DETECTING DENIAL OF SERVICE ATTACK IN WIRELESS SENSOR NETWORKS

A Thesis Presented to the Department of

Computer Science,

African University of Science and Technology, Abuja.

In Partial Fulfillment of the Requirements

For The Degree of

MASTER OF SCIENCE

By
Adebajo Fisayomi Yetunde

Abuja, Nigeria.

December, 2014.

DETECTING DENIAL OF SERVICE ATTACK IN WIRELESS SENSOR NETWORKS

By
Adebajo Fisayomi Yetunde

A THESIS APPROVED BY THE COMPUTER SCIENCE DEPARTMENT

RECOMMENDED: ……..
Supervisor, Professor Ousmane THIARE

……..
Dr Dame DIONGUE

……..
Head, Department of Computer Science

APPROVED: ……..
Chief Academic Officer

……..
Date

ABSTRACT

Wireless sensor networks, thanks to recent technological advances, has become prevalent and offer a variety of applications ranging from environmental monitoring to support and automate chores fields. However, this very promising technology faces many inherent constraints (sensor node architecture, runtime, etc...). All these, because the network face many challenges such as energy efficiency, routing, self-organization and self-maintenance, data aggregation, security, mobility, etc. A wireless sensor network is a special case of ad hoc networks and therefore inherits certain characteristics of ad hoc networks. Due to the nature of the wireless environment, the sensor nodes face many security challenges. Intruders may enter the network and cause disruption of its normal operation. Nodes usually perform energy-saving mechanisms that allow them to switch to standby (sleep) mode from time to time. However, an evil intentioned node can join the network and thus prohibit nodes wishing enter standby mode from turning off their radio. This can be termed as sleep deprivation torture also known as Denial of sleep attacks. It is achieved by making them believe that there is data to be transmitted or just has to stay awake for monitoring. Much overhead is introduced in most of the existing works on sleep deprivation attacks detection, leading to poor performance. The need of the day is to therefore develop energy efficient methods by which the attack can be mitigated. In this work, a strong link-layer authentication and Anti-replay protection is proposed for TMAC protocol to mitigate Denial of sleep attacks. Simulation results show that our proposed mechanism is able to reduce the effects of Denial of sleep attacks in Wireless Sensor Networks.

ACKNOWLEDGMENT

I give a big thanks to my distinguished Supervisors, Professor Ousmane THIARE and Dr. Dame DIONGUE for their support, encouragement and unfailing attention during the course of writing this thesis. You are both wonderful people.

I am grateful to my Head of Department, Professor Mamadou Kaba TRAORE for his advice and encouragement all though my stay in A.U.S.T.

I appreciate my caring and loving parents and also my siblings for their love, care, financial and spiritual support. May you reap the fruit of your labour. (Amen)

I also appreciate my wonderful and loving friend, Ojuri Folorunso for his constant support and encouragement and all my colleagues especially, Adekunle Oluwaseun for their care and support.

Finally, I say thank you to all PHD students and AUST staff for making my stay a memorable one.

DEDICATION

This thesis is dedicated to Almighty God, the Author and the finisher of my faith, who through his infinite love and mercy has seen me through the course of obtaining my M.Sc. and through my stay in African University of Science and Technology, and to my distinguished Parents, for their love and innumerable support.

TABLE OF CONTENTS

TABLE OF FIGURES

CHAPTER 1

1.0 INTRODUCTION

1.1 Background

Wireless Sensor Network (WSN), is composed of several spatially distributed nodes, and connected to one or more sensors, which monitor a large physical environment. The nodes (wireless devices) are typically small in size and capable of performing sensing, on-board processing, communication and storage. WSNs [1] offer economically viable solutions for a variety of applications such as current implementations to monitor factory instrumentation, pollution levels, freeway traffic, and the structural integrity of buildings. Other applications include climate sensing and control in office buildings, and home environmental sensing systems for temperature, light, moisture, and motion. The Development of wireless sensor networks resulted mainly from the military applications [2] such as battlefield surveillance. In 1978, the Defense Advanced Research Projects Agency (DARPA) organized the Distributed Sensor Nets Workshop, focusing on sensor network research challenges such as networking technologies, signal processing techniques, and distributed algorithms. DARPA also operated the Distributed Sensor Networks (DSN) program in the early 1980s, which was then followed by the Sensor Information Technology (SensIT) program. Currently, WSN is viewed as one of the most important technologies for the 21st century (21 Ideas for the 21st Century, 1999). WSN is becoming a more commonplace and can be found in research projects and civilian applications as well as defense projects. The sensor nodes are often deployed to remote and inaccessible areas and thereby increase their exposure to malicious intrusions and attacks. WSN is therefore faced with several security challenges when deployed to remote areas. One of the most challenging security threats is a *Denial of Service Attack (DoS)* which is the result of any action that prevents any part of a WSN from functioning correctly or in a timely manner [3]. It can be viewed as a malicious attempt to make network resource unavailable to legitimate users, thus is considered one of the most general and dangerous attacks endangering network security.

Types of DoS attacks [4] include Jamming attack, Exhaustion attacks, Selective Forwarding attacks, Flooding, Denial of Sleep, and Sinkhole among others which will be discussed later. It is important to develop ways of preventing/detecting these attacks from occurring to get maximum functionality of the Network. A specific type of DoS is the Denial of sleep attack which comes in the form of sending useless control traffic and forces the nodes to forgo their sleep cycles so that they are completely exhausted and hence stop working [5]. This work reviews several ways of detecting the denial of sleep attacks and determines an efficient way to mitigate the attacks.

1.1.1 Wireless Sensor Network: An Overview

Sensing is simply an art used for obtaining information about a physical object or process such as changes in temperature or pressure. Any object that is able to perform such task is referred to as a *Sensor.* When many sensors co-operatively monitor large physical environments, they form a Wireless Sensor Network[2] . The sensor nodes communicate with centralized control called base stations also known as the sink nodes. A base station normally allows dissemination of information to another network, a powerful data processing or storage center, or an access point for human interface. Communication with the base station could either be *single-hop*, where the nodes transmit data directly to the base station or *multi-hop*, where some nodes serve as relays for other sensor nodes, that is, they collaborate to propagate sensor data towards the base station. There could be variation in the processing and communication capabilities of the sensor nodes in WSN. Some could be Simple nodes while others categorized as complex nodes depending on their configurations. The two important operations of a WSN are data dissemination (send data/queries from sinks to sensor nodes) and data gathering (send sensed data from sensor nodes to the sinks) [6]. The architecture of the network could either be "*flat*", where each node plays the same sensing task and there is no global identifier in a sensor network or "*hierarchical*", where sensor nodes are divided into the clusters, where cluster members send their data to cluster head and which further send the data to the sink node. The IEEE 802.11 family of standards, which was introduced in 1997, is the most common wireless networking technology for mobile systems. However, the high-energy overheads of IEEE 802.11-based networks make this standard unsuitable for low-power sensor networks.

This has led to the development of a variety of protocols that better satisfy the networks' need for low power consumption and low data rates. These sensor nodes however possess some major characteristics described below.

1.1.1.1 Characteristics of Wireless Sensor Nodes

- Limited Resource: Power consumption is highly constrained as nodes depend on batteries or energy captured from the environment. Memory and processing capacity of the nodes is also limited due to the small sizes of the nodes. Energy is a very crucial resource for sensor networks. Therefore, developing energy saving techniques has a great impact in the network architecture.

- Large Scale of Deployment: A sensor network may consist of thousands of heterogeneous nodes with one or more centralized control called Base Stations. The network structure, and resource used are often ad hoc (without planning).

- Specific Application: A sensor nodes is usually designed to serve a specific application. The nature of the sensor's application may affect the cost and physical size of the sensor nodes.

- Harsh Environments condition: Sensor networks often operate in environments with harsh conditions and should possess the ability to withstand these conditions.

- Node Failure Recovery: Due to the fact that the nodes are usually deployed in remote and hostile environments, there is usually little or no human intervention. The network topology should therefore have the ability to tolerate the failure of nodes and activate self-configuring schemes to avoid network partition

- Self-Management: When deployed in remote/harsh environments, the nodes should be able to configure themselves, adapt to failures without human intervention. In these energy-constrained devices, the self-management features must be designed and implemented such that little overheads are incurred.

1.1.1.2 Requirements for WSNs

- Fault Tolerance: Despite the fact that the sensor nodes are prone to errors as a result of node failure due to harsh environment, there should be consistency in the network functionality.

- Lifetime: The nodes are dependent on either batteries or energy scavenged from the environment for power supply. The nodes should therefore be able to function maximally before completely exhausting the batteries. Thus, energy saving and load balancing must be taken into account in the design and implementation of WSN platform, protocols and application.

- Scalability: The protocols defined in the network should be able to adapt to high densities and numerous number of nodes.

- Real-time: Strict- timing constraints for sensing, processing and communication are necessary since the network is tightly related to the real world.

- Production cost: Since large number of nodes is being deployed, the cost of production should be low.

- Security: The need for security in WSNs is evident due to the nature of the nodes. The remote and unattended operation of sensor nodes increases their exposure to malicious intrusions and attacks. Some attacks are mainly targeted at the power of the nodes to prevent successful sensor communications. The main focus of this thesis is to provide security mechanisms for the nodes in the network.

1.2 PROBLEM STATEMENT

Due to the power limitation of the sensor nodes, they are scheduled periodically to go into sleep mode, but attackers /intruders prevent the nodes from transiting to sleep mode.

This is usually done by sending unnecessary fake packets, making their radio turned on (trying to process the fake packets) thereby completely exhausting the power supply and reducing their lifetime from years/months to days. With this, the overall network performance is reduced.

1.3 MOTIVATION

Ideally, the sensor nodes should be able to capture, analyze and process data in a timely fashion. This is because the network is usually applied in real life situations that require optimum and efficient results such that the nodes are not expected to in any way lose their functionality. However when some attackers successfully intrude the network and completely drain the power of the nodes, the consequence could be extremely costly as it could result in casualties. Denial of service attack makes it impossible for the network to function as expected. It is more disastrous when the power of the nodes is targeted since they are highly dependent on batteries. This reduces the overall performance of the network. Several techniques can be developed and implemented to identify and mitigate these attacks. Our main focus is to detect attacks targeted at the Link Layer.

1.4 RESEARCH OBJECTIVES

This project aims at achieving the following:

- Review of various technical intrusion detection in wireless sensor networks.
- Determine the procedures of denial of service attack (standby).
- Implement a method for detecting and isolating intruders from the network

1.5 RESEARCH METHODOLOGY

In order to achieve the aforementioned objectives, the following approaches were adopted:

- We surveyed the different types of Denial of Service attacks and ways by which the attacks can be initiated.
- Since denial of sleep attacks occur at the Data link/MAC Layer, we reviewed the various MAC protocols for WSN and Denial-of-sleep vulnerabilities on the state-of-the-art WSN MAC protocols were analyzed.
- Then, different techniques to mitigate Denial of Sleep attacks was investigated and analyzed and the limitation(s) of each was discussed

- Finally, an efficient algorithm was proposed and implemented using simulation frameworks such as Castalia, OMNeT++ to provide experimental analysis on the behavior of the algorithm.

1.6 ORGANIZATION OF THE DOCUMENT

This work is organized as follows:

Chapter 2 introduces the various Denial of Service attacks in Wireless Sensor Network, WSN MAC protocols and Related Works in Detecting Denial of Sleep attacks in WSN. Chapter 3 presents the analysis of related works and presents the algorithm to detect denial of sleep attacks. Chapter 4 discusses the implementation of the proposed algorithm and evaluation of results. Chapter 5 provides the conclusion and future work.

