread Spectrum (DSSS) access mode. The data rates are very low compared to other types of WPAN as seen in Table 3.1. Besides radio on/off operation, the physical layer supports functionalities for channel selection, link quality estimation, energy detection measurement and clear channel assessment to assist the channel selection. The physical layer provides an interface between the MAC sub-layer and the physical radio channel.

PROJECT	Data Rate	Range	Configuration	Other Features
802.15.1 (Bluetooth)	1 Mbps	10M (class 3) 100M (class 1)	8 active devices Piconet/ Scatternet	Authentication, Encryption, Voice
802.15.3 High Rate	22, 33, 44, 55 Mbps	10M	256 active device Piconet/ Scatternet	FCC part 15.249 Qos, Fast Join Multi-Media
802.15.4 Low Rate	Up to 250 /kbps	10M nominal 1M-100M based on settings	Master/Slave (256 Devices or more) Peer-to-Peer	Battery Life: multi-month to infinite
802.15.2 Coexistence	Develop a Coexistence Model and Mechanisms Document as a Recommended Practice			

Table 3.1. Comparison between Wireless Personal Area Networks (IEEE 802.15)

The physical layer performs the following tasks:

- *Activation/Deactivation of radio transceiver*: Turn the radio transceiver into one of the three states, that is, transmitting, receiving, or off (sleeping) according to the request from MAC sub-layer.
- *Energy Detection (ED)*: It is an estimate of the received signal power within the bandwidth of channel. The result from energy detection can be used by a network layer as part of a channel selection algorithm, or for the purpose of clear channel assessment (CCA) (alone or combined with carrier sense).
- *Link Quality Indication (LQI)*: The measurement is performed for each received packet. The PHY layer uses receiver energy detection (ED), a signal-to-noise ratio (SNR), or a combination of these to measure the strength and/or quality of a link from which a packet is received.

- *Channel Selection*: As discussed above, the Wireless links under 802.15.4 can operate in 27 different channels but a specific network can choose to support part of the channels. Hence the PHY layer should be able to tune its transceiver into a certain channel upon receiving the request from MAC sub-layer.
- *Clear Channel Assessment (CCA) for Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)*: The PHY layer is required to perform CCA using energy detection, carrier sense, or a combination of these two. In carrier sense mode, the medium is considered busy if a signal with the modulation and spreading characteristics of IEEE 802.15.4 is detected.
- *Transmission/Reception of packets over physical medium*: Here Modulation and spreading techniques are used.

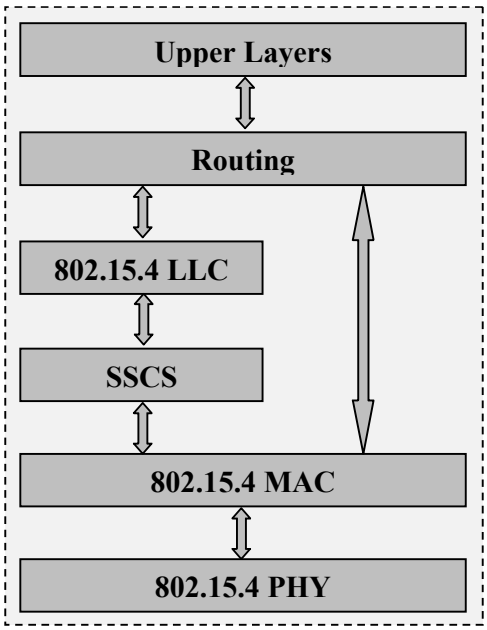

Fig. 3.5. Layer approach of IEEE 802.15.4

3.3.3. The MAC Sub-Layer

The MAC sub-layer provides an interface between the service specific convergence sub-layer (SSCS) and the PHY layer as shown in Figure.3.5. The MAC sub-layer provides two services, namely, the MAC data service and the MAC management service. It is responsible for the following tasks:

- *Generating and managing beacons*: If the device is a coordinator then the coordinator can determine whether to work in a beacon enabled mode, in which a superframe structure is used.

- *Association and disassociation with personal area network (PAN) coordinators*: To support self-configuration, 802.15.4 embeds association and disassociation functions in its MAC sub-layer. This not only enables a star to be setup automatically, but also allows for the creation of a self-configuring, peer-to-peer network.
- *Channel access*: Employing the carrier sense multiple access with collision avoidance (CSMA-CA) mechanism for channel access. Like most other protocols designed for wireless networks, 802.15.4 uses CSMA-CA mechanism for channel access. However, the new standard does not include the request-to-send (RTS) and clear-to-send (CTS) mechanism, in consideration of the low data rate used in LR-WPANs.
- *Guaranteed Time Slot management*: Handling and maintaining the guaranteed time slot (GTS) mechanism. When working in a beacon enabled mode, a coordinator can allocate portions of the active superframe to a device. These portions are called GTSs, and comprise the contention free period (CFP) of the superframe.
- *Frame validation and Acknowleged frame* delivery: It provides various mechanisms to enhance the reliability of the link between two peers, among them are the frame acknowledgment and retransmission, data verification by using a 16-bit CRC, as well as CSMA-CA.

3.3.4. The Superframe Structure

The superframe is bounded by network beacons and divided into aNumSuperframeSlots (default value 16) equally sized slots. The coordinator sends out beacons periodically to synchronize the attached devices and for other purposes. A device attached to a coordinator operating in a beacon-enabled mode can track the beacons to synchronize with the coordinator. This synchronization is important for data polling, energy saving, and detection of orphanings. A superframe is divided into two parts: Inactive and active period. In Inactive period all the stations are sleep whereas an active period will be divided into 16 slots. These slots are “MACRO” slots. These 16 slots can further divided into two parts: Contention access period (CAP) and Contention free period (CFP). The CFP is an optional and may accommodate up to seven so-called guaranteed time slots (GTSs), and a GTS may occupy more than one slot period. However, a sufficient portion of the CAP shall

remain for contention-based access of other networked devices or new devices wishing to join the network.

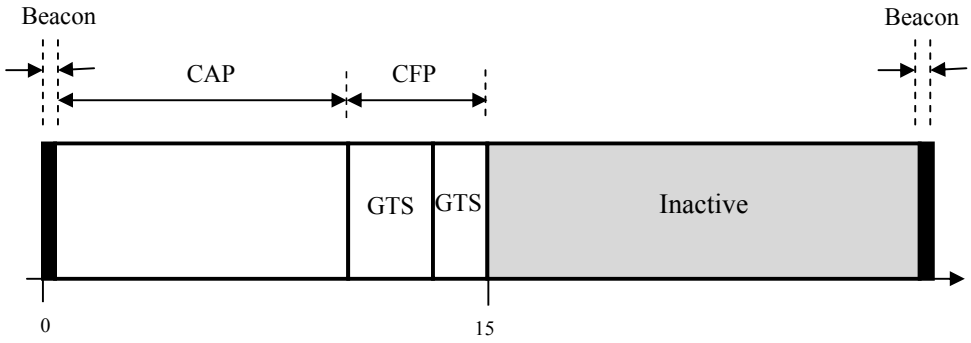

Fig. 3.6. A superframe structure

A slotted CSMA-CA mechanism is used for channel access during the CAP. All contention-based transactions shall be complete before the CFP begins. Also all transactions using GTSs shall be done before the time of the next GTS or the end of the CFP.

3.3.5. Carrier Sense Multiple Access – Collision Avoidance

CSMA-CA [8, 9] gives solution of hidden node problem in CSMA-CD that a node cannot detect another node that also wants to transmit packet resulting a collision. The CSMA-CA algorithm will be used before the transmission of data of MAC command frames transmitted within the CAP. CSMA-CA protocol uses four-way handshake.

