1-1-2016

Utilization Of A Large-Scale Wireless Sensor Network For Intrusion Detection And Border Surveillance

Mosad Helsan Alkhathami
Wayne State University,

UTILIZATION OF A LARGE-SCALE WIRELESS SENSOR NETWORK FOR INTRUSION DETECTION AND BORDER SURVEILLANCE

by

MOSAD ALKHATHAMI

DISSERTATION

Submitted to the Graduate School of

Wayne State University,

Detroit, Michigan

in partial fulfillment of the requirements for

the degree of

DOCTOR OF PHILOSOPHY

2016

MAJOR: ELECTRICAL AND COMPUTER ENGINEERING

Approved By:

_____

Advisor Date

_____

_____

_____

_____

DEDICATION

I dedicate my humble work to my mother, who raised me and still prays for me to be a successful person to both people and community, my father who encouraged and supported me to follow the right path, my wife who gave love, patience, and the support I needed and to all my family members and friends who gave me support and helped finish my dissertation.

ACKNOWLEDGEMENTS

I would like to thank all those who have helped to make this dissertation a success. First, I would like to thank God for giving me the opportunity to start studies and leading me to finish my PhD. Praise be to God, the Cherisher and Sustainer of the worlds. Several people gave me support to achieve this dissertation and I would like to use this opportunity to thank them all for their help and assistance. First of all, I would like to express my sincere appreciation to Professor Caisheng Wang, Professor Lubna Alazzawi, and Professor Ali Elkateeb who contributed tremendous time and guidance in my research. Appreciation is also due to Professor Mumtaz Usmen, and Professor Feng Lin for their constructive comments and valuable suggestions. Professor Hao Ying didn't hesitate to offer any kind of help and advice, Thanks a lot Professors.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1 Introduction

Wireless Sensor Networks (WSNs) have been widely considered as one of the most important technologies for last decade. WSNs provide distributed network and internet access to sensors, controls, and processors deeply embedded in equipment, facilities, and the environment. WSN has many applications such as; the monitoring of buildings, wildlife, pipelines, manufacturing, healthcare, environmental monitoring, and overall security. One of the most recent monitoring applications of WSNs is border control. These kinds of applications are becoming critical due to the increase of the risks of intrusion on borders. Border patrolling is vital to the security of a nation and its citizens. All countries' borders and ports are busy hubs, with tens of millions of cargo containers and hundreds of millions of legal travelers entering each year. This does not include the instances of illegal border traffic.

Border control pertains to measures adopted by a country to regulate and monitor its borders. It regulates the entry and exit of people and goods across a country's border. Border security is a primary concern of the national security agenda in this era of terrorist threat. The problem with protecting these boundaries is the distance covered and the intensity of labor in maintaining those borders. Conventional systems of border patrol consist of troops and checkpoints on international roads and ports. At these checkpoints, patrollers stop traffic, inspect cars, and curtail any illegal activity. In the border zones, patrols occur along predetermined routes and in set intervals, requiring extensive human resource to patrol even a small area [1,2]. Therefore, monitoring the border in real-time with accurate results and minimum human involvement requires several complementary technologies. A WSN can provide accurate detection and tracking of intrusion with minimal human participation. The role of WSNs in

border control focuses on information gathering from various types of sensors, such as seismic, and motion detectors. WSNs process these raw data and send an abstracted alarm, or aggregated data, to the command center which, in turn, takes the appropriate defensive action. Using this concept, we can identify a stranger or terrorists entering the country border. Figure 1 below shows a typical wireless sensor network.

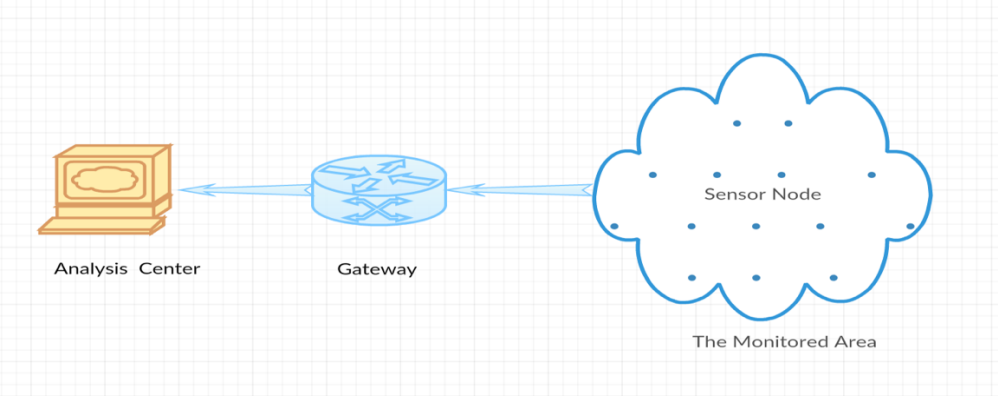

Figure 1: A Typical Wireless Sensor Network [11]

1.2 Problem Statement

Understanding an object's movement in an area such as country's border is a challenging scientific problem and a very fertile domain that needs to be addressed. Current border systems are unable to provide the required measure to deter illegal movements of goods, drugs, and humans from crossing into the country through stretches of the porous borders. Due to global risks nearby the borders area, our application will reduce and affect any unauthorized movement. Wireless Sensor Networks (WSNs) have been emerging in the last decade as powerful tools for connecting both the physical and digital worlds. WSNs can be used in several applications such as health monitoring, environmental surroundings, and border control. The goal of this thesis is to examine new application methods involved with the implementation of the types of sensor nodes used to detect and reduce intrusion risk in border surveillance. Surveillance application is becoming critical due to the risks affecting borders and the intrusion of borders.

1.3 Objective and Motivation

The objective of this thesis is to create a more adequate system for patrolling a country's borders and to provide solutions to the most addressed challenges by using wireless sensor nodes in different cases. The main objective is to develop a border security system using wireless sensor nodes for reducing the illegal immigrants and patrolling the borders from many challenges which require addressing before a practical realization occurs. My technical contribution is to provide solutions to these challenges in order to control suspect activities. This includes methods for securing large areas and deployment techniques suitable for large monitored areas of sensors to be used in border surveillance applications. For example, the design of new sensor nodes that will use less energy to accomplish a wider range. Adding a camera to each node will increase the detection rate of any an intruder in the border area. Also we proposed a solution for WSNs to extend the range of the sensor nodes for deploying the network in a large area, which will improve the system's performance and reduce the total cost. Moreover, my motivation in this thesis is to make this surveillance system application featured with object detection to track any type of activities on the border. Also, to prove whether automated systems, such as the WSN, are capable of providing adequate intrusion detection overall.

1.4 Literature Review

The Wireless Sensor Network (WSN) is an emerging technology that uses distributed sensors with communications infrastructure to monitor or record environmental conditions. WSN provides distributed network and Internet access to sensors, controls, and processors that are deeply embedded in equipment, facilities, and the environment. WSN has enormous applications in every field include disaster relief, agriculture, environment monitoring, medical applications, security, etc. One of the most recent monitoring applications of WSNs is the border control

application. This kind of application is becoming critical due to the increase of the intrusion risks on borders. Border control using wireless sensor network is one way to improve security measures [1]. It is a well-known fact that the border control is vital to the security of the nation and its citizens all over the world.

A Wireless Sensors Network (WSN) is made up of nodes, also known as motes, which work together to form a network. WSN provide disseminated network and Internet access to sensors, controls, and processors that are profoundly installed in gear, offices, and the surrounding environment. The WSN network is another monitoring and control ability for applications in transportation, fabricating, medicinal services, environmental monitoring, and wellbeing and security. WSN utilizes the MEMS (Micro-Electric Mechanical Systems) technology to generate smaller motes. Concerning the use of WSNs at the border, several works in the field of security surveillance have been accomplished. I found many studies relating their analyses to border control systems and I focused my research on how to help increase border control security.

Border patrol is currently based extensively on human involvement. The relative cost for the increasing number of personnel, as well as the diminishing accuracy through almost exclusively human surveillance, has required the involvement of high-tech devices. Among these, Unmanned Aerial Vehicles (UAVs) for aerial surveillance have recently been used to automatically detect and track illegal border crossing [2]. Other studies have been done so far in border control, using wireless sensor networks.

Study [3] found that many works have addressed border surveillance applications based on WSNs. Many solutions using WSNs have organized the network nodes as a line-sensor, where every movement going over a barrier of sensors is detected. In this case, sensor nodes' deployment should guarantee barrier coverage. Compared to full coverage, barrier coverage

based on a perfect linear deployment requires fewer sensor nodes and may experience radio disconnection due to sensor failure and depletion. Study [4], Liu et al, investigated the construction of the sensor barrier on long strip area of irregular shape when sensors are distributed according to Poisson point process. To ensure that trespassers cannot cross the border undetected, multiple disjointed sensor barriers will be created and distributed, covering large scale boundaries. A segmentation technique has been proposed to achieve continuous barrier coverage of the whole area.

In Study [5], researchers from the University of California proposed the deployment of WSN to help pursuers detect and track evaders. They made it into a game involving two teams and located of the opposing team members and caught them. They deployed a miniature test bed with 25 motes running TinyOS on a remote control.

In study [6], a researcher from The Ohio State University deployed 90 sensor motes with metal object detection capabilities. The main objective of their project was to detect and classify moving metallic objects, such as tanks and armed vehicles. The researchers considered a surveillance scenario of breaching a perimeter within a region. The system should have provided target detection, classification, and should have tracked for moving metallic and nonmetallic objects. They used an algorithm called Logical Grid Routing Protocol for the routing and the localization. For the implementation, they used 90 MICA motes equipped with magnetic sensor nodes.

In Study [7], researchers from Georgia Tech, King Saud University, and University of Nebraska have proposed a hybrid approach to achieve coherent border patrol applications. Integrating multimedia WSN, ground sensors with different underground sensing capabilities, they mobilized them. Border Sense provides several advantages compared with the traditional

WSN border control techniques.

In study [8], researchers from New Mexico Tech suggest the usage of neural networks along with wireless sensor network for border detection. The concept of using neural networks is to find a sample that describes an intrusion activity and to train neural networks to discover them. The proposed system uses a set of 32 MicaZ sensor nodes.

In study [9], researchers from Germany developed a sensor network prototype consisting of 200 nodes, which they called "iSense". This sensor was equipped with Passive Infrared (PIR) sensors covering a 500 m-long land strip. The objective was to ensure the integrity, authenticity, and availability of generated alarms. They developed two types of protocols, trespasser detection protocol and node failure detection protocol

Table 1: A Summary of Experimental Setup of Surveyed Literature.

Work	Platform	Sensors	Quantity	Functionality	Features
[5]	MICA	Photodiodes, temperature, magnetometers, accelerometers, Microphones, and sounders.	25	Help pursuer detect and track evaders	Interaction between sensor nodes and remote controlled vehicles
[6]	MICA	Magnetometers	90	Detection of perimeter breach	
[8]	MICAZ	Microphones and light sensors	32	Detection of intrusion activity within monitored area	Usage of artificial neural networks to detect and classify patterns
[9]	iSense	Passive Infra-Red	200	Intrusion detection within a covered passage area	Introducing a protocol for detecting trespasser and another protocol for checking the integrity of the network

CHAPTER 2: BORDER INTRUSION DETECTION SYSTEMS

2.1 Introduction

In the last decade, the usage of wireless sensor network (WSN) has become a powerful tool that connects both the physical and digital worlds. Currently, WSNs are applied in numerous applications such as the monitoring of buildings, wildlife and habitats, smart electrical grid control and border control. Among countries, border protection is a sensitive issue and measures are being taken to improve security at the borders. In addition to physical fencing, smart methods using technology are being employed to increase the alertness of security officials at the borders. Border control using wireless sensor network is one way to accomplish this task. The conventional border patrol systems are highly labor intensive, requiring constant human involvement, which also includes human error. However, in recent years, unmanned aerial vehicle, grouped sensors and camera equipped surveillance towers have been added as additional patrol measures [1]. Moreover, such systems suffer from problems ranging from false alarms to line of sight limitations. In addition, there is the lack of a coordination unit to provide accuracy to the system. Therefore, this study presents the simulation of border surveillance using WSN arrays as a method of surveillance and intrusion detection system to measure and solve the above referenced critical issues.

The wireless sensor network consists of spatially distributed autonomous and battery-powered sensors to monitor the physical or the environmental conditions; pressure, sound, temperature, vibration, motion, and working cooperatively to pass the data throw network to the base station [11]. The electronics measure ambient conditions relating to the environment surrounding the sensor and transforms them into an electric signal.

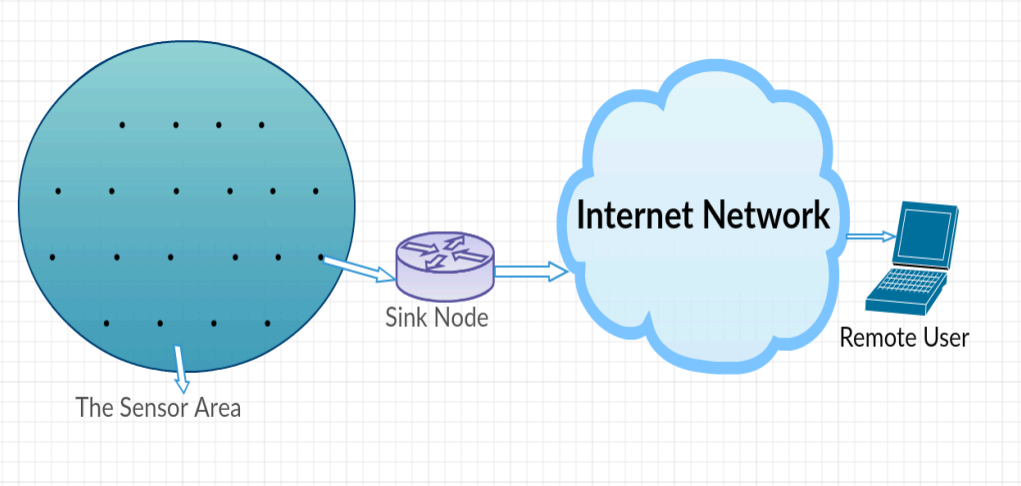

Figure 2: WSN System Architecture [10]

A large number of these sensors can be networked in many applications that require unattended operations. The WSN contains hundreds and/or thousands of sensor nodes. All of these sensors can interface or be directed to the base station for communicative purposes. Also, there are many sensors which allow sensing with greater accuracy over larger geographical regions [12].

By using the WSNs for the border control, it provides the following advantages:

- Ground-based sensors provide information on intruder movement even in cases of blockage by an obstacle.
- The camera and night vision sensors provide detailed and accurate information, as well as a wide detection range.
- The underground sensors guarantee support for above ground devices in cases where they cannot detect concealment.
- The mobile sensors can track and locate a detected intruder.
- The arrangement of the devices as a sensor network provides a connected and cooperative action approach that reports results to a remote location [13, 14].

2.2 Existing Border Patrol Techniques

The current system is based solely on personnel. This human-based system is creating an ever-increasing demand, higher costs, and less accuracy with each additional staff. The increasing demand for human workers led to the involvement of unmanned aerial surveillance vehicles to add mobility to cover extensive areas of the border [1]. However, even these vehicles can only cover a certain area for a given period, leaving some areas unmonitored. Moreover, the vagaries of weather decrease the capabilities of these vehicles.

The government introduced sensors connected with fiber optics that can measure pressure waves caused by intruders to complement the UAV systems. However, due to the dependability of the system on a single wire connection, any point of failure within the system affects very long distances [15]. In addition, the harsh environment along most borders makes them unsuitable, and the high deployment costs limit the practicality of the application. Compared to these wired sensors, ground sensor nodes tested on most military deployments are robust, thereby guaranteeing their usability. However, the limitations of the sensors, such as false detections, necessitate the addition of other sensor nodes that coordinate with the ground nodes to identify human intrusion accurately [16]. Moreover, visibility of these devices provides opportunities for damage by animals, vehicles, and intruders. Finally, the existing systems lack a coordination unit to improve accuracy.

2.3 Surveillance Scenarios

2.3.1 First Scenario (Maritime Borders):

The WSN has been implemented in marine surveillance and maritime border protection units for many years. The implementation demonstrated the detection of enemy and rouge vessels in maritime borders. The system detects enemy vessels by installing audio sensor nodes

in shallow water as shown below in Figure 3.

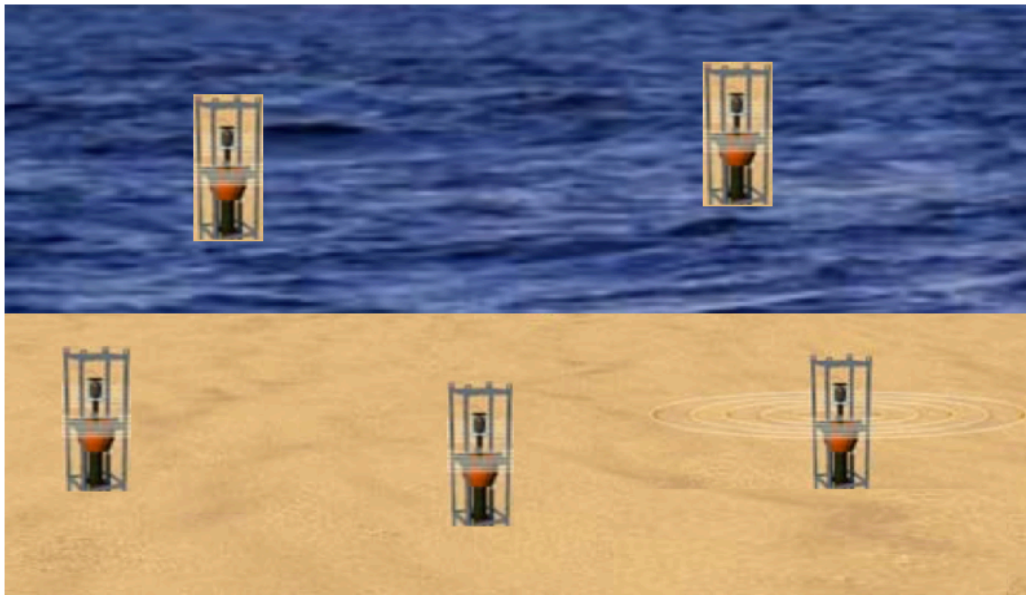

Figure 3: The Sensor Nodes in Water [1]

The ship intrusion detection system uses wireless sensor networks near harbor facilities. It exploits the V-shaped wave generated on the water surface by the movement of the ship [17,18]. The system consists of a three-axis accelerometer-measuring device with floats on the sea surface.

The deployment of sensors consists of a grid topology with predetermined locations. The sensor nodes are time synchronized prior to deployment, and have accelerometers to measure wave movements. The sensors provide readings that can detect the speed of a passing ship. Other nodes provide added motion and computational methods to sense the movement of crafts around the border, as shown in Figure 4.

Figure 4: Sensors with Buoys [1]

2.3.2 Second Scenario (Hybrid WSN Architecture For Border Patrol Systems):

This system is heterogeneous in architecture and consists of three different detection nodes (ground, underground and the mobile nodes). These nodes are used to provide different coverage capabilities.

2.3.3 Ground and Underground Sensors

The ground and underground nodes are resource-constrained, low-power scalar sensors performing simple tasks; taking vibration measurements and sending information to the data sink or processing hub. The underground sensors can either communicate with the ground sensors or with other underground sensors. Due to the complex underground channel characteristics, new physical layer propagation techniques are needed to realize the connections, such as: underground electromagnetic wave technologies [1,19, 20].

2.3.4 Mobile Sensors

The mobile sensor can host very powerful and reliable multimedia sensors. These sensors are resource-rich, high-power devices with higher processing ability and larger communication

range. As a result, these components are used as local processing hubs. The multimedia sensors are responsible for more complex tasks, such as: collecting the sensing reports from the ground/underground sensors, detecting possible intrusion according to the sensing reports, as well as the local image/video information. As a result, the false alarm rate of the ground/underground sensors can be significantly reduced. After the surveillance towers confirm intrusion detection, they report the detection results to the remote administrator and inform the mobile sensors the position of the intrusion for target tracking.

2.4 Deployment of Hybrid Wireless Sensor Network

In border patrol applications, the established monitoring network should cover a significantly large monitoring area. However, the sensing radius of a single sensor node is normally limited. Thus, a large number of sensor nodes are expected to fulfill the coverage requirement. Moreover, different types of sensor nodes provide different coverage capabilities. In addition, each sensor type is characterized by different costs, a sensing radius, and sensing accuracy. Thus, an optimal deployment strategy is required to determine the number and locations of sensor nodes with heterogeneous capabilities [22].

2.4.1 Deployment of The Ground and Underground Sensors:

As discussed, the sensing ranges of ground/underground sensors should cover a required area. A seismic sensor can detect moving heavy vehicles (such as tanks) from a distance of up to 500 m and walking humans from up to 50 m. To guarantee the detection of every type of intrusion, the sensing range of humans who are on foot is used in this scenario which is denoted as RUGS. For sufficient detection accuracy and system robustness, *k*-barrier coverage is required for the belt region in front of the border. The definition of *k*- barrier coverage denotes a region covered by a sensor crossing paths with another *k*- sensor through the coverage area. Both

underground and ground sensors are deployed at predetermined positions. To achieve optimal manual deployment of the *k*- barrier area of the belted region, k rows of sensors are deployed along the shortest path possible [23,24].

Although the manual deployment strategy is the most efficient, it is not applicable in this situation. In this scenario, aircrafts or vehicles are used in order to reduce the deployment cost of the system. This sub-section analyzes the requirements of the density and deployment area for the ground,and underground sensors in order to achieve *k*- barrier coverage. The sensors are distributed in the strip area of the border according to a Poisson process point with spatial density λ with *d* designating the length of the section in front of the border. The *w* indicates width, the sensing range is denoted by *r* and if the width is asymptotically greater than the computation of the area, $w = \Omega(logd)$, the probability of the sensor density λ in the *k*- barrier area reaches a certain value. To fulfill the random deployment scenario:

- The sensors should be deployed with a strip width larger than:

$$w = \Omega(logd) \tag{2.1}$$

- The deployment density of the sensors should be larger than λ,

$$\lambda = \frac{2(klog\ 6+2)}{(1-kR_{UGS}/w)R^2{}_{UGS}} \tag{2.2}$$

Where $k > 0$ is a constant determined by simulations [1,25,26].

