Study and Development of Vulnerability Analysis Tool for IEEE 802.15.4 Wireless Networks

A Project Report

submitted by

ANJAN REDDY KASIREDDY (EE11M001)

in partial fulfilment of the requirements
for the award of the degree of

MASTER OF TECHNOLOGY

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY MADRAS.

May 2013

THESIS CERTIFICATE

This is to certify that the thesis titled **Study and Development of Vulnerability Analysis Tool for IEEE 802.15.4 Wireless Networks**, submitted by **Anjan Reddy Kasireddy (EE11M001)**, to the Indian Institute of Technology, Madras, for the award of the degree of **Master of Technology**, is a bona fide record of the research work done by him under our supervision. The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Dr. Radha Krishna Ganti
Project Guide
Assistant Professor
Dept. of Electrical Engineering
IIT-Madras, 600 036

Shri D. A. Roy
Project Guide, Scientific Officer - H
Reactor Control Division
Bhabha Atomic Research Centre
Mumbai, 400 094

Place: Chennai

Date: 07th May 2013

ACKNOWLEDGEMENTS

I would like to take this opportunity to thank my parents for their support and encouragement without which learning in and becoming a part of such a prestigious institution would not have been possible. I would like to dedicate this work to them.

I am ever thankful to Dr. Radha Krishna Ganti and Shri D.A.Roy for their continual support and invaluable advice throughout the duration of my project. I feel honoured and encouraged to have worked under their guidance. I would also like to take this opportunity to thank my professors at IIT Madras, Prof. David Koilpillai, Prof. R. Aravind, Prof. K. Giridhar, Dr. Sri Krishna Bhashyam, Dr. Arun Pachai Kannu, Dr. Krishna Jagannathan and Dr. Andrew Thangaraj who have imparted knowledge and have motivated me to learn the intricacies of the subjects.

I thank my teachers of Zilla Parishad High School, Ravipadu for laying down the stepping stones of my life. They have encouraged me a lot which made me to reach the stage of studying M-Tech in this prestigious institution. I thank lecturers of Sri Pratibha Junior College, Ongole especially Appa Rao sir, Sunil sir, Suresh sir, Hari Kumar sir and Babu sir for their concepts, suggestions and encouragement which led me to do B-Tech in one of the best universities of A.P., JNTU Anantapur. I am grateful to Dr. Rama Naidu, Dr. Sumalatha, Dr. Ramana Reddy of ECE department in JNTU Anantapur and lecturers in ACE institute, Hyderabad who have imparted knowledge and have motivated me to learn the intricacies of the subjects, which helped me to secure good rank in GATE 2011.

Last but not the least, I would like to thank my friends, classmates and lab-mates for their help and encouragement. A special mention to Bikshu for his help with Latex although I wanted to go for Lyx initially. I had fun filled trips and birthday parties with my classmates. I had fun filled sessions in the lab with my friends Sudharsan, Varsha, Abishek, Gopal, Aseem, Debayani, Ravi, Bikshu, Anji babu, Prashanth, Arjun, Ajay, Laxman, Pranitha and enjoyed through and through my stay here.

ABSTRACT

KEYWORDS: wireless sensor network, beacon enabled network, jamming, guaranteed time slots.

Wireless sensor networks based on IEEE 802.15.4 have wide applications in office and industrial automation. Shared wireless medium and vulnerabilities in the protocols are making these networks prone to attacks. There are very few tools for analyzing IEEE 802.15.4 (ZigBee) wireless sensor networks. We studied some of the possible attack scenarios which exploit security vulnerabilities of IEEE 802.15.4 networks. Based on the study, we developed a tool which will simulate these attacks to analyze network vulnerability. We studied and simulated attacks on Physical layer like jamming (constant, deceptive, random and reactive jamming), Link layer jamming which exploits periodic nature of protocol, attacks on MAC layer especially on the management of GTS. This tool will also serve as test bench to work out better and more robust protocols for wireless sensor networks.

Channel sharing in wireless sensor networks making easy for adversaries to conduct radio interference or jamming attacks that effectively cause a denial of service of either transmission or reception functionalities. These attacks can easily be accomplished by an adversary by either bypassing MAC layer protocols or emitting a radio signal targeted at jamming a particular channel. In this thesis we explained different jamming attacks that may be employed against a sensor network.

For time critical applications and applications requiring separate bandwidth, GTS mechanism has been provided by IEEE 802.15.4 standard. Various vulnerabilities in the GTS management, which can be exploited by the insider attackers are discussed in this thesis. Based on the structure of beacon enabled network, we have developed algorithms to launch outsider attacks energy-efficiently which are discussed along with simulation results in this thesis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Definitions

Beacon-enabled personal area network (PAN) : A PAN in which all coordinators emit regular beacons.

Association : The service used to establish membership for a device in a network.

Contention access period: The period of time immediately following a beacon frame during which devices wishing to transmit will compete for channel access using a slotted carrier sense multiple access with collision avoidance mechanism.

Coordinator: A device in an low rate wireless personal area network (LR WPAN) that provides synchronization services to other devices in the LR WPAN.

Encryption: The transformation of a message into a new representation so that privileged information is required to recover the original representation.

Orphaned device: A device that has lost contact with its associated coordinator.

Personal area network (PAN) coordinator: A coordinator that is the principal controller of a PAN. An IEEE 802.15.4 network has exactly one PAN coordinator.

Full function device: A device capable of operating as a coordinator.

Reduced function device: A device that is not capable of operating as a coordinator.

Acronyms and abbreviations

CFP : contention free period

MAC : medium access control

PAN : personal area network

RSSI : receive signal strength indicator

CAP : contention access period

WSN : wireless sensor network

LR-WPAN : low rate wireless personal area network

RFD : reduced function device

FFD : full function device

GTS : guaranteed time slot

CSMA-CA : carrier sense multiple access with collision avoidance

DSSS : direct sequence spread spectrum

CHAPTER 1

Introduction

Wireless sensor networks based on IEEE 802.15.4 have a wide range of applications including industrial monitoring, health and environmental monitoring, biomedical signal processing, wireless communication, intrusion detection in computer networks, surveillance for security and military applications such as battle-field surveillance and enemy tracking. In a wireless networking environment, security and integrity of the data is of prime importance. There are many attacks possible on wireless sensor networks which are limiting its usage in security critical applications.

The attacks can be classified according to the layers of network, whose vulnerabilities are exploited for attacking. In general wireless sensor network nodes have physical layer, MAC layer, network layer and application layer. We can classify the attacks depending on the layer, whose vulnerabilities are exploited. If we have the simulation environment for the possible attacks on wireless sensor networks, then we can apply some defense strategies and can check for the robustness of the protocol. It is necessary to analyze wireless sensor networks to check its vulnerability to various attacks like jamming, flooding, insider and outsider attacks, selective forwarding, wormhole, data replay etc. While a number of tools and frameworks exist for analyzing vulnerabilities of Wifi networks (eg Kismet, Aircrack, Airpwn, etc), there are very few tools for analyzing IEEE 802.15.4 (ZigBee) wireless sensor networks

In this project, attacks on ZigBee networks (popularly known wireless sensor networks) and results of the simulations of the simulator that we have developed are provided.

1.1 Motivation

In a wireless networking environment, security and integrity of the data is of prime importance. Hence it is necessary to analyze wireless sensor networks to check its

vulnerability to various attacks possible. While a number of tools and frameworks exist for analyzing vulnerabilities of Wifi networks (eg Kismet, Aircrack, Airpwn, etc), there are very few tools for analyzing IEEE 802.15.4 (ZigBee) wireless sensor networks. Simulation tools will serve as test bench to work out better and more robust protocols for any network. The protocols in sensor networks are optimized for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security. Because of its vulnerabilities for attacks many applications are not using the sensor networks. Studying and developing simulation tool for the possible attacks will help in the development of robust protocols. The survey Melgares (2011) will give the necessity of the development of simulation tool for the possible attacks on WSNs.

1.2 IEEE 802.15.4 based Wireless Sensor Networks

The characteristics of a low rate wireless personal area networks (LR-WPAN) are as follows:

- Over-the-air data rates of 250 kb/s, 100 kb/s, 40 kb/s and 20 kb/s.
- Star or peer-to-peer operation.
- Allocated 16 bit short or 64 bit extended addresses.
- Optional allocation of guaranteed time slots (GTSs).
- Carrier sense multiple access with collision avoidance(CSMA-CA) channel access.
- Fully acknowledged protocol for transfer reliability.
- Use of frame check sequence (FCS) for transfer reliability.
- Low power consumption.
- Energy detection (ED).
- Link quality indication (LQI).
- 16 channels in the 2450 MHz band, 10 channels in the 915 MHz band and 1 channel in the 868 MHz band.

Low rate wireless personal area network nodes which are using IEEE 802.15.4 standard for physical and MAC layer are called as ZigBee nodes. ZigBee technology is a

low data rate, low power consumption, low cost, wireless networking protocol targeted towards automation and remote control applications. Low power usage allows longer life with smaller batteries. ZigBee operates in the industrial, scientific and medical (ISM) radio bands: 868 MHz in Europe, 915 MHz in the USA and Australia and 2.4 GHz in most jurisdictions worldwide. Data transmission rates vary from 20 to 250 kilobits/second. The specification goes on to complete the standard by adding four main components: network layer, application layer, ZigBee device objects (ZDOs) and manufacturer defined application objects which allow for customization and favor total integration. Besides adding two high-level network layers to the underlying structure, the most significant improvement is the introduction of ZDOs. These are responsible for a number of tasks, which include keeping of device roles, management of requests to join a network, device discovery and security.

The figure 1.1 shows the protocol stack of a ZigBee device.

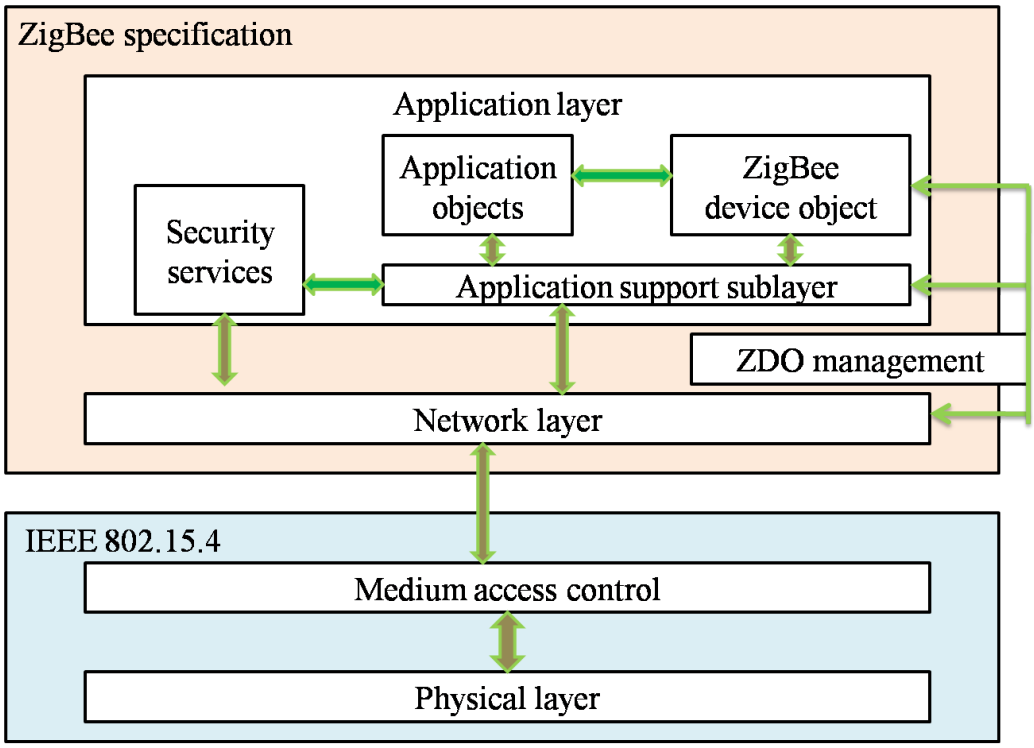

Figure 1.1: ZigBee protocol stack

Two different device types can participate in an IEEE 802.15.4 network. They are full function device(FFD) and reduced function device(RFD). The FFD can operate in three modes serving as a personal area network(PAN) coordinator, a coordinator or a

device. An FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD. An RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor. RFDs do not have the need to send large amounts of data and may only associate with a single FFD at a time. Consequently, the RFD can be implemented using minimal resources and memory capacity.

IEEE 802.15.4 LR-WPAN can operate in either of the two topologies: the star topology or the peer-to-peer topology.

In the star topology, communication is established between devices and a single central controller, called the PAN coordinator. A device typically has some associated application and is either the initiation point or the termination point for network communications. A PAN coordinator may also have a specific application, but it can be used to initiate, terminate, or route communication around the network. The PAN coordinator is the primary controller of the PAN. All devices operating on a network of either topology shall have unique 64 bit addresses. This address may be used for direct communication within the PAN, or a short address may be allocated by the PAN coordinator when the device associates and used instead. The PAN coordinator might often be mains powered, while the devices will most likely be battery powered. Applications that benefit from a star topology include home automation, personal computer (PC) peripherals, toys and games, and personal health care.