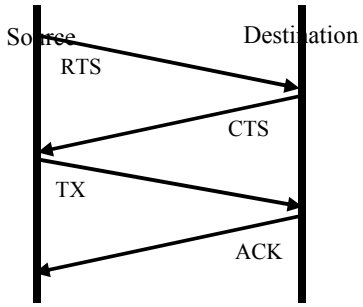

Fig. 3.7. Timing diagram for CSMA-CA

The node will listen (sense a voltage level) before transmit any packet. If it detects there is a signal, it will waits for a random period before listens to the network again. If no signal is detected, the node will send ready-to-send message (RTS) to all nodes. The RTS contains destination address and period of the transmission. The destination

will reply with clear-to-send message (CTS) that denotes that the node can send message without collision. The destination/receiver will send acknowledgement for every packet it received. If ACK is not received, the packet is assumed lost or corrupted and will resend the packet until ACK is received. The IEEE 802.15.4 uses two types of channel access mechanism, depending on the network configuration.

3.3.5.1. Slotted CSMA-CA

Beacon-enabled networks use this channel access mechanism, where the backoff slots are aligned with the start of the beacon transmission. Each time a device want to transmit data frame during the CAP, it shall locate the boundary of the next backoff slot and then wait for a random number of backoff slots. If the channel is busy, following this random backoff, the device shall wait for another random number backoff slots before trying to access the channel again. If the channel is idle, the device can begin transmitting on the next available backoff slot boundary.

3.3.5.2. Un-slotted CSMA-CA

Non-beacon-enabled networks use this channel access mechanism. If a device wants to transmit data frames or MAC commands, it will wait for a random period. If the channel is found to be idle, following the random backoff, the device shall transmit its data. If the channel is found to be busy, following the random backoff, the device shall wait for another random period before trying to access the channel again.

Un-Slotted CSMA-CA is a method of accessing channel before data can be transmits. Since our simulation is based on this algorithm, we are discussing it in detail. This algorithm is working at Layer 2. The Un-slotted CSMA-CA is based on basic time unit called *Backoff Period* (BP). BP is equal to 0.32 ms that refer to *aUnitBackoffPeriod* (80 bits) [8]. The Un-slotted CSMA-CA backoff algorithm is depends on two variables:

- The Backoff Exponent (BE) enables the computation of the backoff delay, which is the time before performing CCAs. The backoff delay is a random variable between 0 and $(2^{BE} - 1)$.
- The Number of Backoffs (NB) represents the number of times the un-slotted CSMA-CA algorithm was required to backoff while attempting to access the channel. This value is initialized to zero before each new transmission attempt.

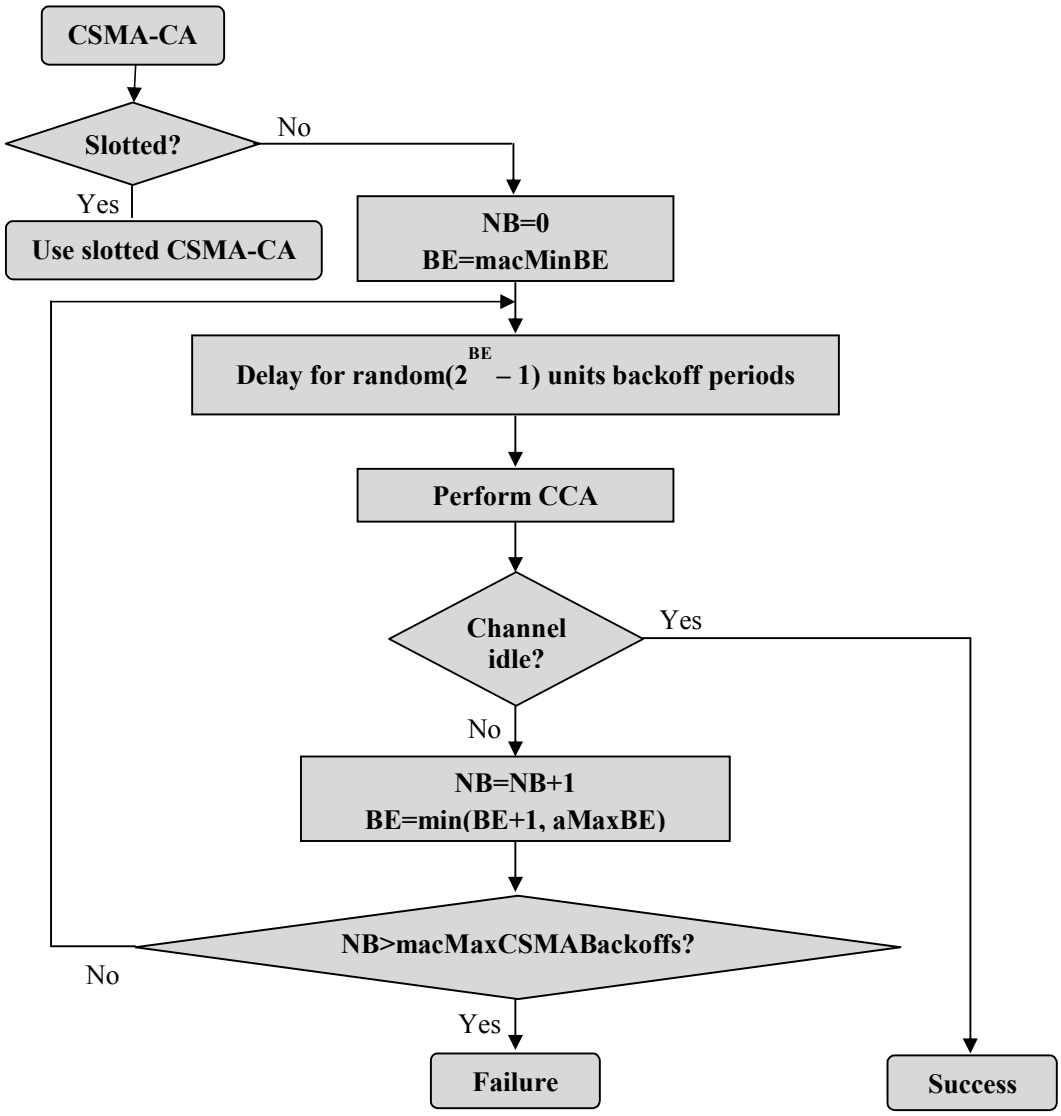

Fig. 3.8. Un-slotted CSMA/CA flow chart

First step of Un-slotted CSMA-CA is initializing NB=0 and BE=2 (depends on Battery Life Extension which is by default value is 3). Then, second step is counting down the random number of BPs that uniformly generated between 0 to $(2^{BE} - 1)$. Take note that the counting must start at the boundary of a BP. The third step is performing CCA at the boundary of the BP to access channel activity. Then, if the channel is idle, channel access is allowed. Therefore, un-slotted CSMA-CA will be performed to send the packet. If the channel is busy, the flow will go to fourth step. The fourth step will increment NB and BE. BE can't exceed the setting maximum value. Incrementing the BE makes the probability of backoff delays becomes big.

Then, if the NB exceeds the maximum number of allowed backoffs, the transmission is fail. If NB hasn't reached the maximum value, it will repeat the second step. The un-slotted CSMA-CA will be activated each time transmission of a new packet. The same has been described in Figure 3.8.

3.3.6. Data Transfer Model

Data transfer can happen in three different ways: (1) from a device to a coordinator; (2) from a coordinator to a device; and (3) from one peer to another in a peer-to-peer multi-hop network. The date transfer model is also classified as direct data transmission, indirect data transmission and GTS data transmission.

Direct data transmission applies to all data transfers, either from a device to a coordinator, from a coordinator to a device, or between two peers. Un-slotted CSMA-CA or slotted CSMA-CA is used for data transmission, depending whether non-beacon enabled mode or beacon-enabled mode is used. Whereas indirect data transmission only applies to data transfer from a coordinator to its devices. Occasionally, indirect data transmission can also happen in non-beacon enabled mode. Although GTS data transmission only applies to data transfer between a device and its coordinator, either from the device to the coordinator or from the coordinator to the device. No CSMA-CA is needed in GTS data transmission.

CHAPTER 4

PROBLEM STATEMENT & OBJECTIVE

4.1. Problem Statement

Most current WSN routing protocols assume that the wireless network in benign and every node in the network strictly follow the routing behavior and is willing to forward packets for other nodes. Most of these protocols cope well with the dynamically changing topology. However, they do not address the problems when misbehavior nodes are present in the network.