2.4.2 Sensor Distance Strategy

As it has been mentioned above, the proposed sensor deployment models do not take into account the effects of natural environments. These models are based only on the sensor range *Rs*. Nonetheless, in real contexts, due to the radio effects, every sensor does not have a uniform range

distribution according to the propagation direction. Due to the radio effects we denote by *Rsi* the sensor range direction of *i* (the value of *i* varies is between 0 and 359). In Figure 5, the surface covered distance of the node sensor is shown:

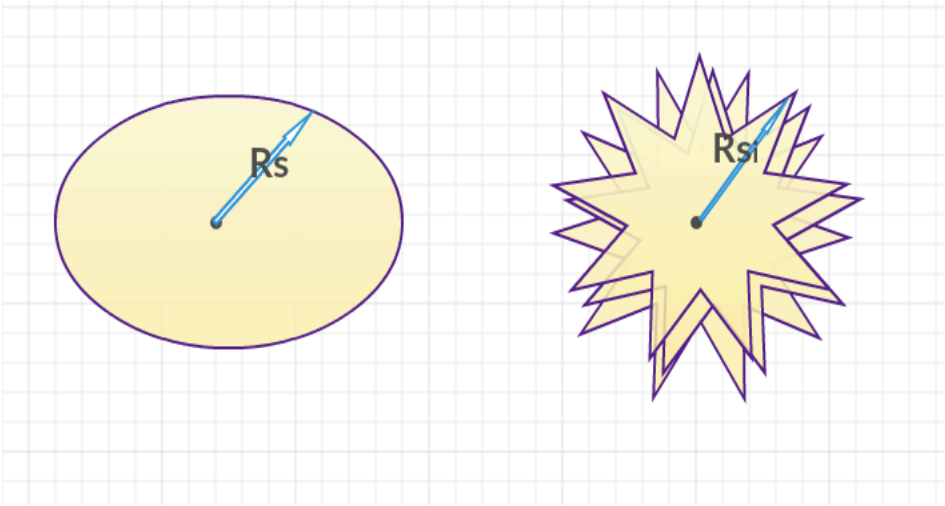

Figure 5: Sensor Distance Equation

When the distance of sensor *S* has a perfect circular form, *k* sensors should be present in the disc centered in *S* of the radius *Rs* +*Rt*. Where *Rs* is the sensor sensing range and *Rt* is the target radius, the *k*-coverage condition is fulfilled in the neighborhood of *S*. In other terms, the sensor density ρ_S is given by the following formula.

$$\rho_S = \frac{k}{\pi(Rs+Rt)^2} \tag{2.3}$$

From this equation, we adapt a result by considering the disc of radius *Rt* and expanding this area with the respective *Rs* in each direction which represent the coverage domain of the sensor [17].

2.4.3 Deployment of Towers Surveillance

The deployment positions of surveillance towers should be predetermined. The surveillance towers are deployed along the border line with 1-barrier coverage, due to the higher cost. Hence, the deployment problem of the surveillance towers can be viewed as a special case

of the *k*-barrier coverage where $k = 1$. Assuming that the sensing range of one surveillance tower is *R*tower.

Then, the minimum number of surveillance towers to cover a border with distance *d* is:

$$\text{The number of surveillance towers} = \frac{d}{2R_{tower}} \tag{2.4}$$

Also, it should be noted that since the sensing range of the surveillance towers is much larger than the range of the ground/underground sensors, the required number of the surveillance towers is much less than the number of the ground/underground sensors.

2.5 Operational Framework

Since the WSN consists of three different types of sensory equipment, the data provided must complement each other. A collaborative strategy is adopted to utilize the set of distributed sensors in order to provide accurate data to reduce the rate of false alarms. Upon sensing intrusion, the underground and ground sensors initiate a collaborative procedure. In the next phase, the imaging sensors from the towers trigger to improve the accuracy of the information. Thirdly, mobile aerial or ground devices move to the area of intrusion to provide actual confirmation of the intruder. It is only after verification of the information that the controllers dispatch the patrol personnel [1]. The collaboration consists of intruder detection cooperation, tracking, and detection oriented communication.

2.6 Challenges of the System

Any system hardware or software constraints must be addressed to achieve an effective and efficient operation of WSNs. The system architecture requires the use of cameras to validate the detections from the ground and underground sensors. Due to the restricted amount of towers and cameras, the system must reduce the number of detected events sent to the towers [25]. The

applied algorithm should adaptively provide and determine the detection threshold and determine what data is sent to the tower system, based on the number of ground and underground sensors involved. Although fixed tower cameras play a greater role in intrusion detection, they are unusable in cases of intruders with an obstructed view. Moreover, the camera has an expected range of cover that hinders their ability to focus on objects beyond their range. Mobile detectors are equipped with cameras to provide coverage in such situations to limit this problem [26,27,28]. Furthermore, one must enhance the coordination of the tower-to-tower cameras to include rotation phase shift.

CHAPTER 3: MODELS AND TECHNIQUES ANALYSIS OF BORDER INTRUSION DETECTION SYSTEMS

3.1 Introduction

This chapter will explore the model and techniques analysis of the border intrusion detection systems, including the wireless sensor detection method, a system that detects humans, animals, and objects which was I previously published [29]. An alarm is triggered when an intruder crosses a perimeter and the mechanism can specify the level of threat presented. The system needs to be able to differentiate between human and non-human intrusion. Low cost surveillance lacks that capability. The stratagems outlined here will demonstrate how shapes are used to train neural networks in the development of a system and how mathematical derivations are necessary to achieve proper intrusion detection. Borders of all nations in the whole world are at risk because they cannot be observed in their entirety during every portion of the day. Security is considered to be the primary concern of most of the countries in the world today. The increase in other related crime activities have raised the need to develop and implement intrusion detection system that can raise an alarm whenever there is danger. There are many applications of intrusion detection mechanisms.

Most of the intrusion detection systems have employed wireless sensor networks to facilitate the communication [30]. Wireless sensor networks provide not only easy implementation procedures, but also rapid alternatives for stacking the network. The coordinates of the sensor devices can follow a particular distribution pattern, according to the mode of deployment. The mode of distribution of the sensor devices relies on the nature of the perimeter under surveillance. The analysis of the distribution mode can be solved using three dimensional field models, including non-uniform deployment [31]. Conversely, deterministic deployment works for easily accessible fields. The system will be deployed to sensitive areas and root out signs of suspicious

activity. The model developed here makes use of wireless sensor networks to be controlled from a central point. The wireless sensor networks will track the detection signals obtained from each individual sensor. Architectural design, the Network Model for WSN, and specific types of sensors used in intrusion detection will be a focal point of this section of the thesis. This chapter will cover the intrusion detection system architectural design, different types of sensors that used intrusion detection. I will also focus on a Network Model for WSN and detection system techniques.

3.2 Intrusion Detection System Architectural Design

The design of a successful intrusion system will have to incorporate a given perimeter that will be defined by the monitoring system. Typical intrusion systems are normally developed to monitor a given perimeter, which in most cases, is defined by a border wall. The entire security perimeter of the border is coordinated from a central base station [32]. Any detection segment is sent to the central base station. It should be also mentioned the activity of such systems need support 24/7, allowing them to run continuously during their life cycles. This ensures constant monitoring of the defined region. Additionally, the deployment of the sensors should be made in such a way that the perimeter is entirely covered without any unattended spaces in between the nodes. This requires accurate and effective orientation and positioning of the sensor devices [33]. It can also be said that such a system requires a design where intruders are less likely to notice the location and placement of the sensors. There is also need for the sensor devices to communicate internally. This can only be accomplished through the use of line topology where the sensor devices are placed in a straight line of a semi-straight. This implies that routing will be very important in deriving the communication protocols for the sensors [34].

3.3 Intrusion Detection Sensors

The decision on the location and distribution of the sensors is contributes largely to the

success of the system. Human intrusion can be detected using many sensor modalities. These sensors do not emit a signal and sense how targets may modify it. Magnetic sensors detect that the trespasser, for instance a person carrying weapons, has material that is magnetically sensitive [35]. Ferromagnetic material generates a particular magnetic signature, which can be sensed by means of a magnetometer. Footsteps of humans and animals, birds flapping their wings, etc., correspondingly make sounds over and above the entity's voiced sound. Sensors designed to take measurements of sound are fundamentally hydrophones and microphones. Conversely, vibration-based motion sensors sense displacement, velocity, and acceleration using ismometers/geophones, velometers, and accelerometers, respectively. Additionally, in the case of heavy vehicles, there might be coupling between the acoustic noise and ground vibrations [36]. The acoustic waves travel at different speeds and their amplitudes decrease at different rates with distance or get absorbed at different rates. This sensitivity helps in distinguishing the type of intruding vehicle or other noise source. Table 2 shows a comparison between different types of sensors when used in detecting intrusions such as human beings, animals, or objects.

Table: 2 Comparison of the existing intrusion detection sensors [12]

Sensor	Low Power	Reliability	Cost
Infrared (Thermal)	Yes	Medium	Low
Ultrasound	No	High	High
Accelerometer (Seismic)	Yes	Low	High

Infrared, ultrasound and accelerometer are the most prevalent intrusion detection sensors. The infrared sensor has better movement detection properties than the accelerometer [37]. In addition, an infrared sensor requires less energy and has an analogue output signal that gives the direction of an object's movement. Ultrasound sensors can locate intruders using the high frequency acoustic waves reflected off of objects. The delay between the transmission of the ultrasound pulse and the echo return determines the object's distance. The accelerometer is a general low power dynamic sensor used to determine position, velocity, orientation, tilt, impact, vibration and shock.

3.4 Intrusion Detection Sensor Models

Intrusion Detection Sensor Models refer to a model of a real time intrusion detection system that is capable of detecting penetrations, break-ins and other forms of abuse. It helps determine distinct pattern that describe an abnormal or intrusion activity. The discovered distinct pattern is used to train the detection model to recognize abnormalities and intrusion. The models are built using low cost sensors that send sound and light data to help the model make an automated decision and report an abnormality or intrusion activity. Each network model monitors the local region and communicates through the wireless channels with the other nodes during a collaborative production of high-level representation on the state of the environment [38]. There are multiple types of sensor models that can be employed in an intrusion detection system. Different kinds of WSN can be utilized depending on the area to be covered and the type of space. Most of the outdoor applications employ microwaves, infrared, ultrasonic or radar sensor systems. The effectiveness of these models depend on the target to sensor distance, environment, propagation characteristics, size and motion pattern of the target, amount of energy emitted, and capability of the sensor [35]. Below are detailed descriptions about the most common detection sensor models.

3.4.1 Probabilistic Model

A Probabilistic Model is an accurate sensing model adopted in the analysis of WSN quality coverage. It takes into account the detection probabilities of the sending device, which decay with factors such as distance, hardware configuration and environmental conditions [39]. The Probabilistic model helps develop an intrusion detection system in which the sensors are deployed and distributed in a manner meeting the system requirements at minimum cost. Probabilistic sensor model relies on the threshold distance within which an intruder can be detected wirelessly. This implies that the threshold distance is governed by the perimeter of the space within which the detection should occur. In relation to Elfes' model, the detection probability can be described by such physical parameters of the sensors that are accommodated by the generic model parameters. If the target sensor distance is abbreviated *d,* the detection probability is an exponentially decaying function of *d.* The rate of decay is determined by two parameters; *y* and *B* which reflect the sensor characteristics [40]. The likeliness that a sensor would detect a target can be found using the following relation.

$$P_d = \begin{cases} 1 & if\ d \le d_1, \\ e^{-\lambda}\,(d-d_1)^{\beta} & If\ d_1 < d < d_2\ , \\ 0 & if\ d_2 \le d, \end{cases} \tag{3.1}$$

According to the formula above, the probabilistic sensing model sensor detects a target object with a probability of 1 if the distance between the target and the sensor *d* is below the threshold distance d_1. This is a simplified formula using *d* alone that can be deployed indoors where the light of sight is ensured. According to the following, conditions:

If $d_2 \le d$ then P_d= 0. However, the detection probability used, if the target object lies in a range of d_1<*d*< d_2, then an exponentially decaying function is deployed, using the parameters β and λ.

The parameters β, λ, d_1 and d_2 are adjusted based on the physical characteristics of a sensor. Different detection models can be illustrated using the following Figure 6. The Figure shows three common detection models that are governed by different technical parameters.

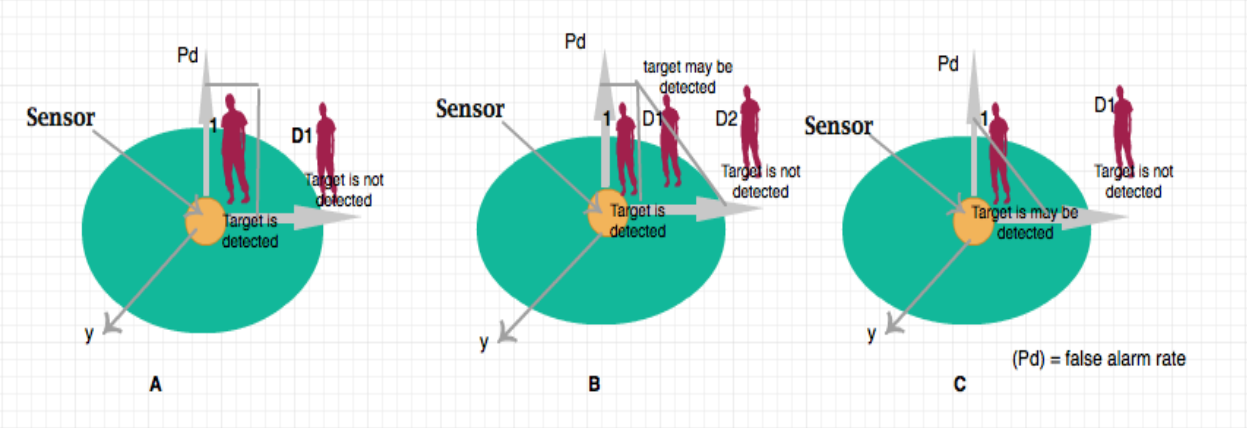

Figure 6 a) Binary Detector b) Elfes's Detector, c) Neyman-Pearson detector

The probabilistic model is founded on the concept that the sensors will operate in the presence of additive white Gaussian noise. It is also assumed that the signal will undergo path loss. There are two hypotheses that represent the presence and absence of a target setup. The NP detector serves to compute the likelihood ratio which is used to compare the detection results against a threshold false alarm constraint [41]. The formulation of NP is provided below where Gaussian noise and path loss are assumed.

$$pd=1-\Phi(\Phi^{-1}(1-\alpha)-\sqrt{\gamma(d)}) \tag{3.2}$$

The above relation incorporates both target distance and the cumulative distribution function of zero mean unit variance Gaussian random variable at the point x. If the standard bounds are introduced into the system, then the probability can be computed as calculated below. In the above formulation, $\gamma(d)$ is a signal to noise ratio at the sensor, when a target is at a distance d. *The*

$\Phi(x)$ represents the cumulative function of the zero mean and unit variance Gaussian variable at a point x. The equation uses the proportionality $\gamma(d) \sim d$. The formula below is derived using the standard bounds on $\Phi(x)$.

$$pd \approx A(\gamma(d), \eta, \alpha) exp\{\Phi^{-1}(1-\alpha) - \sqrt{\gamma(d)}\} \quad (3.3)$$

Where A(γ(d), η, α) is the signal to noise ratio level. It can be emphasized that the above model has demonstrated an exponentially decaying factors that is governed by the sensor-target distance [42].

$$S_r = \frac{A}{C_n}(x_{sys}, x_{env}) \quad (3.4)$$

where S_r is the successful rate of detection and C_n is the coverage of a sensor nodes, A is the size of the area you want to cover, while x_{sys} is the system parameter vector containing the information of system configuration such as an antenna, and motion sensor. The x_{env} is the environment parameter vector containing the information weather and geographic conditions. The probabilistic model of a sensor node in detecting various subjects such as (human beings, animals, vehicles, and plans are in table 3 represent the combination of parameters considered and the present of the detection. The successful rate of this system could detect up to 91%, also in Figure 7 shows the rate if success versus the combination considered.

Table 3 Combination of Parameters Considered

Variable	Subject	Configuration	Sensor Nodes	nvironmental Condition	Distance (m)	Detection Accuracy
1	Human	Camera	100	Cold/Snow	5	
2	Animal	No Camera	200	Normal	25	
3	Vehicle	Typical Antenna	300	Hot	50	
4	Plane	Enhanced Antenna	400	Rainy	75	
5		Motion Detector	500	Dusty	125	
						0.91

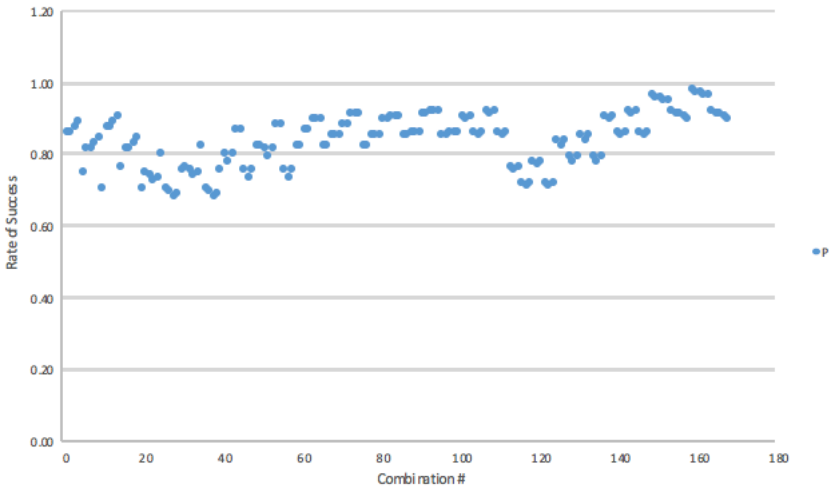

Figure 7 Rate of Success Versus the Combination Considered

$$A = td_a.2R + \pi R^2 \tag{3.5}$$

Based on equation 3.5 we could know the active area of random sensing schedules of all nodes which have the same sensing period and active. We consider object movements from left to right on *x* -axis. Where *A* is the active area of the object, and td_a is travel distance. *2R* is the rectangle area width, and the two half disks with radius *R*.

3.4.2 Exposure-Based Sensor Model

This model is based on the fact that the received energy level provides a clue on the observability. The expected level of observability within the monitored space is referred to as exposure. The total amount of energy that is received by the sensors at different points on the breath path is normally defined as the path of exposure [43]. The level of detection energy can be expressed as shown below.

$$S_i(d) = \frac{k}{d^k} \tag{3.6}$$

Where, S_i *(d)* represents the signal energy of the target in the above formulation. The signal energy for the target is a measure from an *i*th sensor, and the distance between the target and the sensor is *d*. Where *K* is barrier coverage or the decay factor of the energy and d^k is detection energy. *k* is a

nonnegative constant that satisfies the condition k,$2<k<5$ [44]. A multiplicative factor can be included in the system to cater for the effects of obstacles and other sources of errors. The most essential designing factor is the fusion of exposure levels where different types of sensor devices are deployed [45]. Any target can be detected using the preceding sensing and exposure model and knowing the threshold energy. Finally, the advantage of exposure-based coverage assessment is the inclusion of a practical object detection probability that is based on signal processing, signal distortion, as applicable to specific sensor types.

3.4.3 Shape Based Intrusion Detection Models

There is a need for an intrusion detection system to ascertain the identity of the intruder. The system is required to distinguish between animal intrusion, human intrusion and any other object that may be used to intrude any object. Since this chapter is meant for human and object intrusion detection mechanism, the algorithm developed will focus on the human and other will focus on object detection mechanisms. Most of the low-cost surveillance systems lack the capability of discerning the intrusion of animals from humans. The shape of a human being and the intruding objects are simplified through a removal of the redundant points that connect short and straight line segments. The technique can be employed to search for best-matched contour within the database to distinguish humans from other objects using different viewing angles and distances [46].

This methodology of differential motion analysis detects the scene change within the perimeter of the region being surveyed. The object contour is extracted by determining the difference between a reference and the test image. The differential motion analysis method eliminates illumination variations through subtraction. The polygon approximation technique integrated into the system to extract contour in order to remove the noise and as such eliminate

redundant data points. This makes the shape to be represented using a fixed number of points. The shapes are described in a way that making them invariant to rotation. Scaling and translation use shape representation techniques such as turn angle and bend angle function. The collected shape features are used to measure similarities between the test contour and the contents of the database.

Through training, the intrusion detection system beneath this model contains a database composed of the different shape features of possible objects. The shape features include images taken from different times, locations, angles and distances. More recent shape features of a target object are calculated from the contour and compared to a reference in the system database. The target and reference shape are matched based either on a similarity or a dissimilarity measure. The best shape match for a target object is one with a high similarity measure or a minimum dissimilarity measure with a reference shape feature. Matching determines the intrusion object. Figure 8 below shows the basic steps used to extract human shapes.

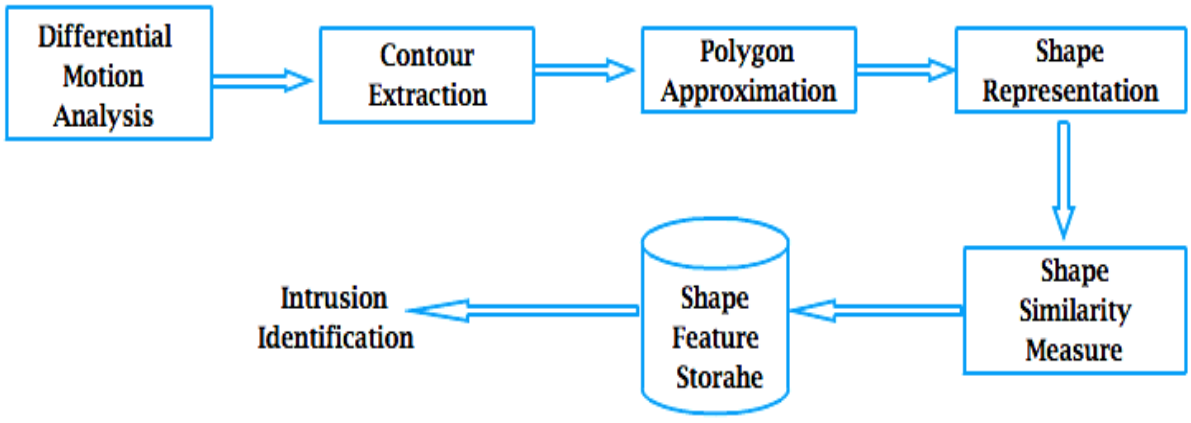

Figure 8: Basic steps used to extract shape of human being

3.4.4 Barrier Coverage Intrusion Detection Models

Any kind of movement or crossing could be detected by the barrier coverage model. The purpose of barrier coverage is to detect intruders who attempt to cross from one side to the other

side of the border area that you want to detect. Barrier coverage model is a technique whose goal is to minimize the probability of an undetected intrusion through a sensor network or a barrier. In some situations, it is not necessary for detecting both direction of crossing the belt. Therefore, barrier coverage is not suitable model since it may not differentiate the illegal intruders from the legal [47]. The barrier coverage can be considered as the coverage with the goal of minimizing the probability of undetected penetration through the barrier. The barrier coverage problem start and end points of the path are selected from bottom and top of the area. The selection of the path also depends on the objective.

3.5 Intrusion Detection System Techniques

Intrusion involves an activity that violates the security policy of a protected area or system, while intrusion detection is the process of identifying an intrusion. Monitoring illegal movement across a border is a challenging task. WSN is an emerging technology that is expected to provide new ways of energy and cost efficient border intrusion detection. An intrusion detection system technique is usually deployed as a line of defense to protect a border. Intrusion detection system techniques include the cost effective techniques deployed for monitoring critical applications ranging from border monitoring to industrial control. Intrusion detection techniques provide accurate detection and tracking of intrusion with minimal human intervention [48]. Some of the existing intrusion detection techniques include Dynamic Mechanical Analysis, Infrared Intrusion, Neural Network, and Image Processing Detection System.