The peer-to-peer topology also has a PAN coordinator, however it differs from the star topology in that any device may communicate with any other device as long as they are in range of one another. Peer-to-peer topology allows more complex network formations to be implemented, such as mesh networking topology. Applications such as industrial control and monitoring, wireless sensor networks, asset and inventory tracking, intelligent agriculture, and security would benefit from such a network topology. A peer-to-peer network can be ad hoc, self-organizing and self-healing. It may also allow multiple hops to route messages from any device to any other device on the network.

IEEE 802.15.4 protocol uses two modes of operation : 1. beacon enabled mode 2. non-beacon enabled mode

1.2.1 Beacon enabled mode

In this mode of operation as defined in pro (2011), either personal area network coordinator or coordinator transmits periodically synchronizing frames called beacon frames. All the other nodes will communicate with the personal area network coordinator or coordinator only if they receive beacon frames. This mode is widely used because of active and sleep durations to save energy. The format of the super-frame is defined by the coordinator. The super-frame is bounded by network beacons sent by the coordinator and is divided into 16 slots of equal duration. The super-frame can have an active and an inactive portions. During the inactive portion, the coordinator is able to enter a low power mode. The beacon frame transmission starts at the beginning of the first slot of each super-frame. If a coordinator does not wish to use a super-frame structure, it will turn off the beacon transmissions. The beacons are used to synchronize the attached devices, to identify the PAN, and to describe the structure of the super-frames. Figure 1.2 shows an example of the super-frame structure. Any device wishing to com-

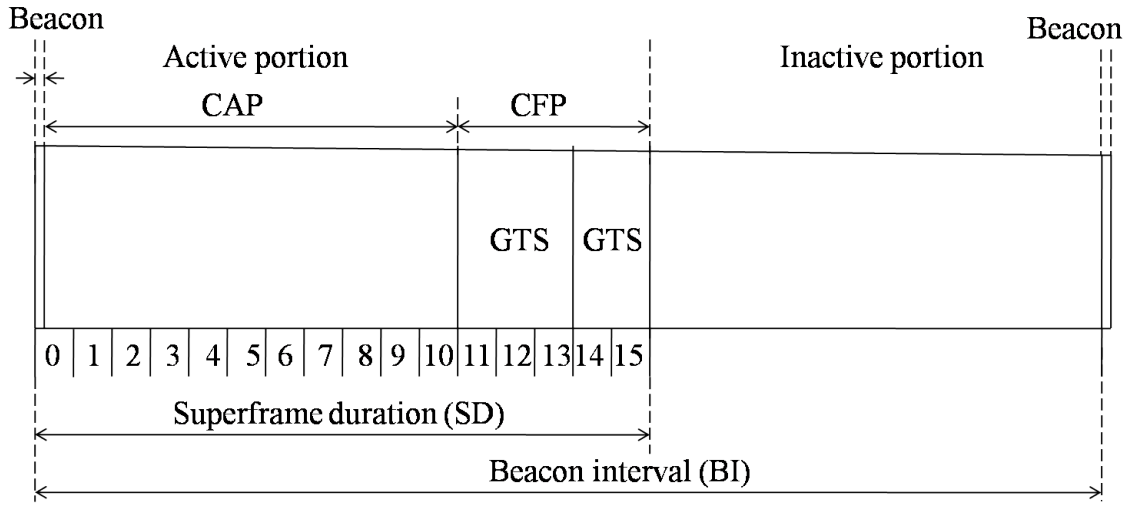

Figure 1.2: Super-frame structure of beacon enabled network

municate during the contention access period (CAP) between two beacons competes with other devices using a slotted CSMA/CA. For low latency applications or applications requiring specific data bandwidth, the PAN coordinator dedicates portions of the active super-frame to that application. These portions are called guaranteed time slots (GTSs). The GTSs form the contention free period (CFP), which always appears at the end of the active super-frame starting at a slot boundary immediately following the

CAP. The PAN coordinator allocates up to seven of these GTSs, and a GTS is allowed to occupy more than one slot period. However, a sufficient portion of the CAP remains for contention based access of other networked devices or new devices wishing to join the network. All contention based transactions are completed before the CFP begins. Also each device transmitting in a GTS ensures that its transaction is complete before the time of the next GTS or the end of the CFP. In CFP nodes communicate without using CSMA/CA(transmit when ever data is present).

1.2.2 Non-beacon enabled mode

In this mode of operation synchronization among network nodes is done by polling for any data pending at the personal area network coordinator or coordinator. Here channel access is done by using unslotted CSMA/CA. GTSs are not used here. Nodes should be active all the time so as to receive data from other nodes which is not energy efficient.

1.3 Security Services in Wireless Networks

Wireless networks are designed such that communication between the devices can be established anywhere, in a decentralized manner with out the support of an established infrastructure. Like any communication network, the true potential of wireless networks cannot be exploited without considering and adequately addressing the security issues. The security services are authentication, confidentiality, integrity and availability. Any data transmitting network must ensure the above mentioned services to be performed.

The security service of authentication provides the assurance that any particular entity (wireless device) is the one who it claims to be. With the perspective of wireless networks, the service of authentication is further divided into two components: (i) access authentication and (ii) origin authentication. The objective of access authentication is to ensure that only legitimate devices can access the network services. This in-turn protects the network from illegal access and malicious jeoperdization. The origin authentication ensures that within the authenticated network nodes, a node must be able to prove its identity for every communication session with any other node in the net-

work. This ensures that an authenticated node cannot impersonate another legitimate node in the network. Consequently, the network is protected against misbehaving and compromised nodes.

One of the methods used for authentication is asymmetric key cryptography. In this cryptographic technique the identity of the user/device is bound with a private and a public key. The public key is known to everyone while the private key is known only to the device that owns the key. Suppose device A intends to communicate with device B, it encrypts the message using its private key and a publicly known encryption algorithm. Upon receiving the message, device B verifies if A transmitted the message by decrypting the message using public key of device A. If the message is successfully decrypted (correctness of a message is verified through cyclic redundancy check (CRC)), the message is considered to be originating from the authentic device A, otherwise, it is assumed that an unauthenticated device is impersonating the device A.

Confidentiality ensures that the information transmitted across the network is accessible only by the intended recipients. In the example of the preceding paragraph, to ensure the confidentiality of the information, device A encrypts the message using public key of device B. Upon receiving the message, device B decrypts the message using its private key. In this case, a device can decrypt the message successfully only if it is in possession of valid private key of device B. Since the private key of device B is only known to the device itself, only the device B can decrypt the message successfully, ensuring the message confidentiality. In network security, confidentiality can be achieved with data encryption. Data encryption scrambles plain text data into unreadable cipertext data. Confidentiality attack tools focus on the content of the data and are best known for encryption cracking.

Integrity can be defined as unimpaired, complete, undivided, or unbroken. In network security this means that the message has not been tampered. No portion of the message has been removed, rearranged, or changed. The basic security measure to ensure integrity is to generate a cryptographic checksum of some sort to guarantee the message is unaltered. Integrity attacks tools focus on the data in transmission and include frame insertion, man in the middle, and replay attacks.

Finally, availability means that data should be accessible and usable upon demand by an authorized user or process. An availability attack consists of some sort of denial of service (DoS) attack. A DoS attack prevents the user or device from accessing a particular service or application.

Having strong network security does not mean one can prevent the network from being attacked. It simply means that the security mechanisms implemented are just that secure and have not been broken yet. Computer and network security is constantly evolving. Strong security mechanisms must also evolve. As older mechanisms are broken or cracked, new ones must be developed.

1.4 Wireless Sensor Network Characteristics Favourable for Attacks

Wireless sensor networks are basically low data rate, low distance and low cost devices which contains limited number of resources and runs on 2 AA batteries for years. For doing this wireless sensor networks spend much of their time in sleep to avoid power wastage. Following are some of the characteristics which may be exploited by the attackers :

- Due to limited resources associated with low cost sensor hardware like limited processing capability and memory.
- Channel sharing by all wireless networking devices allows for radio interference attacks that target communication. Traditional denial of service attacks are concerned with filling user domain and kernel domain buffers, where as jamming attacks exploit the shared nature of the wireless medium in order to prevent devices from communicating or receiving. Spread spectrum technique is used to detect signal even in the presence of the jammer which is useful in military systems but most sensor networks do not employ sufficiently strong spreading techniques to survive jamming.
- Use of carrier sensing (CSMA/CA) for medium access control(MAC) layer, makes these systems susceptible to a simple and severe jamming problem. An adversary can simply disregard the medium access protocol and continually transmit on a wireless channel. By doing so, he or she either prevents users from being able to commence with legitimate MAC operations or introduces packet collisions that force repeated back-offs or even jams transmissions.

- Sensor devices have extremely limited and often non-replenishable(not replaced again) power supplies.
- Battery lifetime and cost constraints put severe limits on the security overhead these networks can tolerate.
- Periodic nature of Beacon enabled WSNs.

In Wood and Stankovic (2002) various attacks on different layers of WSNs are given. In Law *et al.* (2005),Yee Wei Law propose link layer jamming attacks by looking at the packet inter-arrival times in three representative MAC protocols S-MAC, LMAC and B-MAC, derived several jamming attacks that allow the jammer to jam S-MAC, L-MAC and B-MAC energy-efficiently. Based on the ideas given in paper Law *et al.* (2005) for MAC protocols S-MAC, LMAC and B-MAC, we have developed certain algorithms on beacon enabled network 4, which makes attacker to attack energy efficiently. In JUNG (2011) and Sokullu *et al.* (2008) insider attacks on beacon enabled networks, in particular on the management of GTS are provided. Xu et al. propose 4 generic jammer models in Xu *et al.* (2006). Karlof and Wagner (2003) describes various security aspects of different routing protocols used in wireless sensor networks. In Sokullu *et al.* (2007), investigation of various attacks on IEEE 802.15.4 MAC layer are given. A MAC layer protocol for defeating stealthy jammers with IEEE 802.15.4 based hardware is discussed in paper Wood *et al.* (2007).

1.5 Choice of Open Source Simulator

NS2 (network simulator 2) is a discrete event network simulator. OMNeT++ (objective modular network testbed in C++) is an object-oriented modular discrete event network simulator. For the development of the simulator for the attacks, we first thought of choosing NS2, but we have chosen OMNeT++ for the following reasons.

- Wireless sensor networks simulations in OMNeT++ are much more scalable than NS2. OMNeT++ is better than other simulator in large-scale wireless sensor network simulation.
- OMNeT++ is a flexible and generic simulation framework than NS2. One can simulate anything that can be mapped to active components that communicate by passing messages.

- OMNeT++ has a well written and up-to-date manual (there are also tutorials for quick introduction). OMNeT++'s simulation API is more mature and much more powerful than NS2's.
- In OMNeT++ parameters of a simulation experiments are written in the omnetpp.ini, which enforces the concept of separating model from experiments. In NS2 topology, parameters, model customizations, result collection etc usually in the same Tcl script, which makes "separation of concerns" difficult.
- Coding in OMNeT++ requires only C++ to be known and easy to code due to dividing tasks in to smallest possible, where as in NS2, we have to learn many languages and hard to code.

The manual of OMNeT++ Varga (2011), gives information about how to code for getting network simulations in OMNeT++.

1.5.1 Choice of framework in OMNeT++

In OMNeT++ many frameworks exists, each has different protocols implemented and for different applications. Some of these frameworks are INET, INETMANET, MIXIM and Castalia. Among these INETMANET, MIXIM and Castalia are supporting for wireless network simulations. But none of the frameworks have full ZigBee network simulation support. INETMANET and MIXIM are designed for the simulation of wireless networks, but for each module there will be so many interconnections with other modules. Castalia simulator is based on real radio and channels using real data taken from real applications which can be used for different applications for wireless sensor networks and is designed specially for wireless sensor networks. We finally choose Castalia simulator for conducting the attacks. The structure and implementation details of Castalia are given in document Boulis (2009).

1.5.2 Challenges in simulation of attacks

The following are the various challenges that we faced before starting simulations:

- Limited implementation of MAC layer of IEEE 802.15.4 protocol for beacon enabled mode.
- No graphic visualizer for Castalia.

- Lack of routing protocols.

1.5.3 Work done so far

We have done the following work for the purpose of simulation of attacks :

- Provided Network Animator (NAM) support for visualizations, any simulation of any number of nodes will automatically generates NAM file, by using which we can see the network scenarios.
- Simulated 4 different jamming attacks with the limited implementation of MAC layer of IEEE 802.15.4 protocol for beacon enabled mode, which is enough for conducting jamming attacks.
- For the purpose of MAC layer attacks, full MAC layer of IEEE 802.15.4 protocol has implemented.
- Star routing protocol has implemented for simulation of attacks.
- We simulated 4 different insider attacks on the management of GTS
- Written algorithms for 3 new outsider attacks on beacon enabled networks and simulated.

