

Study on Embedded Sensor Networks

Bhavnes Jain



DEPARTMENT OF ELECTRICAL ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
DELHI- 110042 (INDIA)
June, 2020

A Thesis

on

Study on Embedded Sensor Networks

Submitted in partial fulfilment of the requirements for the degree
of

Doctor of Philosophy

in

Department of Electrical Engineering

by

Bhavnesht Jaint

(2K12/PhD/EE/07)

Under the supervision of

Prof. S. Indu

**Department of Electronics and Communication Engineering,
Delhi Technological University, Delhi**

and

Prof. Neeta Pandey

**Department of Electronics and Communication Engineering,
Delhi Technological University, Delhi**



**DEPARTMENT OF ELECTRICAL ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY**

(Formerly Delhi College of Engineering)

DELHI- 110042 (INDIA)

June, 2020

DECLARATION

I hereby declare that the work which is being presented in this thesis entitled “**Study on Embedded Sensor Networks**”, submitted in the Department of Electrical Engineering of the Delhi Technological University, Delhi, in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy, is an authentic record of my own work carried out during the period from 2012 to 2020 under the supervision of Prof. S. Indu and Prof. Neeta Pandey, Department of Electronics and Communication Engineering, Delhi Technological University, Delhi. The content of this thesis has not been submitted either in part or whole to any other university or institute for the award of any degree or diploma.

(Bhavnesht Jaint)
2K12/PhD/EE/07
Department of Electrical Engineering
Delhi Technological University
(Formerly Delhi College of Engineering)
Delhi, INDIA-110042

CERTIFICATE

This is to certify that the thesis entitled “**Study on Embedded Sensor Networks**” being submitted by Bhavnesh Jaint to the Department of Electrical Engineering, Delhi Technological University, Delhi, for the award of the degree of Doctor of Philosophy, is a record of bona fide research work carried out by her under our guidance and supervision. In our opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted to any other university or institute for the award of any degree or diploma.

Prof. S. Indu
Professor
Department of Electronics and
Communication Engineering,
Delhi Technological University
Delhi-110 042

Prof. Neeta Pandey
Professor
Department of Electronics and
Communication Engineering,
Delhi Technological University
Delhi-110 042

ACKNOWLEDGMENTS

Firstly, I bow my head before the almighty for vesting in me the wisdom and stranding by me at every step for all what I am today.

I would like to express my deep respect and sincere gratitude to my Supervisor, Prof. S. Indu, Professor, Dean, Student Welfare, Department of Electronics and Communication Engineering, DTU, New Delhi for her valuable guidance, suggestions, help and necessary support time to time during course of my study.

I extend my sincere thanks to the Co-Supervisor, Prof. Neeta Pandey, Professor, Department of Electronics and Communication Engineering for providing moral support, valuable suggestions and necessary support from time to time during present study.

My heartfelt gratitude to the members of Departmental Research Committee and Students Research Committee for kind motivation and support.

I would like to express my sincere thanks and gratitude to Prof. Madhusudan Singh Yadav, Ex- Head of the Department of Electrical Engineering and Dean UG and Prof. Uma Nangia, Head of the Department, Electrical Engineering for her invaluable help, moral encouragement and providing all the necessary facilities during the course of this research work.

Special thanks are extended to the all faculty members of the Department of Electrical Engineering specially, Prof. D.R. Bhaskar, Prof. Mukhtiar Singh, Prof. S.K.B. Valluru, Prof. Narender Kumar, Prof. Bharat Bhushan, Prof. Priya Mahajan, Prof. Rachna Garg, Prof. M.M. Tripathi, Prof. Dheeraj Joshi, Prof. Mini Sreejeth, Sh. Ram Bhagat, Ms. Garima, Sh. Kuldeep Singh, Sh. A.R. Kulkarni and Dr. Priyanka Jain, Department of Electronics and Communication Engineering and all my teachers for their valuable help and constant inspiration to me during Ph.D. Programme.

I convey sincerely thankful to Dr. Anup Mandpura, Assistant Professor, Department of Electrical Engineering for his help in compilation and editing of the manuscript and Dr. Himanshu Sharma for his valuable support.

Special thanks are extended to my parents for their best wishes and support. I also thank my brothers, sister, father in-law, brother in- laws and sister in-laws and my niece, nephew for their affection, best wishes and support. I would like to express special thanks to my affectionate husband, Dr. Mukesh Kumar, my kids Master Agrim and Master Arnav for their silent sacrifice and patience who had to miss a number of affectionate hours that truly belonged them to complete this endeavor successfully.

Finally, I would like to thank everybody who has given contribution to the successful realization of this work and express my apology that I could not mention their names individually.