3.5.1 Dynamic Mechanical Analysis Detection System

The Dynamic Mechanical Analysis (DMA) system is considered to be a powerful technique that can be used to process the shape of a human being. The processing assists in distinguishing the shape of human beings from animals. It also helps the system to differentiate

humans from other objects. Using the PIR will show the human body temperature is 36 degrees more than the animal which will show the type of intruders. Also by the height, If the intrude is below 1m this could be an animals, and if it is above 1m this will be human. The following expression can compute the data point reduction [46].

$$K(s_1, s_2) = \frac{|\beta(s_1,s_2)-180|l(s_1)l(s_2)}{l(s_1)+l(s_2)} \tag{3.7}$$

The above formula is a curve evolution technique comparing the relevance measures of the vertices on the contours. The relevance measure for the curve evolution method is *K*. *K* has been modified to eliminate redundant points while maintaining the significance of the contours. β is the turn angle on the vertex between the line segments s_1 and s_2. $l(s_1)$ and $l(s_2)$, representing the normalized lengths from a vertex to the two adjacent vertices. Applying the formula of the modified curve evolution reduces short and straight line segments, providing scant information about the overall shape of an object. Shape similarity is measured easily, as a fixed number of data points will preserve detail shape information, unlike other techniques, which may lose data points containing critical shape information. The any given bend angle function; the similarity of the two shapes can be established through Fourier expansion as shown below.

$$\Theta(1) = \mu_0 + \sum_{n=1}^{\infty}(a_n\ cos\ nl + b_n\ sin\ nl) \tag{3.8}$$

The Fourier descriptors derived above is used to measure the similarity between two shapes [49]. an and bn are the coefficients for each frequency component. The below formulation shows how the coefficients can be derived considering that $\Theta(1)$ is a step function.

$$\mu_0 = -\pi - \frac{1}{L}\sum_{k-1}^{m}\lambda_k\,\theta_k \tag{3.9}$$

$$a_n = -\frac{1}{n\pi}\sum_{k=1}^{m}\theta_k\,sin\frac{2\pi n\lambda_k}{L} \qquad b_n = \frac{1}{n\pi}\sum_{k=1}^{m}\theta_k\,cos\frac{2\pi n\lambda_k}{L} \tag{3.10}$$

$$Where\ \lambda_k = \sum_{i=1}^{k}1_i \qquad and\ \ L = \sum_{i=1}^{m}1_i\ = the\ \ total\ lenght \tag{3.11}$$

3.5.2 Infrared Intrusion Detection System

Infrared is one of the techniques that can be employed to detect presence of intruders. In this system valuable information can be obtained from the human such as the location and the other necessary signal that will confirm presence of a human being. The system is known to make use of the rate of the heartbeat to detect human beings. The system makes use of infrared sensor that comprise of a light emitting diode which is adjacent to a phototransistor. The infrared sensor is used to measure the distance between the detector and the intruder. The infrared sensor consists of infrared LED and a pair of silicon phototransistors. The high intensity and long range infrared distance sensors can be used to determine the presence of an intruder accurately and precisely. [50]

This technology makes use of infrared light that is absorbed well in blood and weakly in human tissue. As such, if light that is reflected back from the skin of an intruder on account of blood passages is captured by the detector. The reflected light consists of intensity variations that occur as a result of variations in the blood volume in the tissue which give rise to variations in output voltages of the detector. The voltage variations are used to detect the heart rate. When the voltage variations are found to match those of the heart rate, positive results of the detection are assumed. [51]

3.5.3 Neural Network Intrusion Detection System

A neural network is composed of computational units jointly implementing complex mapping functions, focusing on the face of the subject. Two main stages are involved in the detection process; application of a set of neural network-based filters to the image and the arbitration of filter outputs. High resolution cameras have the ability to capture live images. The system then processes those images. They are then introduced to a set of filters which search for the location plane containing the face. Once the face has been located, the arbitrator merges

detections from individual filters, eliminating any overlap. The initial component receives the image at a specified pixel determined by the filter. The filter processes the image and gives an output, signifying the presence or absence of a face.

The filter is normally applied at every location of the image in order to detect the face. Faces that may be larger than the window size are normally subsampled by a factor of 1.2 and the filter applied to each scale. The processed window is passed through a system of neural networks which will determine the presence of the face. The neural network is normally trained prior to the detection on the general features of a face. This implies that neural networks are relied upon in confirming the presence of a face and therefore the presence of an intruder. It should also be noted that a minimum threshold on the number of detections is set in order to eliminate false detections [52]. The purpose of using neural network is to discover patterns that describe an intrusion activity and train the neural network to discover them. The neural network system uses a set of 32 MicaZ sensor nodes. The nodes distributed along a perimeter to detect single and group intrusion.

3.5.4 Image Processing Detection System

An "Image Processing Detection System" is a method for utilizing images to determine whether there is a presence of trespasser/human intruder or not. Image processing based human intruder location framework is broadly supported by numerous professionals when contrasted with robber alert frameworks and radar-based human intruder recognition, principally because of these four reasons:

a. It helps catch pictures. The connected security camera is an extraordinary device to catch a photo of the robber when they are attempting to break into a precluded domain.
b. More probability of the intruders being captured. Control rooms have the capacity to view the photos from the cameras to distinguish intruders for easier arrests.

c. Security cameras are extraordinary aversion instruments. Robbers are known for dodging region that has great security, particularly those fitted with security cameras.

d. Security cameras can secure defenseless ranges. At the point when control is inside the foundation's edge and needs to see what is going on outside of the adjacent building for security, security cameras are the most ideal approach for this objective securely.

In general, the image processing-based trespasser detection system could be a divided to two main categories[53].

The first is night vision/IR spectrum image processing-based human intruder detection system which can divide to digital video surveillance and analog video surveillance. The second one is vision spectrum image processing-based human intruder detection system which can known as type of video recording system applying digital technology.

3.6 Recommended Technique for Intrusion Detection System

Several techniques exist that are associated with intrusion detection systems. The DMA is considered to be the most powerful technique that can be used to process the shape of a human being. This process helps to distinguish the human beings from animals. It also helps the system to differentiate humans from other objects. Using DMA on the fact that is has capability of discerning human beings from animals and vehicles. The use of DMA is considered to be cost effective. It does not involve a lot of costs and time of installation. DMA is also known to consume less amount of energy when compared to other methods that were considered in the chapter. Its processing time is also considered to be the least in considerations to other techniques mentioned in this chapter. The devices use simple electronic motion detection sensors that monitor motion and locate objects within a secured perimeter.

DMA is the most suitable and easily scalable. It extracts the contours of an intruding object

for shape feature analysis. Contour points are simplified by removing the redundant points connecting short and straight line segments. Its intrusion detection techniques were developed to best match contour features in a database that targets objects expertly. The matching process of a target and database shape feature are accomplished from different angles and distances. Barrier and sensor coverage are important in WSN. Communication issues and breach path problems are elements equally as essential and will be included and analyzed in future studies.

CHAPTER 4: LARGE SCALE BORDER SYSTEMS MODELING AND SIMULATION WITH OPNET

4.1 Introduction

Security along national borders is becoming more critical daily. Using the security approach, sensor nodes are deployed strategically on parts or the entirety of the border depending on potential intrusion or common routes to collect sensors' information through a network of communicating nodes on a controlled radio channel. These radio signals are used to connect with the environment components that generate variable events, such as movement. The Wireless Sensor Network's (WSN) function is to facilitate information exchange between the sensor nodes and an application platform [54]. This system is capable of detecting a security breach and tracking the direction of the trespasser to a marked location, which enforcement officials in border surveillance can then target. It would, therefore, be a real-time, all-time border security control system that could render a country and its cities safer.

In addition, WSN consists of both hardware and software components. The hardware components include a power source, a sensor, a communication element (i.e. a radio transceiver), a location finding system, a memory device and a processor. The software components include a sensor driver, communication drivers, communication processors, middleware, and basic applications. WSN combine micro-sensor technology, low power signal processing, low power computation, and low power, minimal effort wireless networking capacity in a compact system. Late advances in integrated circuit technology have empowered construction of much more proficient sensors, radios, and processors with ease, permitting large scale manufacturing of refined systems that connection the physical world to networks. Scales will range from local to worldwide, with applications including pharmaceutical, security, processing plant mechanization, environmental monitoring and condition-based maintenance. The WSN is composed of agents that

are used to generate events of interests for the rest of the nodes. In many cases, the agent can cause a variation regarding the physical magnitude that propagates through the entire environment and stimulates the sensors [55]. The mote collects data, processes the data and finally packages it. Afterward, it communicates with other motes using radio transmitters and receivers. Therefore, WSN operates through the communication that takes place between motes.

OPNET will be an essential tool in the establishment of such networks. It will enable the implementing team to explore the limits of the network and its operation. Simulation of the network will emulate the real network and, therefore, provide a clear understanding of the real network. OPNET software is a graphical tool that has the capability of simulating the network. The OPNET GUI representation enhances the functional effectiveness of the WSN by allowing simulation of various border security scenarios that a country could face. The graphical representation can then be used to design the best deployment strategy of the WSN and recommend better configurations of the network.

4.2 Large Scale of Border Security System

The border security system is a system used in the maintenance of security along the borders. Border surveillance is one of the very essential parts of a nation's security. WSN are used as border security systems since they have sensors that can monitor physical activities at the border and report trespassers. Sensors are effective in monitoring the border because border security requires continuous, reliable monitoring at all times, and WSN rarely raise false alarms. The placement of sensor nodes, the intruder detection rate, and sensor node power consumption influence the whole system performance significantly. It can be stated that these features play a critical role in making sure that all issues to do with the management are developed to make sure that all things to do with the management of security are well addressed using the WSN

technologies. The border security system that uses the WSN has the advantage of locating accurately where motion was detected. The security system, therefore, will give real time information on the movement along the border. Over the previous years, wireless sensor network (WSN) in border surveillance and their application in a various situation have been looked into around the world. A standout amongst the most interesting situations for utilization of WSNs related to its utilization in the monitoring systems territories [56]. WSN is a one of a kind system that can utilized for the surveillance of critical regions, for example, borders, etc. Border patrol systems and techniques have, as of late, increased interest to address the concerns about national security. With the development of distinctive electronic patrol techniques, this association diminished that inclusion. Subsequently, Unmanned Aerial Vehicles (UAVs) permits to minimize human association in border patrol because of their expansive scope of ranges and high versatility of those gadgets [57]. UAVs are being utilized to detect naturally and track illegal border crossing. With the assistance of UAV critical human resources can be diverted to choice administration exercises and information processing taking into account the information from these gadgets.

4.3 Wireless Sensor Node In Border Surveillance

The performance surveillance wireless sensor network is usually generally measured using defection capabilities that exist at any given monitored zone. The ability is usually affected by various metrics and the sensor count. The sensor range and the area can also be significantly affected. This aspect of WSN, in border surveillance, as in most WSN applications, concentrates on information gathering from different types of sensors; seismic, heat detecting cameras, and motion detectors [58]. Some exceptional WSN process this information and send a disconnected alert or amassed information to the command focus, which, makes the appropriate protective move. Numerous specialists from diverse associations have recommended answers for border

surveillance problems. A wireless sensor node is a famous arrangement, yet it is troublesome to run a main supply to the sensor node. Considering that wireless sensor node frequently is put in a difficult locales, consistent battery changing can be an expensive and inconvenient problem [59]. An important angle in the arrangement of a wireless sensor node is ensuring that there is constantly sufficient energy accessible to control the system. The following, Figure 9, describes the way general sensor detection works.

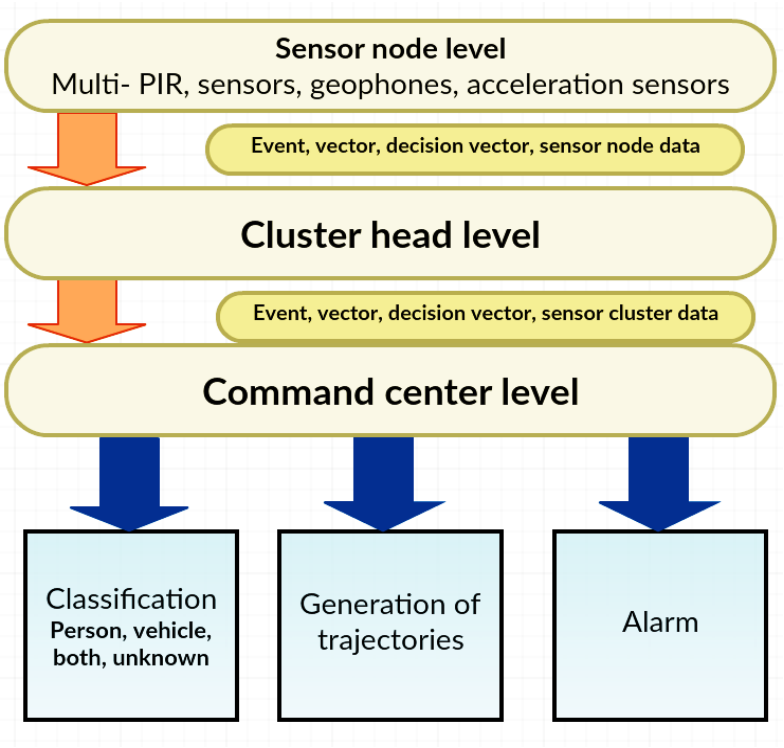

Figure 9: Sensor detection Flow Chart

4.3.1 Types of Sensor Nodes

A sensor node can defined as many components within a network that collect data and distribute it to each other, via network. Sensor nodes, also known as motes, are said to be the sensor in the network which is capable of performing some level of processing. Motes are also able to collect sensory information and establish communication with other connected nodes in the network. Some of these nodes are ANT, WiSense and AquisGrain. Other types of sensor nodes

are normal, advanced and super nodes. These sensor nodes perform the functions that their names suggest of each type of sensor node. Therefore, performance increases from normal to advance and subsequently super. Other sensor nodes are classified according to the work they perform such as basic sensor node (passes data to another node), data node (stored data), and aggregator nodes (collect data).

The sensor node is divided into three layers. The first is the lowest layer consists of hardware sensor. Secondly, the next layer has the hardware drivers and sensor drivers. Finally, the upper layer hosts the middleware. There is a buffer layer between the second lowest and the upper layer, which handles the processes for that specific node operation. Consequently, the sensor nodes are composed of communication devices, memory, power supply, controller and also sensor actuators that are used in making sure that the sensor node can operate effectively. The role of the controller is to make sure that communication protocols are working. The communication device is used to establish the correct communication device used, the memory used for storage [60]. The Figure 10 below shows a various components of a sensor node.

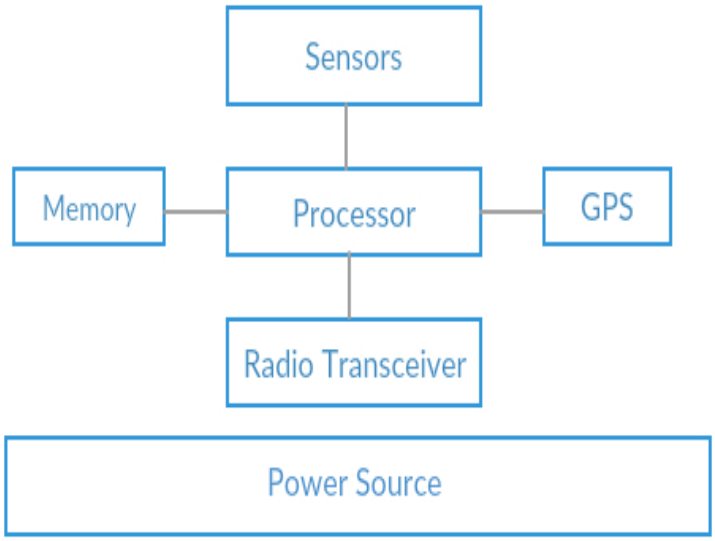

Figure 10: Digram of the sensor nodes

4.3.2 Deployment of Sensor Nodes

Since the border requires to be monitored at every location, thereby making it significantly difficult to carry out an intrusion, multiple sensors can be deployed to simultaneously monitor given points within the border, guaranteeing that the failure of one node would not necessarily compromise the network's integrity. A WSN deployment can usually be categorized either as a dense deployment or a sparse deployment depending on the number of nodes that are required to suitably cover the network. Sensory nodes can be installed in the forest to detect fire as soon as it starts. In this case, the deployment of the land monitoring and detection radars. The wideband wireless communication modules are used by the border surveillance system to pass the signal from one point to another [61]. Monitoring of the system and sensors is done at a central point where all signals are received. The monitoring is made possible by software and visual tools such as LCD monitors that display digital maps of the area for the operators.

4.4 Performance Evaluations of WSN In Border Surveillance

The performance of the WSN structure include the power consumption of the nodes and the topology configuration of the structure of the network. The topology comes into play since the number of nodes connected to the network and the gateway determines the way in which the network performs. It is essential to follow strict guideline when the construction of the network is being done. Therefore, have to know the number of nodes that will be used in a non-router network and the number of nodes when the routers are being used in the network. Without a router, it is advisable to use no more than eight nodes for one gateway and up to 36 nodes when using router nodes.

In the evaluation of the performance of the network, OPNET comes in handy since the working of the network will be viewed in the graphical presentation. Sensor sensitivity must be

optimized in order to maximize detection range. Due to the central limits of background clamor, a maximum detection range exists for any sensor. Accordingly, it is critical to get the best sensitivity and to create compact sensors that may be generally dispersed. Plainly, micro electromechanical systems (MEMS) is the technology that provides a perfect path for implementation of these very dispersed systems [62]. WSN sensor integration relies on structures that are flip-chip attached to a low temperature, co-let go ceramic substrate. This sensor-substrate, also known as sensors rate, is a stage for backing of interface, sign processing and communication circuits.

4.5 OPNET AND WSN DESIGN

4.5.1 Network Simulation

The innovation of powerful computer systems made the simulation modelling of complex networks possible. There are generally two methods of communication networks simulation. The first method is called analytical modelling and the second one is called machine based simulation. Analytical modelling model is the network by the set of mathematical equations. The disadvantage of this modelling is too much simplicity and it cannot model the dynamic nature of the network. To model the complexity of the network behaviour, the discreet even simulation (DES) is the most famous approach in research and development. DES is event based driven and provides very close to the reality results. The event can be considered as generating a single packet and the simulator model the behaviour of the packet and impact on the network performance. OPNET is one of the most accurate and widely used DES simulator [63].

4.5.2 OPNET Simulator

Optimized Network Engineering Tool (OPNET) runs a DES engine for modelling the communication networks and analyzes the results for various performance parameters. It supports a large set of network environments from a simple LAN network to satellite communication.

OPNET comes with rich tools and models which facilitate researchers with the standardize environment to effectively study the effect of network behaviours before deployment in the real world. The most important features of OPNET are given below.

- Modeling and simulation feature of OPNET give the user a frame work to first built the model, execute it and then analyze the results as shown in the Figure 11.
- OPNET has hierarchical structure, each layer of an OPNET has its own set of parameters and characteristics
- OPNET comes with rich models of library with all world leading network hardware manufacturer devices and all available protocols and also provide programming interface to develop new protocols for the researchers.

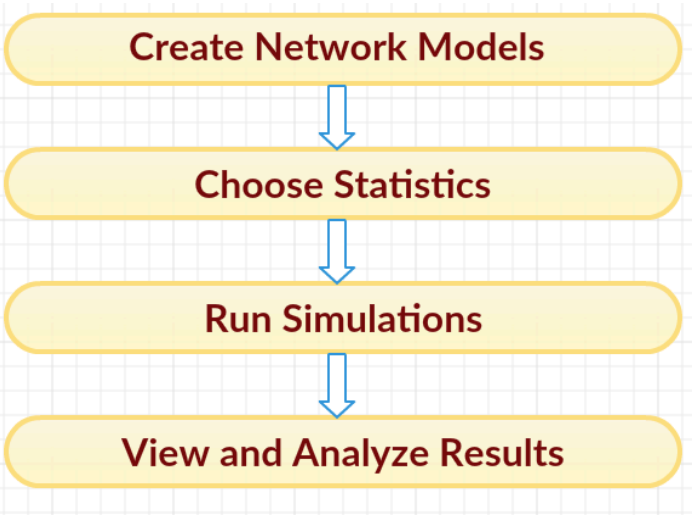

Figure 11: Simulation Steps of OPNET

4.5.3 OPNET Structuring

OPNET is structured on the sets of editor in hierarchical manner. These models work from low level programming language to higher level GUI. The model in each level can be access by its upper level with the basic editors in OPNET [64].

4.5.4 Network Editor

The top most editor of the system is the network editor where the actual network architecture is deployed. Providing GUI and consists of routers, switches etc. It can model a complex network in term of sub network which can be office network, enterprise network or the network through specific area of the world. All the low level models can be access from project editor. A project editor is shown in the Figure 12.

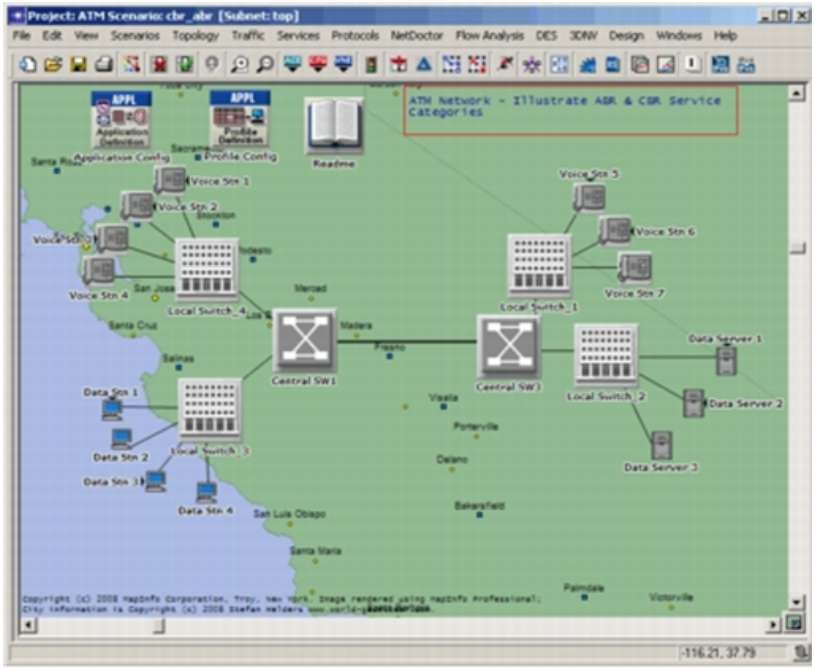

Figure 12: network editor

4.5.5 Node Editor

Node editors specify the behavior of each node inside the project editor. The behavior is defined in term of different modules. Each module specifies a unique behavior of the node like data creation, storage, transmission etc. The node model is shown in the Figure 13.

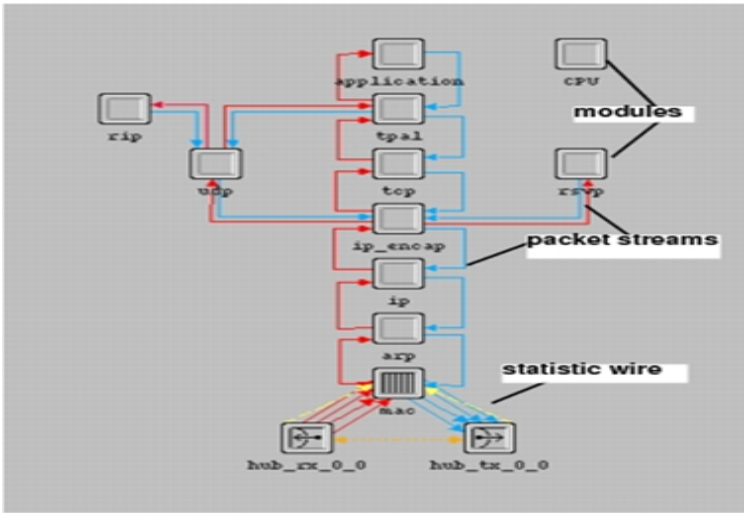

Figure 13: node editor

4.5.6 Process Model Editor

The process model provides the editor to create different processes which runs by the node created in the node editor. OPNET DES engine works on finite state machine (FSM) which is developed in the process model. The operation runs in each state are control by C and C++ as shown in the Figure 14.