1.6 Thesis Organization

In this thesis, we examined the vulnerabilities of IEEE 802.15.4 based wireless sensor networks and presented some of the possible attacks. For the purpose of simulating the various attacks, we have chosen Castalia framework in OMNeT++ simulator. We developed the MAC 802.15.4 protocol and star routing protocol for the simulation of the proposed attacks.

The organization of the thesis is as follows: In Chapter 2, we explain various attacks possible on physical layer such as jamming and tampering. Effects of various types of jamming on beacon and non-beacon enabled networks is discussed. Simulation results have been provided. Certain defenses against jamming are mentioned.

In Chapter 3, we present different insider attacks possible on guaranteed time slots of beacon enabled networks. Simulation results are also provided. Some of the defense mechanisms against the attacks are discussed here.

In Chapter 4, we present various outsider attacks possible on beacon enabled networks which exploit the semantics of the IEEE 802.15.4 MAC layer. Simulation results are also provided. Some of the defense mechanisms against the attacks are discussed here.

In Chapter 5, conclusion and future work are provided.

CHAPTER 2

Attacks on Physical Layer

2.1 Classification of Attacks

Jamming is the primary physical layer attack against WSNs.

2.1.1 Overview of the jamming problem with an example

Suppose Alice and Bob are socializing with each other at a party and suddenly, the malicious Mr.X walks up. Without any regard for proper social etiquette, he interrupts them and begins to take over the conversation. Each time Alice tries to talk, Mr.X interrupts her and tells an inane(silly or stupid) story. Bob, likewise doesn't fare any better. Alice and Bob both wait a polite amount of time in order to give Mr.X an opportunity to remedy his behavior. However, after some time, it becomes clear that Mr.X will not give in and that our two heroes are destined to have a poor reunion and regret ever attending the party.

The story of the social party is a simple, motivating example for the problem of wireless radio interference. In the case of wireless communication, Alice and Bob correspond to two communicating nodes A and B, while Mr.X corresponds to an adversarial interferer X. The adversary X, who may or may not be intentionally trying to disrupt communication, may interfere with A and B's ability to communicate by either ignoring MAC layer protocols (e.g. perhaps X does not know the proper MAC layer etiquette or perhaps he actively chooses to ignore MAC protocols) or by emitting a signal of sufficient energy on the channel used by A and B.

From the adversary point of view, he/she can build MAC layer jammers by having the wireless devices simply disregard the medium access protocol. An adversary may employ a powerful device driver to bypass card firmware and repeatedly send out

packets. As a consequence, all devices within the radio range of X will think that the channel is occupied and will defer transmission of data. Similarly at the physical layer, an adversary may use any device (e.g. waveform generator) capable of emitting energy in the frequency band corresponding to the channel A and B are communicating on. Furthermore, though not necessary legal, many off-the-shelf jamming devices are available for different purposes. Cell phone jamming units can be purchased and installed in classrooms or theaters to block cell phone reception signals. Beyond those intentional jammers, unintentional RF interference can be witnessed in our daily life as wireless networks have become increasingly popular.

2.1.2 Characteristics of WSNs favouring jamming attack

- Use of CSMA/CA for channel access.
- Lack of strong spreading to receive signal even in the presence of interference.
- Frame Check Sequence(FCS) usage causing legitimate nodes to discard the packet even if one bit is in error, so attacker work is to provide interference to cause atleast one bit to go error.

Jamming which exploits physical layer can be classified in to four basic categories

- Constant jammer
- Deceptive jammer
- Random jammer
- Reactive jammer

The above jamming attack types were proposed by Xu et al in paper Xu *et al.* (2006).

Tampering is another physical layer attack.

2.2 Constant Jammer

The constant jammer continually emits a radio signal, and it can be either a malicious jamming attack where adversary purposely interfere with network communication, or

unintentional radio interference where the interferer is always emitting RF signal. We can implement a constant jammer using two types of devices. The first type of device is a waveform generator which continuously sends a radio signal. The second type of device is a normal wireless device. In this thesis, we will focus on the second type, which bypass its MAC protocol. Our constant jammer continuously sends out random bits(preamble may not be same as that of IEEE 802.15.4 networks) to the channel without following any MAC layer etiquette. Specifically, the constant jammer does not wait for the channel to become idle before transmitting. IEEE 802.15.4 devices have different clear channel assessment(CCA) methods to check whether the channel is idle or not for CSMA/CA usage.

If CCA mode is energy above threshold, the underlying MAC protocol determines whether a channel is idle or not by comparing the signal strength measurement with a fixed threshold, which is usually lower than the signal strength generated by the constant jammer, a constant jammer can effectively prevent legitimate traffic sources from getting hold of channel and sending packets. In non-beacon enabled networks, nodes use unslotted CSMA/CA for channel access. Since all the nodes sense the busy channel, no transmissions occur. All the data present will be overflown form the buffers. In beacon enabled networks, nodes use slotted CSMA/CA for channel access except for beacon transmission. Since all the nodes sense busy channel, no transmissions except beacon frame occurs. But all the nodes receives beacon frame with interference and any single bit error causes the frame to be discarded. If four consecutive beacons are lost then nodes will declare themselves as lost synchronization and orphaned. So nodes will be disassociated from the network. All the data present will be overflown form the buffers.

If CCA mode is carrier sense only, CCA shall report a busy medium only upon the detection of a signal compliant with IEEE 802.15.4 standard with the same modulation and spreading characteristics of the physical layer that is currently in use by the device. This signal may be above or below the ED threshold. Since constant jammer transmits random data which is not compliant with IEEE 802.15.4 standard, the device always sense the idle channel. In non-beacon enabled networks all the nodes sense the idle channel and transmits data or command frames. All the nodes receive command and

data frames with interference and any single bit error causes the frames to be discarded. All the data will be dropped due to no acknowledgement after maximum number of retransmissions allowed. In beacon enabled networks, all the nodes sense the idle channel and transmits data or command frames. All the nodes receives command and data frames with interference and any single bit error causes the frames to be discarded. All the data will be dropped due to no acknowledgement after maximum number of retransmissions allowed. Similarly, all the nodes receive beacon frame with interference and any single bit error causes the beacon frame to be discarded. If four consecutive beacons are lost then nodes will declare themselves as lost synchronization and orphaned. So nodes will be disassociated from the network.

2.3 Deceptive Jammer

The deceptive jammer constantly injects regular(compliant with IEEE 802.15.4 standard) packets to the channel without any gap between subsequent packet transmissions. As a result, a normal communicator will be deceived into believing that there is a legitimate packet and will be duped to remain in the receive state. For example, in TinyOS, if a preamble is detected, a node remains in the receive mode, regardless of whether that node has a packet to send or not. Hence, even if a node has packets to send, it cannot switch to the send state because a constant stream of incoming packets will be detected. Further, we also observe that it is adequate for the jammer to only send a continuous stream of preamble bits (0xAA in TinyOS) rather than entire packets.

In deceptive jamming scenario, irrespective of the clear channel assessment(CCA) mode used, all the nodes will be in the receiving mode only. In non-beacon enabled networks all the nodes are in the receive mode only. All the data present will be overflown form the buffers. In beacon enabled networks, all the nodes are in the receive mode only. All the data present will be overflown form the buffers. But all the nodes receive beacon frame with interference and any single bit error causes the frame to be discarded. If four consecutive beacons are lost then nodes will declare themselves as lost synchronization and orphaned. So nodes will be disassociated from the network.

2.4 Random Jammer

Instead of continuously sending out a radio signal, a random jammer alternates between sleeping and jamming. Specifically, after jamming for t_j units of time, it turns off its radio, and enters a sleeping mode. It will resume jamming after sleeping for t_s time. t_j and t_s can be either random or fixed values. During its jamming phase, it can either behave like a constant jammer or a deceptive jammer. Throughout this thesis, our random jammer will operate as a constant jammer during jamming. The distinction between this model and the previous two models lies in the fact that this model tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply. By adjusting the distribution governing the values of t_j and t_s , we can achieve various levels of trade-off between energy efficiency and jamming effectiveness. Random jammer can either represent a malicious jammer or unintentional interferer that interfere with network communication from time to time.

Since we considered constant jammer during the active portions of the jammer, the following effects will occur. If CCA mode is energy above threshold, the underlying MAC protocol determines whether a channel is idle or not by comparing the signal strength measurement with a fixed threshold, which is usually lower than the signal strength generated by the constant jammer, a constant jammer can effectively prevent legitimate traffic sources from getting hold of channel and sending packets. In non-beacon enabled networks, nodes use unslotted CSMA/CA for channel access. Since all the nodes sense the busy channel, no transmissions occur. All the data present will be overflown form the buffers. In beacon enabled networks, nodes use slotted CSMA/CA for channel access except for beacon transmission. Since all the nodes sense busy channel, no transmissions except beacon frame occurs. But all the nodes receives beacon frame with interference and any single bit error causes the frame to be discarded. If four consecutive beacons are lost then nodes will declare themselves as lost synchronization and orphaned. So nodes will be disassociated from the network. All the data present will be overflown form the buffers.

If CCA mode is carrier sense only, CCA shall report a busy medium only upon the detection of a signal compliant with IEEE 802.15.4 standard with the same modulation

and spreading characteristics of the physical layer that is currently in use by the device. This signal may be above or below the ED threshold. Since the random jammer that we considered, transmits random data which is not compliant with IEEE 802.15.4 standard, the device always sense the idle channel. In non-beacon enabled networks all the nodes sense the idle channel, transmissions occur. All the nodes receive command and data frames with interference and any single bit error causes the frames to be discarded. All the data will be dropped due to no acknowledgement after maximum number of retransmissions allowed. In beacon enabled networks, all the nodes sense the idle channel, transmissions occur. All the nodes receive command and data frames with interference and any single bit error causes the frames to be discarded. All the data will be dropped due to no acknowledgement after maximum number of retransmissions allowed. Similarly, all the nodes receive beacon frame with interference and any single bit error causes the beacon frame to be discarded. If four consecutive beacons are lost then nodes will declare themselves as lost synchronization and orphaned. So nodes will be disassociated from the network.

During sleep periods of the jammer, normal communication occur in non-beacon enabled networks. In beacon enabled network, beacons will be received and re-association with the network will occur. Hence normal communication occur in beacon enabled networks.

The above three jamming models are called as active jammers which jams the channel irrespective of the traffic pattern on the channel. Active jammers are usually effective because they keep the channel busy all the time. But these methods are relatively easy to detect.

2.5 Reactive Jammer

The reactive jammer will not jam the channel when nobody is communicating. The jammer stays quiet when the channel is idle, starts transmitting a radio signal as soon as it senses activity on the channel. As a result, a reactive jammer targets the reception of a message. We would like to point out that a reactive jammer does not necessarily conserve energy because the jammer's radio must continuously be on in order to sense

the channel. The primary advantage for a reactive jammer, however, is that it may be harder to detect.

In non-beacon enabled networks all the nodes receive command and data frames with interference and any single bit error causes the frames to be discarded. All the data will be dropped due to no acknowledgement after maximum number of retransmissions allowed. In beacon enabled networks all the nodes receive command and data frames with interference and any single bit error causes the frames to be discarded. All the data will be dropped due to no acknowledgement after maximum number of retransmissions allowed. But the nodes receive beacon frame with interference and any single bit error causes the beacon frame to be discarded. If four consecutive beacons are lost then nodes will declare themselves as lost synchronization and orphaned. So nodes will be disassociated from the network.

Since jammer node has to sense the channel activity and switch from reception to transmission, smaller packets may not be interfered effectively to make the nodes to drop the packet. So nodes far from the jammer when compared to PAN coordinator may receive beacons with out error(no loss of synchronization) but any communications with the PAN coordinator will be failed because of the interference from the jammer. So in beacon enabled networks, nodes far from jammer may not lose synchronization but communication is disrupted by the jammer. So effectively we are making the nodes to lose data due to no acknowledgement even after maximum number of retransmissions.

Advantage of reactive jammer over remaining jammers is that it is very difficult to detect comparatively. One more advantage is that if there is mechanism of detecting jamming and hopping to some other channel for communication in legitimate nodes, reactive jammer will not sense any activity for a long time then it can scan the remaining channel to switch and jam the communication over the new channel. This advantage is not there in active jammers, where we may employ periodic scanning for detection of change of channel by legitimate nodes.

2.6 Simulation Results

We choose Castalia framework of OMNeT++ for conducting jamming attacks which is popularly known for wireless sensor networks. IEEE 802.15.4 protocol is partially implemented in Castalia-3.2 which is enough for conducting jamming attacks. We considered 3 legitimate nodes, 1 PAN coordinator (node 1), 2 associated nodes (nodes 0 and 2) which transmit data to the PAN coordinator on beacon enabled network with beacon order = 7, super-frame order = 6. We considered malicious node near to node 0. Arrangements of nodes are on a horizontal line with PAN coordinator in between the two associated devices as shown in figure 2.1. Here node 1 is PAN coordinator, nodes 0 and 2 are transmitting to the PAN coordinator.