CHAPTER 2

2.0 STATE OF ART

Wireless Sensor Network is widely applied in different areas, thus, making the network available for its intended use is essential. One of the main features to consider in Wireless Sensor Network [7] is the rate of energy consumption, so many efforts are focused on power saving techniques. The broadcast nature of the transmission medium and their intrinsic characteristics make Wireless networks more vulnerable to external intrusion than wired networks [7][8]. There could be a great damage in the health and safety of the people due to attacks against the network. There is therefore a need to establish proper security mechanisms in controlling how the Wireless network works [3]. The detail about Denial of service attacks is discussed in this chapter. We first describe some of the energy saving protocols used in WSN.

2.1 MEDIUM ACCESS CONTROL PROTOCOLS FOR WIRELESS SENSOR NETWORK

Due to the power-constrained nature of the sensor nodes, maximizing the lifetime of the nodes is very essential. Most research is focused on the design of low power electronic devices to minimize the energy consumption of the Sensor nodes. It is often difficult/not feasible to replace or recharge the batteries used for Sensor nodes while on board. Energy efficient MAC protocols should therefore be designed in other to prolong the network lifetime of the sensor nodes. Several MAC protocols have been designed to increase the lifetime of the sensor nodes. One fundamental task of the MAC protocol is to avoid collisions from interfering nodes. These protocols can either be contention based, or Time division multiple access (TDMA) based [6]. This work reviews some of the existing MAC protocols. Frame delimiting and recognition, addressing, transfer of data from upper layers, error protection (generally using frame check sequences), and arbitration of access to one channel shared by all nodes are the main functions of the MAC layer. The major characteristics of an efficient MAC protocol are energy efficiency as well as scalability and adaptability to changes in network size, node density and topology.

It is highly important to understand the normal and malicious sources of energy loss in other to design a secure MAC layer protocol. The amount of power saved by the protocols depends largely on the ability to overcome the radios major sources of energy loss, which includes:

- Collisions: Energy is wasted when several packets collide in communication medium. Data can be corrupted at the receiving end if a transmission of sufficient signal strength interferes with a data packet being sent. Error-correcting codes (ECCs) can be used to recover corrupted data but this introduces transmission overhead, which even results in increase in energy consumption.
- Control Packet Overhead: Several control packets such as RTS (Request to send) and CTS (Clear to send) packets which are used in most MAC protocols may have to be received by all nodes within radio range of the sender, which largely drains the power of nodes in the network.
- Overhearing: Energy loss is achieved when the radio of a node is in receive mode when a packet is being transmitted to another node. The way to avoid this is simply to ensure that a node is only awake when there is traffic destined for it. This is done by ignoring packets destined for other nodes after hearing an RTS/CTS exchange.
- Idle Listening: Energy consumption of nodes while receiving data is equivalent to energy consumption while just monitoring the channel. Power is wasted when a node is set to listen when there is no packet destined for it.

2.1.1 Contention-based Protocols

In these protocols, [9] the nodes try to gain access of the wireless medium but only one node (the winner) is granted access to the channel and allowed to transmit. Examples of contention based protocols are ALOHA and CSMA (Carrier Sense Multiple Access). CSMA protocols can easily accommodate newly added nodes (adaptive), do not require strict synchronization among nodes, and can support a large number of sensor nodes (scalable). In CSMA, a node senses the channel to know if the channel is busy or clear before transmitting.

The transmission is postponed if the channel is found to be busy but starts transmission if the channel is clear. CSMA/CA (CSMA/Collisions Avoidance) is a technique used by MAC protocols to reduce collisions in Wireless Sensor Networks. RTS (Request To Send) and CTS (Clear To Send) mini packets are exchanged prior to data transmission. The transmitter initially sends a RTS packet to the receiver. The receiver, after receiving the RTS packets replies by sending a CTS packet.

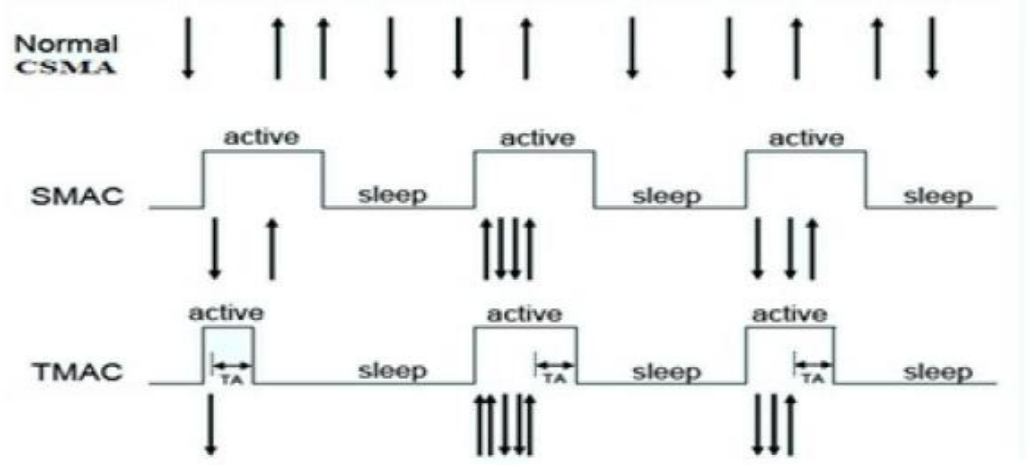
Some CSMA/CA MAC protocols are introduced in this section. Contention Based protocol allows access to the medium is in a distributed manner [10] thus, central coordination is not needed to access the medium.

- S-MAC: Sensor MAC [11] uses a periodic sleep-listen schedule for optimization. It regulates sleep periods to conserve energy and increase lifetime of the nodes [12]. Radios in networks using this protocol uses fixed duty cycle, with a default of 10% and will be asleep 90% of the time [13] thereby producing an almost tenfold improvement in node life. In SMAC, active periods are divided into two sub periods: one for exchanging SYNC packets and the other one for exchanging data packets [9]. A node upon joining the network broadcasts its schedule in a SYNC packet (which contains the sender's address and senders sleep time) if it does not hear a schedule from another node after listening for some time. The SYNC packets are periodically sent to immediate neighbors and each node maintains a schedule table that stores the schedules of all its known neighbors [14]. If a node receives SYNC packet before choosing a schedule, it subtracts the packet transmission time and use the new value to adjust its timer and if a node receives a different schedule after broadcasting its own, it adopts both schedules [11]. The period for a node to send a SYNC packet is called the synchronization period. RTS (Request to send) packets followed by CTS packets (Clear to send) are sent before the, DATA is transferred. This is the handshaking technique used in S-MAC. In S-MAC, long messages are divided into frames and sent in a burst (message-passing), which reduces communication overhead. Periodic sleep may result in high latency (sleep delay) [13] especially for multi-hop routing algorithms, since all immediate nodes have their own sleep schedules.

The constant Sleep and listen periods, decreases the efficiency of the algorithm under variable traffic load. Adaptive listening technique is proposed to improve the sleep delay, and thus the overall latency.

- T-MAC: T-MAC (Timeout MAC) is a contention based mac protocol that improves S-MAC by using dynamic sleep schedule for power conservation. The arrows in the Fig. 1 indicate transmitted and received messages. T-MAC uses the same SYNC mechanism to form virtual clusters as S-MAC. Unlike S-MAC, which uses a fixed sleep period, an adaptive timeout (TA) mechanism is used in T-MAC to transit the nodes to sleep mode when there is no traffic in the cluster. The TA [12], is however based on the longest time that a hidden node would have to wait before hearing the beginning of a CTS response message. TA = 1.5 × (C + R + T) where C is the length of the contention interval, R is the time to send an RTS packet, and T is the time between the end of an RTS packet and the beginning of a CTS packet. TMAC also introduces a FRTS (Future request to send) mechanism and full buffer priority, to avoid early sleeping problem for converging type of data communication.

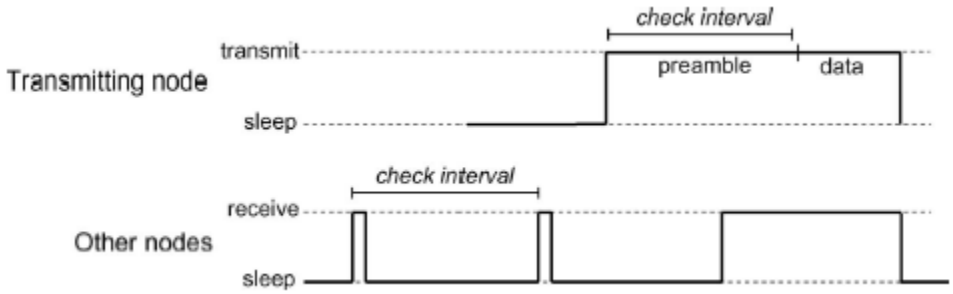
Figure 2.1 SMAC & TMAC



- B-MAC: Berkeley MAC [13] uses low-power listening (LPL) to reduce energy consumption. This means that the nodes poll the wireless channel at a set check interval and spend the rest of the time in low-power sleep mode.

The nodes are briefly awake at a fixed interval and the wireless channel is checked for valid preamble bytes that indicate a pending data transmission from another node. A preamble that is longer than the interval between receiver samplings is transmitted by a node with data to send to ensure that all nearby nodes have the opportunity to detect the preamble and receive the subsequent data packet. Clear channel assessment (CCA) technique is used by BMAC to decide if a packet is arriving when node wakes up[5]. The sensor node can change any operating variables in the protocol, such as back off values. This provides a flexibility interface. CCA and packet bakeoffs are used by BMAC for channel arbitration and link layer acknowledgments for reliability. There is no synchronization, RTS, CTS in BMAC [15]. B-MAC could have duty cycles as low as 1% in a low-traffic network [16].

Figure 2.2 BMAC

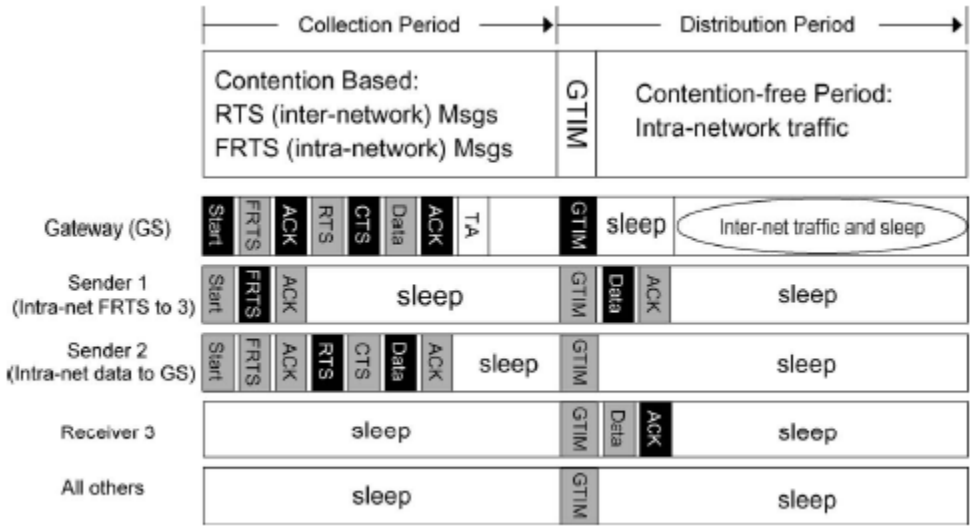


2.1.2 TDMA Based Protocols

This class of protocols is based on reservation and scheduling. TDMA protocols are collision free and perform best in single-hop networks. Although energy conservation is highly achieved in TDMA based protocols compared to contention based protocols, TDMA protocol usually requires the nodes to form real communication clusters, like Bluetooth, and LEACH [11]. Communication is restricted between nodes in a cluster, which increases interference. TDMA cannot easily adapt to changes such as increasing number of nodes. This makes contention-based protocols better in terms of scalability.