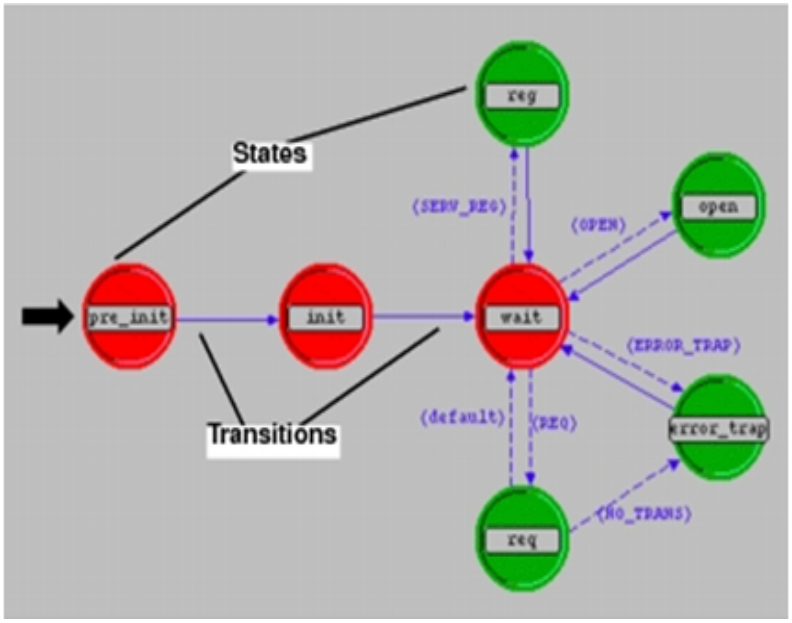

Figure 14: process model editor

4.5.7 Link Model Editor

Link model specify different attributes to link or to develop a new link model with specific defined parameters. The link editor model is shown in the Figure 15.

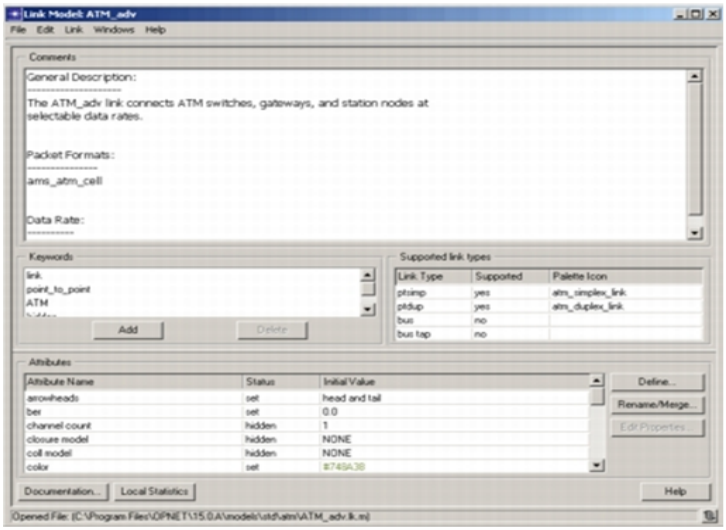

Figure 15: link model editor

4.5.8 Path Editor

New path route can be defined using this editor. All protocols which are using virtual circuits or logical circuits can use paths to route traffic. The path editor is shown in the Figure 16.

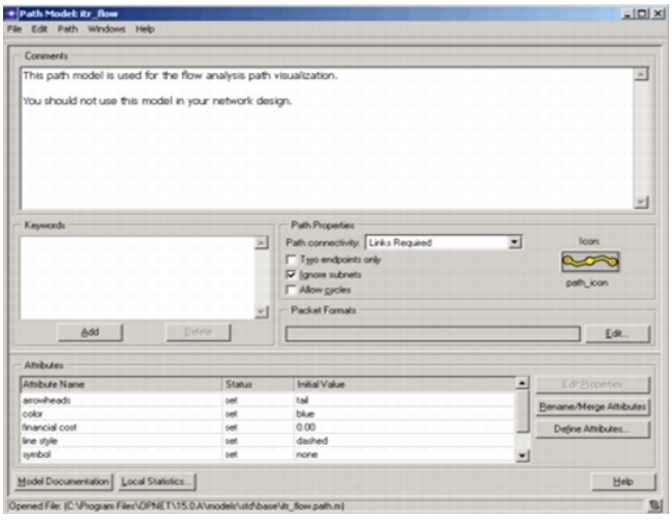

Figure 16: path editor

4.5.9 Probe Editor

Probe editors specify an interface to collect additional statistics as defined in the network editor. Various types of statistics can be defined using probe editor which are link statistics, local statistics, global statistics and different other animation statistics. The probe editor is shown in the following Figure 17.

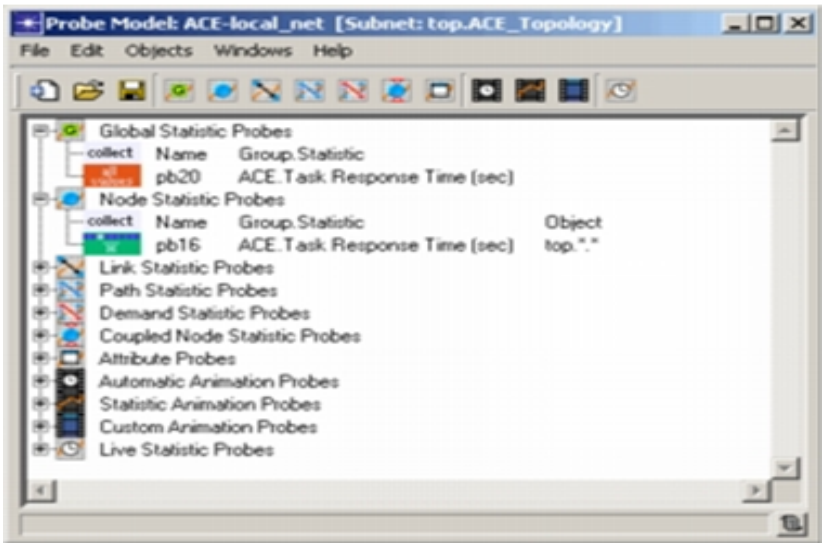

Figure 17: path editor

4.5.10 Network Design

There are two deployment methods in the OPNET. The first method is to use OPNET providing utility for deploying the nodes in the network editor, but the supported option for that case is limited. The approach that is followed here is use the manual method of deploying nodes. The first step is to start placing the nodes is to assign the area of deployment. The area that is chosen for this simulation is around 2x2km for the clustered tree and mesh topologies. OPNET does not support clustered trees by default. The open source clustered tree model is available from open-ZigBee [65]. The model is integrated inside the OPNET to enable the clustered routing

features. After placement of the coordinator, routers and end nodes in the network editor, the design looks like as shown in the Figure 18.

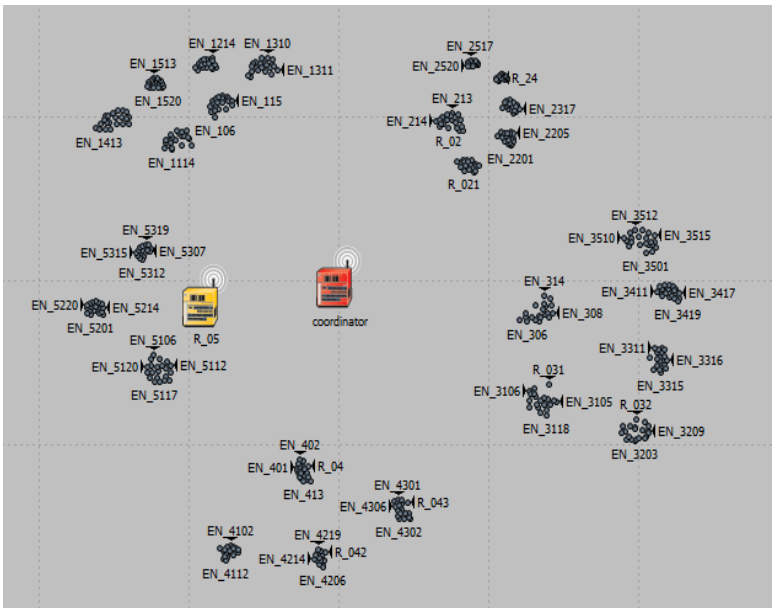

Figure 18: Custer Tree Topology

The mesh routing is supported in the default ZigBee libraries. The same manual placement procedure is followed for mesh routing as well. The nodes are placed in the network editor as shown in the Figure 19.

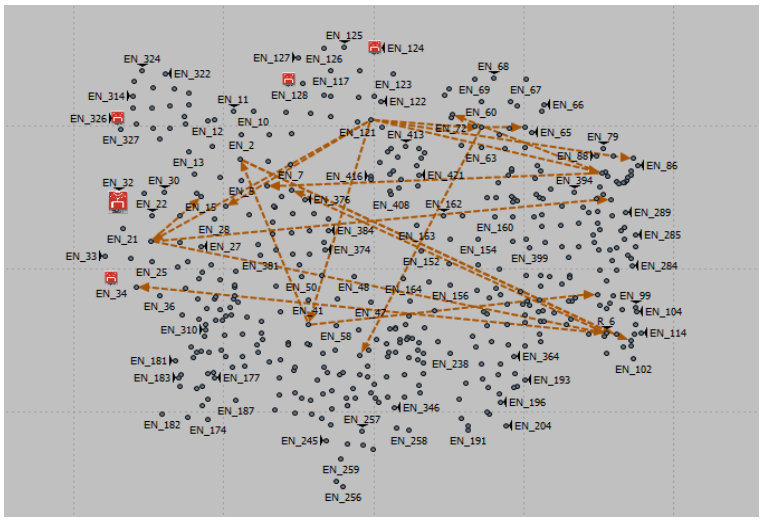

Figure 19: Mesh Topology

4.5.11 Cluster Tree Topology

The cluster tree topology needs proper planning before deployment because of the cluster tree addressing requirements. The network behaves in the hierarchical manner, expanding from the coordinator to the tier 1 routers at depth 1 and tier 2 routers at depth 2 and the corresponding nodes. The planning has been made by keeping the maximum number (500) of nodes in the mind [66]. The following important consideration have been made before deploying the nodes.

1- The tree will consist of maximum depth level 3 as shown in the Figure 20.

2- The coordinator is at the depth 0. The first R03 is at depth 1 and coordinator is the parent router for it. The remaining routers R031, R032, R033, R034 and R035 are at the depth of 2 and R03 is the parent for all the routers and the associated nodes of them. The end nodes are at depth 3 and the above routers are the parents for them.

3- The maximum number of nodes per parent will be 20.

4- The addressing values are based on the Cm, Rm and lm. The Cm is the maximum number of child of a router. The Rm is the maximum number of child router of a router while lm is the maximum number of depth of the tree.

5- The important values obtained on the basis of above assumption and to finalize the addressing for each nodes is shown in the Table 4.

Figure 20: Tree structure

Table 4: Addressing values

Description	Value
Cm	25
Rm	5
Lm	3
Cskip (0)	151
Cskip (1)	26
Cskip	1

There are 3 total networks that are deployed for cluster tree design with node counts of 100, 200, 300, 400 and 500. As there is no way to assign the addressing to all the nodes automatically therefore each node is manually configured for the addressing parameters. Considering the single node R031, the configured addressing looks like as shown in the Figure 21.

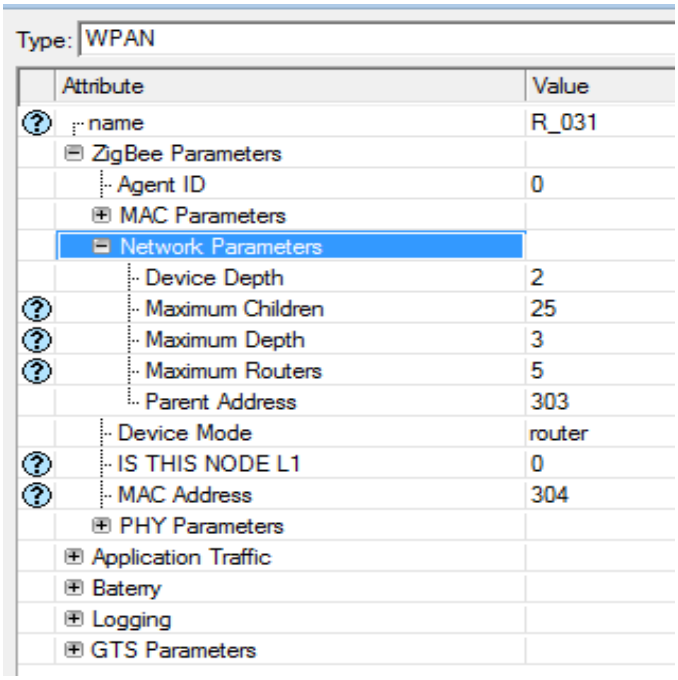

Figure 21: Addressing configuration on nodes

It can be seen that the router is at depth 2 with maximum children of 25 and the maximum depth value of 3. The parent to this device is associated has a mac address of 303 while its own mac

address is 304. The group of sensors represent the parent router with its associated child. All the sensor nodes generate traffic and the destination for the traffic is the coordinator, which is the central point to collect data from all the sensors. The mac layer parameter including CSMA-CA parameters is also configurable in the cluster tree topologies. In the Figure 22, the configured parameters from one of the router are taken which is similar to other nodes in the network.

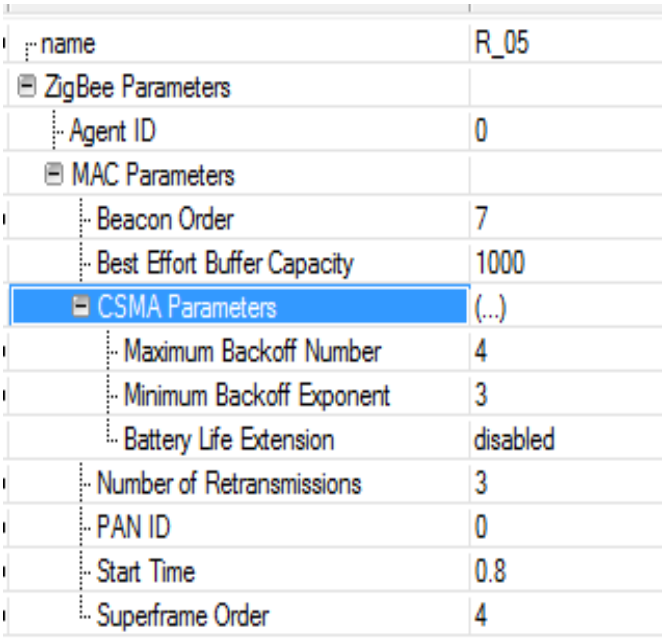

Figure 22: CSMA CA Configs

Since a cluster tree has a battery module the batteries are also configurable. The configured parameters from battery module can be seen in the Figure 23.

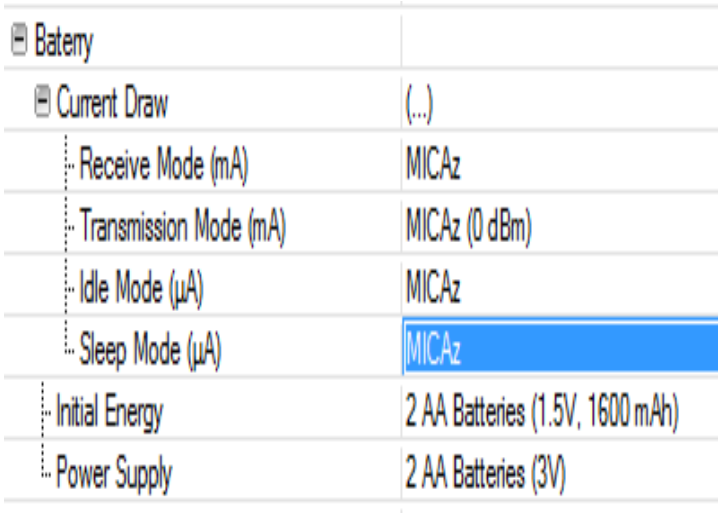

Figure 23: Battery modules

4.5.12 Mesh Topology

Mesh routing is quite easy to deploy in the OPNET because of its default libraries. The addressing is also very simple and the OPNET take care of all the auto assignment of addressing for each nodes. Therefore, there is no need to configure the addresses manually for each node, which become very time consuming, if we talk about assigning manual addresses to 500 nodes. The only configuration required is at the coordinator, which is the central point for configuring the routing for all the routers and the end sensors. It is important to carefully place the routers by considering the amount of end sensors and each sensor automatically associate with one of the best path available router. In the Figure 24 it can be seen that two routers are placed to cover the sensors communication and provide the path towards the coordinator.

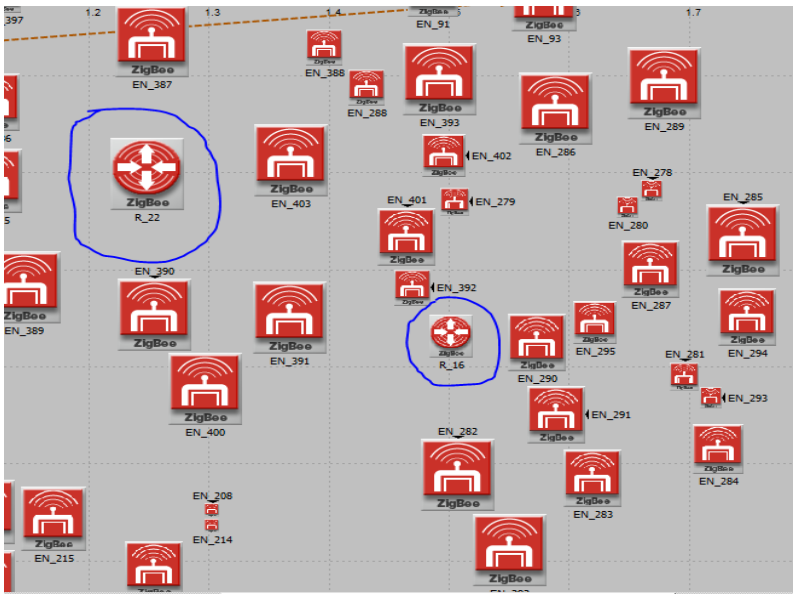

Figure 24: Mesh router placement

The routing is configured on the coordinator which automatically configured all the routers to follow the same routing behavior. The mesh routing configuration of the coordinator can be seen in the Figure 25. The network layer configuration is available only in the coordinator.

Attribute	Value
name	coordinator
trajectory	NONE
ZigBee Parameters	
MAC Parameters	
Physical Layer Parameters	
Network Parameters	(...)
Beacon Order	6
Superframe Order	0
Maximum Children	7
Maximum Routers	5
Maximum Depth	5
Beacon Enabled Network	Disabled
Mesh Routing	Enabled
Route Discovery Timeout	10
PAN ID	10
Application Traffic	

Figure 25: Network layer configs for mesh

The mac layer parameters are also configurable in the default model of ZigBee. The configured

mac parameters used for this chapter is shown in the Figure 26.

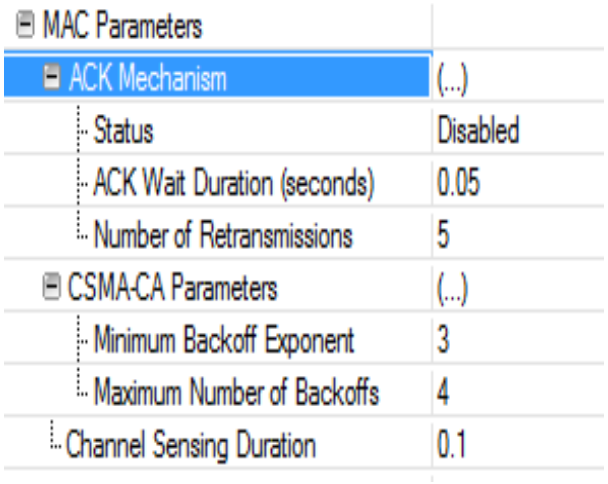

Figure 26: Mesh nodes Mac configs

Since no battery modules are present in the OPNET default ZigBee libraries. Therefore, battery power is not considered for mesh routing.

4.6 Simulation and Results

4.6.1 Performance Metrics

This section will evaluate the critical analysis of various graphs that are obtained on the basis of configuration earlier in this chapter. The effect of increasing of increasing number of nodes on the network performance will also be discussed with the respect to the obtained graphs. The communication network is the backbone for the application running on it. Therefore, performance in term of throughput, delay and failover are the main important parameters to take in to consideration. OPNET generate results in term of graphs and the values will be evaluated for the increasing number of nodes and the performance of wireless mesh and tree topologies. OPNET has three different types of techniques for collecting results, which are.

- Global statistics

- Node statistics
- Link statistics

Global statistics show the average of all the nodes in the network, e.g. global end-to-end delay is the average end-to-end delay of all the nodes in the graph. Node statistics give the statistics at the node level. E.g. end-to-end delay in the node statistics will give the end-to-end delay of only that node and the link statistics give the link level performance [67].

In order to compare the results, the simulations are divided into 10 scenarios. Five scenarios for clustered trees and Five for mesh routings. The differentiator in each scenario is the number of nodes and the routing protocol of each. All these scenarios were done in an area of 16093.4 meters (10 Miles) of area in both cluster and mesh topologies. In the cluster topology there will be 100 nodes sending traffic to coordinator at the center of the network then 200 sensors, 300, 400 and 500 sensors nodes. The mesh network will also start with 100 and subsequently 200, 300, 400 nodes to 500 nodes. Each 100 sensor nodes cover up to 3218 m and distributed along 3 lines, each line has approximately 32 sensor nodes.

Based on the equation 3.4 and the number of nodes with different type of intruder such as human and an animal the probability of detection is showing in table 5 and the probability of Identification is showing in table 6

Table 5: Probability of Detection

Probability of Detection	P=0.90	P=0.80	P=0.70
N=100	90	80	70
N=200	180	160	140
N=300	270	240	210
N=400	360	320	280
N=500	450	400	350

Table 6: Probability of Identification

Probability of Identification	P=0.70	P=0.75	P=0.80	P=0.85	P=0.90
N=100	70	75	80	85	90
N=200	140	150	160	170	180
N=300	210	225	240	255	270
N=400	280	300	320	390	360
N=500	350	375	400	425	450

We extensively use two general results from theory of probability. First, the Probability of Detection, second is the Probability of Identification based on the number of nodes (500). Also based on the intruder with different kind of x_{sys} and x_{env}.

4.6.2 Collecting Results

There are two phases in collecting results. First phase is to enable the request statistics in the OPNET and then define the simulation time for the amount of the time the results are requested to collect. OPNET supports different types of results but the main focus here will be on delay and throughput of the network, as well as the battery performance of the parent routers in case of clustered tree topology. The mesh routing does not support a battery module. OPNET provides a complete list of statistics and the required statistics related to this simulation has been set to collect as shown in the Figure 27. After collecting the results, the simulation has been run for the required amount of time to get the results.