A commonly observed misbehavior is packet dropping. Practically, in a WSN, most devices have limited computing and battery power while packet forwarding consumes a lot of such resources. Thus some devices would not like to forward the packet for the benefit of others and they drop packets not destined to them. On the other hand, they still make use of other nodes to forward packets that they originate. These misbehaved or malicious nodes are very difficult to examine that whether the packet dropping is intentionally by malicious node or dropped due to link error. WSNs have many characteristics that make them very vulnerable to malicious attacks. These are:

- A wireless channel is open to everyone. With a radio interface configured at the same frequency band, anyone can monitor or participate in communications. This provides a convenient way for attackers to break into WSNs.
- Due to standard activity, Most routing protocols for WSNs are known publicly and do not include potential security considerations at the design stage. Therefore, attackers can easily launch attacks by exploiting security holes in those protocols.
- Due to the complexity of the algorithms, the constrained resources make it very difficult to implement strong security algorithms on a sensor platform. To design such security protocols is not an easy task. A stronger security protocol costs more resources on sensor nodes, which can lead to the performance degradation of applications. In most cases, a trade-off must be made between security and performance. However, attackers can break weak security protocols easily.

- A WSN is usually deployed in hostile areas without any fixed infrastructure. It is difficult to perform continuous surveillance after network deployment. Therefore, a WSN may face various attacks.

The problem, detection of the malicious nodes, has been addressed separately in different protocols, which are either extensions or based on secure routing protocols. There are various ways for providing security to networks. These are encryption, steganography, and securing access to the physical layer; frequency hopping can provide this service to sensor networks.

4.2. Objective and Sub-Tasks

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. The primary objective of this thesis is secure routing in WSNs which was achieved by the following manner:

- To analyze, implement and evaluate AODV protocol.
- 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. First examine the throughput without using frequency hopping then, compare it with throughput by using frequency hopping.
- After that, throughput from source and from malicious node is compared.
- So, the objective is to develop security in Wireless Sensor Network using frequency-hopping method, and to analyze the throughput before and after the implementation of frequency hopping.

CHAPTER 5

INSTALLATION, SIMULATION & DESIGN

5.1. Fedora Core 4

Fedora Core is a free operating system based on Linux. The development of Fedora is sponsored by Red Hat; and being developed by the open source community and the Red Hat engineers. Some primary features of FC4 are extensive performance improvements, support for Intel-based Macs and a new Graphical User Interface (GUI) virtualization manager.

5.2. The Network Simulator (NS2)

Simulation can be defined as "Imitating or estimating how events might occur in a real situation". It can involve complex mathematical modelling, role plying without the aid of technology, or combinations. The value lies in the pacing you under realistic conditions that change as a result of behaviour of others involved, so you cannot anticipate the sequence of events or the final outcome.

5.2.1. NS2 Overview

NS is an event driven network simulator developed at University of California at Berkeley, USA, as a REAL network simulator projects in 1989 and was developed at with cooperation of several organizations. Now, it is a VINT project supported by DARPA. NS is not a finished tool that can manage all kinds of network model. It is actually still an on-going effort of research and development. The users are responsible to verify that their network model simulation does not contain any bugs and the community should share their discovery with all. There is a manual called NS manual for user guidance.

NS is a discrete event network simulator where the timing of events is maintained by a scheduler and able to simulate various types of network such as LAN and WPAN according to the programming scripts written by the user. Besides that, it also implements variety of applications, protocols such as TCP and UDP, network elements such as signal strength, traffic models such as FTP and CBR, router queue management mechanisms such as Drop Tail and many more.

There are two languages used in NS-2; C++ and OTcl (an object oriented extension of Tcl). The compiled C++ programming hierarchy makes the simulation efficient and execution times faster. The OTcl script which written by the users the network models with their own specific topology, protocols and all requirements need. The form of output produce by the simulator also can be set using OTcl. The OTcl script is written which creating an event scheduler objects and network component object with network setup helping modules. The simulation results produce after running the scripts can be use either for simulation analysis or as an input to graphical software called Network Animation (NAM).

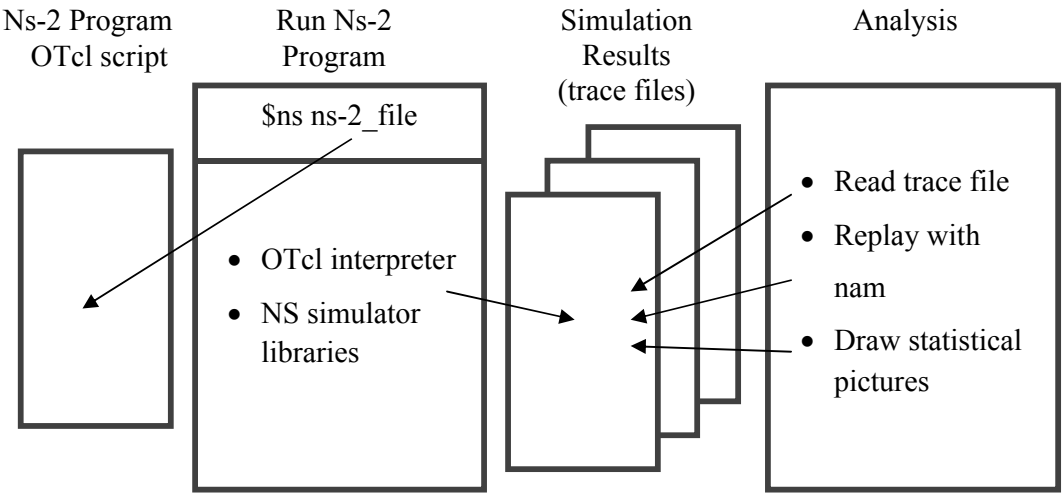

Fig. 5.1. Running NS2 program

NS-2 is an event driven network simulator that can be implements in Linux-based platform. This report will explain on how to install NS-2 in Fedora Core platform. The NS-2 files (recommended to download a piece of file which includes all the needed files called ns-allinone-2.xx from http://www.isi.edu/nsnam/ns/ must be downloaded into any media storage, most preferred is inside the computer itself where the NS-2 is going to be installed. Since, we are using NS 2.29. It is not recommend logging in as a root because installation at root may interfere with any important Linux files.

5.2.2. Tool Command Language (Tcl)

Short for Tool Command Language, Tcl is a powerful interpreted programming language developed by John Ousterhout at the University of California, Berkeley. Tcl is a very powerful and dynamic programming language. It has a wide range of usage,

including web and desktop applications, networking, administration, testing etc. Tcl is a truly cross platform, easily deployed and highly extensible. The most significant advantage of Tcl language is that it is fully compatible with the C programming language and Tcl libraries can be interoperated directly into C programs.

5.2.3. The Network Animation (NAM)

The network animator (NAM) began in 1990 as a simple tool for animating packet trace data. This trace data is typically derived as output from a network simulator like ns or from real network measurements, e.g., using tcpdump. Steven McCanne wrote the original version as a member of the Network Research Group at the Lawrence Berkeley National Laboratory, and has occasionally improved the design as he's needed it in his research. Marylou Orayani improved it further and used it for her Master's research over summer 1995 and into spring 1996. The nam development effort was an ongoing collaboration with the VINT project. Currently, it is being developed at ISI by the SAMAN and Conser projects.

5.2.4. The Trace File

The trace file is an ASCII code files and the trace is organized in 12 fields as in Figure 5.2. below.

Event	Time	From node	To node	Pkt type	Pkt size	Flags	Fid	Src addrs	Dst addrs	Seq num	Pkt id

Fig. 5.2. Fields of trace file

The first field is the event type and given by one of four available symbols r, +, - and d which correspond respectively to receive, enqueued, dequequed and dropped. The second field is telling the time which the event occurs. The third and fourth fields are the input and output node of the link at which the events takes place. The fifth is the packet type such as continuous bit rate (CBR) or transmission control protocol (TCP). The sixth is the size of the packet and the next field is some kind of flags. The eighth field is the flow identity of IPv6 which can specify stream color of the NAM display and can be use for further analyze purposes. The ninth and tenth fields are the source and destination address in the form of “node.port”. The eleventh is the network layer protocol’s packet sequence number. NS keeps track of UDP packet sequence number for the analysis purposes. The twelfth that is the last field is the unique identity of the

packet. Results of simulation are stored into trace file (*.tr). Trace Graph is used to analyze the trace file.