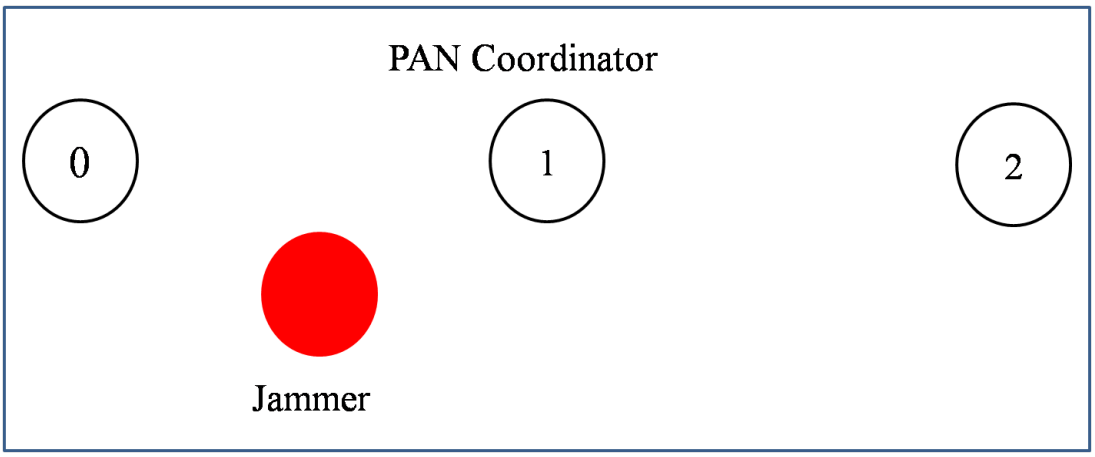

Figure 2.1: Network used for jamming attacks

2.6.1 Normal communication

Figure 2.2 shows the received signal strength indicator (RSSI), taken near the node 1 of beacon enabled network with beacon order = 7, super frame order = 6 for normal communication between legitimate nodes with out the presence of the jammer. The simulation has carried out for a period of 100 seconds. Here node 1 is PAN coordinator, node 0 and 2 are transmitting to the coordinator. Nodes 0 and 2 transmits 300 packets each to node 1. Table 2.1 gives packets transmissions and receptions related information at nodes 0,1,2.

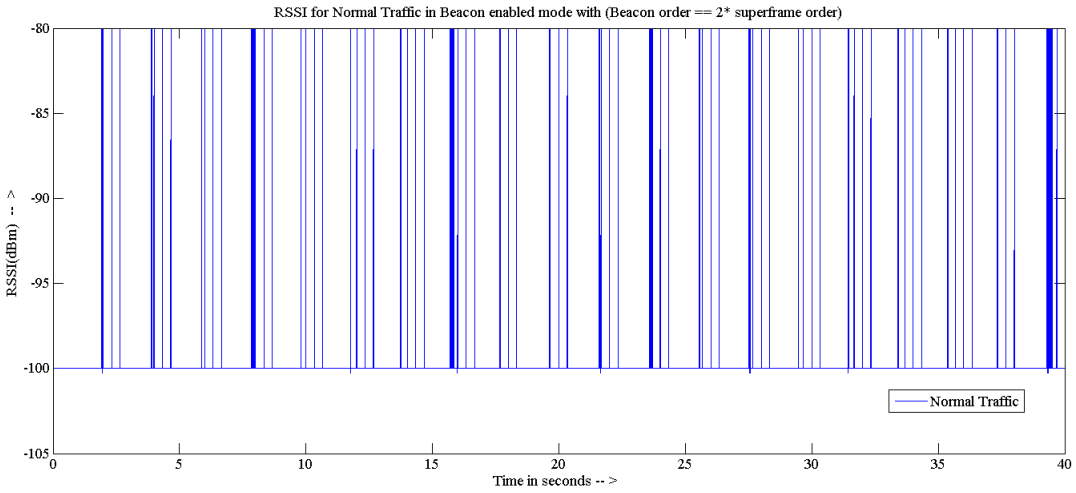

Figure 2.2: RSSI with out the presence of jammer

Table 2.1: Packets information at all nodes in normal communication with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Time with PAN
No Jammer	0	307	49 (beacons)	0	0.9951
	1	51 (beacons)	575(293+282)	0	-
	2	290	48 (beacons)	3	0.9961

2.6.2 Constant jammer

Figure 2.3 shows the received signal strength indicator (RSSI), taken near the node 1 of beacon enabled network with beacon order = 7, super frame order = 6. The simulation has carried out for a period of 100 seconds. Here jammer is activated after 10 seconds of the simulation. So for the first ten seconds of the simulation normal communication occurs, which can be seen in RSSI plot. Nodes 0 and 2 transmits 300 packets each to node 1. Table 2.2 gives packets transmissions and receptions related information at nodes 0,1,2.

We considered CCA mode of energy detection for our simulations. From RSSI plot in figure 2.3, we can see that channel has always signal after 10 seconds of simulation, which prevents transmissions(gives channel busy). Since nodes 0 and 2 are always sensing busy channel, packets will be dropped from queue(buffer overflown) and beacons are lost due to interference with whole beacon packet at both the nodes, which we can observe from table 2.2. From fraction of time associated with PAN column in table, we can see that nodes 0 and 2 are disassociated from the network.

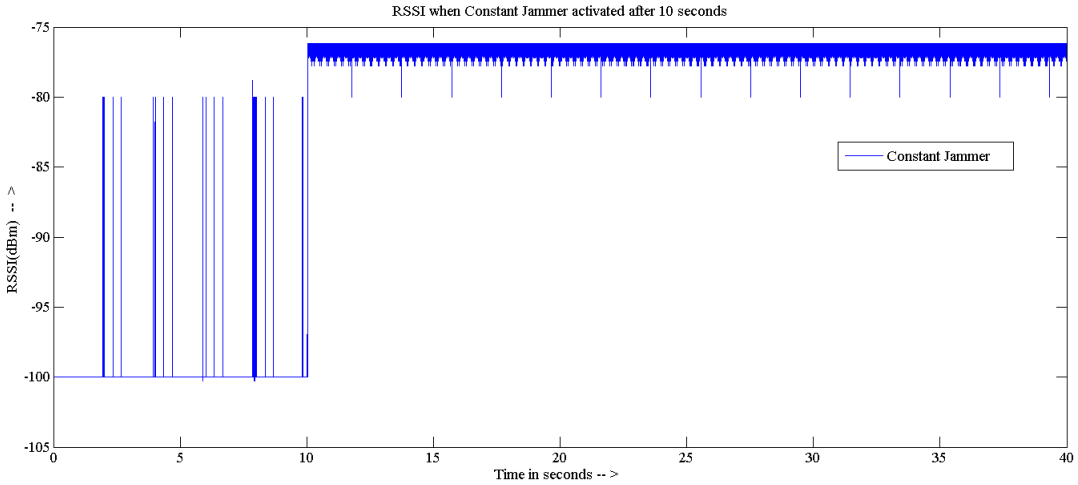

Figure 2.3: RSSI with constant jammer

Table 2.2: Packets information at all nodes in constant jamming scenario with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Time with PAN
Constant Jammer	0	23	4 (beacons)	244	0.1573
	1	51 (beacons)	51 (21+30)	0	-
	2	32	11 (beacons)	233	0.453

2.6.3 Deceptive jammer

Figure 2.4 shows the received signal strength indicator (RSSI), taken near the node 1 of beacon enabled network with beacon order = 7, super frame order = 6. The simulation has carried out for a period of 100 seconds. Here jammer is activated after 10 seconds of the simulation. So for the first ten seconds of the simulation normal communication occurs, which can be seen in RSSI plot. Nodes 0 and 2 transmits 300 packets each to node 1. Table 2.3 gives packets transmissions and receptions related information at nodes 0,1,2.

We considered CCA mode of energy detection for our simulations. From RSSI plot in figure 2.4, we can see that channel has always signal after 10 seconds which prevents transmissions(channel busy) irrespective of CCA mode. Since nodes 0 and 2 are always sensing busy channel, packets will be dropped from queue(buffer overflown) and beacons are lost due to interference with whole beacon packet at both the nodes, which we can observe from table 2.3. From fraction of time associated with PAN column in table, we can see that nodes 0 and 2 are disassociated from the network.

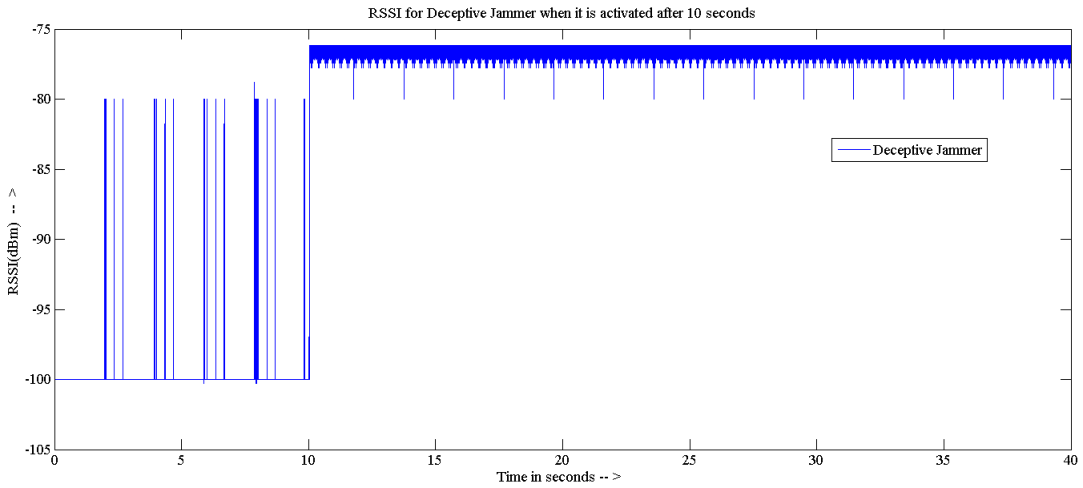

Figure 2.4: RSSI with deceptive jammer

Table 2.3: Packets information at all nodes in deceptive jamming scenario with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Time with PAN
Deceptive Jammer	0	23	4 (beacons)	244	0.1573
	1	51 (beacons)	51 (21+30)	0	-
	2	32	11 (beacons)	233	0.453

2.6.4 Random jammer

Figure 2.5 shows the received signal strength indicator (RSSI), taken near the node 1 of beacon enabled network with beacon order = 7, super frame order = 6. The simulation has carried out for a period of 100 seconds. Here jammer is activated after 10 seconds of the simulation. So for the first ten seconds of the simulation normal communication occurs, which can be seen in RSSI plot. Nodes 0 and 2 transmits 300 packets each to node 1. Table 2.4 gives packets transmissions and receptions related information at nodes 0,1,2.

we considered t_s = 100 milli seconds and t_j = 100 milli seconds for random jammer that means jammer will be jamming for 100 milli seconds and will be sleeping for remaining 100 milli seconds. We used constant jamming when the jammer is active and CCA mode of energy detection. So whenever jammer is active, beacons are lost due to interference. Data and command frames are not transmitted because of busy channel. Whenever jammer is sleeping, nodes will receive beacons and transmit packets(normal communication occurs). Based on table 2.4 we can see that only half of the packets

are lost and half of the packets are transmitted effectively. The same thing can be observed in RSSI plot, where signal strength is high and low periodically. During sleep periods, we can observe that some signal strengths are present, which represents normal communication.

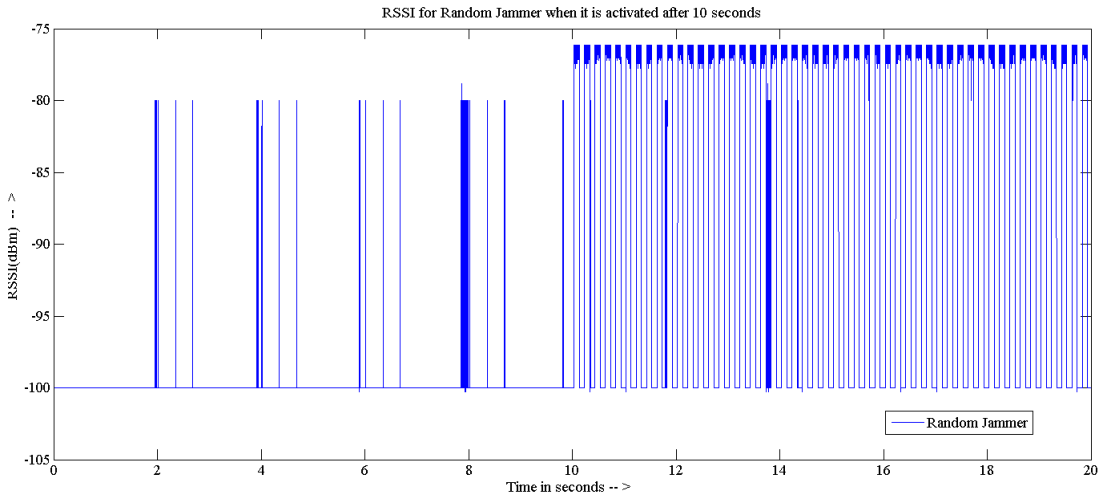

Figure 2.5: RSSI with random jammer

Table 2.4: Packets information at all nodes in random jamming scenario with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Time with PAN
Random Jammer	0	135	24 (beacons)	141	0.961
	1	51 (beacons)	252(119+133)	0	-
	2	149	31 (beacons)	135	0.961

2.6.5 Reactive jammer

Figure 2.6 shows the received signal strength indicator (RSSI), taken near the node 1 of beacon enabled network with beacon order = 7, super frame order = 6. The simulation has carried out for a period of 100 seconds. Here jammer is activated after 10 seconds of the simulation. So for the first ten seconds of the simulation normal communication occurs, which can be seen from RSSI plot. Nodes 0 and 2 transmits 300 packets each to node 1. Table 2.5 gives packets transmissions and receptions related information at nodes 0,1,2.