- G-MAC: This protocol is a clustered protocol that combines a contention-based slot reservation period with a time-division multiple-access (TDMA) period for data dissemination. Gateway MAC protocol is divided into a collection period and a contention-free distribution period. A future RTS (FRTS) message is transmitted by nodes with outgoing traffic to a gateway node during the collection period. The gateway is elected [13] using a periodic resource-adaptive election process in which nodes volunteer based on current resource levels. Traffic destined for other clusters is also transmitted to the gateway node during the contention period using an RTS/CTS/DATA/ACK exchange. The gateway node then transmits a gateway traffic indication message (GTIM) at the end of the contention period that provides a mechanism for cluster synchronization while broadcasting a schedule of message transactions between nodes. There is an exchange of data between nodes during the contention-free period.

Figure 2.3 GMAC



New elections are indicated by a flag in the GTIM message. Overhearing is eliminated in G-MAC, except for a minimum amount of control traffic that a node might overhear while waiting to transmit an FRTS during the contention period.

2.2 DENIAL OF SERVICE ATTACKS IN WIRELESS SENSOR NETWORK

Denial of Service as earlier described is generally any event that diminishes the proper functioning of a network. This can be initiated in several ways [8], such as Hardware failures, software bugs, resource exhaustion or even environmental conditions. The simplest way of introducing DoS attack is to try to completely exhaust the resources available to the victim node, by sending unnecessary extra packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. Several Denial of Service attacks can be performed in different layers in a wireless sensor network. There could be jamming and tampering at the *Physical layer*; Collision, Unfairness, Denial of sleep at the *Data link layer*; neglect and greed, Selective forwarding, sink hole, black holes, homing, misdirection at the *network layer;* malicious flooding and de-synchronization at the *Transport layer*; overwhelm and path-based DoS at the *Application Layer*. Security mechanisms should be employed at each layer to create proper defense against the attacks. We briefly discuss the attacks at each layer but more emphasis on attacks at the Data link layer.

2.2.1 Categories of Attacks

- External attacks: These attacks are usually initiated by nodes outside the logical network. The nodes do not have internal information such as cryptographic information about the network.
- Internal attacks: These include attacks launched by either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes and who then use one or more laptop-class devices to attack the network.

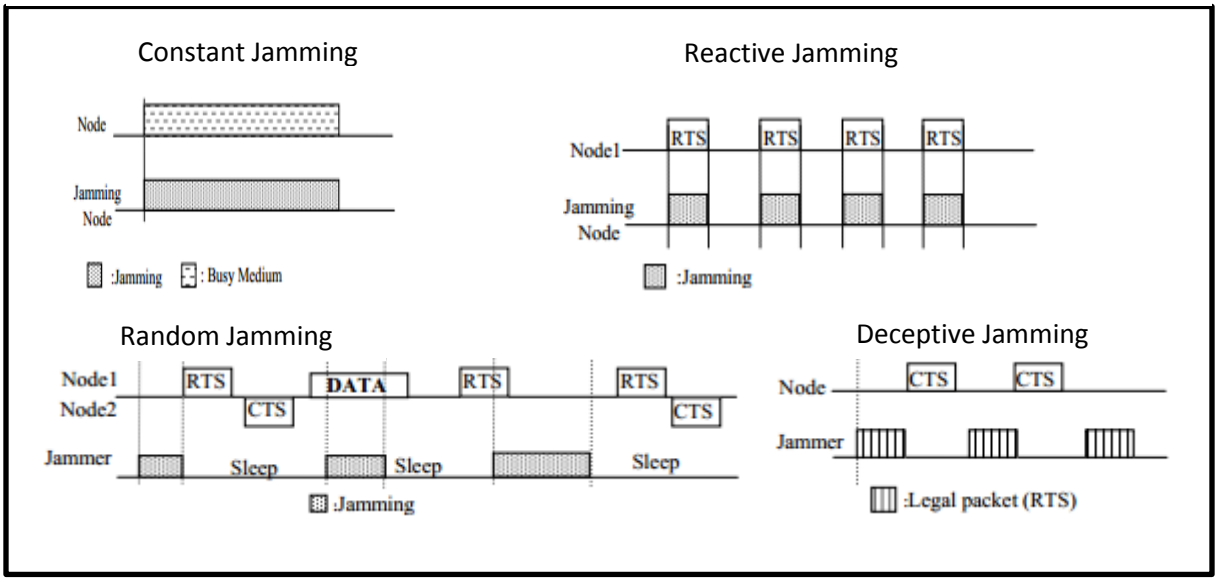
2.2.1 Physical Layer

The sensor nodes are likely to be deployed in insecure environments where the physical layer can be easily attacked. The most common physical layer attacks are Jamming and tampering.

Tampering: In this type of attack, the attacker physically alters the node(s) since it could be difficult to watch over several thousands of nodes deployed in hostile regions. The attacker could replace the node with a malicious node to create a compromised node, which the attacker controls. The attacker can also damage the nodes and computation hardware or extract sensitive material such as cryptographic keys to gain unrestricted access to higher levels of communication. A defense to this attack could be tamper-proofing the node's physical package. Other physical defenses include camouflaging or hiding the nodes.

Jamming: The radio frequencies used by the sensor nodes are interfered in this type of attack. The entire network or just a portion of the network could be disrupted in this attack depending on the power of the jamming nodes around the network. Attacking just a portion of the network is enough to bring down the whole network. Jamming could be initiated in various ways. Reactive jammer [17] constantly check the medium and send multiple RTS/CTS or data packets if the medium is found to be busy. Random jammers switch between sleep and active state thereby reducing their power dissipation. Constant jammers on the other hand send packets repeatedly without delay once the medium is available. Deceptive jammers send out multiple legal RTS packets so as so always receive CTS packets from the nodes thereby exhausting the energy of the legal nodes

Figure 2.4 Variants of Jamming



Defenses against jamming involve various forms of *spread-spectrum* communication, priority messages, lower duty cycle, region mapping, and mode change among others.

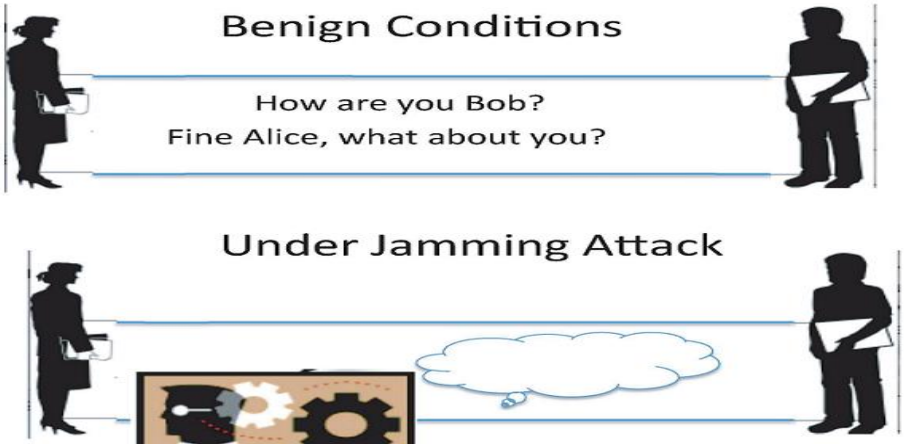
2.2.2 Data link Layer

The Data link layer is divided into the MAC layer and Link layer. WSN MAC [18]protocols earlier discussed are designed to establish cooperation between the nodes to use the communication medium making them particularly vulnerable to DoS attacks. These protocols however operate at the link layer. The link layer decides when the radio should transmit frames and listen to the channel. The MAC protocol [19] is responsible for managing the radio of sensor, which is the main source of power consumption. More energy is consumed at the transceiver than the other WSN component.

2.2.2.1 Link Layer Attacks

Collision attack: In this type of attack, [17] the attacker node, known as the jammer, continuously checks the communication channel to know if the channel is busy. If found as busy, the jammer assumes that some packets such as RTS, CTS or data packets are in the medium and thereafter sends some jamming packets to collide with the real packets. This could prevent receivers from receivers getting the expected number of packets after sending out CTS to the sender. An illustration of collision attacks is shown in Fig. 2.5.

Figure 2.5 Jamming attack



An ideal jam [20] should have high energy efficiency, low probability of detection and disrupt communications to the desired or maximum possible extent. For instance, in order to maintain a low probability of detection, the jammer can adopt techniques that are consistent with MAC layer behaviors. This attack however consumes less energy of the attacker but causes disruptions to the operation of the network.

Exhaustion attack: The attacker may also send out many RTS packets so that the nodes will continuously send out CTS packets thereby exhausting the power. It is assumed that the attacker has a prior knowledge of the MAC protocol used so as to know the ideal time to send the packets.

Unfairness attack**:** This is a weaker form of Dos attack in which the attacker degrades the network performance rather than preventing legitimate nodes from having access to the channel. For example, the attack could cause users of a real-time MAC protocol to miss their deadlines. A proposed solution is to use small frames so that an individual node can capture the channel only for a short time. Framing overhead could however be increased provided long messages are transmitted. Furthermore, this solution is susceptible to further unfairness if the adversary responds quickly rather than randomly delaying.

2.2.3 Network Layer

The best path for efficient routing mechanism is modeled at the Network layer. This layer is responsible for routing the data between the nodes. It uses algorithms such as SMECN (Small Minimum Energy Communication Network) and LEACH (Low Energy Adaptive Clustering Hierarchy) protocol to improve energy efficiency.

Neglect and greed: Malicious nodes can simply neglect to route some messages to the destination. The node receives the data may even acknowledge reception of data to the sender but somehow drops the messages. The node can also be greedy if it gives priority to its own messages. Multiple routing paths or sending redundant messages can reduce the effect of this attack by making it necessary for an adversary to subvert more sensor nodes.

Homing: In most clustered networks, some nodes such as Cluster heads, cryptographic key managers have special responsibilities.

The attacker uses traffic pattern analysis to identify and target these nodes since they provide critical services to the network. The network codes are then destroyed by the attacker. One way to prevent this attack is to provide confidential information (encryption) for both message headers and their content although it doesn't completely prevent traffic analysis. Using "dummy packets" [21] was suggested to prevent traffic analysis throughout the network. However, the energy of the sensor nodes are significantly wasted using this method.

Misdirection: Another way of attacking [3] the network layer is to forward messages along wrong paths. The attacker achieves this by diverting traffic away from its intended destination. All packets are misdirected to a victim node, which is continuously flooded. The victim node can be scheduled to sleep mode if there is an observation of a flooded link to overcome this attack.

Black holes: In this attack, the malicious node advertises the best path (zero-cost routes) to every other node in the network [22], forming *routing black holes* within the network. Since this path is considered the best path, more traffic is routed in that direction and thereby making the nodes to compete for limited bandwidth. The nodes while trying to contend for resources may be exhausted causing a hole or partition in the network.