Date: 09th June 2020
Place: DTU, New Delhi

(Bhavnesht Jain)

Abstract

Wireless sensor networks (WSNs) are widely used in a range of applications in the real world. WSNs have demonstrated their applicability in the field of medical, military, and broad range of surveillance applications and monitoring. This thesis focuses on three major aspects related to WSN namely Energy efficiency, Security and real time application of WSN. The contributions are

Energy efficiency in wireless sensor networks (WSN) is important as the sensor nodes are operated with restricted battery life. The choice of modulation scheme and error control code play a significant role in energy consumption of WSN. The analysis shows that the energy consumption in WSN may be reduced by selecting optimal combination of modulation scheme and error control codes. Our simulation results show that by using BPSK modulation with Reed Solomon (RS) code saves 48 % energy in WSN at an internode distance of 60 meters in comparison to other modulation schemes.

In general, wireless sensor networks comprises of large number of sensor nodes. The communication among them depends on behaviour of each sensor node. Hence for securing the network, it is necessary to identify malicious nodes. In this thesis we present various techniques for malicious node detection and prediction.

Home automation is one of the applications of WSN. We present low cost, compact and flexible ZigBee based home automation for remote control of house hold devices. This system assures optimal usage of electricity, thereby reducing carbon footprint.

we propose an intelligent auto-dipping system that will be placed on the dashboard of a vehicle. Once headlight of an oncoming vehicle is detected, the vehicle's high beam will be automatically dipped, with a dipper flash to signal the approaching vehicle. The

system can be most successful when it is mounted in every vehicle. This system can help to avoid accidents caused by the dazzling created by oncoming high beams. The proposed system uses a USB web cam and Raspberry Pi for real time processing. The validation of the system has been done using both simulation and actual hardware.

CONTENTS

Declaration	i
Certificate	ii
Acknowledgement	iii
Abstract	iv
Contents	vi
List of Figures	x
List of Tables	xiii
List of Abbreviations and Symbols	xiv
1.0 Introduction	1
1.1 Wireless Sensor Network	1
1.2 Motivation	5
1.3 Research Objectives	8
1.4 Research Contributions	8
1.4.1 Energy Efficient Communication Techniques for Wireless Sensor Network	9
1.4.2 Malicious Node Detection and Prediction	9
1.4.3 Applications of Embedded systems and WSN	10
1.5 Thesis Outline	11
2.0 Literature Review	13
2.1 Error Control Codes and Modulation Schemes in WSN	13
2.1.1 Modulation Techniques in Wireless Sensor Networks (WSN)	14
2.1.2 Error Control Codes and Modulation Schemes in WSN	15
2.2 Malicious Node Detection and Prediction	20
2.3 Real Time Applications	23

2.3.1	Smart Home Automation	23
2.3.2	Auto Dipper System	28
2.4	Research Gaps	29
3.0	Energy Efficient Communication Techniques for Wireless Sensor Networks	31
3.1	Introduction	31
3.2	Digital Modulation and Error Control Coding (ECC) Schemes in WSN	32
3.2.1	Digital Modulation Schemes	33
3.2.2	Error Control Coding Schemes in WSN	34
3.2.3	Types of Error Control Codes	35
3.3	System Design Methodology	38
3.4	Energy Model of Sensor Node	40
3.4.1	Variation of Signal Energy with ECC and Modulation Techniques	44
3.4.2	Variations of Node Energy with ECC and Modulation Parameters	46
3.5	Experimental Setup and Simulation Results	47
3.5.1	ZigBee Home Automation Scenario in Qualnet 5.0 Simulator	47
3.5.2	Implementation of the WSN Node Energy Model Equations in MATLAB	48
3.5.3	Simulation Results	49
3.6	Conclusion	59
4.0	Malicious Node Detection and Prediction	60
4.1	Weighted Trust Evaluation	61
4.1.1	Operation of Weighted Trust Evaluation	61
4.1.2	Network Model and Topology	62

4.1.3	Error Detection	63
4.1.4	Weight Modification	64
4.2	Cluster-Based Weighted Trust Evaluation	64
4.2.1	Algorithm	65
4.2.2	Simulation and Modelling	66
4.3	Malicious Node Detection in WSN Using Support Vector Machine: (A Machine Learning Approach)	73
4.3.1	Malicious Node Detection Strategy	74
4.3.2	Simulation Results	80
4.3.3	Comparison of SVM and AR for Performance Parameters	85
4.4	Extended Kalman Filtering (EKF) Technique to Detect Byzantine Attack in a WSN	88
4.4.1	Byzantine Attack Detection Strategy	89
4.4.2	Extended Kalman Filter (EKF)	90
4.4.3	Time Series Prediction using EKF for Malicious Node Detection and Byzantine Attack	91
4.4.4	Working	94
4.4.5	Simulation Results	95
4.4.6	Conclusion	101
5.0	Real Time Applications	102
5.1	Home Automation System Configuration	102
5.1.1	Master Unit and its Operation	104
5.1.2	Slave Unit and its Operation	105
5.1.3	Working of the Proposed System	107