In reactive jamming scenario, where jammer transmits whenever there is activity,

one node will be completely orphaned which is near to the jammer (node 0), where as other node will receive beacons some times (node 2). The node which receives beacon perfectly, may sense the channel as idle but the PAN coordinator which is near to jammer is receiving packet in interference with the jamming signal transmitted by reactive jammer, hence PAN coordinator will not send any acknowledgement. So all the packets are lost because of no acknowledgement, as a result all packets are dropped with no acknowledgement status.

The RSSI plot at PAN coordinator is shown in figure 2.6, which shows that RSSI is similar to normal traffic but all transactions were failed. Because of the node far from malicious node which receives beacons from PAN coordinator sometimes without error will transmit packets with repeated retransmissions will be the cause of RSSI plot to look like this, otherwise if both nodes are in the attacking range of malicious node then 18 seconds after jammer has activated, no transmissions will occur (both devices lost synchronization) except beacon frames. We can see that node 0 has disassociated based on fraction of time associated with PAN.

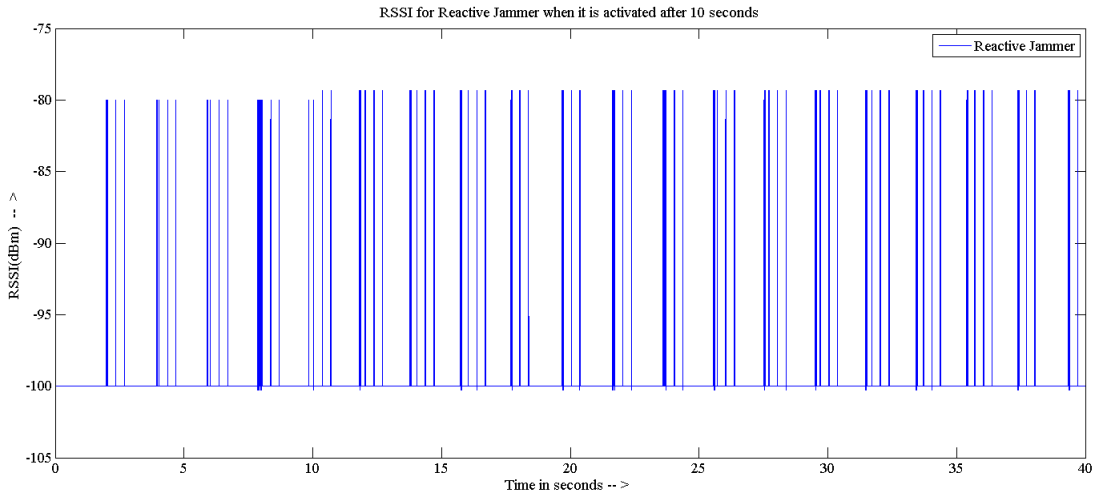

Figure 2.6: RSSI with reactive jammer

Table 2.5: Packets information at all nodes in reactive jamming scenario with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Time with PAN
Reactive Jammer	0	23	4 (beacons)	244	0.1573
	1	51 (beacons)	51 (21+30)	0	-
	2	833	47 (beacons)	267 (no ack)	0.961

2.7 Tampering

An attacker can also tamper with nodes physically, interrogate and compromise them threats that the large scale, ad hoc, ubiquitous nature of sensor networks exacerbates. Realistically, we cannot expect control access to hundreds of nodes spread over several kilometers. Such networks can fall prey to true brute force destruction, but also to more sophisticated analysis. An attacker can damage or replace sensor and computation hardware or extract sensitive material such as cryptographic keys to gain unrestricted access to higher levels of communication. Node destruction may be indistinguishable from fail silent behavior.

One defense involves tamper proofing the node's physical package. Second defense is that the node should react to tampering in a fail-complete manner. It could, for example, erase cryptographic or program memory. Other traditional physical defenses include camouflaging or hiding nodes.

2.8 Countermeasures Against Jamming

Spread spectrum communication is a common defense against physical layer jamming in wireless networks. Unfortunately, low power, low cost sensor nodes are usually limited to simple radios that cannot use these techniques. If WSN nodes can identify a jamming attack, a logical defense is to put sensors into a long-term sleep mode and have them wake periodically to test the channel for continued jamming. Although this won't prevent a DoS attack, it could significantly increase the life of sensor nodes by reducing power consumption. An attacker would then have to jam for a considerably longer period, possibly running out of power before the targeted nodes do.

Two kinds of strategies can be applied for coping with jamming. The first strategy involves avoiding the jammer in either the spectral or spatial sense, which can be achieved by changing channel allocations or, in mobile sensor networks, by moving nodes away from the jammer. The second strategy involves competing with the jammer by adjusting the transmission power levels and employing error correction in order to have more resilience against jamming. Development of energy effective spread spec-

trum communication will also help to make nodes to communicate even in the presence of jammer.

CHAPTER 3

Insider Attacks on Beacon Enabled IEEE 802.15.4 Networks (MAC layer attacks)

Most of the applications use beacon enabled network because of its sleep and active durations to save energy. This chapter explains various insider attacks on beacon enabled mode of operation along with the simulation results.

3.1 Insider Attacks on Beacon Enabled IEEE 802.15.4 Networks

For low latency applications or applications requiring specific data bandwidth, the PAN coordinator dedicates portions of the active super-frame to that application as shown in figure 1.2. These portions are called guaranteed time slots (GTSs). The GTSs form the contention free period (CFP), which always appears at the end of the active super-frame starting at a slot boundary immediately following the CAP. The PAN coordinator allocates up to seven of these GTSs, and a GTS is allowed to occupy more than one slot period. However, a sufficient portion of the CAP remains for contention based access of other networked devices or new devices wishing to join the network. There are two types of GTSs which can be requested by a device to PAN coordinator. They are transmit GTS which means device has to transmit data to PAN coordinator and accordingly device will be in transmit mode and PAN coordinator will be in receive mode. Second one is receive GTS which means PAN coordinator has to transmit data to device and accordingly PAN coordinator will be in transmit mode and device will be in receive mode.

PAN coordinator attempts to detect when a device has stopped using a GTS by using the following rules as defined by standard pro (2011) :

- For a transmit GTS, the PAN coordinator shall assume that a device is no longer using its GTS if a data frame is not received from the device in the GTS at least every $2 * n$ super-frames, where n is defined in equation 3.1.
- For receive GTSs, the PAN coordinator shall assume that a device is no longer using its GTS if an acknowledgement frame is not received from the device at least every $2 * n$ super-frames, where n is defined in equation 3.1. If the data frames sent in the GTS do not require acknowledgment frames, the PAN coordinator will not be able to detect whether a device is using its receive GTS. However, the PAN coordinator is capable of deallocating the GTS at any time.

The value of n is defined as follows:

$$n = 2^{(8-macBeaconOrder)} \text{ for } 0 \leq macBeaconOrder \leq 8 \tag{3.1}$$

$$n = 1 \text{ for } 9 \leq macBeaconOrder \leq 14$$

There are various vulnerabilities in the management of GTSs. Based on these vulnerabilities, we have considered various possible attacks.

3.1.1 Vulnerabilities of GTS management scheme

- No device checks whether any GTS has allocated for it with out requesting for GTS.
- Deallocation of unused GTSs by PAN coordinator after certain conditions are satisfied.
- No mechanism to track whether any device is continuously sending GTS requests.
- If a node sends data in every GTS, PAN coordinator will not deallocate it, though rate of traffic sent by the node is very less compared to the allocated GTS.

An insider attacker is one who have the access to network resources. Based on the vulnerabilities mentioned above, we can launch four different insider attacks on beacon enabled networks especially on the management of GTS.

Insider attacks discussed in this thesis are

- GTS jamming attack.
- False data injection attack.

- Denial of service against GTS requests.
- Stealing network bandwidth attack.

3.2 GTS Jamming Attack

In beacon enabled networks, PAN coordinator will send periodically beacons, which contains information about nodes having pending data at the PAN coordinator and GTS related information. In general, beacon frame is processed for GTS allocation or deallocation only when device has requested for it. But any compromised nodes can see what are the nodes having GTS, GTS length and starting slots which is kept in the beacon frame for at-most aGTSDescPersistenceTime and can be stored by the attacker. To conserve its energy, GTS jammer may sleep during CAP and wake up whenever GTS slot on which it wants to attack will start and attacker will simply jam the entire slot. One best thing is that attacker can jam the GTS with longer length. The IEEE 802.15.4 standard pro (2011) says that if PAN coordinator doesn't receive any valid data (satisfy FCS) for at-most $2 * n$ super-frames then it will deallocate GTS. where n is given in equation 3.1.

The advantage of this attack is that it cause the legitimate nodes to lose their contention free way of communication and making them to compete with other nodes to send large amount of data they have (in general nodes will request for GTS for sending large amounts of data without any CSMA/CA), thereby buffer will overflow because of lack of sufficient memory to store incoming data and channel availability to send it. The legitimate node may request again for GTS, we will repeat same process, which causes legitimate nodes to waste time and resources in sending many GTS requests. The above attack is described in paper Sokullu *et al.* (2008).

3.3 False Data Injection Attack

While a legitimate node is not in the GTS list, a malicious node can send a GTS allocation request and try to send data using the legitimate node's ID during GTS. Having

checked the node's IDs and sequence number, the PAN coordinator accepts the data sent by the malicious node that contain false information. For example if a legitimate node is transmitting current temperature data during the CAP, the malicious node sends a GTS allocation request with the spoofed ID, and pretends to be the legitimate node to inject false data during CFP. Based on the false data received, node may perform unusual action. This attack is described in paper JUNG (2011).

3.4 Denial of Service Against GTS Requests

The malicious node forges 7 different IDs (a single device pretends to be of 7 different devices has associated with seven different IDs) depending on the maximum number of available GTSs. This attack performs exhaustion and unfairness by occupying all 7 GTSs and not allowing legitimate nodes to reserve GTSs. This attack is described in paper JUNG (2011).

To perform this attack, a malicious node keeps monitoring the available GTS slots with the intent of completely occupying them. The malicious node simply jams the GTSs which are not belonging to it. Since PAN coordinator deallocate GTS, when it doesn't receive any valid data (satisfy FCS) for at-most $2 * n$ super-frames. where n is given in equation 3.1. Now many GTSs are available to occupy. Then, the attacker sends several GTS allocation requests to fill up all the available GTSs in the super frame. The advantage of this attack is that the malicious node can reduce its energy consumption by not sending any data during its GTS. The malicious node simply checks in beacon frame to see if the PAN coordinator is deallocating any of its GTSs. If any GTS is deallocated then malicious node will request GTS again.

The effect of this attack is that, it makes legitimate nodes not to use much of the active period duration. As a result, many packets will be overflown from the buffer due to less available active period. This attack makes GTSs to be not available to request. If any node is using GTS already, it is jamming that particular GTS.

3.5 Stealing Network Bandwidth Attack

The malicious node forges 7 different IDs (a single device pretends to be of 7 different devices has associated with seven different IDs) depending on the maximum number of available GTSs. This attacks perform exhaustion and unfairness attacks by occupying all 7 GTSs and not allowing legitimate nodes to reserve GTSs.

Similar to the denial of service against GTS requests, in this attack, an attacker observes the GTS list in order to eventually occupy the available GTS slots. The malicious node simply jams the GTSs which are not belonging to it. Since PAN coordinator deallocate GTS, when it doesn't receive any valid data (satisfy FCS) for at-most $2 * n$ super-frames. where n is given in equation 3.1. Now many GTSs are available to occupy. Then, the attacker sends several GTS allocation requests to fill up all the available GTSs in the super frame. However, in this attack, the malicious node sends data at the assigned time slots. The purpose of data transmission is to prevent the PAN coordinator from dropping the assigned GTSs. The time slots will never be vacant during the CFP of every super-frame, which can cause both exhaustion and unfairness against legitimate nodes. The effect of this attack is that, it makes legitimate nodes not to use much of the active period duration. As a result, many packets will be overflown from the buffer due to less available active period and no available GTSs to request. This attack is described in paper JUNG (2011).

3.6 Simulation Results

We choose Castalia framework of OMNeT++ which is popularly known for wireless sensor networks for conducting various GTS based attacks. We implemented IEEE 802.15.4 MAC protocol fully for conducting the attacks. We considered 5 legitimate nodes, 1 PAN coordinator (node 1), 4 associated nodes(nodes 0,2,3 and 4) which transmit data to different nodes on beacon enabled network using star routing protocol with beacon order = 8, super-frame order = 7. Arrangement of nodes is as shown in figure 3.1 for all simulations in this chapter.