Selective Forwarding: In a multi-hop WSN, the sensor nodes forward the entire message received to the appropriate destination. A node may however be compromised by an attacker such that it does not forward the entire message by dropping off some packets. This is called Selective forwarding. A defense mechanism could be to create multiple paths to send the data.

Sink Hole: Here, the attacker compromise a node and makes it route more attractive to its neighbors by forging routing information. As a result, the compromised node is seen as the best path for forwarding data.

2.2.4 Transport Layer

This layer is responsible for the end-to-end connections of the nodes. Simple protocols are used to minimize the communication overhead of acknowledgments and retransmissions. However, this layer is vulnerable to some known attacks such as:

Flooding: Here, the attacker tries to establish connection to the victim node severely by sending many connection requests. The node upon receiving these requests allocates resources to maintain the state of each connection until the resources required by each connection are exhausted or reach a maximum limit. This attack can be prevented by reducing the number of connections but this could prevent legitimate nodes from connecting to the victim, especially when the table is filled with abandoned connections. A defiance mechanism is to make it mandatory for nodes to solve some client puzzles while trying to establish connection before receiving a connection. The aim is to make the adversary node waste its resources while trying to flood the server with valid connections. Although it creates overhead for the legitimate nodes since more computational energy is required, wasting radio transmissions is more costly.

De-synchronization**:** De-synchronization is a way of disrupting an already established connection between two end points. This can be achieved by repeatedly sending forged messages that causes the end points to request retransmission of missed frames. This prevents the end points from exchanging useful information as energy is wasted in an endless synchronization-recovery protocol. Authentication of packets between hosts can be used to defeat this type of attack.

2.2.5 Application Layer

Overwhelm Attack: Large volumes of traffic can be forwarded to the base station if an attacker makes an attempt to overwhelm the sensor nodes with sensor stimuli [18]. The overall network bandwidth is consumed as a result of this attack and therefore drains the energy of the nodes. This attack can be mitigated by carefully tuning sensors such that the sensors are triggered by specifically desired stimulus. The effects of this attack can also be reduced by Rate-limiting and using efficient data aggregation algorithms [23].

Path-based DOS attack: This involves injecting spurious or replayed packets into the network at leaf nodes. Bandwidth and energy is wasted while trying to transmit the traffic as the packet is forwarded along the path to the Base Station. Resources are consumed on the path to the base station and thus starvation of legitimate traffic and other nodes are prevented from sending data to the base station. Packet authentication and anti-replay protection can be combined to prevent this attack.

2.3 DATA LINK LAYER ATTACKS AGAINST MAC PROTOCOLS

Denial of Sleep Attacks: Denial of sleep attack usually occurs at the link layer and it continually keeps the node's radio on thereby preventing the nodes from transiting to sleep mode. This kind of attack can drain the battery of the nodes only in few days. The MAC protocols however controls the functionality of the transceiver and hence, become a natural focus for Denial of sleep attacks [19]. In this thesis, an efficient algorithm was implemented to mitigate Denial of sleep attack on TMAC protocol. There are several ways by which the attack can be initiated. We describe some of the attacks in detail.

a) Unintelligent Attack: Here, the attacker has no knowledge of the MAC protocol as well as no ability to Penetrate Network. Recorded traffic is replayed into the network, causing nodes to waste energy while trying to receive and process these extra packets. Nodes that do not implement anti-replay mechanisms are vulnerable to this type of attack causing replayed traffic to be propagated through the network. The replaying of events has adverse effect on the network lifetime and overall performance of WSN.

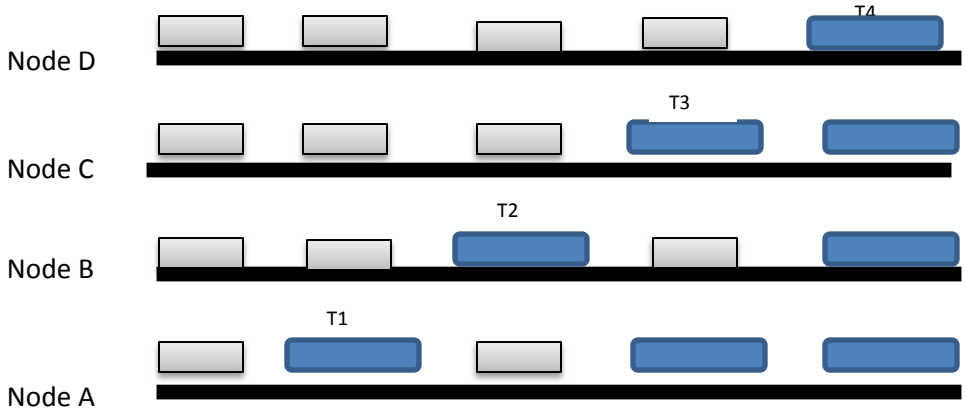
b) Unauthenticated Broadcast Attack: The attacker here also has full knowledge of the MAC protocol used but has no ability to penetrate the network. The attacker simply broadcasts unauthenticated traffic into the network and publish larger duty-cycle schedule in order to reduce the network lifetime by obeying the rules of the MAC protocol. The messages are the received by the nodes in the network but are discarded. This attack causes the nodes to extend their listen period trying to receive the packets, which however leads to increase in energy consumption and reduction in network lifetime.

c) Full Domination attack: This classification is [24] one in which the attacker has full protocol knowledge and has also penetrated the network. This attack is usually initiated using one or more compromised nodes in the network. For example, knowing fully well the S-MAC protocol, the attacker sends a SYNC message at a frequency just short of the duty cycle to keep delaying the transition to sleep mode. In T-MAC, the attacker sends continuous packets at an interval slightly shorter than the adaptive timeout (TA) to prevent the nodes from transiting to sleep mode.

2.3.1 Attack on SMAC

In a situation when the attacker knows about the MAC protocol being used but has no penetration (Unauthenticated Broadcast Attack), the attacker is able to determine the sleep time of the nodes when from the SYNC packets. The attacker can then make nodes to always listen more than the normal time at every SYNC exchange. This will prevent the nodes from going to sleep. It is known as the "Synchronization attack". This kind of attack is very effective on SMAC protocol. In Fig. 2.6, at time T1, Node A extends its listen time due to an attack, which was only heard by Node A. At time T2, Node A follows the normal listen sleep protocol and tells Node B to extend its listen time. At time T3, Node B follows the normal listen-sleep protocol and tells Node C to extend its listen time and so on. The attack on Node A successfully propagates to Node B, Node C and Node D.

Figure 2.6 illustration of Synchronization attack



2.3.2 Attack on TMAC

The Synchronization [25] attack described above is not effective on T-MAC because of T-MAC's adaptive timeout mechanism. The nodes transit to sleep mode when there is no activity in the network for a period defined as TA. Despite the advantage of TMAC over SMAC protocol, TMAC is vulnerable to a simple denial of sleep stack by sending constant stream of small packets at an interval just short of the network's adaptive timeout. This can make the sensor nodes to be awake all through.

2.3.3 Attack on GMAC

The GMAC protocol [26] eliminates the broadcast attack from the nodes within a cluster, therefore does not affect the sleeping nodes but the attacker can continuously send broadcast messages to the gateway node and force the gateway node to receive the entire message before discarding it due to authentication failure. Therefore, a link layer denial of sleep attacker can only affect one node at a time, because nodes alternate the gateway responsibilities based upon incremental decrease in battery levels. Since n-1 nodes will always be sleeping during the broadcast, the network lifetime for an attack increases linearly with the number of nodes.

2.4 LITERATURE REVIEW OF DENIAL OF SLEEP ATTACKS IN WIRELESS SENSOR NETWORK

Several solutions have been proposed to detect the Denial of sleep attack. However, majority of the proposed solutions have some limitations. A review of existing works is described in this section.

2.4 1 An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks

A fake schedule switch [27] method was proposed with RSSI measurement aid. This method is implemented on S-MAC algorithm, which adopts active/sleep switch and lower duty cycle for conserving power. Due to the mechanism used in S-MAC, introducing energy silent mechanism also creates the possibility for attackers to disrupt the normal communication of the system.

There is an increase in energy consumption when there is constant jamming even for the attackers. In other words, for a long-term interference and breakage, attackers need to adopt an energy efficient scheme in other to successfully invade the network. This makes the intruders to focus more on understanding the mechanism used for communication in the network. Due to this, the proposed method was mainly to prevent attackers from getting full details on the mechanism used.

a) Fake Schedule Switch

If an attacker joins the system, the aforementioned attacks can be originated. Therefore a fake schedule switch is introduced to defeat these attacks. When RTS/CTS packets are delayed or there is loss of packets, there is a possibility of collision attacks. Therefore when receivers do not get expected number of packets or a sender do not get an acknowledgment for a particular time out period, a fake schedule switch is initiated. This means that the victims broadcasts a schedule switch SYNC but do not actually change the schedule in other to deceive the attackers. The victims then return to their normal schedule after the expiration of a timer. The attackers however would have changed their schedules and then try to get the new duty cycle algorithm thereby losing out energy.

b) RSSI MEASUREMENT

It is important to note that packet loss or delay in acknowledgement could possibly not be due to the occurrence of an attack. Initializing fake schedule switch could therefore be detrimental if not used properly. This gave rise to the utilization of the RSSI (Received Signal Strength Indication) [12] to protect the switch scheme from been revealed. It is assumed that attackers impede the nodes at close transmission range. Therefore, any node one hop away the attacker will have great possibility to receive consecutive larger RSSI when they enable adaptive listen. Thereby, the victims can estimate the appearance of the attacker within adaptive listen period.

Limitations with this approach

- It requires complex installations
- Energy consumption and transmission delay increases.

2.4.2 Mechanisms for Detecting and Preventing Denial of Sleep Attacks on Wireless Sensor Networks

Manju.V.C et al [25] proposed a solution on the existing mac protocols such as S-MAC and T-MAC. Defenselessness is caused due to inability to authenticate the SYNC packet in S-MAC and T-MAC. Also the network is easily susceptible to replay attack. The proposed solution is based on providing strong authentication to the SYNC packets; so as to defend denial of sleep attack is in the network. The proposed method is therefore divided into two parts such as:

a. Network organization: This is done at the initial deployment of the nodes. The sensor network is then built in a tree-like structure such that every node knows its parent node. Likewise all parent nodes know its child nodes from which SYNC packets is received. The algorithm is described as follows:

- First sink node broadcasts a Hello Packet with its ID.
- The node which receives this Hello packet which is one hop away will take ID in the Hello Packet as its parent and sends Hello Response to the ID also broadcast a new Hello Packet with its ID.
- The node which receives the Hello Packet will check if it does not have a parent yet and it will add the ID in Hello packets as its parent and send Hello Response to its parent.
- On the arrival of Hello response, node will update its child list. It is assumed there is no attack on the network during the network organization stage. All nodes are enforced to be active this stage.

b. Selective level authentication: SYNC packet has two different formats, which are *without authentication* and *with authentication* token. Here, authentication is used when sending SYNC packets and there is a possibility of Denial of sleep attack (possible threshold cross over) while *without authentication* is used during normal operation if the SYNC is under threshold.

Limitations with this approach

- It introduces communication overhead when the attack is suspected due to the structure of the tree. The affected node is traced down to the root with authentication token.
- Energy consumption increases as all nodes are active during the network organization.

2.4.3 Lightweight hierarchical Model for HWSNET

An efficient intrusion Detection system IDS [28], was proposed to overcome the sudden death of the sensor nodes. It uses cluster-based mechanism in an energy efficient manner to build a five layer hierarchical network to enhance network scalability and lifetime.