5.1.4	Electrical Parameters Measurement	108
5.1.5	Control of Electrical Home Appliances	109
5.1.6	Data Storage	110
5.1.7	Hardware Component Description	111
5.1.8	Complete System Work Description	117
5.1.9	Slave Unit Section	120
5.1.10	Web Pages Development	125
5.1.11	Result and Discussions	129
5.2	Auto Dipper System	133
5.2.1	Video Processing for Head Light Detection	134
5.2.2	Algorithm	135
5.2.3	Hardware Implementation	141
5.2.4	Results	145
5.3	Conclusion	148
6.0	Conclusion and Future Work	149
6.1	Conclusions	149
6.2	Future works	152
	References	153
	List of Publications	167

LIST OF FIGURES

Fig. No.	Title	Page No.
1.1	Wireless Sensor Network	2
3.1	Modulation and Error Control Codes in a communication system	32
3.2	Error Correcting Codes (ECCs) in WSN	36
3.3	Codeword for RS code with k data and 2t parity bits	37
3.4	System design methodology for finding energy optimal ECC-modulation pair	39
3.5	Block diagram for WSN design exploration agenda	40
3.6	The consumption of power in SN for various modes of operation	44
3.7	BER performance of various Modulations schemes	51
3.8	Simulation Results ASK, BPSK and OQPSK of in MATLAB	51
3.9	BER performance of M-array PSK	52
3.10	BER performance of BPSK with uncoded and with various ECC	53
3.11	BER performance results of BPSK using different RS Codes	53
3.12	Simulation results of energy consumption in transmit, receive and Idle modes	54
3.13	Normalised signal energy of 4-QAM and 4-PSK w.r.t code word length (N)	56
3.14	Normalized signal energy of 4-QAM, 4-PSK and 4-FSK w.r.t Error Correction Capability (t)	57
3.15 (a)	Variations of sensor node energy with RS code (N=63) and t=2 for varying constellation sizes of MPSK Modulation at different distance (d)	57
3.15 (b)	Variations of SN energy with RS code(N=63) and t=4 for varying constellation sizes of MPSK Modulation at different distances (d)	58
4.1	Hybrid Topology	63
4.2	Flowchart for Cluster Based WTE	67
4.3	Random deployment of SN in an area	68
4.4	CBWTE deployment of SN in an area	69
4.5	Detection time for random deployment	70
4.6	Detection time for Cluster Based deployment	71

4.7	Detection Ratio vs Malicious Nodes (CBWTE Method)	73
4.8	Support Vector with Maximal Margin	75
4.9	Block diagram of the process of SVM	78
4.10	Flow chart for SVM	79
4.11	Simulation of SVM model for Predicted label and True label of data and Error Detection	81
4.12	Detecting Error Instances by Comparing Original (with noise) and Predicted Signal	82
4.13	Prediction time for SVM	83
4.14	Detection ratio for SVM	84
4.15	Mis-detection ratio for SVM	84
4.16	Accuracy for SVM	85
4.17	Detection ratio of AR and SVM prediction	86
4.18	Accuracy for AR and SVM Prediction	87
4.19	RMS Accuracy for AR and SVM Prediction	87
4.20	Kalman Filter response for PT08.S1(CO) data sample size 168 data points i.e. 1-week	96
4.21	Kalman Filter response for NHMC(GT) data sample size 168 data points i.e. 1-week	96
4.22	Kalman Filter response for PT08.S2(NMHC) data sample size 168 data points i.e. 1 week	96
4.23	Kalman Filter response for C6H6(GT) data sample size 168 data points i.e. 1-week	97
4.24	Kalman Filter response for PT08.S3(NO ₂) data sample size 168 data points i.e. 1-week	97
4.25	Kalman Filter response for PT08.S3(O ₃) data sample size 168 data points i.e. 1-week	97
4.26	Performance of EKF on 168 data points, distributed over a period of 7 days	100
5.1	Functional block diagram of the system configuration	103
5.2	Block diagram of Master Unit	105
5.3	Block diagram of Slave Unit	106
5.4	Pin diagram of the UNO along with mapping of Atmega328 pin	112
5.5	Micro storage breakout board of Arduino	116
5.6	Master Unit Hardware	118
5.7	Schematic of Master Unit	121
5.8	Schematic of Slave Unit	123