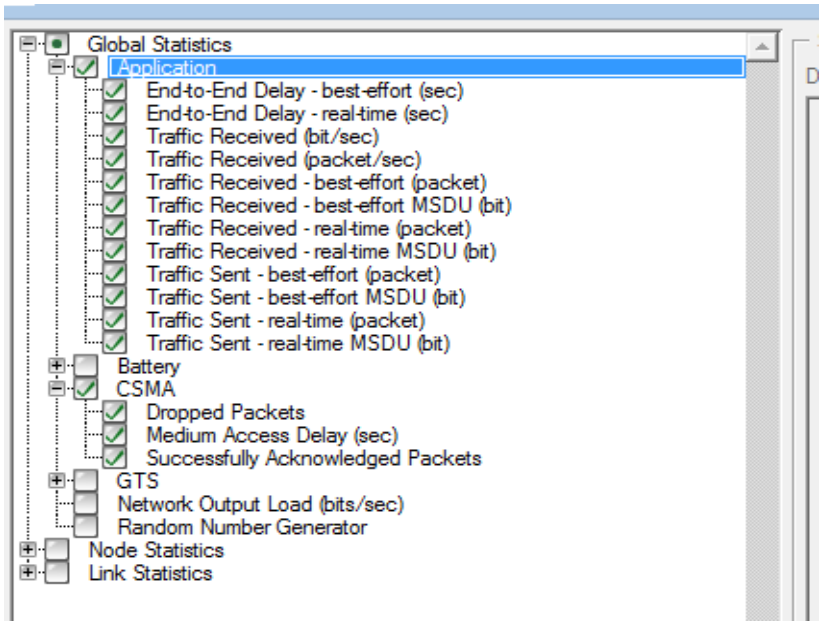

Figure 27: collecting statistics

4.6.3 Cluster Tree Performance

As explained above, the cluster tree has five scenarios for the increasing number of nodes to see its effect on the network behavior. Since wireless sensor mac use CSMA-CA for resource allocation, therefore CMCA mac drop results are collected as the mac layer performance metric. The collective results for all the three scenarios for the CSMA-CA drop and the medium access delay can be seen in the Figures 28&29.

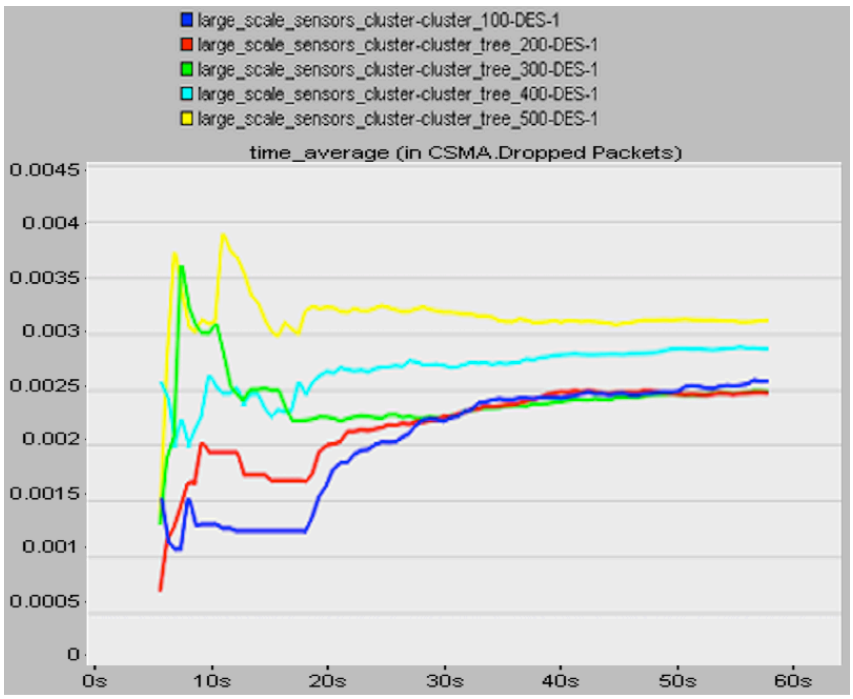

Figure 28: CSMA- dropped packets

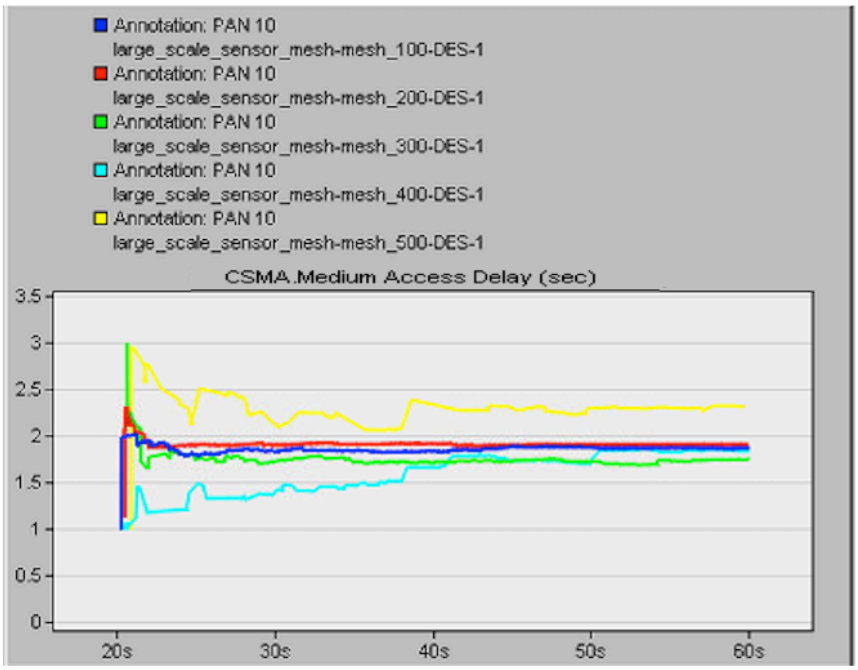

Figure 29: CSMA-Medium access delay

The first Figure shows the packet drops while the second Figure shows the resource allocation delay. The yellow line represents 500 sensors; the turquoise represents 400 sensors, the green

represents 300, the red represents 200 while the blue represents 100 sensors. It can be seen that increasing the sensors in the network adversely affect the performance. The packet drop has increased as the sensors increased and it can be seen that delays are quite higher as well for some sensor in case of 400 and 500 nodes. The main reason for this increase is the parent-child design of the cluster tree routing. The router at tier 1 has initially two child routers and each child routers has 20 nodes. The tier 1 parents served a total of 40 nodes. Now, in case of 500 nodes, the tier router has five child routers with each having 20 nodes. This increased the total number of nodes to 100. This effect can be clearly determined from the graph. As the number of children nodes increased, the load on the parent's nodes increases, which can start causing the drops and delays to the packets. Another important network parameter is to end-to-end delay and network load which explain the application behavior. The end-to-end delay and the total average network load can be seen in the Figures 30& 31.

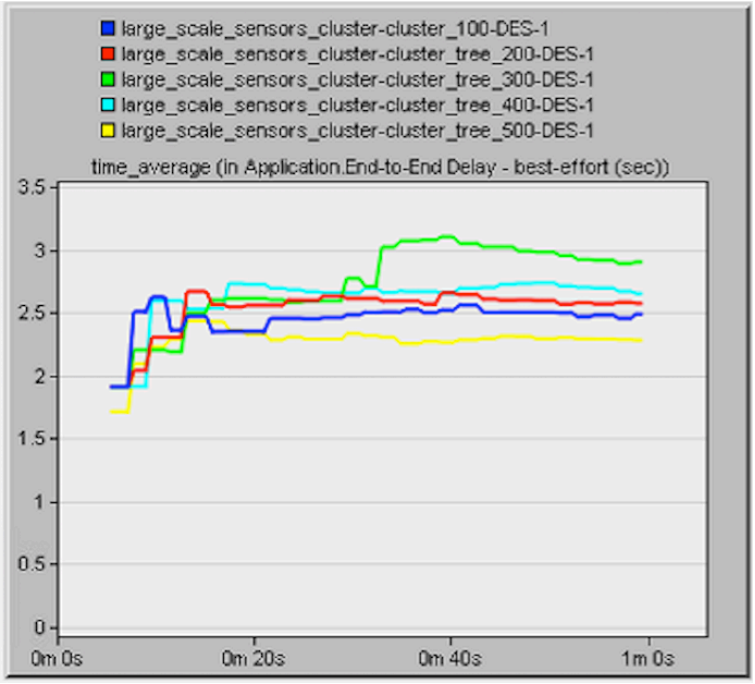

Figure 30: End-to-End delay

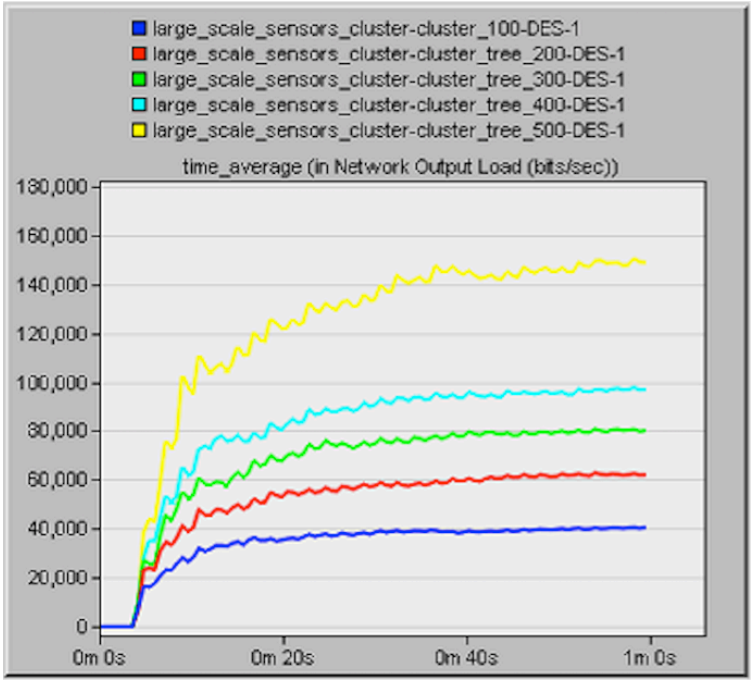

Figure 31: Network Load

It can be seen that end-to-end delay has very irregular pattern and quite high. The delay in the clustered tree topologies is always high because of the intermediate network layer switching involve which causes additional delay. Since the above results are global statistics, which is the average statistics of all the end-to- end delay and packet received, an exact estimation cannot be made from the above graph. The 300 nodes could be showing maximum delay because of the bottleneck of the single router, which affects the average delay of all the nodes. Network load represents the total number of PDUs observed by the network layer. Even in case of 500 nodes the packet drop was noticed as high but network load is still high and the reason for that response is the high number of active nodes. Even the packets are dropping but since the data generated is a lot more therefore the results are showing the higher network load. The throughput of the communication channel evaluates the total number of successful data received by the transmitter or receiver channel per unit time in bits/sec. It is one of the main performance metrics in observing the behavior of the wireless communication network. The throughput is collected by selection of

the parent router, which is R03 in this case, and the results can be seen in the Figures 32&33. Channel Utilization shows the percentage data usage on the channel.

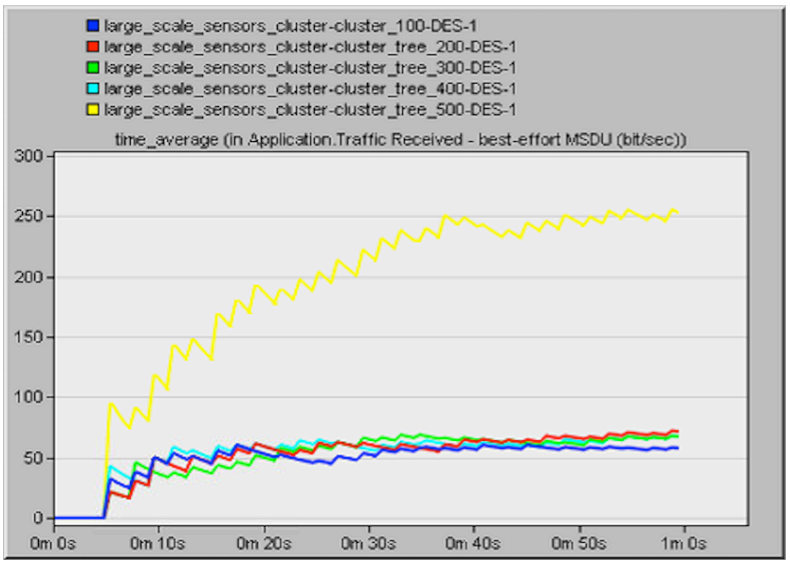

Figure 32: channel utilization

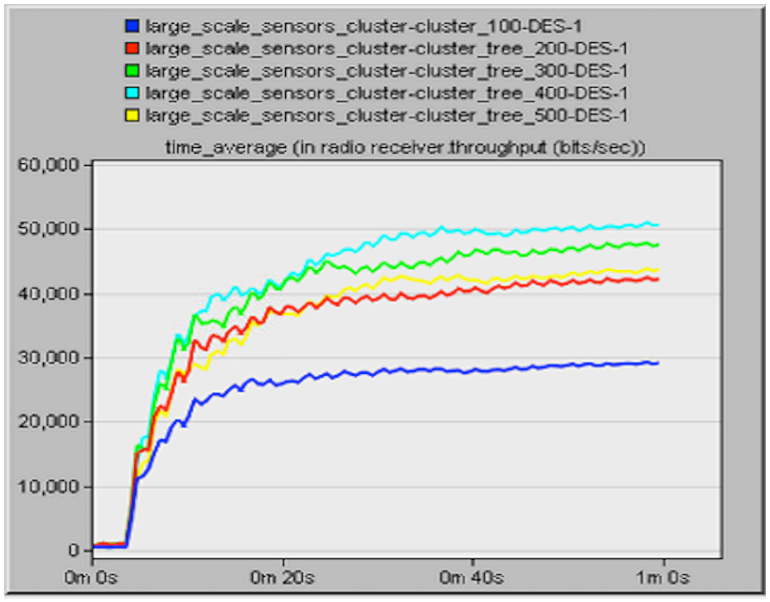

Figure 33: Channel throughput

The first graph represents describe the receiver channel utilization while the second graph shows the throughput of the wireless receiver channel. From the throughput definition, it can be validated from the graph that the successful average data receiver is higher in 400 nodes as

compared to 500 nodes due to packet loss whereas the channel utilization of the 500 nodes is a bite higher than 200 based on its correlation to the overall network load. Battery usage depends on the active cycles used by the nodes and the amount of processing done by the node. The battery usage is collected on the router R03, which has a different number of child routers for the 100,200, 300, 400 and 500 nodes scenarios. It is serving the maximum amount of children in 500 nodes scenario so the expected battery utilization should be higher in this case. The combined battery utilization for all the three scenarios is shown in the Figure 34.

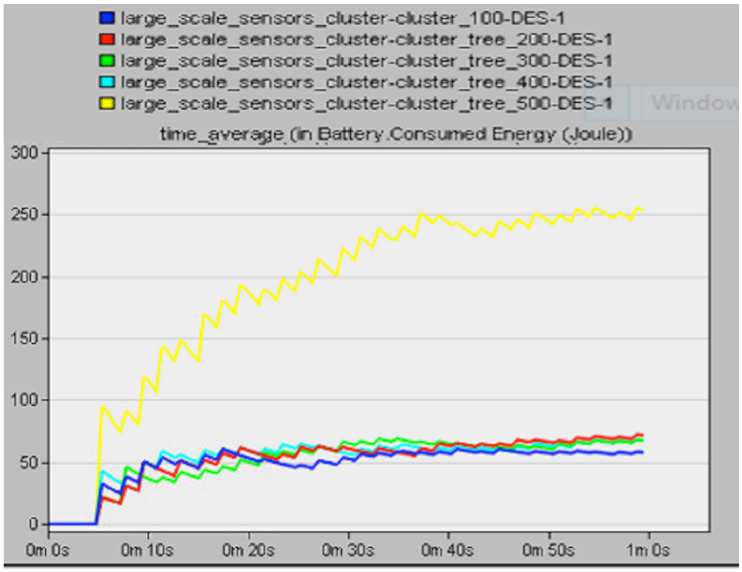

Figure 34: battery consumption

Clearly, there is direct relationship on the performance of battery with increasing numbers of nodes and it is highly recommended to use high powers on the parent nodes which are involved in the process of all the children nodes.

4.6.4 Mesh Routing Performance

Mesh routing architecture is different than the tree. Therefore, the high-performance difference is expected and performance is based on the efficiency of the coding. The mesh routing is the default model libraries from the OPNET. Therefore, its code is much more efficient as

compared to the open source clustered tree model when starting with the mac layer performance of the mesh routing. The similar results will be evaluated as explained for the clustered tree routing. The mac data dropped results defined by OPNET as the values collected for the amount of traffic dropped due to consistently failing transmissions and retransmission. The media access delay is total delay face by the queuing and contention delays of the data frames transmitted by all Mac layer of 802.15.4. This delay is the measure of the arrival of frames from the higher layer, insertion of these frames into the transmission queue until the frame is served and in initially sent on the radio transmission channel. The collective statistic of the mac drop and media access delay is shown in the Figures 35&36.

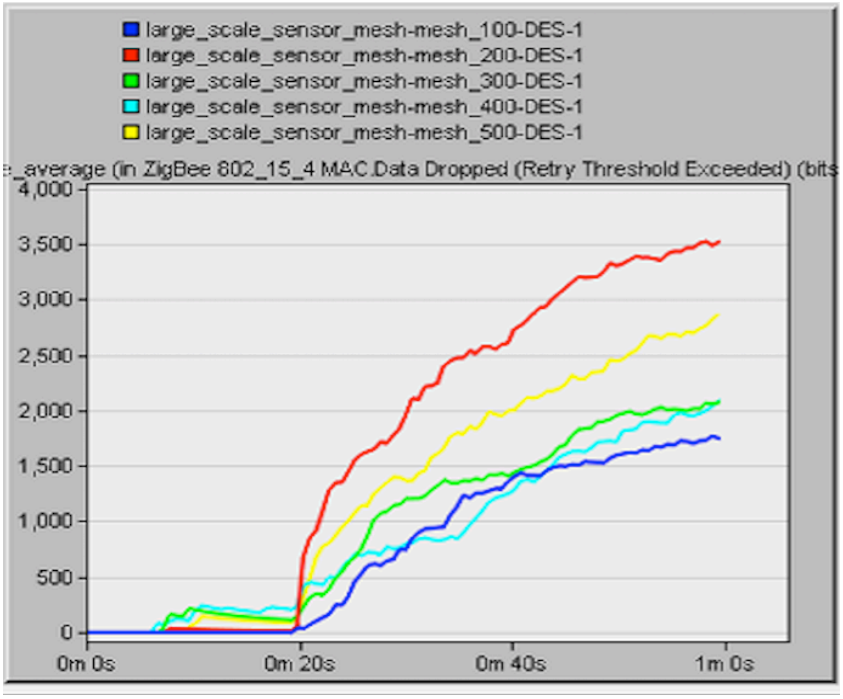

Figure 35**:** Mac drop

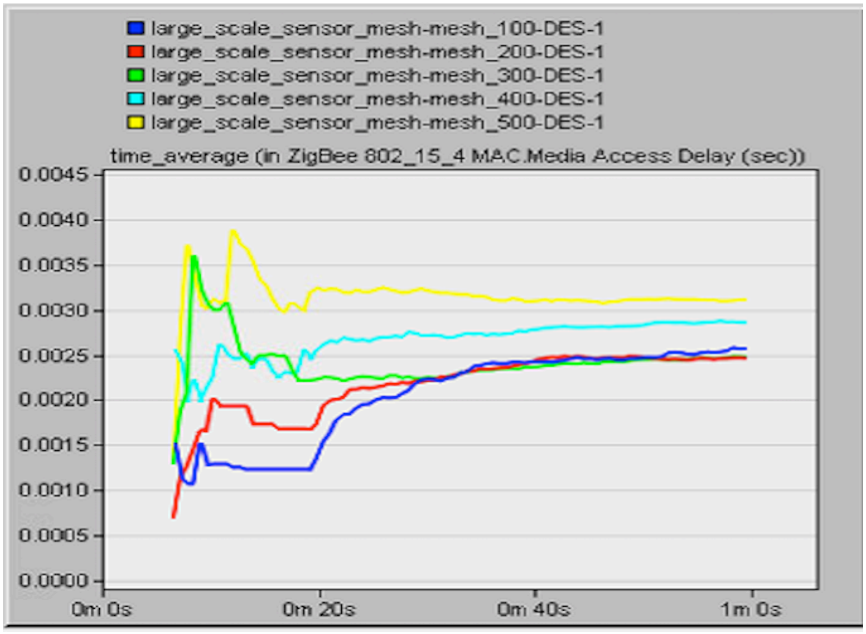

Figure 36: Media Access Delay

The number of end nodes increased, as expected, in the PAN the media access delay behavior changed with higher data drop rate and delay. The ratio of increase in the sensor as compared to serving routers is higher. Therefore, the load affects the network performance. The second reason is the overload of PAN coordinator as well. For the analysis of application performance in any data network, the end-to-end delay is an important factor. End-to-end delay is measured as the change in time of generation and reception of the packet. In OPNET, the difference in time is measured by stamping each packet with the time field. The receiver subtracts the packet stamped time which represents the generation time of the packet from the simulation time to generate the end-to-end delay. The end-to-end delay for all the three scenarios is shown in the Figure 37.

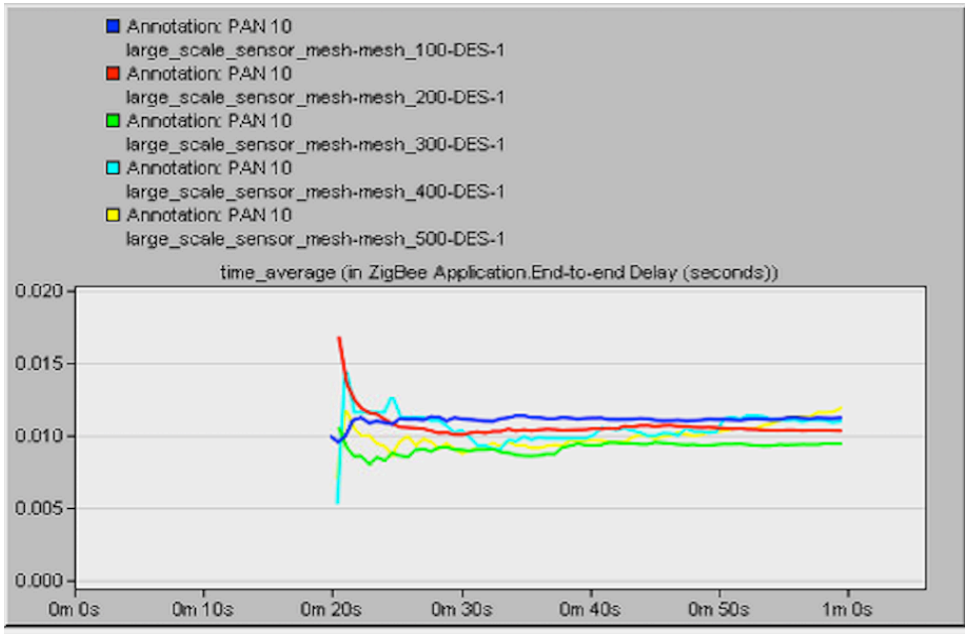

Figure 37: End-to-End delay

According to the graphs, no baseline behavior for end-to-end delay performance can be estimated. The only reason for this behavior could be the starting access request made by a sensor through the intermediate routers. Once the end node receives its data slot for data, the PAN behaves same in term of end-to-end delay for all the three scenarios. Another notable thing in mesh routing is the very low end-to-end delay as compared to clustered tree because of the fast switching in the mac layer. Similarly, to the clustered tree scenarios, the channel utilization, and throughput has also been observed for mesh routing. The Figures 38&39 plotted the throughput and link utilization for the wireless mesh three scenarios of 100, 200, 300, 400 and 500 sensors.