Table 2.1 Terminologies

Term	Meaning
p^{i}_{jk}	Packet sent by i^{th} leaf node of sector j of cluster k
LN^{i}_{jk}	i^{th} leaf node of sector j of cluster k
T^{i}	Time-slot allocated to i^{th} leaf node
insomnia	Result of anomaly detection
L^{i}_{jk}	Standard battery lifetimeof i^{th} leaf node of sector j of cluster k
PW^{i}_{jk}	Initial battery power of i^{th} leaf node of sector j of cluster k
RE^{i}_{jk}	Residual energy of i^{th} node of sector j of cluster k
$CRLT^{i}_{jk}$	Calculated remaining lifetimeof i^{th} node of sector j of cluster k
LRE^{i}_{jk}	Last recorded energy of i^{th} node of sector j of cluster k
Tot^{i}_{jk}	Total number of packets sent by i^{th} leaf node of sector j of cluster k
NP[]	Normal profile
KB[]	Knowledge base
$R_{suspected}$	Rate of energy consumption for suspected node
Truedetect	Count the number of times system detects true intrusion
Phantomdetect	Count the number of times system detects false intrusion

2.4.3.1 System Parameters

PW_{slp} → power required in sleep mode; PW_{tr} → power required during transmission; PW_{idle} → power required in idle mode; PW_{wake}→ power required in wakeup mode; PW_{comp} →power required during computation; $PW_{sensing}$ →power required during sensing data; T_{idle}→ time spent in idle mode; T_{slp}→ time spent in sleep mode; T_{tr}→time spent during transmission; T_{comp} →time spent in computation; T_{wake}→ wakeup duration; $T_{sensing}$ →sensing duration; NEC_{ijk}→ normal energy consumption; $TNEC_{ijk}$ → threshold normal energy consumption; ThL_{ijk}→ threshold lifetime;

ThT_{wk}→threshold wakeup duration; ThT_{sl}→ threshold sleep duration; Th_{buf} →threshold buffer capacity; AWC_{ijk} →authentic wake up coin value; T_{scount} →threshold of allowablesuspected count; T_{per}→ threshold of allowable suspected count percent; T_{reput} → threshold reputation; Th →threshold value

Begin

Case 1: /* Energy consumption rate of any node found to be more compared to preset threshold value of normal energy consumption or calculated lifetime of any node found to be less compared to preset threshold lifetime of the node*/

If $EC_{ijk} > TNEC_{ijk}$ OR $CLT_{ijk} < THL_{ijk}$ then

insomnia ←*1*

Else

insomnia ←*0*

EndIf

Case 2: /* Allotted wakeup period of any node is greater than predefined threshold wakeup schedule and allotted sleeping period is less than predefined threshold sleeping schedule*/

If $T_{wake} > ThT_{wk}$ AND $T_{slp} < ThT_{sl}$ OR $T_{slp} = 0$ then

insomnia ←*1*

Else

insomnia ←*0*

EndIf

Case 3: /* Any node sends packets in a time-slot, but that slot is not allocated to that node*/

If $| T_{slotijk} - T_i | > 0$ then // $T_{slotijk}$→ data actually transmitted by LN_{ijk} during this time-slot

insomnia ←*1*

Else

insomnia ←*0*

EndIf

Case 4: /* Residual energy of any node is found to vary more compared to last recorded energy*/

If $LRE_{ijk} >> RE_{ijk}$ OR $LRE_{ijk} << RE_{ijk}$ then

insomnia ←*1*

Else

insomnia ←*0*

EndIf

Case 5: /*Received packets within a time interval exceeds pre-defined threshold value*/

If (Tot_{ijk} / T_i)*100% > Th_{buf} then

insomnia ←*1*

Else

insomnia ←*0*

EndIf

End Case

End

2.4.3.2 Limitation with this approach

- Each node independently determines intrusions. It gives rise to problem in handling dense network. Therefore stand-alone IDS is not opted for research work in sensor network.

2.4.4 Sleep deprivation Attack Detection in Wireless Sensor network

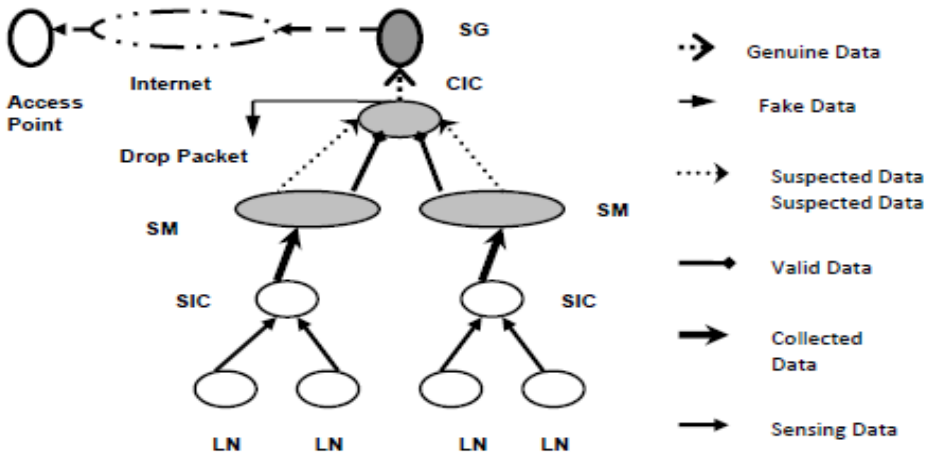
Due to the limitation in the work described above, [5] again, proposed a hierarchical framework based on distributed collaborative mechanism (cluster based mechanism) for detecting sleep deprivation torture in wireless sensor network efficiently. A dynamic detection model is designed here to overcome sudden death of IDS enabled sensor nodes. In this model responsibility of each node dynamically changes to reduce the burden of a single node.

The Sensor nodes are categorized into various roles such as sink gateway (SG), cluster-in-charge (CIC), sector monitor(SM), sector-in-charge (SIC) and leaf node (LN) depending on their battery capacity. The roles of CIC, SM and SIC are changed dynamically to avoid exhaustion of nodes.

Table 2.2 Participating Nodes in Wireless Sensor Network

Nodes	Definition
Sink Gateway(SG)	A layer 4 node having highest capacity provides gateway functionality to other networks.
Cluster-In-Charge(CIC)	A layer 3 node having maximum energy and degree (number of nodes within its coverage area) among all neighbors of SG and capable to take final decision regarding intrusion.
Sector Monitor(SM)	A layer 2 node that is nearest neighbor of CIC and whose detection power is set to maximum within sector and capable to detect anomaly.
Sector-In-Charge(SIC)	A layer 2 node that has maximum energy among neighbors of CIC and capable to collect sensing data.
Leaf Nodes (LN)	A layer 1 node which can only sense data and whose detection power is set to null.

Figure 2.7 Data Collection



Limitation with this approach

In this model, the leaf nodes are directly affected by intruder. If any leaf node receives fake data request from unknown nodes (intruder), it cannot detect it. As a result battery of the affected node may be low or exhausted completely.

2.4.5 A Defense Strategy against Energy Exhausting Attacks in Wireless Sensor Networks

Authentication and encryption [29] solutions was proposed using a cross layer energy efficient security mechanism to protect the network from denial of sleep attacks. The cross layer involves interaction between the network, Mac and physical layers. Fake packets are rejected using by using the routing information at the MAC layer.

The routing path, neighborhood routing tables, and neighborhood routing nodes RSSI value are computed centrally by the BS (base station). Each sensor node knows previously the source of packets that will be received.

2.4.6 Security from Denial of Sleep Attack in Wireless Sensor Network

A detailed analysis of several proposed solution was investigated [19] based on the strengths and weaknesses of each solution. Based on the analysis, it was concluded that the problem of hierarchical framework [5] of attack on leaf node of the cluster can be overcome by using the fake switch schedule [27]at the leaf node of cluster by calculating the RSSI value of the attacker node by the sector node. The leaf node uses detection technique when a malicious packet is sent, while fake schedule switch method is used when same message in sent to leaf node continuously. The overall lifetime of the network is assumed to increase using this method.

2.4.7 The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense

The barrage attack and the sleep deprivation [30] attack were analyzed but more emphasis was placed on the sleep deprivation attack since the barrage attack causes its victims to spend slightly more energy, it is more easily detected and requires more effort on behalf of the attacker. Three different methods to mitigate the sleep deprivation attack were analyzed such as the random vote scheme, the round robin scheme, and the hash-based scheme. Based on the evaluation of these methods, the hash-based scheme was proposed as the best at mitigating the sleep deprivation attack.

Limitations with this approach

- Random vote scheme; It requires more iteration to complete the algorithm.
- Round robin; for large cluster, each node requires an unrealistic amount of per-node storage, which enhances the overhead.
- Hash-based scheme; It only considers intrusion from cluster head side.

2.4.8 A Synchronization Attack and Defense in Energy-Efficient Listen-Sleep Slotted MAC Protocols

The synchronization attack on listen-sleep MAC protocols was presented [31] in this work and simulation shows that under linear network topology, the attack can cause 30% more energy drain (due to loss of sleep and data retransmission) and 100% message loss (due to misalignment of the data periods). A heuristically near-optimal threshold-based scheme was proposed to defend against large scale synchronization attack.

2.4.9 Denial of Sleep Detection and Mitigation

This paper [32] analyzed the MAC protocols available for Wireless Sensor Networks and proposed an algorithm that can enforce deep sleep cycle on the nodes when abnormal activities are detected. This is done by including a register in the MAC protocol before deployment to a save constant that refers to the limit of normal proportion of active time to sleep time during predefine time. The deep sleep cycle is initiated when the condition is violated and the compromised node(s) remains asleep until the deep sleep period is elapsed. The node can continue normal operation after the deep sleep period is elapsed until the condition is violated again. The method drains the attacker's energy, as the attacker is not able to determine when the nodes will transit to deep sleep cycle.

Limitation with this approach

Suspected nodes are temporarily excluded from the network thereby resulting into reduced performance of the overall network.

2.4.10 Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols

The MAC [13] protocols for Wireless sensor Networks were reviewed and description of selected attacks on S-MAC, T-MAC, and B-MAC were Implemented and analyzed in detail. A framework for preventing denial-of-sleep attacks in sensor networks was also introduced such as Strong link Layer Authentication, Anti-Replay Protection, Jamming identification and mitigation, and Broadcast Attack Protection.

2.4.11 Wireless Sensor Network Denial of Sleep Attack

In [26], the energy resource vulnerabilities of wireless sensor networks, models the network lifetimes of leading WSN medium access control (MAC) protocols was analyzed and a new MAC protocol, GMAC was proposed to mitigate many of the effects of denial of sleep attacks. The GMAC protocol has been earlier explained in this chapter.

2.5 TOOLS AND TECHNOLOGIES USED

In this thesis, the proposed algorithm was implemented using simulation software known as Castalia. Castalia [33] is a simulator for Wireless Sensor Networks (WSN), Body Area Networks (BAN) and generally networks of low-power embedded devices, based on the OMNeT++ platform. It is designed for adaptability and also supports expansion. This provides easy importation/implementation of algorithms and protocols for users.