5.9	Slave Unit Hardware	124
5.10	Login page of user	126
5.11	Webpage of monitor and control of devices	127
5.12	Webpage of admin	128
5.13	Controlling and monitoring of AC	129
5.14	Controlling and monitoring of Electric Iron	130
5.15	Controlling and Monitoring of three Devices	131
5.16	Flow chart of the system	135
5.17	Field of view of camera for cropping 30% of image	136
5.18	Prototype Module Hardware	142
5.19	Connection diagram of the dipper system	143
5.20	Original frame	144
5.21	Cropped frame	145
5.22	Greyscale frame	145
5.23 (a)	Frame after Thresholding	146
5.23 (b)	Thresholding at various percentages	146
5.24	MSER regions after processing	147
5.25	Proteus simulation for testing purpose	147

LIST OF TABLES

Table No.	Title	Page No.
2.1	Summary of related work on Modulation ECC and in WSN	18
2.2	Consolidated Comparison Report of all Systems	27
3.1	Comparison of Various Modulation Techniques	33
3.2	Parameters of Reed Solomon (RS) Code	37
3.3	Formulas expressed for T_{on} , SNR_{coded} and E_{sig_norm}	45
3.4	Simulations Parameters	48
3.5	BER of various modulation Schemes	50
3.6	Simulation results in Qualnet for energy consumption in sensor nodes	55
3.7	MATLAB simulation results for RS (N=63) code with t=2 and t=4	58
4.1	Simulation Parameters for CBWTE	68
4.2	Results of CBWTE method for Detection Ratio vs nodes	72
4.3	Simulation parameters for SVM	80
4.4	Performance analysis of simulation results for first 24 data points out of 168 data points	98
4.5	Performance Measure for EKF	100
5.1	Power consumption of different home appliances determined by the system	132

LIST OF ABBREVIATIONS AND SYMBOLS

%	: Percentage
°C	: Degree Celsius
A	: Ampere
ADC	: Analog-to-Digital Converter
AFECCC	: Adaptive Forward Error Correction Code Control
AGWN	: Additive White Gaussian Noise
AHRI	: Aware Home Research Initiative
AR	: Auto Regression
ARQ	: Automatic Repeat Request
ASK	: Amplitude Shift Keying
BCD	: Binary-Coded Decimal
BCH	: Boss, Chaudhuri and Hocquenghen
BER	: Bit Error Rate
BPSK	: Binary Phase Shift Keying
BS	: Base Station
CASAS	: Centre for Advanced Studies in Adaptive Systems
CBWTE	: Cluster Based Weighted Trust Evaluation
CC	: Convolution Codes
CompEM	: Computation Energy Model
CG	: Coding Gain
CH	: Cluster Head
Ckt	: Circuit
DAC	: Digital-To-Analog Converter
DDR	: Daily detection ratio
DMDR	: Daily Misdetection Ratio
DTMF	: Dual Tone Multi Frequency
et al.	: and others
ECC	: Error Control Coding
EEPROM	: Electrically Erasable Programmable Read-Only Memory
EKF	: Extended Kalman Filter
FEC	: Forward Error Correction
Fig.	: Figure
FN	: Forward Node
FS	: frequency synthesizer
FSK	: Frequency Shift Keying
GIT	: Georgia Institute of Technology
GPRS	: General Packet Radio Service
GSM	: Global System Mobile
IDC	: Iteratively Decoded Codes
IFA	: Intermediate-Frequency Amplifier
i.e.	: That is
IOT	: Internet on Things
KF	: Kalman Filter
LBC	: Linear Block Codes
LCD	: Liquid Crystal Display
LDPC	: Low-density Parity Check
LNA	: Low-Noise Amplifier
LPF	: Low-Pass Filter

MAC	:	Medium Access Control
MATLAB	:	Matrix Laboratory
ms	:	Mill second
M-FSK	:	M-ary Phase Shift Keying
M-QAM	:	M-ary Quadrature Amplitude Modulation
MSER	:	Maximally Stable External Regions
OMDR	:	Overall Misdetection Ratio
OQPSK	:	Offset Quadrature Phase Shift Keying
OOK	:	On-Off Keying
PA	:	Power Amplifier
PSD	:	Power Spectral Density
PSK	:	Phase Shift Keying
PWM	:	Pulse Width Modulation
QAM	:	Quadrature Amplitude Modulation
QoS	:	Quality of Service
RadioEM	:	Radio Energy Model
RISC	:	Reduced Instruction Set Complex
RTC	:	Real Time Clock
SD Card	:	Data Storage Card
SMS	:	Short Message Service
SN	:	Sensor Nodes
SNR	:	Signal to Noise Ratio
SVM	:	Support Vector Machine
SMPS	:	Switch Mode Power Supply
SOC	:	System on Chip
SRAM	:	Static Random-Access Memory
sec	:	Second
UWB	:	Ultra Violet Band
<i>viz.</i>	:	Videlicet (namely)
V	:	Voltage
W	:	Watts
WSN	:	Wireless Sensor Network