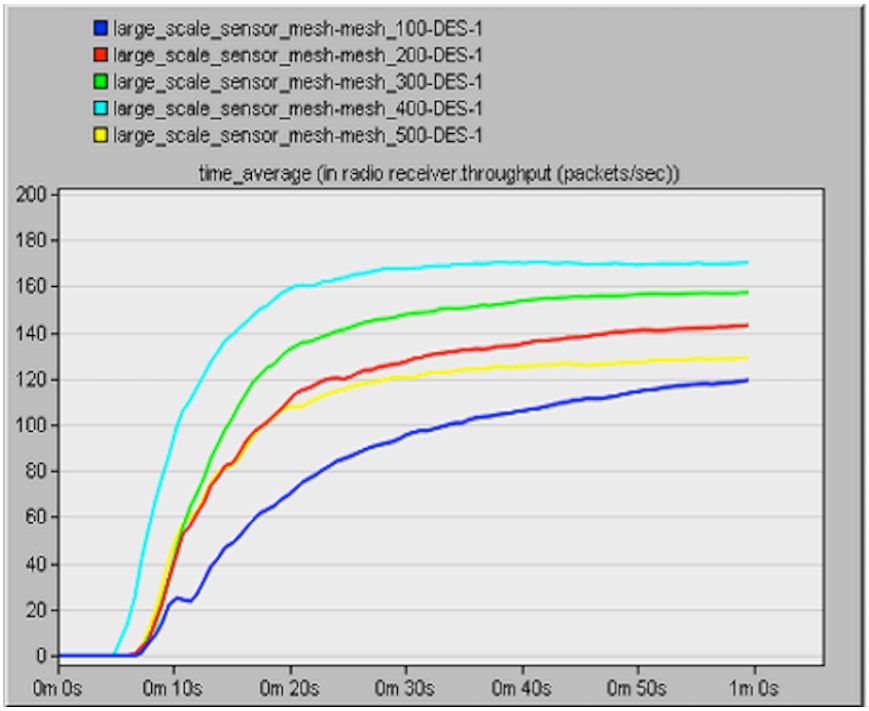

Figure 38: Channel Throughput

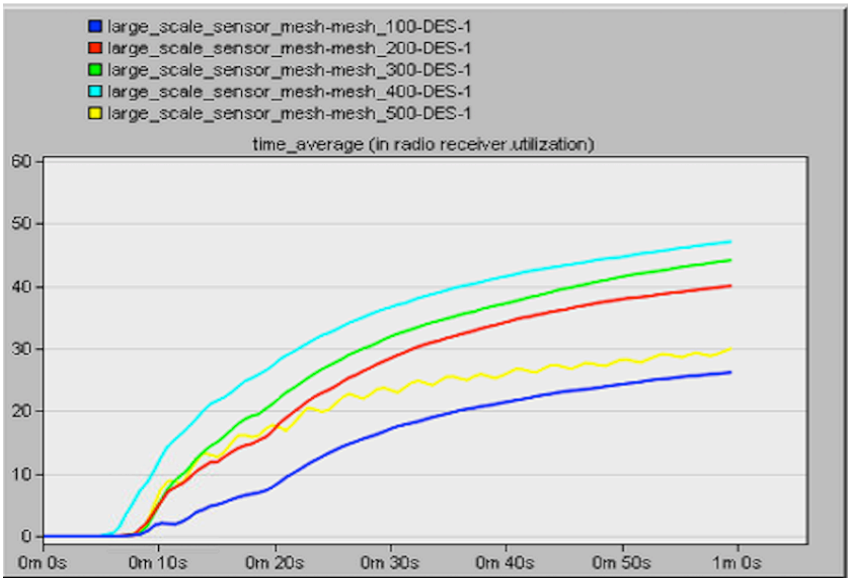

Figure 39: Channel utilization

It can be observed that throughput in mesh routing behave similarly to the graphs obtained for clustered tree routing. The performance improved with the rising number of end nodes. The PAN is showing the best performance with 400 nodes. The network seems to be choked for 500

nodes (green line), the green line intersect the red line for the maximum value of 60 at 10 sec and then performance start degrading as the load in the network get higher. The link utilization has a changed behavior in mesh routing. The justification for link utilization is a single hope towards destination which correlates to the throughput graphs. In the example of clustered tree routing, the graph obtained for link utilization is from the intermediate parent node which represent the combined traffic of all the child routers and sensors attached to this parent.

4.6.5 Performance Results

In terms of overall performance, it can be seen that the network behaves optimally at 100 nodes but at 500 nodes the performance degrades and throughput falls down. The mesh topology performance is observed better than cluster tree in term of end-to-end delay. Because of the flat architecture of the network and multiple path availabilities towards the coordinator with less hop. The advantage of mesh routing is that sensors are independent of any parents, and the failure of the parents does not affect any child, as long second active router is available in the network. Therefore, complete network isolation problems can be easily avoided in this case. Wireless mesh is a costly solution as compared to clustered tree because of the many backbone routers. Despite the cost, network performance is improved and this solution is recommended for high, closely placement of the sensors. In terms of performance in wireless mesh routing, it can be seen that the breakout point is 400 as the network performance degrades with the 500 nodes. The additional parameters can be taken into consideration to improve the performance which can include the addition of another coordinator and more mesh routers.

CHAPTER 5: BORDER SMART SURVEILLANT and AN INTRUDER ALERT SYSTEM USING CMUCAM3

5.1 Introduction

The aim of this chapter is to present the Smart Surveillant – an intruder alert system using a CMUCAM3, and to describe its functionality. This chapter explains the design, application, scope and every restriction of the Smart Surveillant, including how CMUCAM3 works and the techniques that are used to build the Smart Surveillant. The frame differencing technique of CMUCAM3, that is used to do motion tracking, is explained as well.

A plethora of security cameras and surveillance cameras are available on the market and offer a wide range of features, starting from basic surveillance to high level intelligent patrolling camera bots. The most important feature in this chapter is motion tracking. These products hold a considerable cost even though their real time application is not up to the level of what they offer. The aim of this chapter is to build a cost effective solution for general security issues [68]. The Smart Surveillant monitors a specific location and triggers an alert when there is an intrusion. It does this by using the CMUCAM3, a low cost, fully programmable, embedded image sensor. The CMUCAM3 offers a variety of features. The feature utilized in this chapter is the Frame Differencing technique. The Smart Surveillant relies extensively on motion tracking to detect an intrusion and this is achieved through the frame differencing technique. The process involves image processing to identify the difference in the frames captured by the CMUCAM3 sensor.

"Object Tracking" is the process of tracking a specific object throughout its motion, using a vision sensor or camera. The CMUCAM3 is built specifically for object tracking. "Motion Detection" is the process of identifying the motion of objects in a given location is known as motion detection. This can be achieved through the tracking of different objects present in a given

location or by tracking the changes in the number of objects present in the location. The CMUCAM3's frame differencing technique uses a similar algorithm to detect motion [69].

5.2 Smart Surveillant System Components

The components that are used in building the Smart Surveillant are:

1. CMUCAM3 from Parallax Inc.
2. Arduino UNO R3 development board
3. DC power(9V) supply to power Arduino & the cmucam3
4. Connecting wires
5. An alarm system connected to AC power(220-240V) supply

5.3 CMUCAM3 Description

The CMUCAM3 is a low cost, fully programmable embedded image sensor. It provides an open source development environment with a powerful hardware platform. It is based on ARM7TDMI processor. The main processor, Philips LPC2106, is connected to an Omnivision CMOS camera. The CIF resolution camera captures the images into high speed FIFO buffers. The sensor supports an MMC for mass storage using FAT file system [70]. Below is the Block diagram of CMUCAM3 Figure 39. The front and back of the CMUCAM3 Figures 40 & 41.

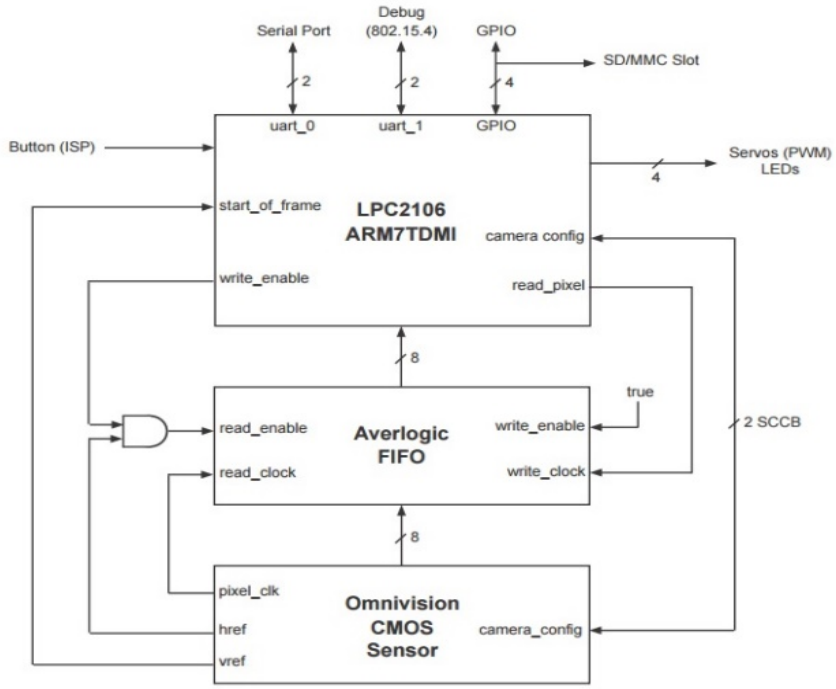

Figure 40: Block diagram of CMUCAM3[70]

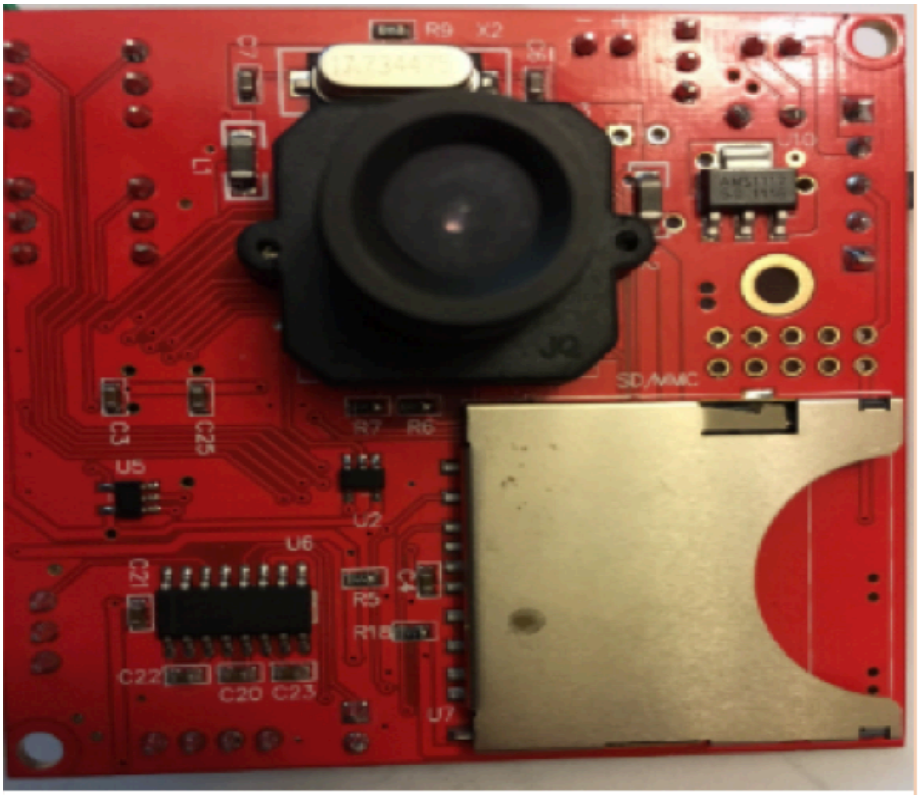

Figure 41 – Front view

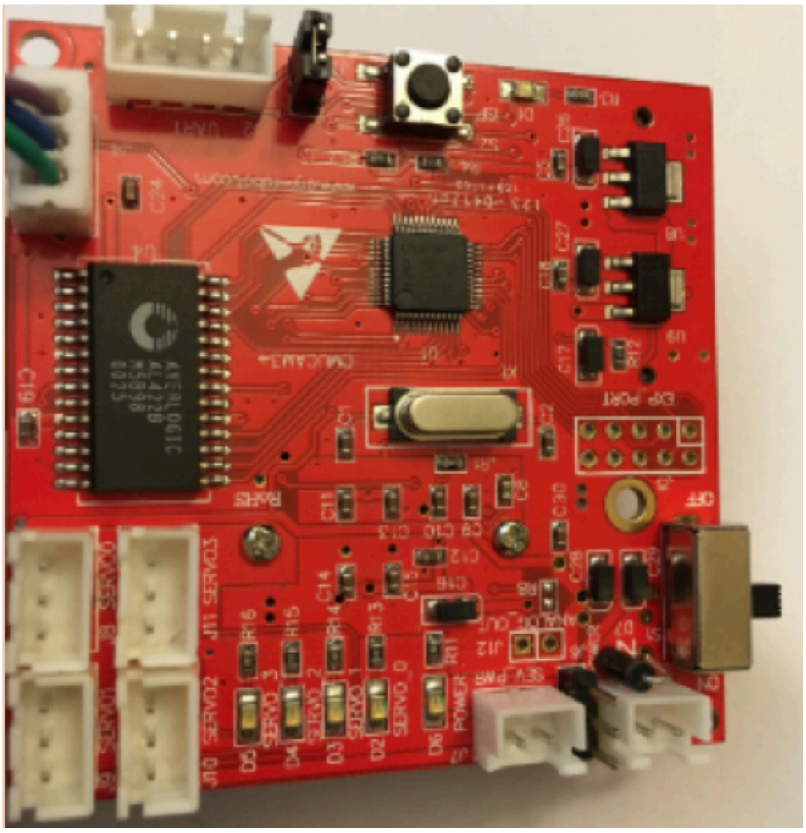

Figure 42 – Rear view

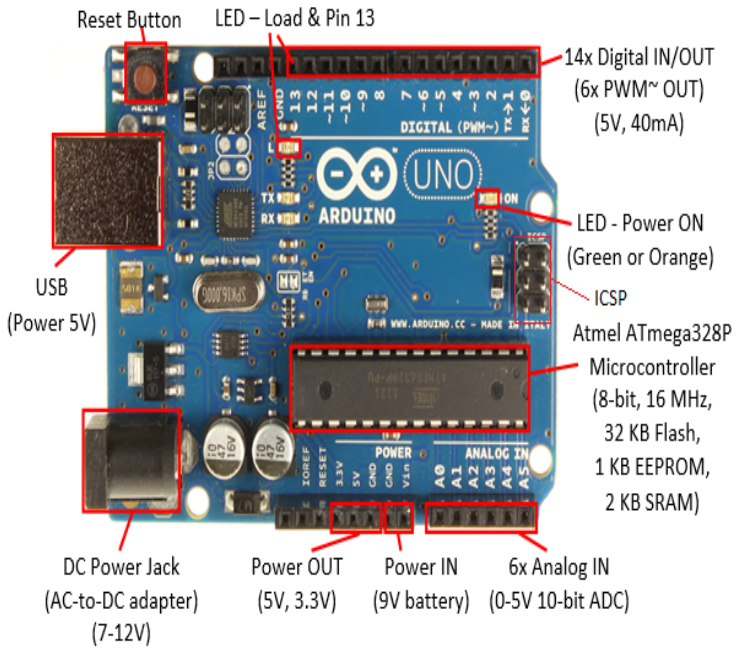

Figure 43 – Arduino UNO pin diagram

Some of the features include of the Arduino as showing in Figure 43.

- Open source development for Windows & Linux
- Load images into memory at 26 fps
- Software based JPEG compression
- Basic image manipulation library such as image downsizing
- Frame differencing
- Object tracking
- Histogram generation

The applications of the CMUCAM3 mostly use the image processing accessible through a serial interface. Typical examples include:

- Robotics
- Surveillance
- Object recognition and tracking

5.4 Design Smart Surveillant System Using CMUCAM 3

This section describes the design involved in building the Smart Surveillant. The CMUCAM3 will be connected to the Arduino board. Then the sensor will be programmed through Arduino to do the required functionality. Once the program is dumped into the Arduino board, the board will be powered up using a DC power supply. The device will be placed in a particular location which needs surveillance. The intruder alert system will be connected to the Arduino board. The CMUCAM3 uses the frame differencing technique to detect motion in the specified location. Once it detects motion, it considers that as an intrusion and triggers the attached intruder alert system. "Frame Differencing" is when the sensor captures an image frame of the location initially and stores it [71]. Then after a specific time interval, the sensor captures another image

frame and compares it with the pre-stored frame. If it finds a difference between the frames which is greater than a particular threshold value, the sensor detects it as a movement of the objects present in the location or addition of new objects into the location. The differentiated output will be given sent through the serial emitter of the sensor. An "Intrusion Alert" occurs once the Arduino receives frame differentiated output from the sensor, it triggers the intrusion alert system connected to it, as shown in the flow Chart in Figure 44.

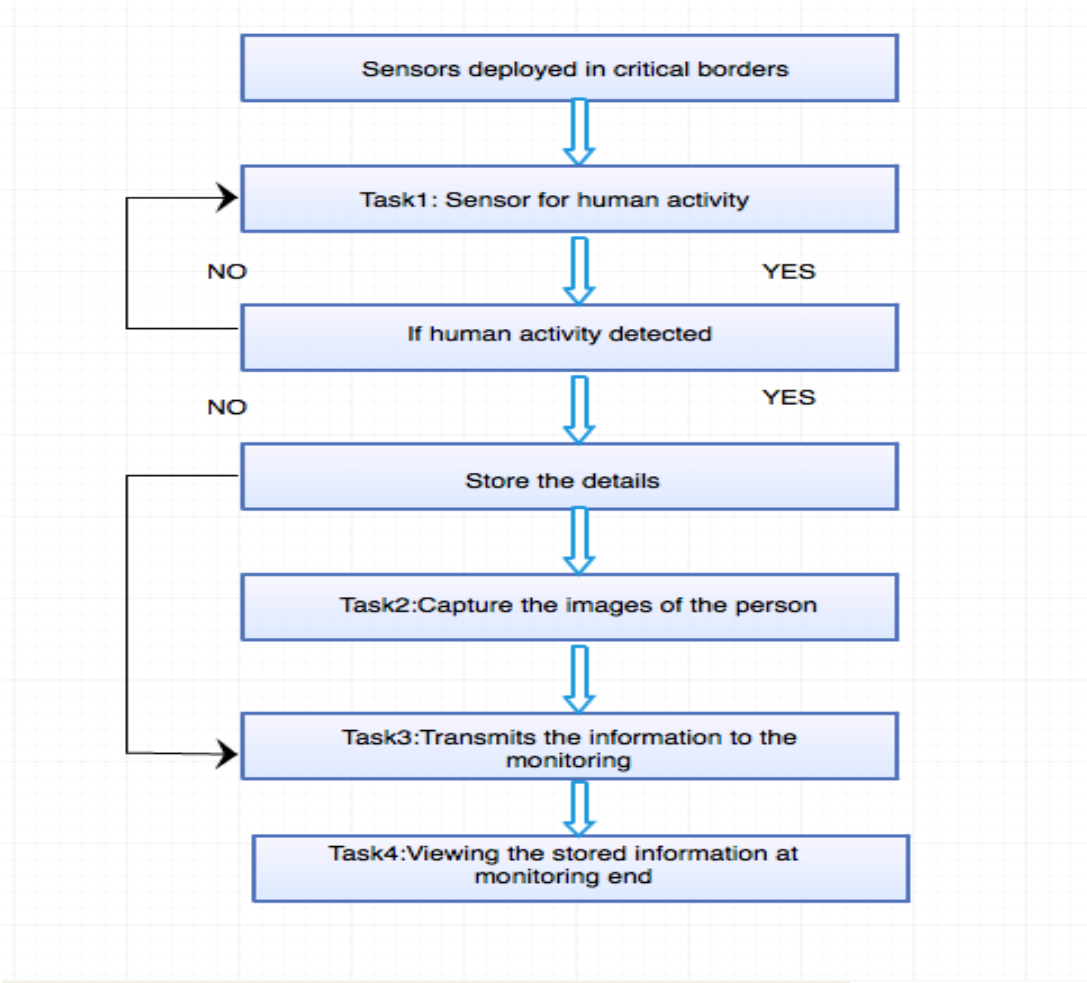

Figure 44 – intrusion alert system flow chart

5.5 Implementation of The Smart Surveillant

This section describes the implementation of the Smart Surveillant, based on the design proposed earlier. Initially, the image sensor shall be connected to the Arduino board's ICSP header

through the serial cable. Arduino UNO will be connected to the PC through the USB cable. Then the code to do the frame differencing and triggering the intruder alarm will be dumped onto the Arduino board. This code involves sending serial communication to CMUCAM3 to capture the image frames regularly and to perform frame differencing on the captured image frames. This output will be read by the Arduino through ICSP and if the sensor reports a motion detection, the digital output pin of the Arduino will be set [72].

No specific software is needed to do the programming for CMUCAM3. The coding can be completed in two ways. One way is to program using a GNU compiler and the other is just to send specific commands to CMUCAM3. The sensor has CMUCAM3 emulated firmware inside. The CMUCAM3 GUI software's functionality is used as the basis of the device's coding. The firmware receives commands from the GUI through serial communication. Those same commands will be sent from the arduino UNO board to the CMUCAM3 through serial communication. The sensor's firmware reads these commands and writes the output through the serial port. In this case, we will be sending the commands LF and FD to do the frame capturing and frame differencing in regular time intervals. LF command indicates for the sensor to load a frame into memory. The FD command directs the sensor to apply the frame differencing technique on both the current frame and the frame in the memory. The FD command is followed by a value to indicate the threshold with which the frame differencing has to be performed. These commands will be sent from the arduino through the ICSP and will be coded in the following format in arduino.

Sample Code:

```
Serial.write('lf'); //loads the frame
Serial.write('fd 8000'); //frame differencing
```

Once the code is dumped, the USB cable can be removed and the arduino and the sensor

should be powered through a DC power supply in order to self-sustain. The device will then be deployed in a location and do what it is has been programmed to do. After deployment, the sensor captures the first frame of the location and stores in it in its memory. The time interval given is 7 seconds. The sensor captures the second frame after 7 more seconds have passed. After capturing the second frame, the frame differencing technique will be applied on the two captured frames. If the difference is greater than the programmed threshold, the sensor detects this as a motion and sends the 'on' signal to the arduino board through the serial cable. If the difference is less than the threshold, the sensor sends an 'off' signal to arduino. If motion is detected, then the first frame will be erased and the second frame will be stored in the memory. This process is repeated indefinitely. The arduino, continuously reading the ICSP, will set the pin13 if an 'on' signal is received.

The intruder alert system is powered by an AC power supply. The arduino shall be interfaced between the intruder alert system and the AC power supply, to act as a switch. The alarm system will be connected to pin13 of the arduino. When frame differencing results in a motion detection, we will wet the pin13, which will turn on the alarm.