2.5.1 Brief Description of OMNeT++

OMNeT++ [34] is an object-oriented modular discrete event network simulation framework. OMNeT++ itself is not a simulator of anything concrete, but rather provides infrastructure and tools for writing simulations. It has a generic architecture, so it can be (and has been) used in various problem domains:

- modeling of wired and wireless communication networks
- protocol modeling
- modeling of queuing networks
- modeling of multiprocessors and other distributed hardware systems
- validating of hardware architectures

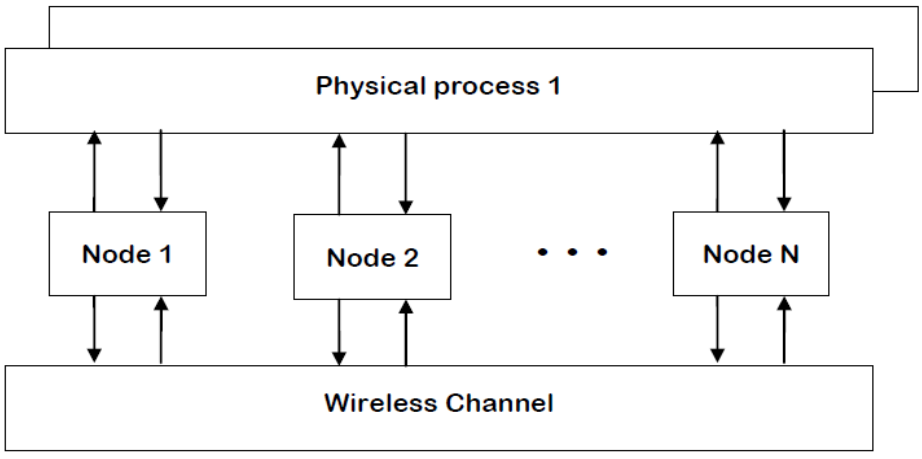
- evaluating performance aspects of complex software systems
- In general, modeling and simulation of any system where the discrete event approach is suitable, and can be conveniently mapped into entities communicating by exchanging messages.

OMNeT's basic concepts are modules and messages. A simple module is the basic unit of execution. It accepts messages from other modules or itself, and according to the message, it executes a piece of code. The code can keep state that is altered when messages are received and can send (or schedule) new messages. There are also composite modules. A composite module is just a construction of simple and/or other composite modules.

2.5.2 Structure of Castalia

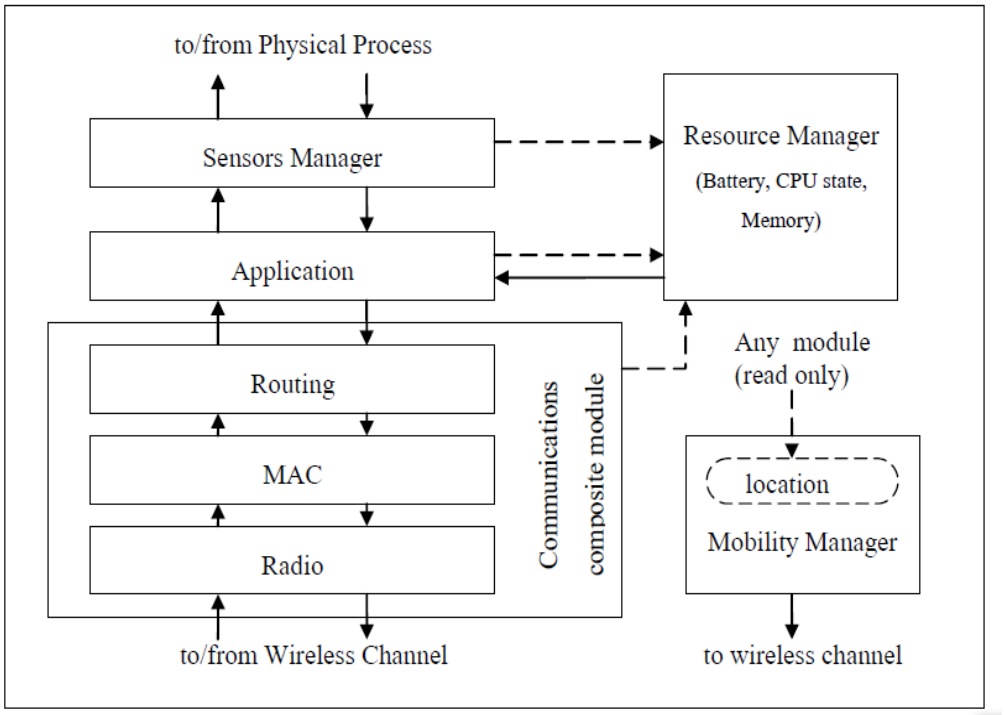
As shown in Fig. 2.8, the nodes connect through the Wireless Channel and are also linked through the physical processes that they monitor. The nodes sample the physical process in space and time (by sending a message to the corresponding module) to get their sensor readings. There can be multiple physical processes, representing the multiple sensing devices (multiple sensing modalities) that a node has.

Figure 2.8 Structure of Castalia



The node module is a composite module and the modules in the node module are represented in Fig. 2.9.

Figure 2.9 The node Module



The solid arrows signify message passing and the dashed arrows signify simple function calling. Our proposed algorithm was implemented in the MAC module.

CHAPTER 3

3.0 ANALYSIS AND PRPOSED METHOD

Most of related works presented in Chapter 2 are generally energy inefficient due to the increased complexity introduced at link layer protocols. In this thesis, we will combine the benefits of two different algorithms proposed from two papers[25][29] and setup a new algorithm to fight against Sleep deprivation attacks.

3.1 ANALYSIS OF EXISTING METHODS

Some of the existing methods were based on flat architecture using MAC protocols at the link layer such as SMAC, TMAC and BMAC while others were based on hierarchical architecture where the nodes are partitioned into different clusters depending on their remaining energy and made to perform different functions. We have been able to establish from literature that the hierarchical architecture is not scalable because it cannot adapt to changes such as increase in the number of nodes. To ensure scalability, we have decided to combine both architectures and develop a way to detect denial of sleep attacks on the Wireless Sensor MAC protocols.

It has also been established that successful attacks can be launched in a Wireless sensor Network just with the knowledge of the MAC protocol adopted. The framework proposed in [13] suggested using Strong link layer authentication, Anti-Replay Protection, Jamming identification and mitigation, and Broadcast Attack Protection on the adopted MAC protocol.

A simple authentication mechanism was used in [29] but was only implemented on SMAC protocol. The fake Schedule switch method proposed in [27] was also implemented on SMAC protocol. Likewise, the threshold-based heuristic approach presented in [31] was also implemented on SMAC protocol. The method proposed in [29] uses a cross-layer mechanism between the network, MAC and physical layers. The Base Station is made to store the identification, geographical position, and energy reserve of all the nodes. Overhead is incurred since all nodes have to send their information to the base station at

the setup phase. This method however was only implemented on the SMAC protocol. It can be concluded that much work has not been done on implementing these algorithms on the other MAC protocols.

We have decided in this research to introduce the benefits of some of the methods proposed in literature and develop a method to detect denial of sleep attacks on TMAC protocol. As discussed in Chapter 2, TMAC uses an adaptive timeout (TA) mechanism to improve the network efficiency. When the node does not hear any activity on the channel for a defined TA, it goes to sleep. This mechanism makes it easier for an attacker to use broadcast attacks to prevent the nodes from transiting to sleep mode. This is done by continuously sending packets at an interval just short of the adaptive timeout. Unauthenticated broadcast attack is therefore the most effective attack on TMAC protocol.

3.2 PROPOSED METHOD

To prevent all nodes from sending information to the Base Station, we adopt the network Organization method proposed in [25] so that each node stores the identification of its parent (the node it can send data to) and the identification of child nodes (nodes one hop away that it can receive data from). According to [25], all the nodes are enforced to be active throughout the network organization stage.

However, when the number of nodes increases, the nodes consume more energy because all the nodes are active throughout the network organization stage. We propose that during the network organization stage, a node can transit to sleep mode upon receipt of Hello Response from all child nodes and when the network organization is complete, all nodes wake up to begin synchronization.

The algorithm for the method in [25] is given below.

Algorithm: Organize Network

BEGIN:

HELLO← create Hello Packet with node ID

Broadcast HELLO

Pack←Wait for Packet from NetWork ();

IF Pack is HELLO {

IF Parent==NULL {

Parent= ID in HELLO

HELLORES← create Hello Response with self-node ID

Send HELLORES to Parent

}

}

ELSE Pack is HELLORES {

Child list← {ID in the Hello Res}

}

END IF

END

To minimize the rate of energy consumption while trying to organize the network, we modified the algorithm such that the nodes can transit to sleep mode once Hello packet has been sent and Hello Response packet received. With this, we believe that the rate of energy consumption will be reduced. An attack is suspected if a node receives a SYNC packet from node(s) not listed as its child. The packet is simply discarded. Our modified Network Organization algorithm is presented below.

Steps (Network Organization):

- First the sink node broadcasts Hello Packets with its ID and RSSI value
- Node which is one hop away receives and replies with Hello Response with its ID and RSSI value, also broadcasts Hello Packet with its ID.
- Node which receives Hello Packet includes the sender as its parent if and only if it has no parent.
- A node updates its child list on the arrival of hello Response packet.
- The node(s) transits to sleep after receiving hello response packet.

Algorithm: Organize Network

BEGIN:

HELLO← create Hello Packet with node ID

Broadcast HELLO

Pack←Wait for Packet from NetWork ();