CHAPTER 1

INTRODUCTION

1.1 Wireless Sensor Network

Sensing can be defined as a procedure, used to collect data about a physical object, process or events. Sensor is a device which can perform this function. Sensors can measure physical parameters such as temperature, concentration of gases, relative humidity, moisture, pressure, light etc. These sensors can be deployed randomly in a region or in a grid depending on the application. Recent advances in wireless communication and electronics have allowed the development of low power, low-cost sensor nodes that are tiny in size and communicate with other nodes over short distances. A large number of sensor nodes work cooperatively to monitor a large physical environment, and forms a wireless sensor network (WSN) as shown in Fig. 1.1. This network will pass information to a base station. Sensor Nodes communicate with each other and the base stations using their wireless links, allowing them to disseminate the data to a remote location for processing, visualization, analysis, and storage systems.

The individual sensing operation of sensor nodes was very incompetent as large amount of energy is dissipated in sensing and transmitting the information individually. Clustering of WSN was presented as a solution to this problem [1]. A comparative study was conducted on different systems for the deployment of sensor nodes and energy efficient clustering protocol with their relative strengths and drawbacks. in [2]-[4] describe the clustering algorithm for energy efficiency in WSN.

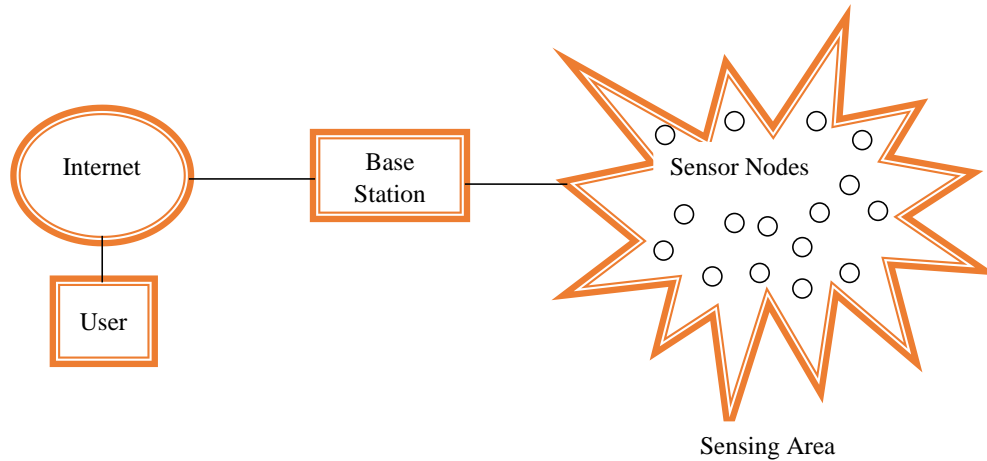


Fig.: 1.1: Wireless Sensor Network

In WSN a group of sensor nodes form a cluster and one node of each cluster is assigned as the cluster head (CH) of respective cluster. The cluster head aggregates the data from all the sensor nodes and finally transmits the sensed data to the (Base station). There are many challenges in designing of WSN such as energy efficiency, node failure, security and the real time applications. In this thesis, we are addressing the above issues.

The reduction of power consumption has always been a core issue in designing WSNs. One of the major limitations of WSN is the dependence on batteries for power and the network is alive only when the battery is alive. Since nodes in WSN are equipped with limited battery, its battery should be consumed in the most efficient manner which outlines the need of energy efficiency and optimum usage of available battery in WSN. An energy efficient WSN minimizes the consumption of energy in the network and extends the network lifetime. Recent research conducted in [5]-[10] suggests alternative ideas to reduce energy consumption and extend network lifetime by proper utilization of resources. A survey study was conducted by [5] on various energy management techniques of sensor nodes making the network live and more efficient. An optimization metric of energy efficiency was proposed by [6], examined the energy efficiency of

Automatic Repeat Request (ARQ) error control strategies and reported that energy efficiency in sensor networks under retransmission strategy of ARQ cannot be improved. In [7], forward error correction (FEC) techniques for energy efficiency in sensor nodes were used and concluded that BCH code performs better as compared to other channel codes because of low encoding and decoding energy consumption. An efficient FEC scheme was proposed by [8] for WSNs to avoid retransmission which not only saves energy but also allows it to handle burst errors. In [9] the effect of error correcting codes and modulation together on the energy consumption of a sensor node is presented. In [10], the authors presented for a Multihop WSN, a model for energy consumption and minimising the error in receiving correct word. They consider encoding in first node and decoding at the base station for energy saving at node level resulting in extending the network life.