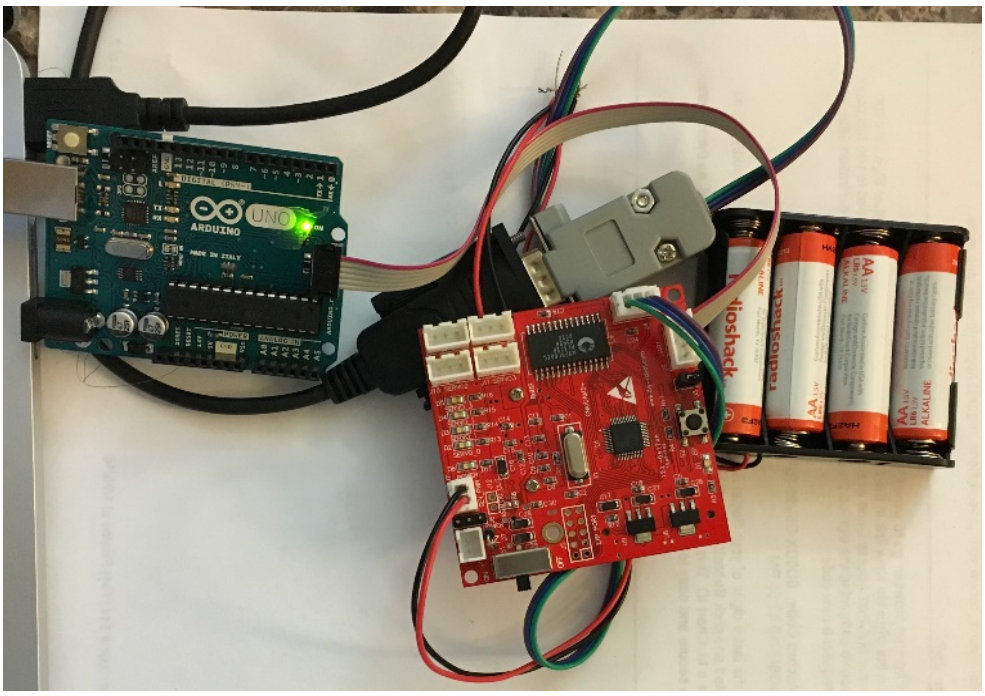

Figure 45 – Smart suveillant assembled system

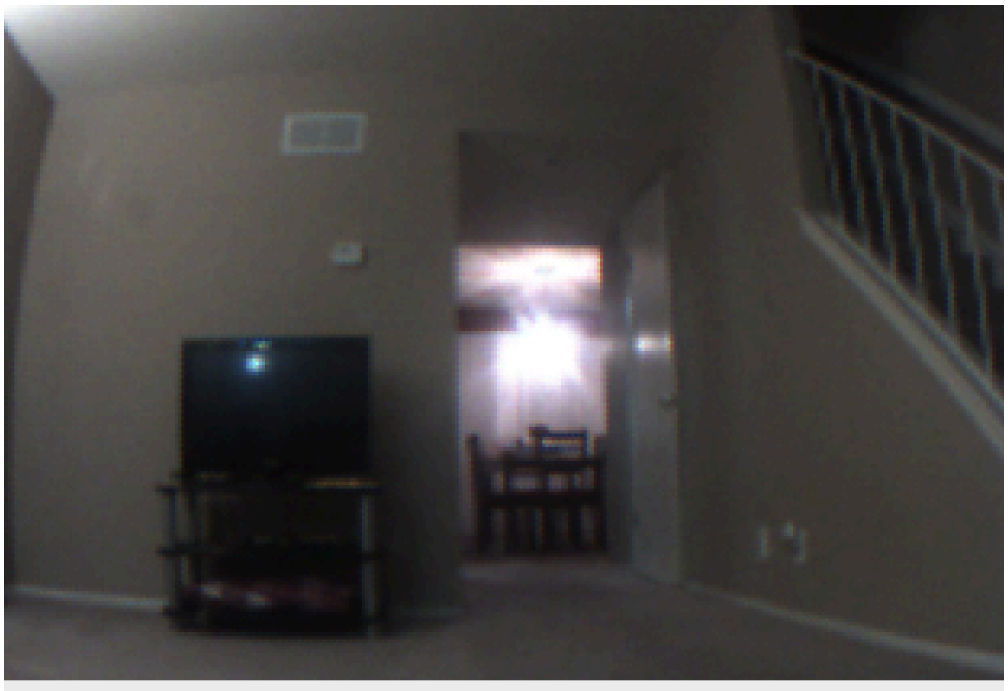

Figure 46 – Smart surveillant monitoring a specific room

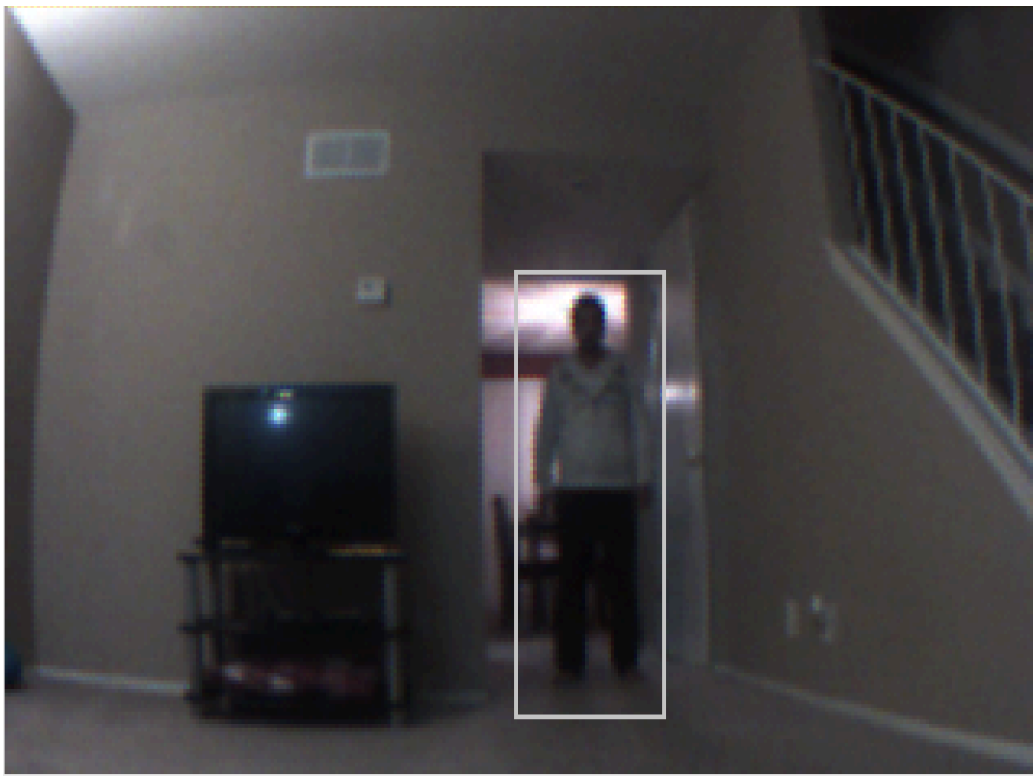

Figure 47 – Smart surveillant detects a person's presence motion detected as intrusion

(The box in second image is manually done; frame differencing does not box the objects)

5.6 Surveillant Application

This section describes the real time application of the surveillant after deployment in a specific location. In this scenario, the camera monitors a room in the house. The sensor has captured the first frame and has kept track of all the objects in the room. After 7 seconds, it has captured the second frame, in which a person is found. It treats that person as an additional object in the room. When the frame differencing is done, the huge difference in the number of pixels exceeds the threshold and detects intrusion. It then sends an ON signal to the arduino. The arduino processes the ON signal and sets the pin13 to HIGH. This triggers the intrusion alert system. In real time, the preferred application of this chapter is as a border security camera between two locations.

5.7 Smart Surveillant System Restrictions

A restriction of this chapter includes ignoring of authorized motion detection, when an authorized person enters the location; the device has to stop doing the motion detection for an amount of time specifically programmed. When the alarm is triggered, it has to be shut down manually and the device must be reset in order to function properly. Another considerable restriction is the range of the sensor. The range of this device relies completely on the threshold given for frame differencing. Low threshold value results in higher range but is not reliable because the sensor triggers the alarm for inconsequential objects. High threshold value results in lower range and might not trigger the alarm for human intrusion. The threshold should be moderate. CMUCAM3's resolution is CIF(352x288). That means 101376 pixels per frame. Human intrusion can have a minimum threshold of 7000 pixels. The ideal threshold value for detecting human intrusion can be in the range of 7000-1000 pixels. The camera's ideal monitoring range is a dimension space of 16x16. These values are preliminary and are purely based on trial and error. Actual values may differ based on the application of the device.

CHAPTER 6: ANTENNA RANGE EXTEND FOR TOLES SENSOR PLATFORM TRANSCEIVER BOARD

6.1 Introduction

During the past few decades, wireless sensor networks, along with their applications, have been undergoing an evolution and becoming an important technology in the world. Wireless sensor networks are spatially distributed sensors which are used to measure the physical and environmental changes in the area of their implementation. The quantities include changes in motion, temperature, pressure and noise. The users of these networks are customizing this technology in the areas of security, agriculture, ecological monitoring and health care services. The control and monitoring of a border are growing tough for most of the countries in the world today. Countries use it to allocate a significant number of financial and manpower resources to address the issue. Despite the amount of the resources invested in the controlling and monitoring of the border, several false alarms are raised, contributing to the difficulty of the task. The implementation of the WSN for the border control facilitates is surveillance, monitoring, and it provides an intelligent solution to the above mentioned problems.

The WSNs combine the characteristics of the decision-making through signal processing, transmission, compact devices, and low-power consumption compared to the conventional monitoring systems currently installed at borders. WSNs detect the intruders in the territories which were previously unknown and are able to detect and investigate the intruders. Each node of the network can detect the intrusion and then communicate with the rest of the nodes in the network to establish a clear idea of the environment as follows.

a) The multimedia sensors provide accurate detection and representation of the threat. The detection range of the sensor is also greater.

b) The ground sensor can provide the additional information about the intrusion which cannot be provided by the multimedia sensors.

c) Mobile tracking capability of the system can track an intruder after its detection.

d) The networking processing allows the heterogeneous nodes to detect the intrusion and report it back to the administrator.

6.2 Designed WSN Architecture

The primary matter of concern in the implementation of the WSNs is related to the power consumption requirements and sources of battery energy. The placement of the WSN in a large geographical area needs a low-power sensor based architecture which is comprised of the components having low-power consumption and reduced monitoring and maintenance requirements. The node architecture is made up of a sensor which is connected to a low-power analog to digital converters. The purpose of the convertor is to change the analog signal obtained from the environment into digital form for the transmission. A spectrum analyzer is also connected to the output of the sensor node with the responsibility of triggering the reaction based on the output obtained from the sensors.

The proposed network consists of several components which are capable of communicating with each other using radio frequency at 2.4 GHz. The network coordinator is a Telos platform attached to an end station. The designed sensor platform includes two levels of hierarchy. The upper level is realized using Telos wireless platform and the lower level sensor specific intelligent signal processing module. For the two-tier processing board, we used Telos, which is commercially available. Each Telos board is based on 8 MHz microcontroller with integrated 2 KB of RAM and 60 KB of flash memory a USB interface and a CC2590 antenna to increase the range of the node. The Telos platforms also include several sensors for the functioning of the

sensor node [73].

A Telos platform includes a 10-pin expansion connector allowing one UART and 12C interface. There two general purpose I/O lines and three analog inputs. The tier one of the hierarchical system is implemented as Intelligent Signal Processing Module (ISPM). They are designed to connect with Telos wireless sensor module in the tier two. The ISPM extends the capabilities of the Telos by adding two dual axis accelerometers. The ISMP's two ADXL202 accelerometers cover the axis of rotation for the sensor module.

The ISMP has its own processor in the shape of MSP430F1232 processor present for sampling and for low level data processing. An alternative way is to use Telo's microcontroller is for the data acquisition and processing. The microcontroller used was selected for the considerations of size and excellent MIPS/mW ratio. An additional microprocessor improves the efficiency of the sensor node causing no significant burden on the power consumption of the sensor node. Other features of the design are 10-bit ADC and timer registers which are used to acquire data from the accelerometers. The selected microprocessor also has the hardware for communication with the Telos board [73].

6.3 Designing Our Board with CC2590 RF Front-End

The CC2590 front-end is installed to an increase in the range of the sensor node. Before the installation of the front-end antenna, the output power of the sensor node was 0 dBm. The receiver sensitivity was -95 dBm and the range of operation for the sensor node was 125 m (maximum). The CC2590 is a range extender for 2.4 GHz RF transceivers, transmitters, and the output power now is 14 dBm. Below, in Figure 48, you can see the block diagram of the CC2590.

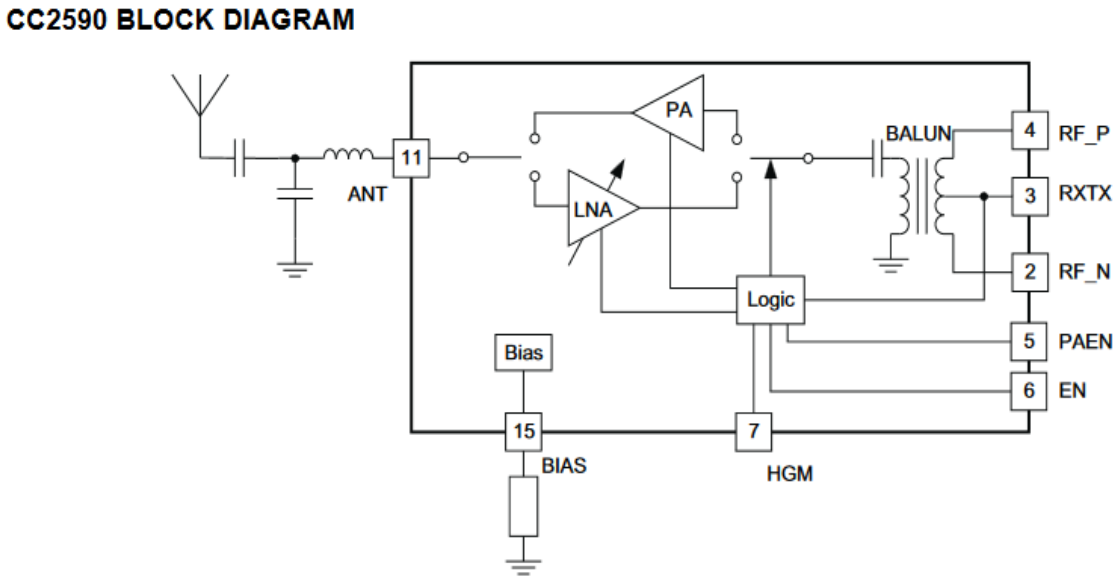

Figure 48: CC2590 Block Diagram [73]

The installation of the front end increases the capability of the link by power amplification and improved sensitivity. The operating frequency and other electronic specifications are given in the table 7 below:

Table 7: new design of CC2590

Old Version	New Version
Output power : max 0dBm	Output power : max 14 dBm
Receiver sensitivity : -95dBm	Receiver sensitivity : -101dBm
Range : max 125m	Range : up to 500m

The RF output power of the front-end antenna is controlled by a 7- bit value in the CC2590 chip with the addition of the front-end antenna the range of the sensor node is increased almost three times. The maximum output power is increased to 14 dbm and receiver sensitivity improved to -101 dbm. The circuit design requires only a few components. The board layout has its influence on the RF performance of the components. The layout and stack-up and schematic design by

Altium for the CC5290. The Altium is a software integration platform which brings together all tools that necessary to create a complete environment for electronic product, in a single application. The Altium Designer includes tools for all design tasks such as: schematic, PCB, circuit simulation, signal integrity analysis, and FPGA-based embedded system.

6.4 Implementing CC2590 RF Front End for Telos board

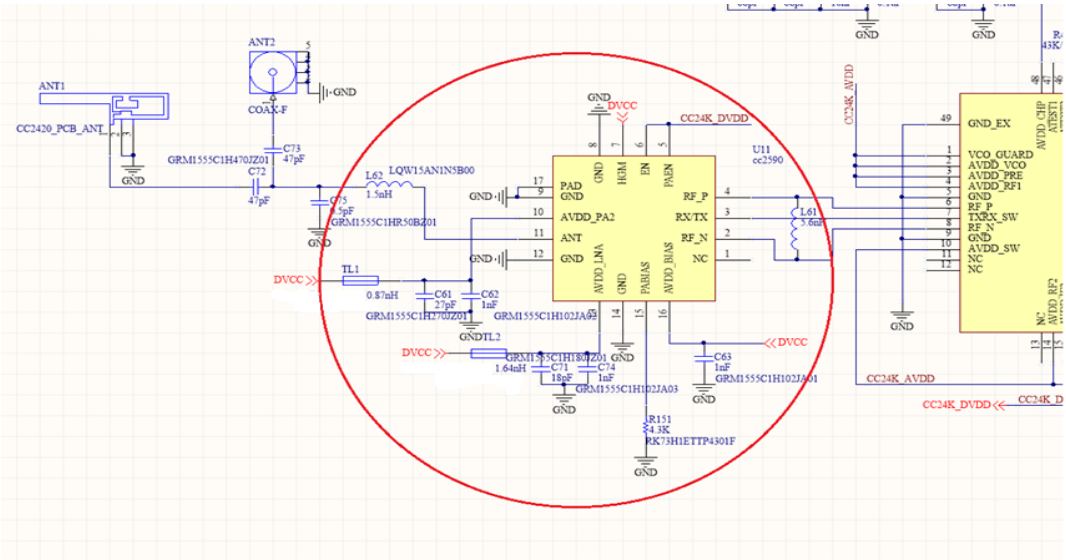

Figure 49: Application Circuit for CC2590

The old version of this toles has been designed using an auto router. These kinds of designs are not suitable, such as: power trace and gnd. So, I designed by manual routing, adding RF single end trace impedance and USB differential pair impedance. The RF impedance is 50 ohm and usb differential pair is 90 ohm.

The main advantages of using CC2590 are as follows:

1.CC2590 is superior RF front-end for low-control 2.4 GHz circuits.

2.CC2590 can be utilized as a part of the current and future systems working at 2.4 GHz having low power RF-handsets.

3.It expansions the affectability by enhancing the yield force and LNA for low power systems.

4.CC2590 has a little size and can be introduced on 4×4 mm bundles.

5.It contains LA, PA switches and RF coordinating including balun for little high of remote wireless networks. The new board that I designed is shown in Figure 50,51 and 52.

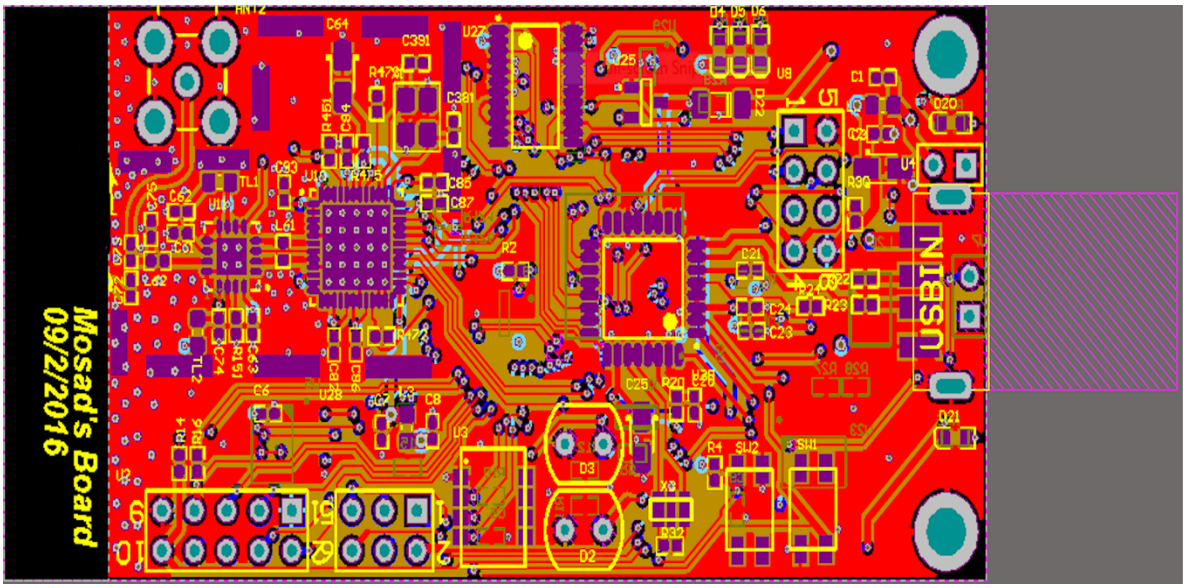

Figure 50: Front Board with CC2590 RF Front End

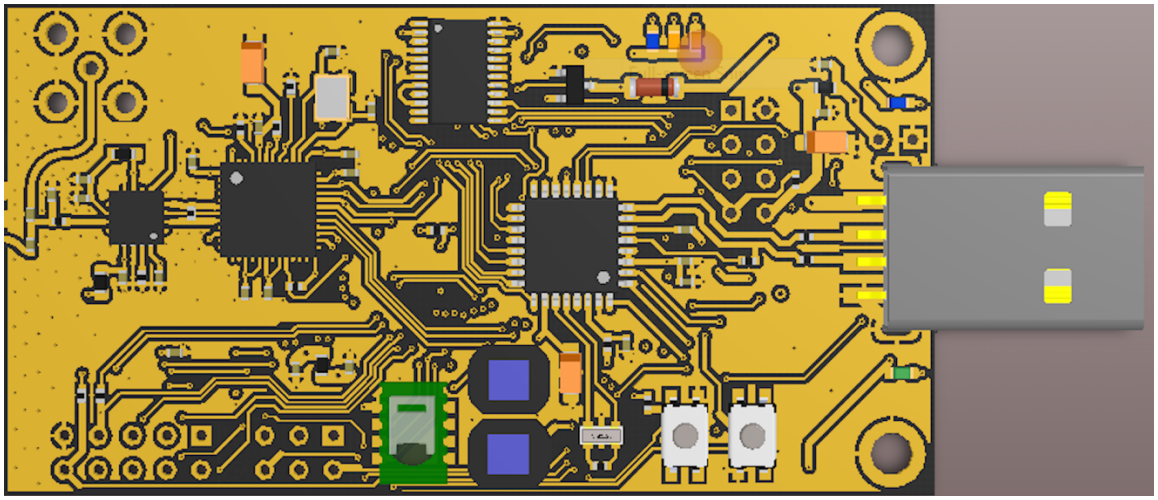

Figure 51: Rear Board with CC2590 RF Front End

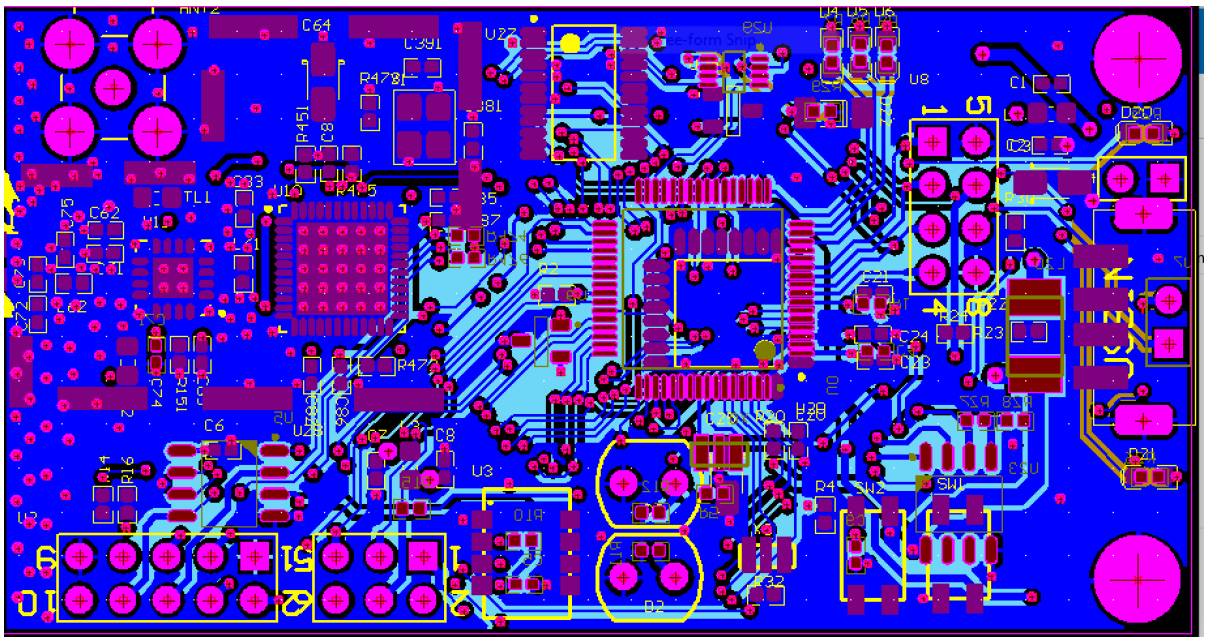

Figure 52: PCB layout with CC2590 RF Front End

By adding CC2590, New Telos design has been improved 20dB than older version. Normally communication range is in proportion to square of gain. Therefore, it may be extended 10 (Sqrt[20dB]=10) times than older version as theory. In result, the new version may be communicating till 500m/indoor~1250m/outdoor since old Telos is 50m/indoor and 125m/outdoor. The CC2590 can be applied to the circuit operating 2.4 GHz ISM band systems. It supports the IEEE 802.154 protocol and extremely efficient ZigBee systems. Its applications are extended to wireless audio systems and wireless consumer systems. Finally, there is the option of using external antennae that have a high gain and can extend more than 1km, if one is mindful of power consumption.