IF Pack is HELLO {

IF Parent==NULL {

Parent= ID in HELLO

HELLORES← create Hello Response with self-node ID

Send HELLORES to Parent

}

}

ELSE Pack is HELLORES {

Child list← {ID in the Hello Res}

Go to sleep for a set duration & wake up after network organization

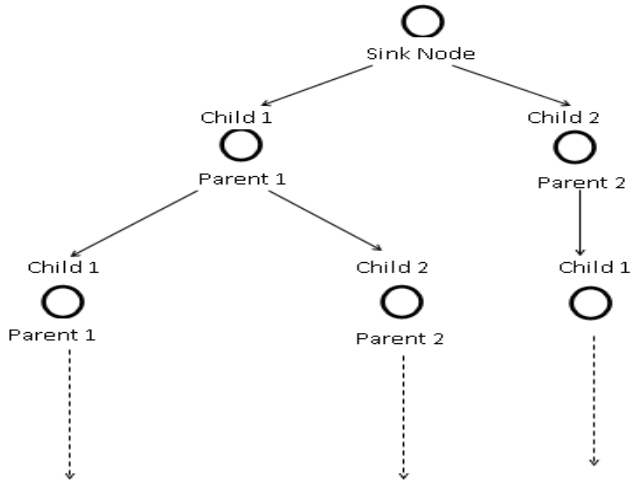
}

END IF

END

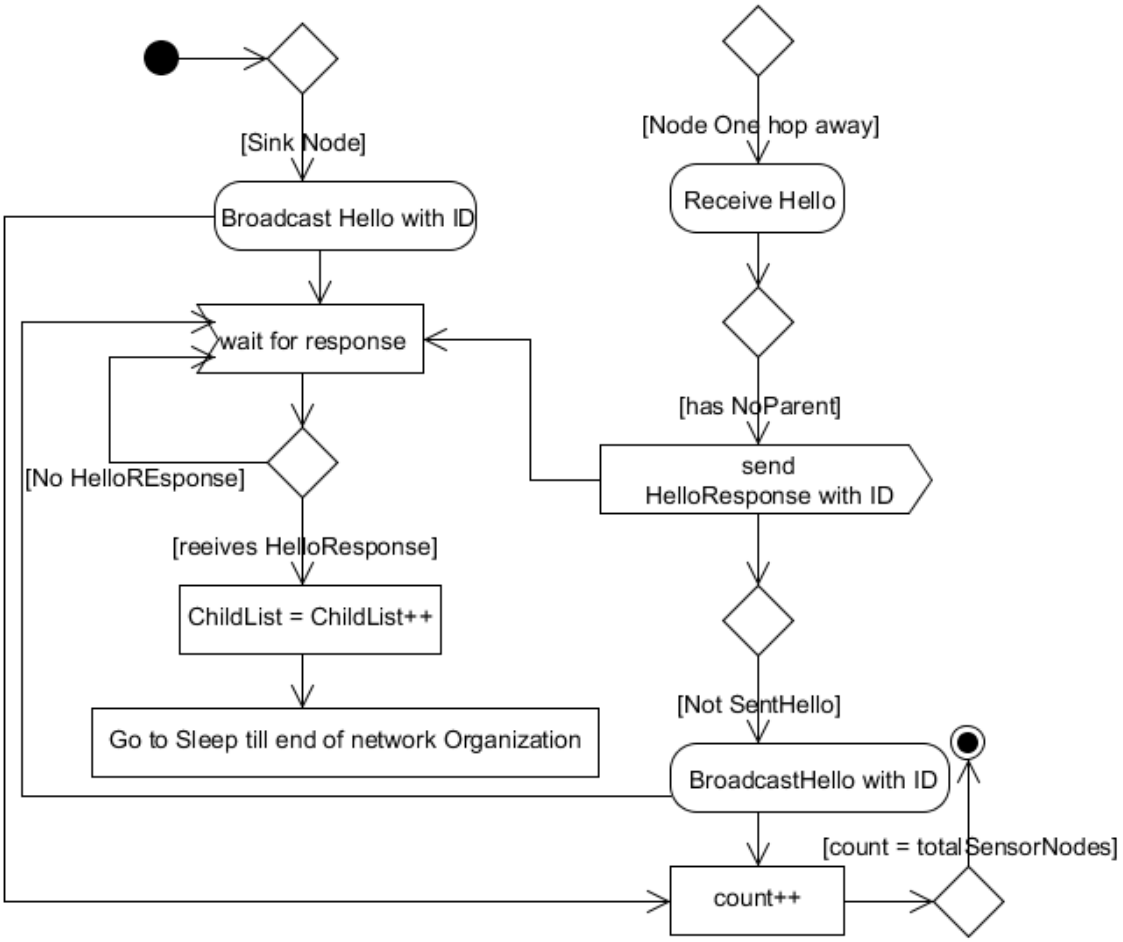
After the network organization is done, the synchronization phase for the MAC protocol is initiated. Only valid nodes are will able to synchronize with neighbors. Then network is built in a tree-like structure as shown in the figure below.

Figure 3.1 Tree Structure



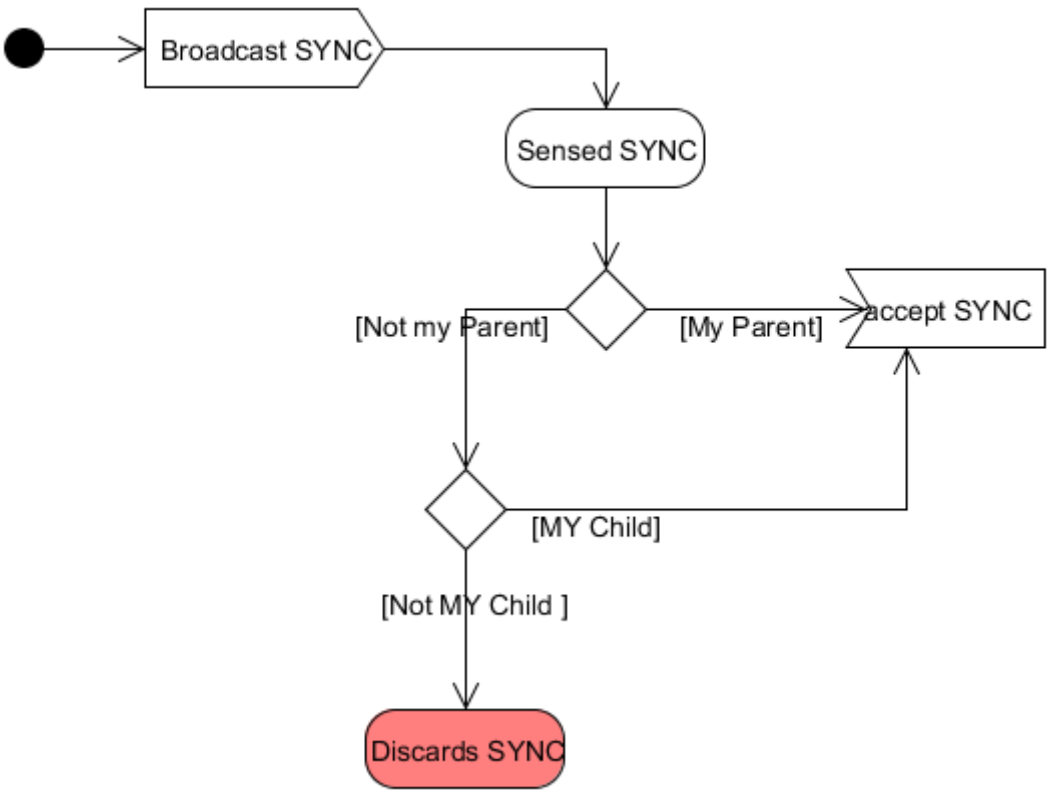
The activity diagram for the proposed model is shown below.

Figure 3.2 Activity Diagram for Network Organization



After setting up the network,we can now begin authentication for the SYNC packets as shown in Fig. 3.3. We only consider the first level of authentication in the Selective Local Authentication proposed in [25] since the synchronization attack is not effective on TMAC protocol due to the adaptive timeout mechanism.

Figure 3.3 Activity Diagram for Selective Authentication



3.2.1 Behavior of Proposed Mechanism under Broadcast attack.

It is assumed that the attacker has a prior knowledge of the MAC protocol used therefore obeys the rules of communication schedules which makes the attack hard to detect. The attacker continuously initiates a broadcast attack to nodes within its range while the simulation is on. In TMAC protocol, the broadcast message is not preceded by RTS packets, making it difficult to authenticate. A broadcast message has to be received before it can be authenticated making the nodes awake all the time while trying to receive the packets. With our security mechanism, a node only receives message from its child node(s). Therefore, denial of sleep attack is totally mitigated with our method with broadcast attacks.

CHAPTER 4

4.0 EVALUATION OF RESULTS

We were able to implement the broadcast attack whereby the attackers continuously send packets at different rates at an interval lower than the adaptive timeout value. Our security mechanism was also implemented on TMAC protocol and the analysis of the performance of our intrusion detection is performed using the Castalia network simulator. Our experimental model is built on varying number of nodes with different field sizes and deployment types.

4.1 ASSUMPTION

- The attacks are initiated by external attackers (cryptographic information not revealed)
- The nodes are static (not mobile).
- There is no attack at the network organization stage.

4.2 SIMULATION PARAMETERS

General Simulation Parameters

Parameter	Value
MAC Layer protocol	TMAC
Transmission Power	57.42mW
Receiving Power	62mW
RTS, CTS, ACK size	13 Bytes
Adaptive Timeout	15ms
Packet spacing	10ms

Table 4.1 General Simulation parameters

4.3 SIMULATION RESULTS

The attackers broadcast data packets continuously at an interval below the adaptive time out. We test the algorithm varying the number of nodes with different Simulation time. The average consumed energy for all nodes in the network is displayed in a graph. We compare the algorithm proposed in [25] with our modified algorithm and also a situation when there is no detection mechanism.

From the simulation graphs,

- **secured** represents the algorithm proposed in [25] on TMAC protocol.
- **unSecured** represents when there is no intrusion mechanism on TMAC protocol.
- **improved** represents our modified algorithm on TMAC protocol.

CASE 1: Number of nodes is 10

Parameter	Value
Number of Nodes	10
Number of attackers	1
Field Size	20x20(meters)
Deployment Type	"5X2"

Table 4.2 Parameters for 10 nodes

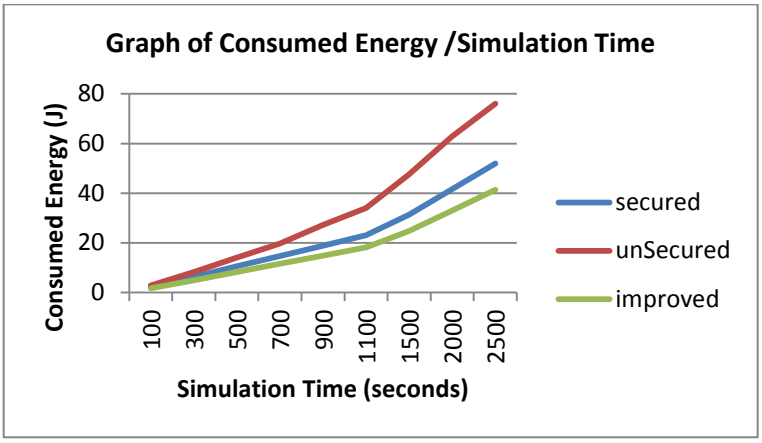


Figure 4.1 Consumed energy with 10 nodes

CASE 2: Number of nodes is 25

Parameter	Value
Number of Nodes	25
Number of attackers	4
Field Size	30X30(meters)
Deployment Type	"5X5"

Table 4.3 Parameters for 25 nodes

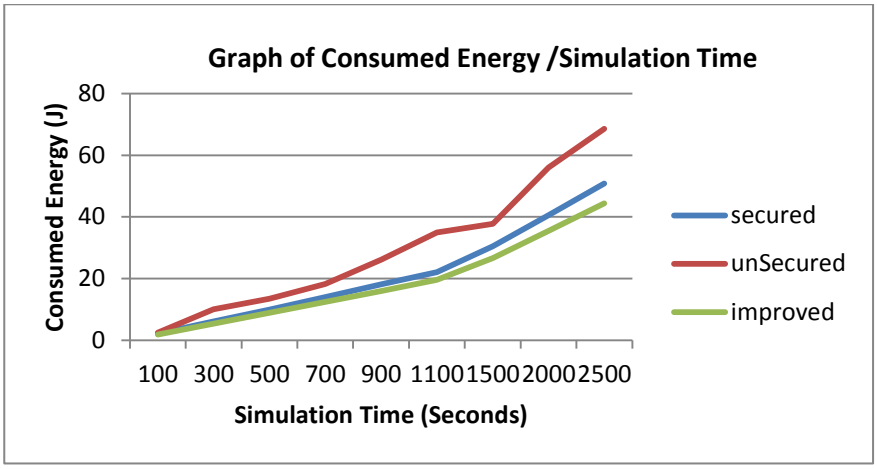


Figure 4.2 Consumed energy with 25 nodes

CASE 3: Number of nodes is 30

Parameter	Value
Number of Nodes	30
Number of attackers	4
Field Size	30X30(meters)
Deployment Type	"6X5"