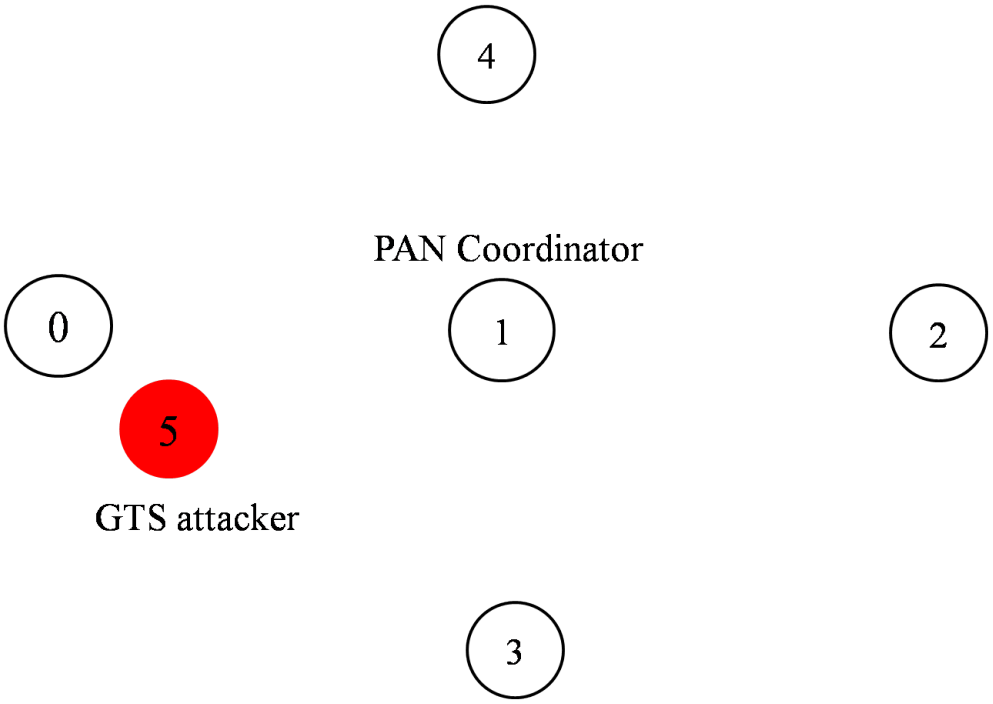

Figure 3.1: Network used for attacks based on GTS

3.6.1 Normal communication

We considered the network as shown in figure 3.1 with the following details to show the effect of different attacks for the nodes 0 to 4 except for the false data injection attack. Node 0 is transmitting to node 3 at a rate of 1 packet for every 250 milliseconds. Node 2 is transmitting to node 4 at a rate of 1 packet for every 1500 milliseconds. Node 3 is transmitting to node 1 at a rate of 1 packet for every 250 milliseconds. Node 4 is transmitting to node 1 at a rate of 1 packet for every 250 milliseconds.

Node 0 has transmit GTS of 2 slots. Node 3 has transmit GTS of 2 slots and receive GTS of 1 slot. Node 4 has transmit GTS of 3 slots. The number of packets that are successfully transmitted from different nodes during CAP and GTS are shown in table 3.1. In table 3.1, b indicates beacons, d indicates data and g indicates number of GTS requests sent by that particular node. Simulation has been carried out for a period of 600 seconds.

Table 3.1: Packets information at all nodes with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Txed in GTS	lost in GTS
No attacker	0	1577(d), 1(g)	152(b)	22	799	0
	1	153(b), 556(d)	2398(node 3), 2386(node 4)	9	2209	0
	2	394(d)	152(b)	6	0	0
	3	1854(d), 2(g)	2376(d, node 0), 152(b)	3	542	0
	4	1347(d), 1(g)	401(d, node 2), 152(b)	24	1032	0

3.6.2 GTS jamming attack

Simulation has been carried out for a period of 600 seconds. We considered the location of the attacker as shown in the figure 3.1. Nodes 0 to 4 are using network information as that of section 3.6.1. Malicious node considered the GTS with highest length to be jammed. Since node 4 has a GTS length of 3 slots which is the highest, malicious node jammed the GTS of node 4. We considered that whenever node loses GTS, it will again request and get GTS. So we can see that node 4 has transmitted 17 GTS requests from table 3.2. Many packets are lost due to no acknowledgement (1 packet is lost if consecutively 4 transmissions does not provide acknowledgement) in GTS. Since each packet has to be transmitted 4 times when there is no acknowledgement, packets will be accumulated in buffer and are dropped. Moreover since in GTS node 4 is not transmitting effectively, it will increase its transmissions in CAP. As a result, other nodes will decrease their transmissions in CAP and increase in GTS which can be observed from tables 3.1 and 3.2. When PAN coordinator deallocate GTS of node 4 then attacker jams the GTS of node 0 whose GTS is next highest. This we can observe from lost in GTS column of table 3.2. GTS jammer is effectively making nodes not to use their GTS.

In table 3.2, b indicates beacons, d indicates data and g indicates number of GTS requests sent by that particular node.

3.6.3 False data injection attack

Simulation has been carried out for a period of 600 seconds. Node 0 is transmitting to node 3 at a rate of 1 packet for every 1500 milliseconds. Node 2 is transmitting to node 1 at a rate of 1 packet for every 1500 milliseconds. Node 3 is transmitting to node 4 at

Table 3.2: Packets information at all nodes in GTS jamming scenario with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Txed in GTS	lost in GTS
GTS jamming	0	1422(d), 1(g)	152(b)	68	933	132
	1	153(b), 537(d)	2398(node 3), 2100(node 4)	3	2206	0
	2	395(d)	149(b)	5	0	0
	3	1638(d), 2(g)	2358(d, node 0), 152(b)	3	759	0
	4	2092(d), 17(g)	397(d, node 2), 152(b)	304	0	1045

a rate of 1 packet for every 250 milliseconds. Node 4 is transmitting to node 0 at a rate of 1 packet for every 250 milliseconds.

Node 0 has receive GTS of 2 slots. Node 3 has transmit GTS of 2 slots. Node 4 has transmit GTS of 2 slots and receive GTS of 2 slots. The number of packets that are successfully transmitted from different nodes during CAP and GTS are shown in table 3.3. In table 3.3, b indicates beacons, d indicates data and g indicates number of GTS requests sent by that particular node.

Here attacker will send GTS request using ID of the node which is not currently using GTS and sends false data to the PAN coordinator to take some unusual actions. In this particular simulation we have node 2 which is not using GTS. So malicious node sends GTS request with node 2 ID and subsequent data in GTS using the same ID. We send an abnormal temperature sensed value during GTS which gives danger indication to the receiver of this message though that is not the actual situation. The graphic visualization, we obtained from NAM is clearly showing the danger situation. From table 3.3 we can see that though node 2 is not using GTS, on its ID packets are received in GTS by the PAN coordinator.

Table 3.3: Packets information at all nodes in false data injection attack scenario with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Txed in GTS	lost in GTS
False data injection	0	394(d), 1(g)	2377(d, node 4), 152(b)	6	0	0
	1	153(b), 578(d)	(396, 147(in GTS))(node 2)	25	4564	12
	2	386(d)	149(b)	4	0	0
	3	1622(d), 1(g)	402(d, node 0), 152(b)	16	761	0
	4	1325(d), 2(g)	2371(d, node 3), 151(b)	19	1057	0

3.6.4 Denial of service against GTS requests

Simulation has been carried out for a period of 600 seconds. We considered the location of the attacker as shown in the figure 3.1. Node 5 is malicious node. Nodes 0 to 4 are using network information as that of section 3.6.1. Malicious node started its actions after 50 seconds. Malicious node has associated with 7 different IDs and try to capture all the vacant GTSs, with each GTS of 2 slots. Malicious node jams the entire duration of the GTS of other nodes and sleeps during its GTS. After sometime PAN coordinator will deallocate GTS due to no data coming from malicious node. Whenever any GTS has been deallocated, then malicious node again requests for GTS. If legitimate nodes are using GTS, malicious node jams all the GTSs which are not belonging to it, which causes legitimate nodes to lose their GTSs. We considered that whenever legitimate node loses GTS, it will again request to get its GTS back. So we can see that nodes have sent many GTS requests from table 3.4. Many packets are lost due to no acknowledgement (1 packet is lost if consecutively 4 transmissions does not provide acknowledgement) in GTS. Since each packet has to be transmitted 4 times when there is no acknowledgement, packets will be accumulated in buffer and are dropped. Number of packets lost in GTS can be seen in table 3.4.

Once legitimate node loses its GTS, then malicious node sends request to capture it. As a result most of the time malicious node only capturing GTSs(at max 7 GTSs can be allocated), so legitimate nodes may not acquire GTSs for much of time. Denial of service against GTS requests can effectively make nodes not to use their GTSs and captures GTSs which limit the CAP and in many situations legitimate nodes may not have GTS availability to request. As a result, incoming flow is high and outgoing flow is less resulting buffer overflow in legitimate nodes.

In table 3.4, b indicates beacons, d indicates data and g indicates number of GTS requests sent by that particular node.

Table 3.4: Packets situation at all nodes in denial of service against GTS requests scenario with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Txed in GTS	lost in GTS
DoS against GTS	0	1644(d), 3(g)	152(b)	754	55	351
	1	153(b), 844(d)	1196(node 3), 1716(node 4)	987	200	160
	2	392(d)	152(b)	6	0	0
	3	1160(d), 3(g)	853(d, node 0), 152(b)	1173	32	69
	4	1622(d), 3(g)	214(d, node 2), 152(b)	649	85	326
	5	32(g)	139(b)	0	0	0

3.6.5 Stealing network bandwidth attack

Simulation has been carried out for a period of 800 seconds. We considered the location of the attacker as shown in the figure 3.1. Node 5 is malicious node. Nodes 0 to 4 are using network information as that of section 3.6.1. Malicious node started its actions after 50 seconds. Malicious node has associated with 7 different IDs and try to capture all the vacant GTSs, with each GTS of 2 slots. Malicious node sends 2 packets during its every GTS for every super-frame. So PAN coordinator will not deallocate GTS of malicious node like in denial of service against GTS requests. Whenever any GTS has been deallocated, then malicious node again request to get its GTS back. If legitimate nodes are using GTS, malicious node jams all the GTSs which are not belonging to it, which causes legitimate nodes to lose their GTSs. We considered that whenever legitimate node loses GTS, it will again request to get its GTS back. Many packets are lost due to no acknowledgement (1 packet is lost if consecutively 4 transmissions does not provide acknowledgement) in GTS of legitimate nodes. We observed that after certain amount of time malicious node has acquired all the available GTSs. Now legitimate nodes does not have sufficient slots to transmit data (CAP is very small) and no GTSs are available to request. Packets will be accumulated in buffer and are dropped. Number of packets buffer overflown can be seen in table 3.5.

Once legitimate node loses its GTS, then malicious node sends request to capture it. As a result most of the time malicious node only capturing GTSs(at max 7 GTSs can be allocated). Stealing network bandwidth attack can effectively make nodes not to use their GTSs and captures GTSs which limit the CAP and once malicious node has acquired all GTSs, legitimate nodes will not have GTS availability to request. As a result, incoming flow is high and outgoing flow is less resulting buffer overflow in

legitimate nodes.

In table 3.5, b indicates beacons, d indicates data and g indicates number of GTS requests sent by that particular node.

Table 3.5: Packets situation at all nodes in stealing network bandwidth attack scenario with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Txed in GTS	lost in GTS
Stealing Bandwidth	0	1835(d), 1(g)	203(b)	1270	55	41
	1	204(b), 1147(d)	1228(3), 1949(4), 2241(5)	1018	200	160
	2	520(d)	203(b)	9	0	0
	3	1193(d), 3(g)	1094(d, node 0), 203(b)	1936	33	82
	4	1838(d), 4(g)	278(d, node 2), 203(b)	1205	91	1105
	5	20(g)	190(b)	0	2240	0

3.7 Countermeasures Against GTS based Attacks

To avoid nodes to get ride of the GTS jamming attack, randomizing the GTS allocation slots can help. To avoid false data injection attack, legitimate node's can check for the presence of GTS on its name irrespective of whether it has request for GTS allocation or not. Once its address has seen in beacon without requesting for GTS, then legitimate node should have the mechanism to inform the PAN coordinator about the false assignment of GTS. Accordingly PAN coordinator can deallocate GTS.

As a defense against denial of service against GTS requests, if the frequency of GTS requests is too high from one node, it may become suspicious that a malicious node is trying to hold the CAP by sending a number of GTS requests because all the commands can be sent during the CAP if there is no contention. In addition, the access control mechanism should keep track of the interval between GTS requests from the same node. If the interval of the same GTS request is too short, this could be an indication that a malicious node is interfering with a legitimate node sending GTS requests. Based on this PAN coordinator can take actions like not allocating GTS for the nodes which are requesting GTS very frequently and not using their GTS.