5.2.5. The Tracegraph

It is a data presentation system for Network Simulator ns-2. The simulator doesn't have any options implemented to analyse simulations results so it's hard to use it. Trace graph system provides many options for analysis, including 250 graphs and statistical reports. It is implemented in MATLAB 6.0 and can be compiled to run without MATLAB. Compiled versions for Linux and Windows systems are available for download at http://www.geocities.com/tracegraph/.

Trace graph supports the following ns-2 trace file formats; wired, satellite, wireless (old and new trace), wired-cum-wireless. Trace file loading stage is divided into 4 stages; automatic trace file format recognition, trace file parsing to extract necessary simulation data which is saved to a temporary file, trace files can contain much more data than is needed by the system, so unnecessary information is omitted to speed up trace file loading, temporary file loading, constants calculations (packets types, packets sizes, flows IDs, trace levels, number of nodes, simulation time) – in order to speed up data processing. Wireless and wired-cum-wireless trace files are parsed and saved in Trace graph format.

5.2.6. The Low Rate WPAN Function Modules

The LR-WPAN function modules were developed by Jianliang Zheng and Myung J. Lee (2006) at The City University, New York. The work was done specially for a newly defined standard; IEEE 802.15.4. They had study and developed several features such as beacon enabled mode and non-beacon enabled mode, association, tree formation and network auto-configuration, orphaning and coordination relocation, CSMA-CA for both slotted and un-slotted and direct, indirect and GTS data transmissions.

- *Wireless Scenario Definition*: It selects the routing protocol; defines the network topology; and schedules events such as initializations of PAN coordinator, coordinators and devices, and starting (stopping) applications. It defines radio-propagation model, antenna model, interface queue, traffic pattern, link error model, link and node failures, super-frame structure in beacon enabled mode, radio transmission range, and animation configuration.

- *Service Specific Convergence Sub-layer (SSCS)*: This is the interface between 802.15.4 MAC and upper layers. It provides a way to access all the MAC primitives, but it can also serve as a wrapper of those primitives for convenient operations. It is an implementation specific module and its function should be tailored to the requirements of specific applications.
- 802.15.4 PHY: It implements all 14 PHY primitives.
- 802.15.4 MAC: This is the main module. It implements all the 35 MAC sub-layer primitives.

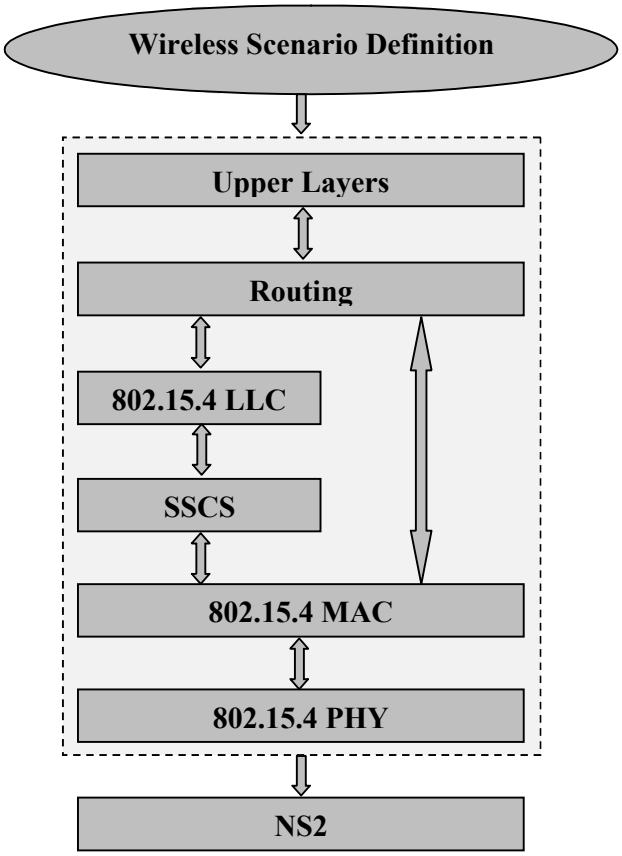

Fig. 5.3. LR-WPAN (IEEE 802.15.4) function modules

5.3. Frequency Hopping

Frequency hopping is a method to make the channel difficult to be access by intruder. The frequency used within the environment/system will be hopped to different frequency/channel frequently. Therefore, it is hard for the intruder to track the data being transmitted. Frequency hopping is one of various ways to provide security in wireless data transmission. If some frequencies are hopping in a limited time set

earlier, if intruders get access to the channel and jammed the channel, it will only affect the particular channel only. There will be one channel affected by it, remaining are still available for data transmission.

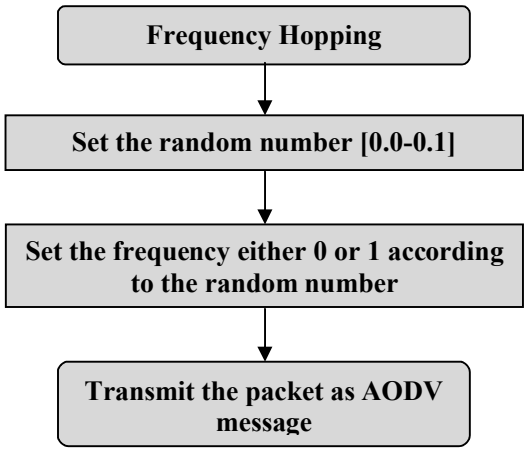

Fig. 5.4. Frequency hopping at transmitting side

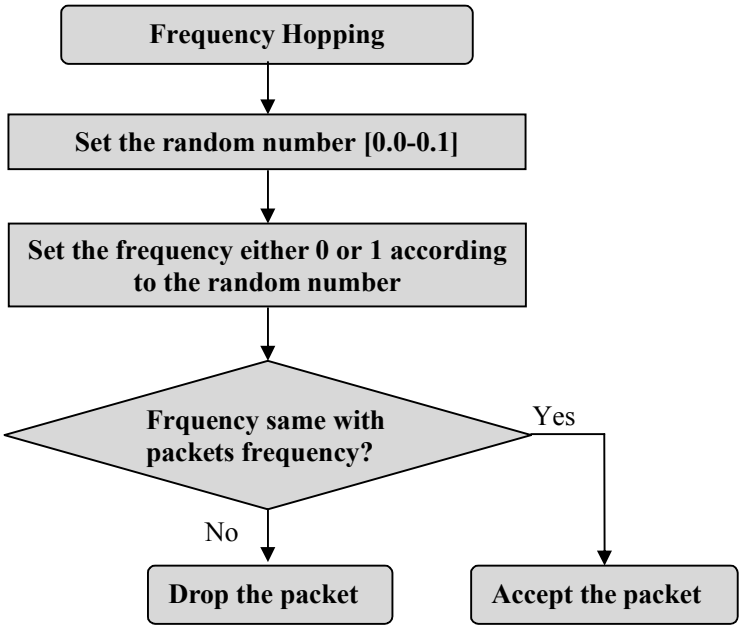

Fig. 5.5. Frequency hopping at receiving side

If the number of frequency used is increase or/and time set of each frequency is random, the probability of intruder accessing the channels and jamming the frequency will be small. In an FH ad hoc network, the phase of hopping sequence, i.e., FH-code

phase is typically derived from the local clock reading of each node. Therefore, network-wide time synchronization is needed in order to get the nodes to simultaneously switch to the same frequency channel, i.e., hop synchronously. The time for each frequency is depends on a random function. Figure 5.4 shows a flow chart of additional coding add inside the AODV function modules that will forward the AODV message. The frequency holds by a packet was set according to the random number generated. The additional coding that is added inside the AODV function modules that will receive the AODV message is shown in Figure 5.5.