Due to the high demand and usages on WSN, it is vulnerable to the attacks due to which its security has to be incorporated properly [11]-[13]. The sensor nodes are constrained in terms of processing, memory, communication and, energy resources. They are distributed and dynamic in nature, and hence connectivity with base stations cannot be taken for granted. The traditional security solutions become irrelevant due to the dynamic and wireless communication characteristics of a WSN. Security solutions for WSNs should thus be distributed, and should utilize only a small subset of the available security primitives. As the security services do not support the core network functionality, it will increase the computational overhead. This is an important issue to be addressed while designing the security systems. Moreover, security solutions for WSNs have to cater for in-network data aggregation operations, data with varying sensitivity being communicated, multi-hop routing, intermediaries with varying levels of trust, and integration with different networks and platforms. Since the nodes are deployed

randomly, unattended environment, an adversary can tamper or damage the sensor node or extract information from it. To avoid these circumstances, the sensor node should be resilient against attackers. If an adversary attacks the sensor node, it can lead to data breach or malfunctioning of that particular sensor node which eventually could also lead to failure of the entire WSN. Incorporating security in WSNs is an active research area and a challenging research topic and has been studied in this thesis.

The applications of WSN are house monitoring, automatic dipper system in vehicles and automation where a number of mixed sensors are installed to find out different actions of users. One of the leading applications of WSN is in home automation and monitoring. People desire to live in smart living spaces equipped with home automation systems. These systems not only provide them convenience, comfort, security but also reduce their daily cost of living by providing energy saving solutions. Hence it is of interest to design and develop a prototype of a smart monitoring and controlling system for household electrical appliances in real time. Such system's principally monitor electrical parameters of household appliances such as voltage and current and subsequently calculate the power consumed. The system should be low-cost, compact, and flexible in operation. In this thesis we have developed a prototype for home automation. and discuss it in Chapter 5.

Another potential application of WSN is detection of high beam light to avoid accidents caused by the sudden glare produced by the oncoming vehicles with high beam. It is therefore of important to develop an automatic system, independent of the human factor, capable of detecting oncoming headlights, and then dipping the high beam of the respective vehicles. The high beam should however remain dipped for a short period of time. Detection of high light beam using a simple, low cost system has been addressed in this work.

1.2 Motivation

IOT is developing very fast in recent years. WSN has a major role in development of IOT. Energy efficient communication is very important for such applications. Hence, we propose energy efficient communication with maximum accuracy. Similarly, security of whole network is also a big challenge. So, we propose Extended Kalman Filter based algorithm for malicious node detection and prediction. Finally, to conclude, we propose WSN based home automation and auto dipper applications

Energy Efficiency

One of the objectives of this thesis is to find an optimal selection of combination of Error Correcting Codes (ECC) and Modulation Techniques for designing an Energy Efficient WSN for improving communication accuracy. The energy consumption of a WSN node depends upon internode distance, desired Bit Error Rate (BER), channel conditions, operating frequency, modulation schemes, and ECCs. Authors [14], [15] studied the node energy variations with ECC and modulation parameters for an energy-optimized node design in the presence of Additive White Gaussian Noise (AGWN). In [16],[17] authors presented selection of energy-efficient modulation methods and multi-access protocol while considering both transmission and circuit energy. Authors [18] have considered fading environments and addressed energy efficiency of adaptive error correction in WSN. In [19] a survey on various methods of how ECC techniques are implemented in WSNs was presented. In view of these studies it is apparent that the choice of a modulation scheme and error control code plays an important role in determining the energy consumption of WSN. This motivate to explore such design space and find an energy-optimal combination of ECC and modulation scheme. The design space parameters are derived from the WSN application and associated constraints. The

specified application gives a deployment range in terms of area, number of nodes, network topology, and channel conditions.

Malicious Node Detection

Environments in which sensor nodes were deployed, the wireless medium and constrained resources (limited energy, processing capability, and storage capacity), pose challenges in designing and implementation of WSN security [20]. Most of WSNs protocols, due to the constrained resources inherent to the sensor node, assume a high level of trust between the communicating among sensor nodes to eliminate the authentication overhead. This creates the danger of adversaries like injecting malicious nodes to the network or to manipulate the operation of existing ones. The adversary may take control of some sensor nodes and use them to inject false data with the sole aim of misleading the network operator [21]. Attacks against security in WSN are caused by the insertion of false information from the compromised node with in the network. According to [22], the most dangerous attack in WSN is the insertion of the malicious node that feeds false data or prevents the passage of true data. Therefore, it is of importance to detect malicious nodes in WSN, for preventing whole network from adversaries.

Application of WSN in Real time

The applications of WSN addressed in this thesis are smart home monitoring and automatic dipper system in vehicles.