Table 4.4 Parameters for 30 nodes

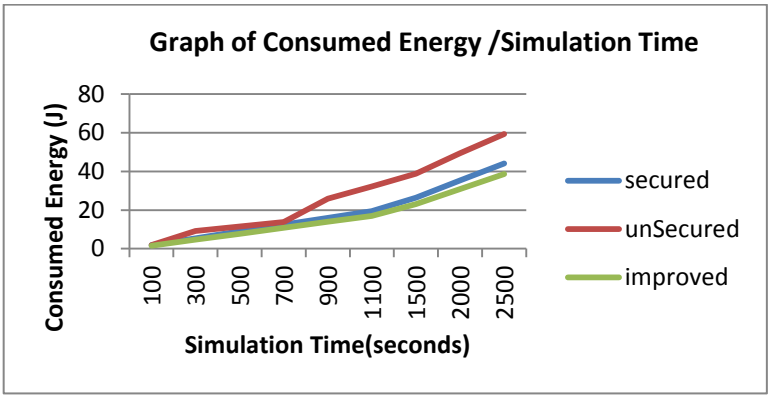


Figure 4.3 Consumed energy with 30 nodes

CASE 4: Number of nodes is 50

Parameter	Value
Number of Nodes	50
Number of attackers	4
Field Size	30X30(meters)
Deployment Type	“25X2”

Table 4.5 Parameters for 50 nodes

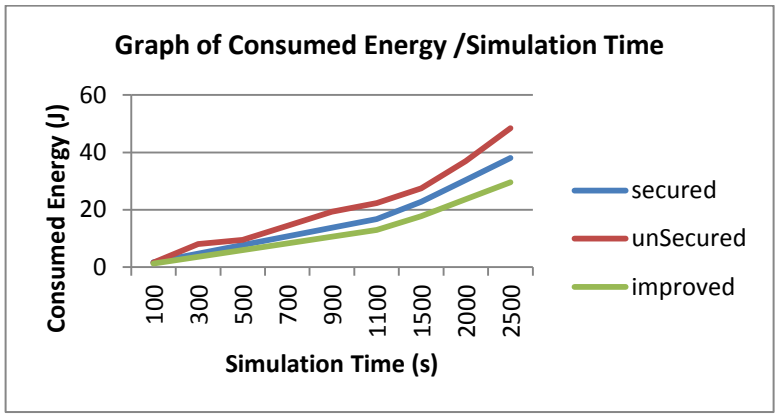


Figure 4.4 Consumed energy with 50 nodes

CASE 5: Number of nodes is 100

Parameter	Value
Number of Nodes	100
Number of attackers	4
Field Size	50x40(meters)
Deployment Type	“10x10”

Table 4.6 Parameters for 100 nodes

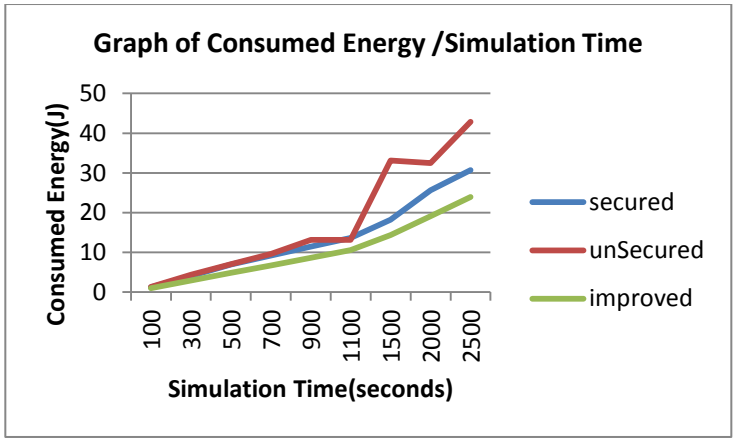


Figure 4.5 Consumed energy with 100 nodes

4.4 INTERPRETATION OF RESULTS

With all nodes having the same transmission and receiving power, the attackers continuously broadcasts fake packets at an interval of 10ms throughout the simulation time. Our graphs show the average energy consumed against each simulation time. We used different field size as the number of nodes increases. After a node has sent hello Packet and received hello response, it simply goes to sleep as described in our proposed method. Based on the simulation results, it can be seen that energy consumed increases with increase in simulation time. Also, our modified algorithm is better in all cases even with increase in the number of nodes. We demonstrated that our security mechanism (improved TMAC) could efficiently mitigate sleep deprivation attacks.

CHAPTER 5

5.0 CONCLUSION AND FUTURE WORK

5.1 CONCLUSION

This thesis explored the various Denial of Service attacks in Wireless Sensor network with more emphasis on the Sleep deprivation attack. This attack mainly increases the energy consumption of the nodes by keeping the nodes in receive mode when they should be in sleep mode. This could however reduce the lifespan of the network from years to days. Various intrusion detection mechanisms were reviewed and their limitations were listed. We developed a method by combining the benefits of the methods proposed in [25] and [29] and was able improve the algorithm to detect denial of sleep attacks. The algorithm was implemented and we have only been able to simulate broadcast attacks on TMAC protocol. Our Simulation results show that the rate of energy consumption is reduced in the face of Denial of sleep attack even with increased number of nodes.

5.2 LIMITATION

This work has been able to improve the algorithm proposed in [25] by enabling the nodes to sleep after sending Hello Packets and receiving Hello Response packets. However, the limitation of this work is given below:

If the nodes transits to sleep before receiving complete hello Response packets from its entire child node, the child node(s) will not be listed as valid nodes. This could make real nodes excluded from the network.

5.3 FUTURE WORK

- To test this Simulation with more deployment scenario and also using uniform or random distribution.
- To test the algorithm with the other classes of denial of sleep attacks.
- To test on the algorithm on larger field sizes.

CHAPTER 6

6.0 BIBLOGRAPHY

[1] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, 2003, pp. 197–213.

[2] W. Dargie and C. Poellabauer, *Fundamentals of wireless sensor networks: theory and practice*. John Wiley & Sons, 2010.

[3] A. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[4] N. Farooq, I. Zahoor, S. Mandal, and T. Gulzar, "Systematic Analysis of DoS Attacks in Wireless Sensor Networks with Wormhole Injection."

[5] T. Bhattasali, R. Chaki, and S. Sanyal, "Sleep Deprivation Attack Detection in Wireless Sensor Network," *ArXiv Prepr. ArXiv12030231*, 2012.

[6] Y. Li, M. T. Thai, and W. Wu, *Wireless sensor networks and applications*. Springer, 2008.

[7] S. Khan, J. Lloret, and J. Loo, *Intrusion Detection and Security Mechanisms for Wireless Sensor Networks*. Hindawi Publishing Corporation 410 PARK AVENUE, 15TH FLOOR,# 287 PMB, NEW YORK, NY 10022 USA, 2014.

[8] S. K. Singh, M. P. Singh, and D. K. Singh, "A survey on network security and attack defense mechanism for wireless sensor networks," *Int J Comput Trends Tech*, pp. 5–6, 2011.

[9] A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung, "MAC essentials for wireless sensor networks," *Commun. Surv. Tutor. IEEE*, vol. 12, no. 2, pp. 222–248, 2010.

[10] J. Kabara and M. Calle, "MAC protocols used by wireless sensor networks and a general method of performance evaluation," *Int. J. Distrib. Sens. Netw.*, vol. 2012, 2012.

[11] W. Ye, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," *Netw. IEEEACM Trans. On*, vol. 12, no. 3, pp. 493–506, 2004.

[12] H. Singh and B. Biswas, "Comparison of CSMA based MAC protocols of wireless sensor networks," *Int J AdHoc Netw Syst*, vol. 2, no. 2, pp. 11–20, 2012.

[13] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, “Effects of denial-of-sleep attacks on wireless sensor network MAC protocols,” *Veh. Technol. IEEE Trans. On*, vol. 58, no. 1, pp. 367–380, 2009.

[14] W. Ye, J. Heidemann, and D. Estrin, “An energy-efficient MAC protocol for wireless sensor networks,” in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, 2002, vol. 3, pp. 1567–1576.

[15] A. Roy and N. Sarma, “Energy saving in MAC layer of wireless sensor networks: a survey,” in *National Workshop in Design and Analysis of Algorithm (NWDAA), Tezpur University, India*, 2010, vol. 96.

[16] J. Polastre, J. Hill, and D. Culler, “Versatile low power media access for wireless sensor networks,” in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, 2004, pp. 95–107.

[17] M. Cakiroglu, A. T. Özcerit, H. Ekiz, and Ö. Çetin, “MAC Layer DoS Attacks in Wireless Sensor Networks: A Survey.,” in *ICWN*, 2006, pp. 45–48.

[18] D. R. Raymond and S. F. Midkiff, “Denial-of-service in wireless sensor networks: Attacks and defenses,” *Pervasive Comput. IEEE*, vol. 7, no. 1, pp. 74–81, 2008.

[19] S. Kaur, M. Ataullah, and M. Garg, “Security from Denial of Sleep Attack in Wireless Sensor Network,” *Int. J. Comput. Technol.*, vol. 4, no. 2b, pp. 419–425, 2013.

[20] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers,” *Commun. Surv. Tutor. IEEE*, vol. 13, no. 2, pp. 245–257, 2011.

[21] J. Deng, R. Han, and S. Mishra, “Defending against path-based DoS attacks in wireless sensor networks,” in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, 2005, pp. 89–96.

[22] S. Cheung and K. N. Levitt, “Protecting routing infrastructures from denial of service using cooperative intrusion detection,” in *Proceedings of the 1997 workshop on New security paradigms*, 1998, pp. 94–106.

[23] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, “Wireless sensor network security: A survey,” *Secur. Distrib. Grid Mob. Pervasive Comput.*, vol. 1, p. 367, 2007.

[24] M. Vidya and S. Reshmi, “Denial of Service Attacks in Wireless Sensor Networks.”

[25] V. C. Manju, S. L. Senthil Lekha, and M. Sasi Kumar, “Mechanisms for detecting and preventing denial of sleep attacks on wireless sensor networks,” in *Information & Communication Technologies (ICT), 2013 IEEE Conference on*, 2013, pp. 74–77.

[26] M. Brownfield, Y. Gupta, and N. Davis, “Wireless sensor network denial of sleep attack,” in *Information Assurance Workshop, 2005. IAW’05. Proceedings from the Sixth Annual IEEE SMC*, 2005, pp. 356–364.

[27] C. Chen, L. Hui, Q. Pei, L. Ning, and P. Qingquan, “An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks,” in *Information Assurance and Security, 2009. IAS’09. Fifth International Conference on*, 2009, vol. 2, pp. 446–449.

[28] T. Bhattasali and R. Chaki, “Lightweight hierarchical model for HWSNET,” *ArXiv Prepr. ArXiv11111933*, 2011.

[29] D. E. Boubiche and A. Bilami, “A Defense Strategy against Energy Exhausting Attacks in Wireless Sensor Networks,” *J. Emerg. Technol. Web Intell.*, vol. 5, no. 1, pp. 18–27, 2013.

[30] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, “The sleep deprivation attack in sensor networks: Analysis and methods of defense,” *Int. J. Distrib. Sens. Netw.*, vol. 2, no. 3, pp. 267–287, 2006.

[31] X. Lu, M. Spear, K. Levitt, N. S. Matloff, and S. F. Wu, “A synchronization attack and defense in energy-efficient listen-sleep slotted MAC protocols,” in *Emerging Security Information, Systems and Technologies, 2008. SECURWARE’08. Second International Conference on*, 2008, pp. 403–411.

[32] M. Wainis, K. Kabalan, and R. Dandeh, “Denial of Sleep Detection and Mitigation,” in *Proceedings of the 18th International Conference on Communications*, 2014.

[33] A. Boulis, “Castalia: A simulator for wireless sensor networks and body area networks,” *Natl. ICT Aust. Ltd Aust.*, 2009.

[34] A. Varga, “Omnet++ user manual version 4.2. 2,” *OpenSim Ltd Last Accessed*, vol. 6, p. 2012, 2011.