5.4. Simulation

We use simulation to evaluate the performance of the proposed AODV routing protocol with and without the malicious node. We simulate a sensor network consisting of 20 nodes randomly deployed in a field of 50m × 50m square area. The base station is located in the middle of one edge. Nodes have same transmission range in one experiment. The simplest and usually the first thing to setup a network is creating a node. A network is build up from its layers components such as Link layer, MAC layer and PHY layer. The components have to be defined before a node can be configured. Table 5.1 shows the parameters used in the simulation.

Parameter Name	Parameter Value
channel type	Channel/Wireless Channel
radio model	TwoRayGround
netif	Phy/WirelessPhy/802_15_4
mac protocol	Mac/802_15_4
number of nodes	25
Number of malicious nodes	1
routing protocol	AODV
grid size	50 x 50 sq.m
packet size	70
simulation time	different
traffic type	Cbr

Table 5.1. Network parameter definition

CHAPTER 6

RESULTS, PERFORMANCE EVALUATION & ANALYSIS

This chapter shows the results of the simulation. The analysis is being done on the basis of the results of *.nam file and the *.tr file with the help of Network Animator (NAM) and tracegraph by plotting the 2D and 3D graphs. We also evaluate the performance of the protocol by using AWK programming. With the help of AWK programming we obtain the results in percentage. Simulation has been divided in four parts that are given below:

- Simple AODV Simulation
- AODV with frequency hopping
- AODV with malicious node
- AODV with malicious node and frequency hopping.

6.1. AODV Simulation

In the simulation of simple AODV, experiment is carried over 25 nodes. In the ns2-allinone package NAM is a build-in program. NAM helps us to see the flow of route request (RREQ) and route reply (RREP). It also shows the packets are dropping or reaching to the destination properly. When the TCL file is written, NAM is invoked inside that file. Figure 6.1 and figure 6.2 are animation capture of WSN with25 nodes. The source (node 10) is broadcasting RREQ message to all its neighbors and Node 1which is the destination node, is sending RREP (route reply) back to the source. The nodes with the same frequency will receive the message and forward it to its neighbor, while the nodes with different frequency will drop the packet. In figure 6.2, a packet of blue color is on transmission from the source (node 10) to the destination (node 1).

Since there is peer-to-peer communication between source node (10) and destination node (1), so no packet will be dropped. In figure 6.3 tracegraph proves that dropped packets are zero. This high throughput is expected because all the nodes are using the same frequency.