Smart Home Automation

There have been significant enhancements in the field of intelligent control and remote monitoring of different home appliances. WSN can be designed for remote monitoring of appliances of at homes, research centres, universities, colleges, hospitals etc. with an

objective to protect and maintain living space [23]. The system explained in [24], [25] [26], [27] provides different ways to control home appliance. Machine to Machine system explained in [28] where communication occurs through the Global System Mobile (GSM) module and it is use Short Message Service (SMS) and attention commands. The server at home is based on SMS/ General Packet Radio Service (GPRS) module. In [29], [30] voice operated control system is proposed that used to enable or disable the home appliance remotely. The Personnel computer that is interface via Universal Serial Bus to the Bluetooth card, sensing network and a Pulse Width Modulation (PWM) circuit. The main disadvantage is that it has very limited range of operation about 10 meters only. By sending instructions through the telephone lines using Dual Tone Multi Frequency (DTMF) [31]. The ZigBee Home application appliances can be used wirelessly [32], [33]. Voice recognition and controller system is used for this aim. Wi-Fi communication technology [34] and Arduino board is used in this system. Light and temperature sensor can be used to control the home appliances. A detailed explanation of different technologies that can be applied to home appliance automation is done [35]. In [36] design of an embedded system which improves the energy utilization rate, reduces the waste of energy consumption. The most general types of methodologies seen from the above surveyed systems are GSM Communication, ZigBee, Bluetooth based, wireless and combinations of these. The motivation of this work to develop a low-cost, compact, and flexible prototype for home automation.

Automatic Dipper system in Vehicles

After sunset or during night time mostly roads are not well illuminated. Hence drivers switch on their high intensity beams for long range visibility. This sudden glare causes a sort of temporary blindness effect for the driver, which is termed as Troxler Effect. [37]

suggested that an automatic dipping mechanism is required to dip the headlight automatically and provides better safety of drivers at night time. Light Dependent Resistor (LDR) based circuits to automatically dip the headlights suggest [38], but it fail during rainy days. Hence, we decided to use camera for headlight detection and subsequent automatic dipping. The headlights should remain dipped for a short period of time. That way at least one of the drivers would be able to avert a possible accident as that driver won't be dazzled anymore.

1.3 Research Objectives

From the above discussion, it is imminent that WSN design methods which not only overcome energy efficiency issues but also handle error detection issues, are to be developed. The main objectives of the thesis are:

- To develop an energy efficient wireless sensor network, using optimal combination of modulation schemes and/or error control codes, for improving accuracy.
- To develop a methodology for malicious node detection and prediction in wireless sensor network using artificial intelligence and machine learning for improving the security of the network.
- To implement real time applications of WSN such as home automation and automatic dipper system using embedded systems.

1.4 Research Contributions

Research contribution to in the thesis in terms of energy efficient communication for WSN, security in terms of malicious node detection and attack, and real-time application of sensor network.

1.4.1 Energy Efficient Communication Techniques for Wireless Sensor Network

A methodology is proposed for evaluating various ECC based communication system for reducing energy consumption of sensor nodes. For this exploration, an integrated framework that computes the radio energy, as well as the computation energy, has been built. Simulation results show that in certain operating conditions, sensor node with Reed-Solomon codes and BPSK modulation scheme consumes the optimal energy. After simulation find at distance (d) =60m an optimal ECC-modulation pair Reed Soloman (RS) (N=63) code with t=4 and BPSK modulations schemes give 48% energy savings.

1.4.2 Malicious Node Detection and Prediction

(a) An Efficient Weight Trust Method for Malicious Node Detection in Clustered Wireless Sensor Network for improving security

Consider a wireless sensor network (WSN) that consists of sensor nodes (SN), cluster head (CH), forward node (FN) and a base station (BS). The information acquired by the SN is sent to the CH, all the CH's send the information to a FN which forwards it to the BS. Fast detection of malicious nodes is imperative to the performance of a WSN and therefore we examine the weighted trust method for malicious node detection. Two scenarios are considered-cluster head without grid and other with multiple cluster head with non-overlapping grid. The results indicate that the scenario with multiple cluster heads with non-overlapping grid requires lesser time for malicious node detection with better accuracy as compared to the scenario with single cluster head without grid.

(b) Malicious Node Detection in Wireless Sensor Networks Using Support Vector Machine: (A Machine Learning Approach):

WSN are employed in a wide range of applications and their challenges make them susceptible to various security threats. The issue of detecting malicious nodes in WSN is addressed with the aid of Machine Learning technique based on SVM. Our study showed that SVM has better accuracy, detection and miss detection ratio than Auto Regression (AR).

(c) Extended Kalman Filtering Technique to detect Byzantine attack in a WSN

The wireless sensor is vulnerable to attacks such as physical tampering, faulty hardware, malware, hacking or any other physical phenomena. Attacks can lead to disruption of the whole network, injection of false data leading to undesirable consequences. Here, we are using the extended Kalman filtering algorithm to detect a Byzantine attack on nodes in a wireless sensor network. The detection algorithm is based on the extended Kalman filter in which time series prediction is used to predict the data of the sensor node by using past values. If the difference between the predicted value of the node and the actual value is greater than the threshold value then it is said that node is under byzantine attack and the data from that node is discarded. It is observed that malicious nodes were marked successfully with high detection ratio and low misdetection ratio. The scheme gives an accuracy of 83.33% and misdetection percentage 16.67% over 168 data points.