CHAPTER 7: CONCLUSION AND FUTURE WORK

7.1 Conclusion

In conclusion, the wireless sensor nodes showcase an emerging technology in intrusion detection and border surveillance system application. Wireless sensor networks have attracted much attention by demonstrating such versatile usages. Now, more than ever, threat assessment and intruder identification are becoming a priority. The optimization of UAV technology has been widely applied in the area of borderline surveillance, as it utilizes coexisting border control techniques and contemporary electronic detection systems. Combining the two detection vectors provides non-linear and linear sight detection systems. The system application is user-friendly and contains high sensing capabilities guarantying user simplicity in the real life implementation of WSNs. In the investigation of the OPNET operating and performance dynamics, we can carry out analysis on how the software enhances performance in the simulation of ZigBee WSNs.

Analysis indicates that the OPNET MODELER showcases an extreme performance in the simulation of ZigBee, as it utilizes a wide range of statistical and reporting techniques that work at various network topologies. Upon running different topologies, the analysis indicates mesh topology is reliable in the implementation of the simulation model, in preference to tree network topology. The wireless nodes have been found to work at close ranges of approximately 50 to 125m radius and, with software, implementation users can increase the existing distance in range. During the deployment phase, it was established that ZigBee WSN is easier to deploy as compared to other existing WSN simulators. The ZigBee WSN was found to decrease performance in its implementation and physical layers because of not properly incorporating the security and energy models. The number of nodes can be simulated and evaluated for the system deployment and operations of the border sense systems, thus testing the application simulation for all complexities.

The wireless sensor system architecture plays a vital role in the implementation of WSN's because placement is conducted in an extended geographical area. Deployment of low power sensor based architecture requires low power consumption components, thus enhancing border control activities. Since WSNs support a large number of sensors in a wide area with low bit rate transformation, the design should implement a multi-hop routing mechanism. This gives the network topology design room for efficient sensor distribution and increased scalability. The node architecture contains various elements that have environmental examining capabilities, therefore it enhances the sharing of physical environmental settings of areas with neighboring nodes under a given radius. This helps in determining whether or not the remote user is altered. With this implementation, the environmental disturbance issues are easily detected.

WSN coverage and connectivity are vital, as they measure the quality of service delivery and signal availability of the sensors' performance assessment. Sensors can effectively survey and monitor the environment and that information is transferred to nodes for data sink. Routing between nodes utilizes the shortest distance algorithm, thus enhancing the calculations of packet delays and determining the level of node transmission. In this work, we developed a solution for the border surveillance problem using WSN. The flexibility, and high sensing, of WSN make it as a part of our daily lives. The WSN application was implemented and tested using an advanced OPNET Modeler. Several tests were carried out to verify this implementation. It can be concluded that this application has achieved WSN assuming reasonable choice of the number of nodes and the data generation rate based on the 100, 200, 300, 400 and 500 nodes. Finally, designing a new board with 500m range while integrating a camera such as CMUCAM3 will help any country to secure their borders and will also reduce numbers of intensive human involvement. As a result, the cost effect will also be reduced.

7.2 Future Work

The wireless sensor networks have become indispensable to the realization of smart technology. The border control implementation can use the WSN to construct smart technology systems. Along these lines, there is some remaining work that needs to be completed in the near future. Future research can focus on associated communication issues and breaching path problems. This regards how secure the system application is in relation to modern day hackers' capabilities to exploit the coexisting flaws in the new design. It is proposed to use a novel object classification algorithm that specifically compares various dynamics for objects, shaped for any existing similarities. The application of algorithms is considered a generic means primarily used for the classification of object types. Integration of novels' extensions in the algorithms tends to reduce instances of false alarms, thereby making the system robust in the incorporation of a wide range of color spectrums and in the fusion of thermal images, thus generating smart visual surveillance systems for real-time monitoring. Moreover, due to limited power, consumption becomes a slight concern to extend the network's lifetime. Therefore, we will propose improvement on the system by creating miniaturized versions of the nodes with embedded solar panels or small wind generators nearby to provide an endless supply of energy in order to extend its lifetime. In future work, we will propose a novel integrating satellite systems with the border detection sensors which will provide live feedback on intruders in areas with harsh climatic or geographical conditions that hinder the deployment of the normal mobile surveillance systems. Finally, sensor nodes will be utilized in real wireless sensor network environments in order to extend the range of detection in any monitoring area.

REFERENCES

[1] Felemban, Emad. "Advanced border intrusion detection and surveillance using wireless sensor network technology." International Journal of Communications, Network and System Sciences vol.6, no. 5 pp. 251, 2013.

[2] Zhi Sun, Pu Wang, Mehmet C. Vuran, Mznah A. Al-Rodhaan, Abdullah M. Al-Dhelaan, and Ian F. Akyildiz "BorderSense: Border patrol through advanced wireless sensor networks," Ad Hoc Networks, vol. 9, no. 3 pp. 468-477, 2011.

[3] Bellazreg, Ramzi, Noureddine Boudriga, and Sunshin An. "Border Surveillance using sensor based thick-lines." In Information Networking (ICOIN), IEEE International Conference on, pp. 221-226, 2013.

[4] Liu, Benyuan, Olivier Dousse, Jie Wang, and Anwar Saipulla. "Strong barrier coverage of wireless sensor networks." In Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing, pp. 411-420, 2008.

[5] Ahmed, Muhammad R., Mohammed A. Aseeri, Xu Huang, and Dharmendra Sharma. "Border Surveillance Framework Using Secure WSN as A New Approach to Avoid Threats." International Border Guard Conference, At Saudi Arabia, Riyadh, 2012.

[6] T. He, S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, J. Hui and B. Krogh, "An Energy-Efficient Surveillance System Using Wire-less Sensor Networks," 2nd International Conference on Mobile Systems, Applications and Services, Boston, 6-9 June 2004.

[7] Sinopoli, Bruno, Courtney Sharp, Luca Schenato, Shawn Schaffert, and S. Shankar Sastry. "Distributed control applications within sensor networks." Proceedings of the IEEE vol.91, no. 8 pp. 1235-1246, 2003.

[8] Arora, Anish, Prabal Dutta, Sandip Bapat, Vinod Kulathumani, Hongwei Zhang, Vinayak Naik, Vineet Mittal et al. "A line in the sand: a wireless sensor network for target detection, classification, and tracking." Computer Networks vol.46, no. 5 pp. 605-634, 2004.

[9] Mishra, Ashish, Komal Sudan, and Hamdy Soliman. "Detecting border intrusion using wireless sensor network and artificial neural network." In Distributed Computing in Sensor Systems Workshops (DCOSSW), 6th IEEE International Conference on, pp. 1-6, 2010.

[10] Rothenpieler, Peter, Daniela Krüger, Dennis Pfisterer, Stefan Fischer, Denise Dudek, Christian Haas, Andreas Kuntz, and Martina Zitterbart. "Flegsens-secure area monitoring using wireless sensor networks." Proceedings of the 4th Safety and Security Systems in Europe 2009.

[11] Bokare, Madhav, and Mrs Anagha Ralegaonkar. "Wireless Sensor Network: A Promising Approach for Distributed Sensing Tasks." Excel Journal of Engineering Technology and Management Science vol.1, no. 1 pp. 1-9, 2012.

[12] Al-Karaki, Jamal N., and Ahmed E. Kamal. "Routing techniques in wireless sensor networks: a survey." IEEE Wireless communications, vol.11, no. 6 pp. 6-28, 2004.

[13] Hill, Jason Lester. System architecture for wireless sensor networks. Diss. University of California, Berkeley, 2003.

[14] Lu, Fei, Guohui Tian, Fengyu Zhou, Yinghua Xue, and Baoye Song. "Building an intelligent home space for service robot based on multi-pattern information model and wireless sensor networks." Intelligent Control and Automation vol.3, no.1 pp. 90, 2012.

[15] Sharma, Shamneesh, Dinesh Kumar, and Keshav Kishore. "Wireless Sensor Networks-A Review on Topologies and Node Architecture." International Journal of Computer Sciences and Engineering vol.1, no. 2 pp. 19-25, 2013.

[16] Everaerts, Jurgen. "The use of unmanned aerial vehicles (UAVs) for remote sensing and mapping." The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences vol. 37no. 9 pp. 1187-1192, 2008.

[17] Ardö, Jonas, Nancy Lambert, Vladimir Henzlik, and Barry Rock. "Satellite Based Estimations of Coniferous Forest Cover Changes: Krusne Hory, Czech Republic." A Journal of the Human Environment vol. 26, no. 3 pp.158-166, 1997.

[18] Aldosari, Saeed A., and José MF Moura. "Detection in sensor networks: The saddlepoint approximation." Signal Processing, IEEE Transactions vol. 55, no. 1 pp. 327-340, 2007.

[19] Girard, Anouck R., Adam S. Howell, and J. Karl Hedrick. "Border patrol and surveillance missions using multiple unmanned air vehicles." Decision and Control, 2004. CDC. 43rd IEEE Conference on. Vol. 1. No.2 , 2004.

[20] Stuntebeck, Erich P., Dario Pompili, and Tommaso Melodia. "Wireless underground sensor networks using commodity terrestrial motes." In 2nd IEEE Workshop on Wireless Mesh Networks, vol. 3, no. 7, pp. 112-114. 2006.

[21] Kalita, Hemanta Kumar, and Avijit Kar. "Wireless sensor network security analysis." International Journal of Next-Generation Networks, vol.1, no. 1 pp. 1-10, 2009.

[22] Mall, Anjana, and Mrs Shusmita Ghosh. "A Neural Network Based Face Detection Approach." International Journal of Computer Technology and Applications vol.3, no. 2, 2012.

[23] Li, Mo, and Yunhao Liu. "Underground structure monitoring with wireless sensor networks." In Proceedings of the 6th international conference on Information processing in sensor networks, pp. 69-78., 2007.

[24] Akyildiz, Ian F., and Erich P. Stuntebeck. "Wireless underground sensor networks: Research challenges." Ad Hoc Networks vol. 4, no. 6 pp. 669-686, 2006.

[25] Schwiebert, Loren, Sandeep KS Gupta, and Jennifer Weinmann. "Research challenges in wireless networks of biomedical sensors." In Proceedings of the 7th annual international conference on Mobile computing and networking, pp. 151-165, 2001.

[26] Srivastava, Neelam. "Challenges of next-generation wireless sensor networks and its impact on society." arXiv preprint arXiv, pp. 1002.4680, 2010.

[27] Baroudi, Uthman, Anas Al-Roubaiey, Samir Mekid, Abdelhafid Bouhraoua, and Yau Garba. "Smart bolts monitoring using wireless sensor network: implementation and performance evaluation." International Journal of Distributed Sensor Networks 2014.

[28] Goodrich, Michael A., Bryan S. Morse, Damon Gerhardt, Joseph L. Cooper, Morgan Quigley, Julie A. Adams, and Curtis Hump. "Supporting wilderness search and rescue using a camera-equipped mini UAV." Journal of Field Robotics vol. 25, no.12 pp. 89-110, 2008.

[29] Alkhathami Mosad , Lubna Alazzawi, and Ali Elkateeb. "Models and Techniques Analysis of Border Intrusion Detection Systems." Global Journal of Researches In Engineering vol. 15, no. 7 pp. 1-11, 2015.

[30] Kim, Dong Seong, Sang Min Lee, Tae Hwan Kim, and Jong Sou Park. "Quantitative intrusion intensity assessment for intrusion detection systems." Security and Communication Networks vol. 5, no. 10 pp. 1199-1208 2012.

[31] Said, Omar, and Alaa Elnashar. "Scaling of wireless sensor network intrusion detection probability: 3D sensors, 3D intruders, and 3D environments." EURASIP Journal on Wireless Communications and Networking, vol. 2 no. 1 pp. 1-12, 2015.

[32] Guo, Chun, Yajian Zhou, Yuan Ping, Zhongkun Zhang, Guole Liu, and Yixian Yang. "A distance sum-based hybrid method for intrusion detection." Applied intelligence vol. 40, no. 1 pp178-188, 2014.

[33] Vokorokos, Liberios, Michal Ennert, Zuzana Dudláková, and Olympia Fortotira. "A Control Node for Intrusion Detection Systems Management." vol. 14, no. 3 pp. 28-31, 2014.

[34] Shamshirband, Shahaboddin, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ahmed Patel. "An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique." Engineering Applications of Artificial Intelligence vol. 26, no. 9 2105-2127, 2013.

[35] Sheltami, Tarek, Abdulsalam Basabaa, and Elhadi Shakshuki. "A3ACKs: adaptive three acknowledgments intrusion detection system for MANETs." Journal of Ambient Intelligence and Humanized Computing vol. 5, no. 4 pp. 611-620, 2014.

[36] Kumar, Anurag. "Wireless sensor networks for human intruder detection." Journal of the Indian Institute of Science, Special Issue on Advances in Electrical Science vol. 90, no. 3 pp. 347-380, 2010.

[37] Absar-ul-Hasan, Ghalib A. Shah, and Ather Ali. 'Intrusion Detection System Using Wireless Sensor Networks'. EJSE Special Issue: Wireless Sensor Networks and Practical Applications pp. 90-99, 2015.

[38] Alkhathami, Mosad H., and Lubna Alazzawi. "Border Security Control via Distributed WSN Technology."International Journal of Scientific & Engineering Research, vol. 6, no. 3, 2015.

[39] Hasan, Osman, ed. Formalized Probability Theory and Applications Using Theorem Proving. IGI Global, 2015.

[40] Fuchsberger, Andreas. "Intrusion detection systems and intrusion prevention systems." Information Security Technical Report vol. 10, no. 3 pp. 134-139, 2005.

[41] Onur, Ertan, Cem Ersoy, Hakan Deliç, and Lale Akarun. "Surveillance wireless sensor networks: deployment quality analysis." Network, IEEE 21, no. 6 pp. 48-53, 2007.

[42] Barry, Bazara IA, and H. Anthony Chan. "Architecture and performance evaluation of a hybrid intrusion detection system for IP telephony." Security and Communication Networks vol. 6, no. 12 pp. 1539-1555, 2013.

[43] Boob, Snehal, and Priyanka Jadhav. "Wireless intrusion detection system." International Journal of Computer Applications vol. 5, no. 8 pp. 9-13, 2010.

[44] Smolinski, Tomasz G., Mariofanna G. Milanova, and Aboul-Ella Hassanien, eds. Applications of computational intelligence in biology Springer: current trends and open problems. vol. 122, 2008.

[45] Cai, Chuan, and Liang Yuan. "Intrusion detection system based on ant colony system." Journal of Networks vol. 8, no. 4 pp. 888-894, 2013.

[46] Haq, Nutan Farah, Abdur Rahman Onik, Md Avishek, Khan Hridoy, Musharrat Rafni, Faisal Muhammad Shah, and Dewan Md Farid. "Application of Machine Learning Approaches in Intrusion Detection System: A Survey." IJARAI) International Journal of Advanced Research in Artificial Intelligence Vol. 4, No.3, 2015.

[47] Sindhuja, L. S., and G. Padmavath. "Clone Detection Using Enhanced EDD (EEDD) with Danger Theory in Mobile Wireless Sensor Network." International Journal of Security & Its Applications vol. 9, No. 4 pp. 185-202, 2015.

[48] Alkhathami, Mosad, Lubna Alazzawi, and Ali Elkateeb. "Border Surveillance And Intrusion Detection Using Wireless Sensor Networks." International Journal of Advances in Engineering & Technology vol. 8, no. 2 pp. 17, 2015.

[49] Janakiraman, S., and V. Vasudevan. "An intelligent distributed intrusion detection system using genetic algorithm." Journal of Convergence Information Technology 4, no. 1 pp.70-76, 2009.

[50] Zhang, Dengsheng, and Guojun Lu. "A comparative study on shape retrieval using Fourier descriptors with different shape signatures." In Proc. International Conference on Intelligent Multimedia and Distance Education vol. 5 no.1. 2001.

[51] Korcák, Michal, Jaroslav Lámer, and Frantisek Jakab. "Intrusion Prevention/Intrusion Detection System (IPS/IDS) For Wifi Networks." International Journal of Computer Networks & Communications vol. 6, no. 4 pp.77, 2014.

[52] Nicholson, Andrew, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke. "SCADA security in the light of Cyber-Warfare." Computers & Security vol. 31, no. 4 pp. 418-436, 2012.

[53] Wong, Wai Kit, Chu Kiong Loo, and Way Soong Lim. "Omnidirectional Human Intrusion Detection System Using Computer Vision Techniques." Effective Surveillance for Homeland Security: Balancing Technology and Social Issues pp. 435-439, 2013.

[54] Yick, Jennifer, Biswanath Mukherjee, and Dipak Ghosal. "Wireless sensor network survey." Computer networks vol.52, no. 12 pp. 2292-2330, 2008.

[55] López, Javier, and Jianying Zhou, eds. “Wireless sensor network security,” IOS Press Books & Journals, Online & Print, vol. 1. no. 3 2008.

[56] Meghanathan, Natarajan, Dhinaharan Nagamalai, and Nabendu Chaki. "Advances in

Computing and Information Technology." vol. 1 no. 5, 2012.

[57] Walsh, Courtney E. "Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the Mosaic Theory and the Limits of the Fourth Amendment." . Thomas L. Rev. vol. 24 pp. 169, 2011.

[58] Natkunanathan, Sivatharan, Joseph Pham, William J. Kaiser, and Greg Pottie. "Embedded networked sensors: Signal search engine for signal classification." In Sensor and Ad Hoc Communications and Networks. First Annual IEEE Communications Society Conference on, pp. 139-144, 2004.

[59] Shifeng Yang Jimin Zhao Daudi S Simbeye. "Aquaculture Environment Control Based on WSN." LAP Lambert Academic Publishing. 2015

[60] Zhu, Chuan, Chunlin Zheng, Lei Shu, and Guangjie Han. "A survey on coverage and connectivity issues in wireless sensor networks." Journal of Network and Computer Applications vol. 35, no. 2 pp. 619-632, 2012.

[61] Varga, András. "The OMNeT++ discrete event simulation system." In Proceedings of the European simulation multiconference (ESM'2001), vol. 9, no. 185, pp. 65, 2001.

[62] Chang, Xinjie. "Network simulations with OPNET." In Proceedings of the 31st conference on Winter simulation: Simulation a bridge to the future Vol. 1 no. 9, pp. 307-314, 1999.

[63] Hammoshi, M., and R. Al-Ani. "Using OPNET to teach students computer networking subject." Tikrit Journal of Pure Science vol. 15, no. 1 pp. 1813-1662, 2012.

[64] Molisch, Andreas F., Kannan Balakrishnan, Dajana Cassioli, Chia-Chin Chong, Shahriar Emami, Andrew Fort, Johan Karedal et al. "IEEE 802.15. 4a channel model-final report." vol 15, no. 04 pp802, 2004.

[65] Pan, Meng-Shiuan, Hua-Wei Fang, Yung-Chih Liu, and Yu-Chee Tseng. "Address

assignment and routing schemes for ZigBee-based long-thin wireless sensor networks." In Vehicular Technology IEEE Conference. VTC Spring, pp. 173-177, 2008.

[66] Gulzar, Kashif. "Camera design for pico and nano satellite applications." Lulea University of Technology, 2009.

[67] Rowe, Anthony, Dhiraj Goel, and Raj Rajkumar. "Firefly mosaic: A vision-enabled wireless sensor networking system." In Real-time systems symposium, 28th IEEE international, pp. 459-468, 2007.

[68] Tsai, Jia-Min. "A Vibrotactile Glove Design and its Rehabilitation Effects on Hand Function in Stroke Patients. 2015.

[69] Hlavac, Vaclav. "Fundamentals of Image Processing." Optical and Digital Image Processing: Fundamentals and Applications pp 71-96, 2011.

[70] Mosad Alkhathami, Lubna Alazzawi. "Overview of Border Control Using Wireless Sensor Network."International Journal of Scientific & Engineering Research, Vol. 6, no 3. 2015.

[71] Polastre, Joseph, Robert Szewczyk, and David Culler. "Telos: enabling ultra-low power wireless research." In Information Processing in Sensor Networks. IEEE Fourth International Symposium on, pp. 364-369, 2005.

[72] Sankar, Gundu Siva, and Suresh Angadi. "Wireless Sensor Network for Border Monitoring." The International Journal Of Engineering And Science (IJES) Vol. 2, no. 4 pp. 65-68, 2013.

[73] Zhang, Wei-Cong, Xin-Wu Yu, and Zhong-Cheng Li. "Wireless Network Sensor Node Design Based on CC2530 and ZigBee Protocol Stack." Jisuanji Xitong Yingyong-Computer Systems and Applications vol.20, no. 7 pp. 184-187, 2011.

ABSTRACT

BORDER SURVEILLANCE AND INTRUSION DETECTION USING A WIRELESS SENSOR NETWORK

by

MOSAD ALKHATHAMI

August 2016

Advisor: Dr. Caisheng Wang

Major: Electrical Engineering

Degree: Doctor of Philosophy

To control the border more effectively, countries may deploy a detection system that enables real-time surveillance of border integrity. Events such as border crossings need to be monitored in real time so that any border entries can be noted by border security forces and destinations marked for apprehension. Wireless Sensor Networks (WSNs) are promising for border security surveillance because they enable enforcement teams to monitor events in the physical environment. In this work, probabilistic models have been presented to investigate senor development schemes while considering the environmental factors that affect the sensor performance. Simulation studies have been carried out using the OPNET to verify the theoretical analysis and to find an optimal node deployment scheme that is robust and efficient by incorporating geographical coordination in the design. Measures such as adding camera and range-extended antenna to each node have been investigated to improve the system performance. A prototype WSN based surveillance system has been developed to verify the proposed approach.

AUTOBIOGRAPHICAL STATEMENT

MOSAD ALKHATHAMI

I was born in Saudi Arabia . I finished my high school from Khatham High School in Asir, Saudi Arabia. I received BS in Electrical Engineering in 2009 from Purdue Calumet University in Hammond, Indiana. To further my education, I applied to DePaul University, Chicago, Illinois where I received my MS in Telecommunication Systems in 2011, in honor standing.