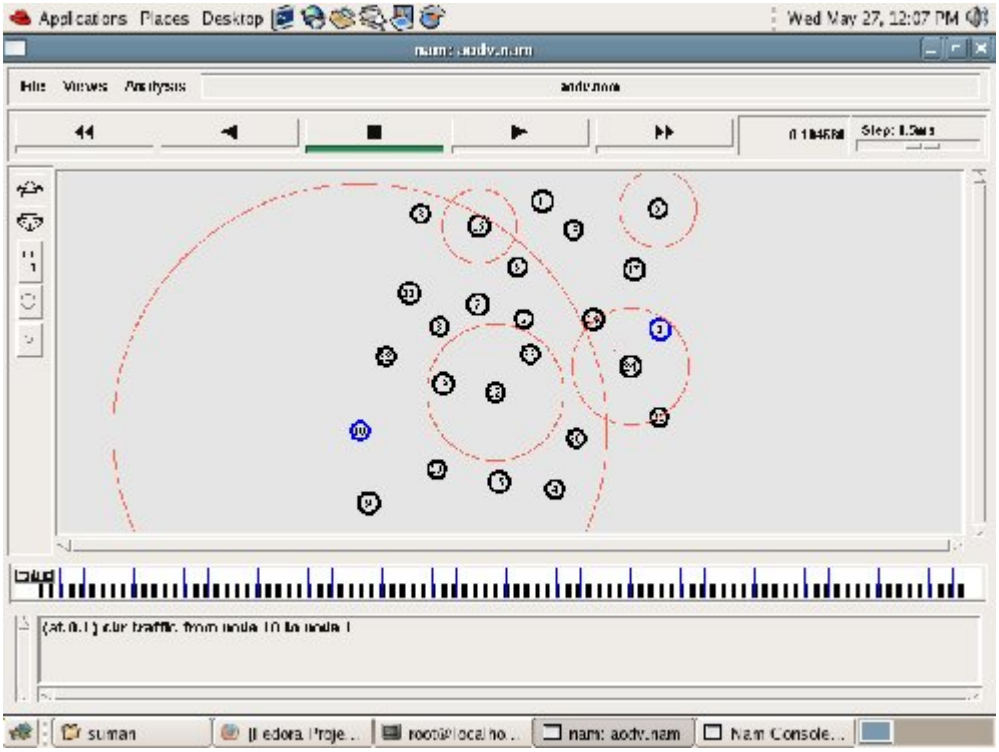

Fig. 6.1. Source node broadcasts RREQ

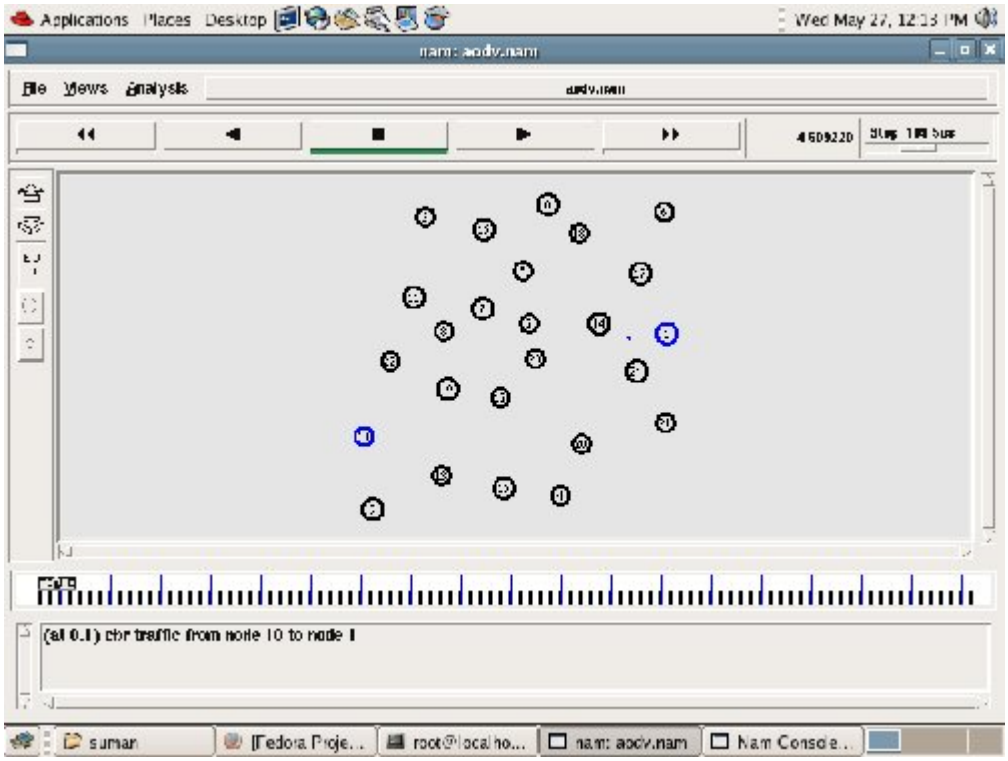

Fig. 6.2. Transmission of data packets from source node to destination node

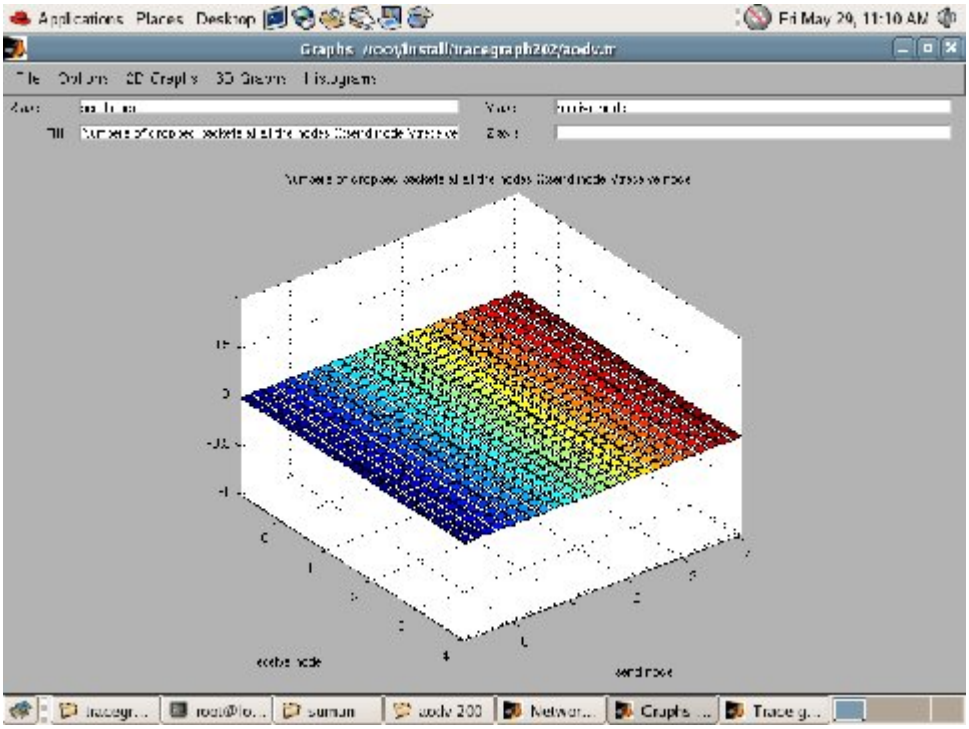

Fig. 6.3. No packet dropping

6.2. AODV with Frequency Hopping

A data packet is received by the destination only when source and destination are using the same frequency. When frequency hopping is applied in the AODV without malicious node, throughput decreases because due to two frequencies in the network all the packets do not reach to the destination and drops in between. The throughput varies as two frequencies are hopped with different period of simulation time. The throughput is increased when period of simulation becomes longer. The throughput has been analyzed with awk script and tracegraph.

Simulation Time(secs)	Throughput in Percentage
50	58.8
100	79.4
200	89.7
300	93.1
400	94.8
500	95.8
1000	97.9
1500	98.6
2000	98.9

Table 6.1 Percentage of received packets at the destination node

In table 6.1. tracegraph shows the received packets on the destination node. The table shows how the throughput changes with different simulation time.

6.3. AODV with Malicious Node

When malicious node (25) is inserted into the network as shown in the figure 6.4, it receives the broadcast packets and tries to behave like regular node of the network. In figure 6.4, malicious node 25 is broadcasting to all network nodes.

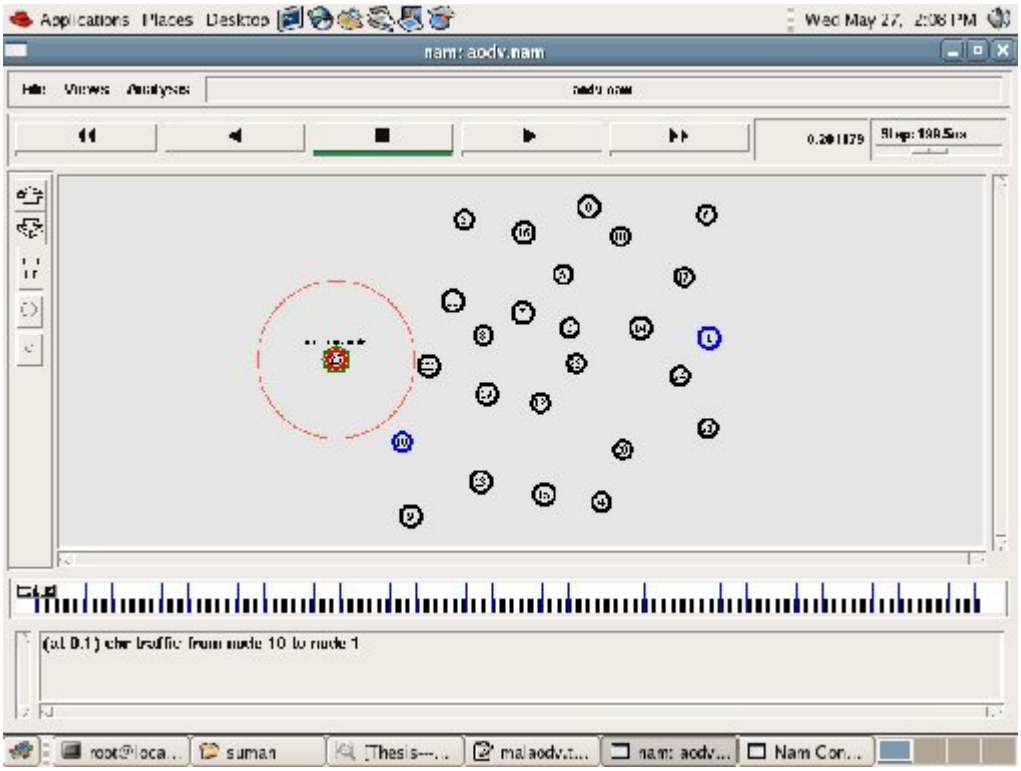

Fig. 6.4. Malicious node broadcasts a RREQ.

Now malicious node (25) receives RREP packet from the destination node and sends its own data to the destination node 1. In figure 6.5, malicious node and source node both are sending their own data to the destination node. The packet from malicious node is of black color and it sends more packets than source node. The malicious node tries to jam the channel by sending more and more packets so that the throughput decreases.