Keeping track of traffic from a particular node using GTS and amount of time GTS allocated for that particular node can make the PAN coordinator to take actions like,

deallocating GTS, if that node is not using GTS efficiently and having it for long time. Next stopping that node to get GTS again for a specified amount of time can be a defense against stealing network bandwidth.

CHAPTER 4

Outsider Attacks on Beacon Enabled IEEE 802.15.4 Networks (MAC layer attacks)

Most of the applications use beacon enabled network because of its sleep and active durations to save energy. In this chapter we considered some outsider attacks possible on beacon enabled mode of operation. Now a days ZigBee devices are coming with programmable pin which helps in association to be allowed only during the programmed duration. This makes insider attackers get reduced. So we are introducing new outsider attacks that can be possible on beacon enabled wireless sensor networks.

4.1 Outsider Attacks on Beacon Enabled IEEE 802.15.4 Networks

A typical wireless sensor node has less protection against radio jamming. The situation becomes worse if an energy efficient jamming can be achieved by exploiting knowledge of the data link layer. Encrypting the packets may help prevent the jammer from taking actions based on the content of the packets, but arrangement of the packets induced by the nature of the protocol can be exploited by the jammer even when the packets are encrypted.

We explained jamming attacks like constant jammer, deceptive jammer, random jammer and reactive jammer in chapter 2, which were proposed by W. Xu in paper Xu *et al.* (2006), which are energy inefficient, meaning they would exhaust their energy sooner than their victims would if given comparable energy budgets. Although random jammers save energy by sleeping, they are less effective. In Law *et al.* (2005),Yee Wei Law propose link layer jamming attacks by looking at the packet inter-arrival times in three representative MAC protocols, S-MAC, LMAC and B-MAC, derived several

jamming attacks that allow the jammer to jam S-MAC, L-MAC and B-MAC energy-efficiently. Based on the ideas given in paper Law *et al.* (2005), we have developed the following new attacks on beacon enabled IEEE 802.15.4 wireless sensor networks.

Our aim in this chapter is to produce jamming attacks that

- Work on encrypted packets.
- At-least as energy efficient as legitimate nodes.

We implemented such jamming attacks by exploiting the semantics of the data link layer and showed the results quantitatively in this chapter. Our analysis of the attacks provides new insights into the timing considerations of MAC protocols with regards to security and provides necessary steps to make the network robust against these kind of attacks. We assume that an attacker has two goals: the primary goal is to disrupt the communication and the secondary goal is to increase the energy wastage of the sensors compared to attacker.

Our attacks depend on the following two assumptions,

- The jammer node know the preamble used by the victim nodes.
- The jammer node can measure the length of a packet.

A preamble is a bit sequence, usually consisting of alternating 1's and 0's, for training the receiver, and its length depends on the data coding scheme. Knowing preamble is easy to satisfy in practice. To satisfy the second requirement jammer node should be compliant with IEEE 802.15.4 standard. So our assumptions are valid. Here jammer node does not need to know the content of the packets, so our attacks work even if the packets are encrypted. Adding to the significance of our attacks is that the attacker does not need to capture and compromise any existing sensor nodes.

In all the attacks discussed in this chapter, we programmed jammer node to receive all packets though they are not intended for this node, record packet length, starting time and inter-arrival time between packets. After this discard the packet. The beacon interval of IEEE 802.15.4 networks can vary from 15.36 milliseconds to 251.658 seconds. So our algorithm tries to find out the super-frame duration for every 12 seconds

and once beacon interval is tracked, tracking is stopped and tries to do the attacks discussed in sections 4.3, 4.4 and 4.5. Beacon interval is the duration from starting time of one beacon to the starting time of next beacon.

4.2 Algorithm to track beacon interval

This section explain the various steps in finding the beacon interval. Beacon interval is the interval with which PAN coordinator/coordinator is transmitting beacons. The beacon interval of IEEE 802.15.4 networks can vary from 15.36 milliseconds to 251.658 seconds at 250 kbps rate pro (2011).

4.2.1 Semantics of the protocol used to track beacon interval

Figure 1.2 shows the structure of super-frame. Where beacon, contention access period (CAP) and contention free period (CFP) all will happen in super-frame duration (active portion). According to the standard if inactive portion exists, then sleep duration will always be 2 multiple of active duration. IEEE 802.15.4 network is fully acknowledged network for reliability, except for beacon frame and orphan notification command. Acknowledgement packet is of fixed length of 11 bytes on physical layer without security support. Acknowledgement packet is transmitted after receiving data or command frame with in macAcknowledgementWaitDuration time in MAC layer. Figure 4.1 shows the communication scenario in normal communication setup.

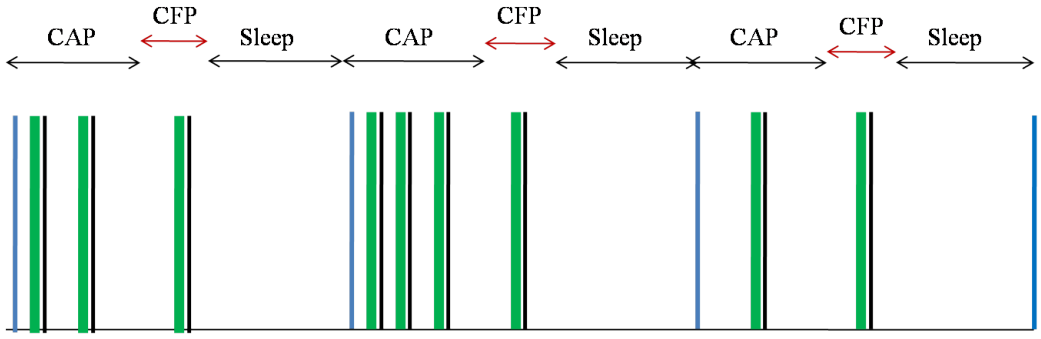

Figure 4.1: Communication in general communication scenario

In figure 4.1, blue colour indicates beacon, green colour indicates data or command

packet and black colour indicates acknowledgement. From figure 4.1, we can observe that all the packet transmissions except beacon are followed by acknowledgement.

IEEE 802.15.4 standard doesn't randomize the beacon interval and to make it vary, network layer or application layer has to send request to change the parameters, based on which guaranteed time slots have to be managed properly in the PAN coordinator as well as the device owning GTS dynamically. So we are considering this fact of unrandomized beacon interval to find out the beacon interval and do energy efficient attacks.

Our algorithm mainly depends on the following principles of the protocol:

- Beacon frame is not followed by any acknowledgement packet.
- With every data or command frame after beacon, acknowledgement will follow.
- If non zero inactive portion is there which is in reality, then inter-arrival time of beacon is always greater than or equal to sum of inter-arrival times after previously recorded packed with no acknowledged after it.

4.2.2 Algorithm

The following steps are used to track the beacon interval

- First, consider the packet with length 5 on MAC layer (acknowledgement packet), important for counting sum of inter-arrival times, let the packet be P_1.
- Track the first packet P_2 after P_1 which satisfy the following conditions assuming non zero inactive portion:
  - Following P_2, next packet should not be a packet with length 5 on MAC layer (acknowledgement packet) within macAcknowledgementWait duration.
  - Sum of inter-arrival times from P_1 till the packet before P_2 should be less than or equal to the inter-arrival time of packet P_2.
- Note down the starting time of P_2.
- After tracking P_2, track P_3 which satisfies the conditions satisfied by P_2. Note down the starting time of P_3.
- The time interval between starting time of P_2 and P_3 is the beacon interval.
- Track P_4 which satisfies the conditions satisfied by P_2 and P_3 and record starting time of P_4.

- Take the time difference between starting times of P_2 and P_3, P_3 and P_4, divide the time by 0.01536(considering 250 kbps rate) and round them to the nearest power of two, record them as R_1 and R_2. Compare the two after doing division and rounding. If these two are equal, then beacon interval will be the value R_1* 0.01536(considering 250 kbps rate). If these two are not equal, then repeat the process with new set of recorded information about the packets.
- Starting times of packets P_2, P_3 and P_4 are nothing but beacon packet transmission times.

4.3 Beacon Attacker

Here attacker will record the data packets related information such as starting time of packet, packet length and inter-arrival time between packets to find beacon interval and beacon transmission time by using the algorithm discussed in section 4.2.2. After tracking beacon timing it will find the next beacon transmission, jam the beacon and sleep till the next beacon. It repeats jamming beacon periodically. The malicious node track the beacon interval after certain amount of time to find any changes in beacon interval and beacon time.

The effects of this attacker are, whenever legitimate node doesn't receive beacon, it won't transmit data and data pending at the PAN coordinator will not be known. So no data transactions occur. After loss of 4 successive beacons, node send orphan command to get realignment command from the PAN coordinator. For orphan command no acknowledgement will be sent back. If no realignment command from the PAN coordinator in a specified time, then it will be disassociated from the PAN. If it receives realignment command, then it will start communicating for that particular super-frame. For the next super-frame since it will not receive beacon, the same process of loosing 4 successive beacons, sending orphan command and receiving realignment command and sending any data present at that node will repeat. It cannot receive any data from the PAN coordinator, because it is not tracking beacon to check any data pending for that node at the PAN coordinator. If it fails to realign due to any problem, then the device will get disassociated. This attack is highly energy efficient because malicious node has to be active only to jam the beacon packet and during beacon interval tracking. Remaining all time malicious node will be in low power mode (sleeping mode).

Beacon frame attacker is effectively making nodes closer to it to use only 1 of 5 super-frames if realignment is successfully happening every-time. If realignment is failed then beacon frame attacker is making legitimate nodes to disassociate from the PAN.

4.4 Active Period Jamming

In beacon attacker, nodes far away from malicious node compared to PAN coordinator may receive beacons perfectly and communicate, to avoid complete communication around the particular PAN coordinator, we can jam only the active period making legitimate nodes to receive beacons with out interference. Effectively malicious node and all legitimate nodes are consuming the same amount of energy (since radio of legitimate node is ON either for transmission or reception for the same amount of time), disrupting communication completely.

To do this malicious node first tracks the beacon interval and then find out the macSuperframeOrder which defines the duration of time nodes will be active. To find out macSuperframeOrder, we have employed the following algorithm to find out macSuperframeOrder considering P_2, P_3 and P_4 as the beacon packets:

- The value of (start time of P_2 - start time of P_3 - inter-arrival time of P_3) will give the time difference between start of beacon and the last packet in the super-frame, note this difference as R_1.
- Similarly find R_2 for P_3 and P_4.
- Divide R_1 and R_2 with 0.01536 and round them to nearest power of 2, let the readings be R_3 and R_4.
- Maximum of R_3 and R_4, multiplied by 0.01536, will be the active duration.

After finding active period (active duration), malicious node allows beacons to be received by all nodes. But it jam the whole active duration either by using constant/deceptive/reactive jamming mechanism and sleep during inactive period. The process repeats periodically.

The effects of this attack are that all the nodes dropped the packets due to busy channel or no acknowledgement after maximum number of retransmissions possible.

4.5 Starting New Personal Area Network

In this attack malicious node recorded all the packet related information like starting time, packet length and inter-arrival time between packets. Based on the algorithm discussed in section 4.2.2, it finds the starting time of the beacon frame and the beacon interval. After tracking beacon, malicious node simply jam the beacon and sleep till the next beacon time. The process repeats periodically till the first four beacon times after tracking. After this malicious node will jam whenever it receives packet of length 18 bytes on MAC layer(orphan command). So legitimate nodes doesn't receive realignment command correctly with in the specified time. Now the devices have disassociated. Malicious node will send beacon frame immediately after jamming normal beacon. Since nodes have disassociated, and are receiving beacons only from malicious node. They will get associated with malicious node treating it as legitimate node only. Here we can find active duration of legitimate PAN also and for the malicious node PAN, we can choose active duration at-least half as that of active duration of legitimate PAN.

Starting new personal area network attacker is effectively making nodes closer to it to be associated with it. All the packets from those nodes are transmitted to malicious node. Malicious node can perform any kind of action on the packets received. One simple activity is to acknowledge and discard the packets without forwarding to the destination. This attack is energy efficient because malicious node has to be active only to jam the beacon packet, during beacon interval tracking and during its active duration, which is at-least half of the active duration of legitimate nodes. Remaining all time malicious node will be in low power mode (sleeping mode).

4.6 Simulation Results

We choose Castalia framework of OMNeT++ which is popularly known for wireless sensor networks for conducting various outsider attacks discussed in sections 4.3, 4.4 and 4.5. We implemented IEEE 802.15.4 MAC protocol fully for conducting the attacks. We considered 5 legitimate nodes, 1 PAN coordinator (node 1) and 4 associated

nodes (nodes 0,2,3 and 4) which transmit data to different nodes on beacon enabled network using star routing protocol with beacon order = 8, super frame order = 7. Arrangement of nodes is as shown in figure 4.2.