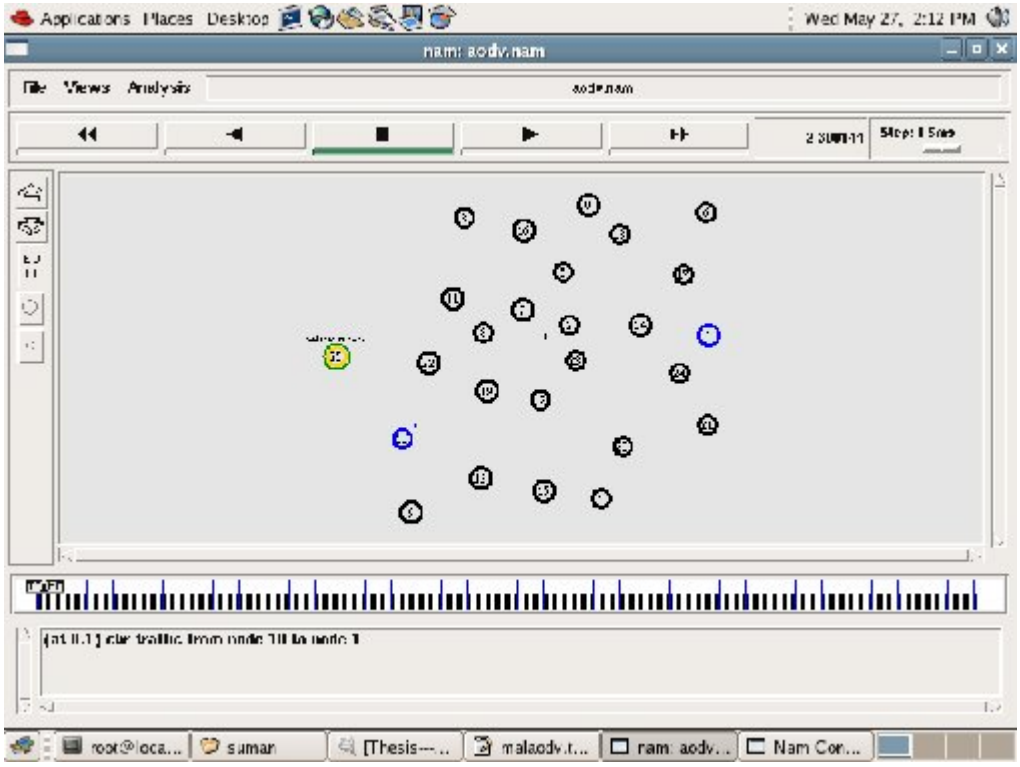

Fig. 6.5. Malicious node attacks the network

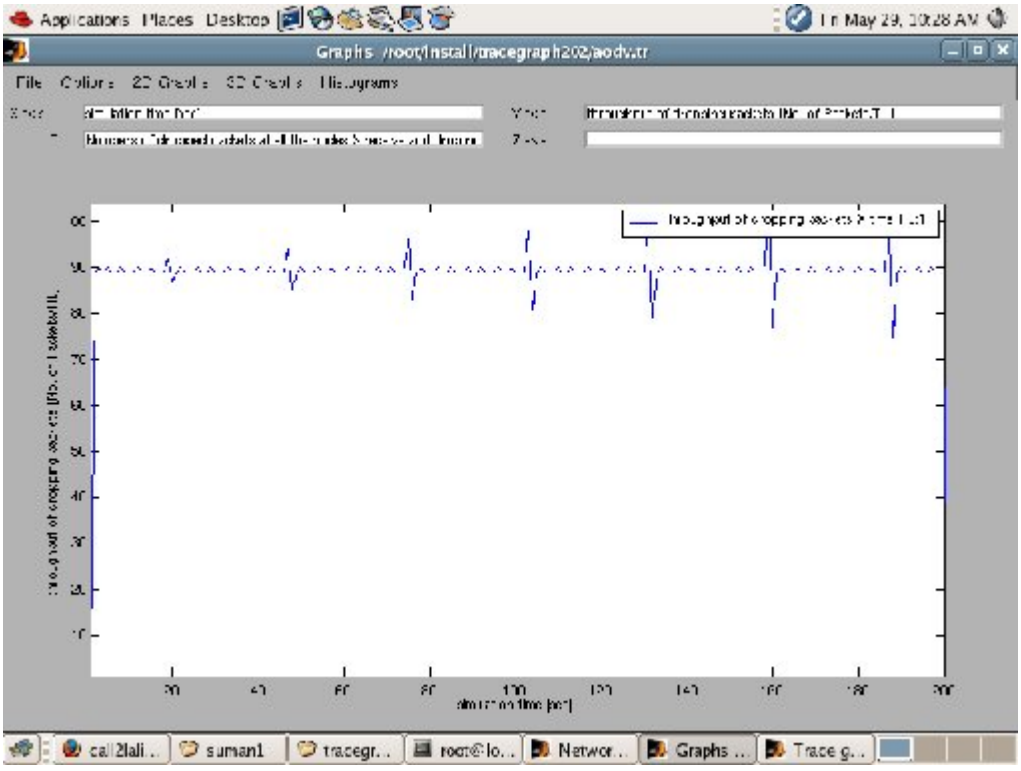

Fig. 6.6. Throughput of dropping packet with malicious node

6.4. AODV with Malicious Node and Frequency Hopping

When frequency hopping is applied to the network (with malicious node), the network performance increases as the simulation time increases. Table 6.2. explains how the throughput increase as the simulation time increases.

Simulation Time(secs)	Throughput in % (10-1)	Throughput in % (25-1)
50	60	.4272
100	80	.2132
200	90	.1065
300	93.3	.0709
400	95	.0532
500	96	.0425
1000	98	.0212
1500	98.6	.0141
2000	99	.0106

Table 6.2. Percentage of received packets at the destination node

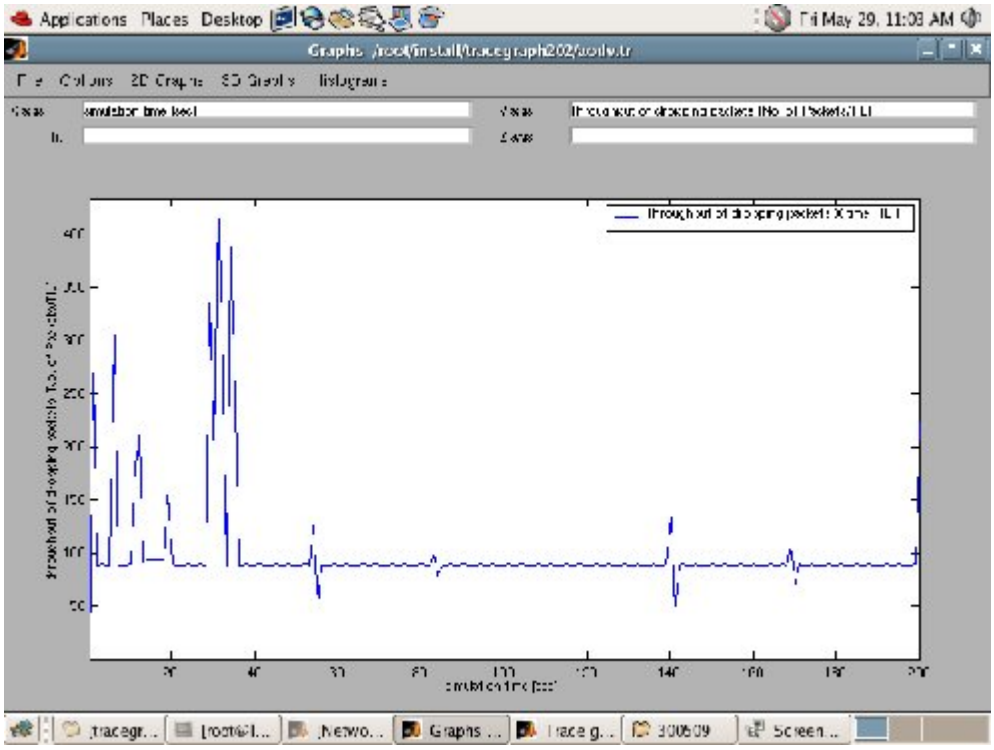

Fig . 6.7. Throughput of dropping packet with malicious node and frequency hopping

CHAPTER 7

CONCLUSION & FUTURE SCOPE

Security is a significant issue in Wireless Sensor Networks. Intrusion of malicious nodes may cause serious impairment to the security. The objectives listed have been carried out. In the presented work, we have discussed all the modes of AODV (simple mode, frequency hopping and malicious node) along with their working. We sincerely hope that our work will contribute in providing further research directions in the area of security based on frequency hopping.

In this thesis work, AODV over WSN is simulated with different operation modes. An important contribution of this thesis is the comparison of the WSN with and without malicious node using the frequency hopping technique.

With the results of AWK programming and tracegraph, we can conclude that in the case of simple AODV there is no packet drop and throughput is 100%. But when two frequencies are hopped in the network with different simulation times, throughput is less than 100% but increases continuously with respect to simulation time. After a simulation time of 2000 seconds (~33 minutes) almost 98 percent packets reach the destination safely.

As the malicious node enters into the network, it tries to capture the network. The performance of the network is affected badly. But, after applying frequency hopping, as the simulation time increases the throughput at the destination node also increases, which means that the network is secure enough to overpower the malicious node. After 1500 seconds throughput is 98.66 percent and after 2000 seconds it is exactly 99 percent. Even malicious node 25 is about not able to affect the network performance for long period of time. So, frequency hopping works well and can be used as a reliable method for IEEE 802.15.4.

Practical WSN security is a balancing act that is constantly in search of the highest level of protection that can be squeezed out of the judicious use of limited resources. A large number of security problems are still open in WSN. One of the open problems is authentication of sensor nodes. To secure the sensor network when a new node

enters into the network, it should be authenticated. Another, aspect of future research direction can be a non-beacon enabled WSN. Further, path hopping is another optional concept that can be used to secure the sensor network.

[1] Chatschik Bisdikian, "*An overview of the Bluetooth Wireless technology*", IEEE Communication Magazine, vol. 39, Dec 2001.

[2] Brain P. Crow, Indra Widjaja, Jeon Geun Kim and Prescott T. Sakai, "*IEEE 802.11 Wireless Local Area Networks*", IEEE Communication Magazine, Vol. 35, Sep 1997

[3] J. Macker and S. C. (chairmen). MANET (Mobile Ad Hoc Networking) working group of the IETF.

[4] K. Jones, A.Waada, S. Olaniu, L.Wison, M. Eltoweissy, "*Towards a new paradigm for Securing Wireless Sensor Networks*", New Security Paradigms workshop 2003, Ascona, Switzerland.

[5] Stephan Olariu, "*Information assurance in wireless sensor networks*", Sensor network research group, Old Dominion University.

[6] J. Zheng and Myung J. Lee (2006). *A comprehensive performance study of IEEE 802.15.4 – Sensor Network Operations*: Wiley Interscience. IEEE Press Chapter 4. 218-237.

[7] IEEE 802.15.4 WPAN-LR Task Group Website: http://www.ieee802.org/15/pub/TG4.html

[8] Jose A' Gutirez et al. "*IEEE 802.15.4: A Developing for Low Rate Wireless Personal Area Network".*

[9] Anis Koubaa, Mario ALVES, Bilel NEFZI, Ye-Qiong SONG, "*Improving the IEEE 802.15.4 Slotted CSMA-CA MAC for Time-Critical Events in Wireless Sensor Network".*

[10] Anis Koubaa, Mario ALVES, Eduardo TOVAR, "*A Comprehensive Simulation Study of Slotted CSMA-CA for IEEE 802.15.4 Wireless Sensor Network".*

[11] Karp and H. T. Kung, "*GPSR: greedy perimeter stateless routing for wireless networks*", in *Mobile Computing and Networking*, 2000, pp. 243–254.

[12] Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "*A survey on sensor networks*", IEEE Communication Magazine, Aug. 2002.

[13] Dr. A.K. Verma, Mayank Dave, R C Joshi, "*DNA-Cryptography a novel paradigm for securing MANETs*", vol-11-2008, no-4PP-393-404" J. Discrete Mathematics Science & Cryptography.

[14] Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar, "*SPINS: security protocols for sensor networks*", in: Proceedings of Mobile Networking and Computing 2001, 2001.

[15] Chris Karlof, David Wagner, "*Secure routing in wireless sensor networks: attacks and countermeasures*", University of California at Berkeley, Berkeley, CA 94720, USA, Ad Hoc Networks 1 (2003) 293–315.

[16] Intanagonwiwat, R. Govindan, and D. Estrin, "*Directed diffusion: A scalable and robust communication paradigm for sensor networks*", in *Proceedings of the Sixth Annual International Conference on Mobile Computing and Networks (MobiCOM '00)*, August 2000.

[17] Elizabeth M. Royer, Charles E.Perkins, "*An Implementation of the AODV Routing Protocols"*.

[18] Ad hoc on-demand distance vector (aodv) routing. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt.

[19] Teemu Vanninen, Hannu Tuomivaara, Juha Huovinen "*A Demonstration of Frequency Hopping Ad Hoc and Sensor Network Synchronization Method on WARP Boards*", WinTech'08, September 19, 2008, San Francisco, California, USA. ACM 978-1-60558-187-3/08/09.

[20] Ye, A. Chen, S. Liu, L. Zhang, "*A scalable solution to minimum cost forwarding in large sensor networks*", Proceedings of the tenth International Conference on Computer Communications and Networks (ICCCN), pp. 304-309, 2001.

[21] Ye, S. Lu, L. Zhang, "*GRAdient broadcast: a robust, long-live large sensor network*", Tech. Rep., Computer Science Department, University of California at Los Angeles, 2001.Braginsky, D. Estrin, "*Rumour routing algorithm for sensor networks*", in: First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.

[22] Ganesan, R. Govindan, S. Shenker, and D. Estrin, "*Highly-resilient, energy-efficient multipath routing in wireless sensor networks*", Mobile Computing and Communications Review, vol. 4, no. 5, October 2001.

[23] J. R. Douceur, "*The Sybil Attack*", in *1st International Workshop on Peer-to-Peer Systems (IPTPS '02)*, March 2002.

[24] Roosta, T., Shieh, S. and Sastry, S. "*Taxonomy of Security Attacks in Sensor Networks and Countermeasures*". Berkeley, California, University Press, 2006.

[25] D. W. Carman, P. S. Krus, and B. J. Matt. "*Constraints and approaches for distributed sensor network security*". Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[26] L. Li, J. Halpern, Z. Haas, "*Gossip-based ad hoc routing*", in: IEEE Infocom 2002, 2002.

[27] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "*Energy-Efficient Communication Protocol for Wireless Microsensor Networks*", Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00), January 2000, pp. 3005–3014.

[28] Y. C. Hu, A. Perrig, D.B. Johnson, "*Packet leashes: a defense against wormhole attacks in wireless networks*", in: IEEE Infocom, 2003.

[29] D. J. Torrieri, "*Fundamental limitations on repeater jamming of frequency-hopping communications*," IEEE Journal on Selected Areas in Communications, vol. 7, no. 4, pp. 569–575, May 1989.

[30] K. Tovmark, Chipcon Application Note AN014, "*Frequency Hopping Systems (Rev. 1.0)*", Chipcon AS, Mar. 2002.

[31] Y. Xu, J. Heidemann, D. Estrin, "*Geography-informed Energy Conservation for Ad-hoc Routing*", In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking 2001, pp. 70-84.

[32] Y. Yu, R. Govindan, and D. Estrin, "*Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks*", University of California at Los Angeles Computer Science Department, Tech. Rep. UCLA/CSD-TR-01-0023, May 2001.

[33] N. Sastry and D. Wagner, "*Security considerations for ieee 802.15.4 networks*," in Proceedings of the 2004 ACM workshop on Wireless security, pp. 32–42, Philadelphia, PA, USA: ACM Press, 2004.

[34] A. Ephremides, J. Wieselthier and D. Baker, "*A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signaling*", Proceedings of the IEEE, 1987.

[35] J. Zyren, T. Godfrey and D. Eaton, "*Does frequency hopping enhance security?"*.

[36] Fedora website. http://docs.fedoraproject.org/install-guide/fc6/en/

[37] Marc Greis. *Ns Tutorial*. http://www.isi.edu/nsnam/ns/tutorial/index.html

[38] S. McCanne and S. Floyd. *Network Simulator*. http://www.isi.edu/nsnam/ns/

[39] TCL Tutorial. http://www.tcl.tk/man/tcl8.5/tutorial/tcltutorial.html

[40] Tracegraph http://www.tracegraph.com/download.html

ACK	Acknowledgement
ADC	Analog to Digital Convertor
AODV	Ad-hoc On-demand Distance Vector
BE	Backoff Exponent
BP	Backoff Period
CAP	Contention Access Period
CBR	Continuous Bit Rate
CCA	Clear Channel Assessment
CFP	Contention Free Period
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA-CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear-To-Send message
DARPA	Defense Advanced Research Project Agency
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
ED	Energy Detection
FC4	Fedora Core 4
FTP	File Transfer Protocol
GENOME	GNU Network Object Model Environment
GTS	Guaranteed Time Slot
GUI	Graphical User Interface I
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
KDE	K Desktop Environment
LAN	Local Area Network
LQI	Link Quality Indication
LR-WPAN	Low Rate Wireless Personal Area Network
MAC	Medium Access Control
MAC	Message Authentication Code

MANETs	Mobile Ad hoc NETworks
MEMS	Micro-Electro-Mechanical Systems
NAM	Network Animation
NB	Number of Backoffs
NS	Network Simulator
OTcl	Object Oriented Tool Command Language
PAN	Personal Area Network
PHY	PHYsical
RREP	Route REPly
RREQ	Route REQuest
RTS	Ready-To-Send message
SNR	Signal-to-Noise Ratio
SSCS	Service Specific Convergence Sub-layer
TCL	Tool Command Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VINT	Virtual InterNetwork Test-bed
WPAN	Wireless Personal Area Network
WSN	Wireless Senor Network

PUBLISHED

- Suman Bala, Gaurav Sharma and A. K. Verma, "*Routing Techniques in Wireless Sensor Networks: An Overview",* International Conference (IISN-09), Feb 14-16, 2009.
- Suman Bala, Gaurav Sharma and A. K. Verma, "*Simulation and Analysis of AODV Protocol in Wireless Sensor Networks*", ISAN-2009, National Conference on Information Security and Networks.