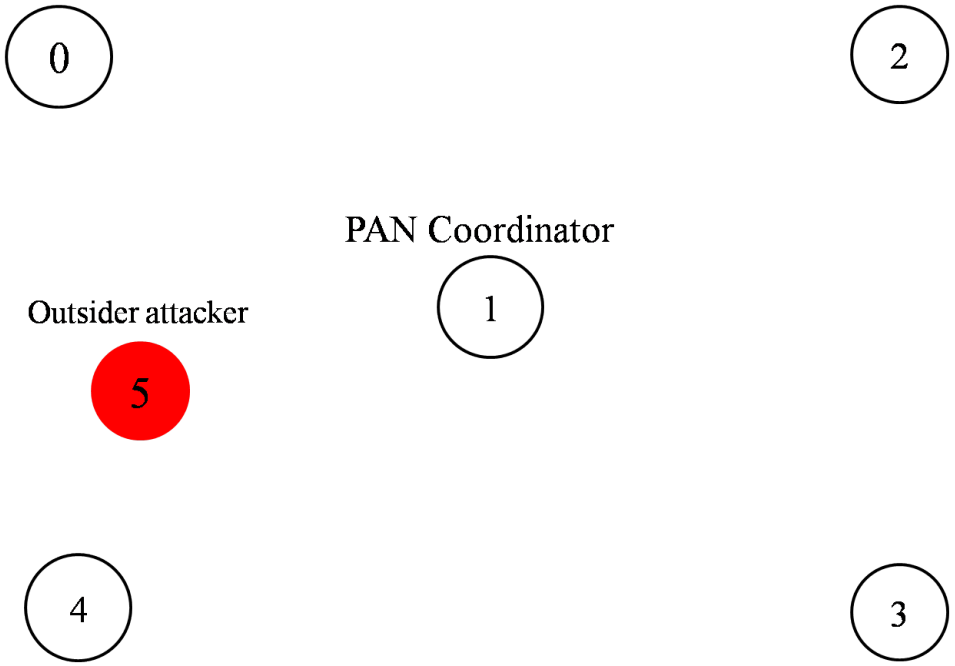

Figure 4.2: Network used for outsider attacks on beacon enabled 802.15.4 networks

4.6.1 Normal communication

We considered the network as shown in figure 4.2 with the following details for nodes 0 to 4 to show the effect of different attacks. Node 0 is transmitting to node 3 at a rate of 1 packet for every 1100 milliseconds. Node 2 is transmitting to node 4 at a rate of 1 packet for every 1500 milliseconds. Node 3 is transmitting to node 1 at a rate of 1 packet for every 1000 milliseconds. Node 4 is transmitting to node 1 at a rate of 1 packet for every 750 milliseconds.

The number of packets that are successfully transmitted from different nodes during CAP are shown in table 4.1. In table 4.1, b indicates beacons and d indicates data sent by that particular node. Simulation has been carried out for a period of 1200 seconds.

Table 4.1: Packets information at all nodes with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Time with PAN
No attacker	0	1088(d)	305(b)	3	0.99659736
	1	306(b), 1902(d)	1198(node 3), 1593(node 4)	3	-
	2	794(d)	305(b)	6	0.9967
	3	1197(d)	1100(d, node 0), 305(b)	5	0.9966
	4	1590(d)	802(d, node 2), 305(b)	10	0.99657682

4.6.2 Beacon attacker

Simulation has been carried out for a period of 1200 seconds. We considered the location of the attacker as shown in the figure 4.2. Node 5 is malicious node. Nodes 0 to 4 are using network information as that of section 4.6.1. Malicious node started its actions after 50 seconds. In this attack malicious node recorded all the packet related information like starting time, packet length and inter-arrival time between packets. Based on the algorithm discussed in section 4.2.2, we found the starting time of the beacon frame and the beacon interval. After tracking next beacon timing, malicious node simply jam the beacon and sleep till the next beacon time. The process repeats periodically.

From table 4.2, we can observe the following effects of the presence of the attacker as explained in section 4.3. Node 0 has lost all the beacons, once attacker starts jamming beacon. It is still associated for a duration of 338 seconds because of coordinator realignment response command from PAN coordinator. But for orphan command there are chances of getting lost due to two nodes sensing channel idle and sending at the same time. For orphaned device, since no acknowledgement comes back for orphan command, it will be disassociated after waiting time. From now since it is not able to receive any beacons it will be always disassociated from network. Packets are overflown from the buffer.

Same scenario occurred for node 4 at 88 seconds itself. From that point node is disassociated. Packets are overflown from the buffer.

Node 2 which is far from attacker compared to PAN coordinator, can receive beacons without any interference. We can see that node 2 has received all beacons successfully and communicating successfully form table 4.2.

Node 3 which is some what closer to the attacker compared to node 2 can receive beacons sometime and lose sometimes which can be observed from table 4.2. But whenever it receives beacon, it is transmitting all the data in the buffers.

Beacon frame attacker is effectively making nodes closer to it to use only 1 of 5 super-frames if realignment is successfully happening every-time. If realignment is failed then making nodes to disassociate from the PAN. In table 4.2, b indicates beacons and d indicates data sent by that particular node.

Table 4.2: Packets information at all nodes in beacon attacker scenario with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Time with PAN
Beacon attacker	0	299(d)	19(b)	780	0.2815
	1	306(b), 120(d)	1200(node 3), 103(node 4)	980	-
	2	800(d)	305(b)	0	0.9967
	3	1200(d)	71(d, node 0), 77(b)	0	0.9966
	4	103(d)	51(d, node 2), 19(b)	1463	0.07204

4.6.3 Active period jamming

Simulation has been carried out for a period of 1200 seconds. We considered the location of the attacker as shown in the figure 4.2. Node 5 is malicious node. Nodes 0 to 4 are using network information as that of section 4.6.1. Malicious node started its actions after 50 seconds. In this attack malicious node recorded all the packet related information like starting time, packet length and inter-arrival time between packets. Based on the algorithm discussed in section 4.2.2, we found the starting time of the beacon frame. By using algorithm discussed in section 4.4. we tracked active period(active duration). Malicious node allows beacon to be received by all nodes, jam the whole active duration either by using constant/deceptive/reactive jammers and sleep during inactive period. The process repeats periodically.

The effects of this attack is that all the nodes dropped the packets due to busy channel. We considered constant jamming for jamming active period. In table 4.3 we can see that packets are overflown, which are mainly because of busy channel after sensing maximum number of times allowed because we have used CCA mode of energy detec-

tion for our simulations. In table 4.3, b indicates beacons and d indicates data sent by that particular node.

Table 4.3: Packets information at all nodes in active period jamming scenario with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Time with PAN
Active period jam	0	75(d)	305(b)	847	0.99659736
	1	306(b), 123(d)	144(node 3), 153(node 4)	147	-
	2	121(d)	305(b)	613	0.9967
	3	123(d)	71(d, node 0), 305(b)	1639	0.9966
	4	108(d)	54(d, node 2), 305(b)	1393	0.99657682

4.6.4 Starting new personal area network

Simulation has been carried out for a period of 1200 seconds. We considered the location of the attacker as shown in the figure 4.2. Node 5 is malicious node. Nodes 0 to 4 are using network information as that of section 4.6.1. Malicious node started its actions after 50 seconds. In this attack malicious node recorded all the packet related information like starting time, packet length and inter-arrival time between packets. Based on the algorithm discussed in section 4.2.2, we found the starting time of the beacon frame and the beacon interval. After tracking beacon, malicious node simply jam the beacon and sleep till the next beacon time. The process repeats periodically till the first four beacon times after tracking. After this malicious node will jam whenever it receives packet of length 18 bytes on MAC layer(orphan command). So legitimate nodes doesn't receive realignment command correctly. Now the devices have disassociated. Malicious node will send beacon frame immediately after jamming normal beacon. Since nodes have disassociated, and are receiving beacons only from malicious node. They will get associated with malicious node treating it as legitimate node only.

From table 4.4, we can observe that node 0 has lost 5 beacons less than in case of normal communication, later it has associated with node 5 and received beacons from it. similarly node 4 also associated with malicious node. If node 3 has lost consecutive 4 beacons any time, since we are not allowing it to realign, node 3 also gets disassociated and will be associated later to malicious node. This has happened in our simulations

and node 3 has associated with malicious node. We can see in table 4.4 that they have transmitted data to malicious node.

Node 2 which is far from attacker compared to PAN coordinator, can receive without any interference. We can see that node 2 has received all beacons successfully and communicating successfully form table 4.4.

Starting new personal area network attacker is effectively making nodes closer to it to be associated with it. All the packets from those nodes are transmitted to malicious node which are not been forwarded by malicious node to the actual destination. We can observe all these in table 4.4. In table 4.4, b indicates beacons and d indicates data sent by that particular node.

Table 4.4: Packets information at all nodes in starting new personal area network scenario with node 1 as PAN coordinator

Case	Node	Txed	Rxed	Overflown	Time with PAN
New PAN	0	1083(d)	300(b)	5	0.99
	1	306(b), 120(d)	136(node 3), 119(node 4)	765	-
	2	800(d)	305(b)	0	0.9967
	3	1192(d)	71(d, node 0), 293(b)	6	0.99
	4	1592(d)	51(d, node 2), 300(b)	5	0.99
	5	282(b)	1013(d, 0), 1072(d, 3), 1489(d, 4)	0	-

4.7 Countermeasures Against Outsider Attacks

The sensor nodes should have mechanism to detect the kind of outsider attack happening. Then it should have ability to randomize the beacon interval and super-frame duration or it can hop to some other channel. If it hops, attacker may track the new channel and do the same attacks. So best countermeasure is randomizing beacon interval and super-frame duration.

CHAPTER 5

Conclusion

We have developed codes for open source simulator Castalia in OMNeT++, which can be used as a test bench for providing robust protocols against various attacks. We mainly discussed various attacks possible on physical and MAC layer of ZigBee nodes. We discussed various jamming attacks and their effects on the normal communication which gives an indication that the development of sensor nodes has to consider anti jamming techniques.

We discussed various insider attacks on beacon enabled IEEE 802.15.4 networks, especially on the management of GTS scheme and the effect of the attacks are discussed. The results shows that modifications are needed in the maintenance of GTS.

We discussed various new energy efficient outsider attacks on beacon enabled IEEE 802.15.4 networks, especially on the periodic structure of beacon transmissions and the effect of the attacks are discussed. The results shows that modifications are needed in structure of beacon transmissions.

Our work mainly emphasis on the fact that many vulnerabilities are present in the development of IEEE 802.15.4 based networks, which is limiting its usage in many applications. This thesis emphasis on the consideration of the security in the development of the protocols for sensor nodes.

5.1 Future Work

- Studying of various attacks that exploit the vulnerabilities of the routing protocol of ZigBee devices.
- Development of codes for the routing protocol of ZigBee in Castalia framework.
- Simulations and providing test bench for the possible attacks on the routing layer of ZigBee devices.

- Reviewing general defense mechanisms against the attacks discussed and to develop new protocols considering energy conservation and security, to get ride of the attacks discussed. Testing of the robustness of the protocol with the simulator already developed.

REFERENCES

1. (2011). Ieee standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (lr-wpans). *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, 1–314.

2. **Boulis, A.** (2009). Castalia. URL http://castalia.npc.nicta.com.au/documentation.php.

3. **JUNG, S. S.** (2011). Attacking and securing beacon-enabled 802.15. 4 networks.

4. **Karlof, C.** and **D. Wagner**, Secure routing in wireless sensor networks: attacks and countermeasures. *In Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*. 2003.

5. **Law, Y. W.**, **L. van Hoesel**, **J. Doumen**, **P. Hartel**, and **P. Havinga**, Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols. *In WIRELESS SENSOR NETWORK MAC PROTOCOLS SANS'05*. 2005. ISBN 1-59593-227-5.

6. **Melgares, R. A.** (2011). 802.15.4/ZigBee Analysis and Security: tools for practical exploration of the attack surface. Technical Report TR2011-689, Dartmouth College, Computer Science, Hanover, NH. URL http://www.cs.dartmouth.edu/reports/TR2011-689.pdf.

7. **Sokullu, R.**, **O. Dagdeviren**, and **I. Korkmaz**, On the ieee 802.15.4 mac layer attacks: Gts attack. *In Sensor Technologies and Applications, 2008. SENSORCOMM '08. Second International Conference on*. 2008.

8. **Sokullu, R.**, **I. Korkmaz**, **O. Dagdeviren**, **A. Mitseva**, and **N. R. Prasad**, An investigation on ieee 802.15. 4 mac layer attacks. *In Proc. of WPMC*. 2007.

9. **Varga, A.** (2011). Omnet++ user manual version 4.2.2. *OpenSim Ltd. Last accessed*, **6**, 2012. URL http://www.omnetpp.org/doc/omnetpp/manual/usman.html.

10. **Wood, A.** and **J. Stankovic** (2002). Denial of service in sensor networks. *Computer*, **35**(10), 54–62. ISSN 0018-9162.

11. **Wood, A. D.**, **J. A. Stankovic**, and **G. Zhou**, Deejam: Defeating energy-efficient jamming in ieee 802.15. 4-based wireless networks. *In Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on*. IEEE, 2007.

12. **Xu, W.**, **K. Ma**, **W. Trappe**, and **Y. Zhang** (2006). Jamming sensor networks: attack and defense strategies. *Network, IEEE*, **20**(3), 41–47. ISSN 0890-8044.