1.4.3 Applications of Embedded systems and WSN

(a) Home Automation

Here wireless sensor network and ZigBee are utilizing for smart home-automation. The proposed system monitors the electrical parameters e.g. voltage, current and power

consumption. The novelty of this system is the implementation of a mechanism to control the appliances using a sensor network on ZigBee. The developed system is a low-cost, compact, and flexible in operation. Further it will help in reducing carbon footprint as it will allow the appliances to work only when desired and thus can save electricity expenses of the consumers.

(a) Auto Dipper System

An intelligent auto-dipping system is proposed that may be placed in front of every vehicle. The high beams of any such vehicle will be dipped automatically the moment it detects headlights of an oncoming vehicle. The system will be most effective when every vehicle has this auto-dipper installed. This system would help prevent accidents caused due to the dazzling created by oncoming high beams. The proposed system uses a USB web cam and Raspberry Pi for real time processing. The validation of the system has been done using both simulation and actual hardware.

1.5 Thesis Outline

Chapter 1: This chapter presents a brief overview of thesis work and research objectives.

Chapter 2: This chapter discusses the state of the art and major research issues in various modulations and error control coding techniques for energy efficient WSN. First, modulation techniques are explored and then the Error Correction Codes for sensor networks is outlined. The goal of the survey is to present comprehensive technological aspects of Modulations and ECCs in the recent literature in the field of WSNs. Malicious Node detection methods based on Weighted Trust Evaluation, AR and machine learning approach. It also includes the survey of application of Embedded sensor network in field of Home Automation and Automatic Dipper System.

Chapter 3: This chapter presents optimal combination of modulation and ECC for energy efficient WSN with maximum accuracy.

Chapter 4: This chapter describes the Cluster based Weighted Trust Evaluation method, Auto-regression Scheme and prediction using SVM for detecting malicious node in WSN. It also describes the use of Extended Kalman Filter for detecting malicious node detection and prediction.

Chapter 5: This chapter presents hardware implementation of auto dipper system as an application of Embedded system, and Mobile/laptop-based home automation system as an application of WSN.

Chapter 6: This chapter presents the conclusions of the proposed work of the thesis and scope for the future work in the area of WSN.

CHAPTER 2

LITERATURE REVIEW

In this chapter review of various ECC and modulation schemes used in energy efficient wireless sensor network, methods of malicious node detection and prediction and sensor network applications like, home automation and auto dipper system, are discussed. The scope of work is also presented towards the end of chapter

2.1 Error Control Codes and Modulation Schemes in WSN

Now a days, the application of wireless sensor networks (WSNs) has become increased in different sectors starting from home, health, and environmental to military, space and industry. WSN are connected with various nodes which are powered by batteries. The replacement/recharging is very difficult of these batteries. With finite energy, a finite amount of information can only be transmitted. Minimum energy consumption for data transmission, is an important consideration in design of WSN. Hence, WSN sensor networks require simple and facile error control code schemes to transmit information secure and energy efficient. A facile error control code and modulation schemes in WSN sensor networks required to transmit data securely and with minimum energy consumption.

In this section, survey with respect to Error Control Code (ECC) and modulation schemes in WSN are compiled based on the previous research and presented.

2.1.1 Modulation Techniques in Wireless Sensor Networks (WSN)

Energy Efficient modulation and MAC for asymmetric RF micro sensor systems with energy minimization techniques have been proposed in [17]. Authors show that non-coherent M-FSK is more energy efficient than M-PSK/M-QAM and achieves significant energy savings. Consistent with the goal of energy efficiency and the need to reduce transmitter start-up time, a fast turn-on architecture based on a fractional-N frequency synthesizer has been proposed [17]. In [16] a comprehensive study of transmission and circuit energy, transmission time, and constellation size trade-offs for both uncoded and coded M-QAM and M-FSK was conducted. For an uncoded system, optimizing transmission time and modulation parameters can increase energy savings. It is also demonstrated that energy savings of up to 80 per cent can be achieved when the system is optimized. In terms of uncoded M-QAM and M-FSK, uncoded M-QAM has more bandwidth and energy efficiency compared to uncoded M-FSK for short-range applications. Uncoded M-FSK, however, can be used in power-limited applications because it requires less transmitting power as compared to M-QAM. For a coded system, coding has benefits which vary with transmission distance and the modulation scheme. For a coded M-QAM system, coding increases energy efficiency and transmission distance increase. The coded M-FSK system, on the other hand, can reduce energy consumption only when the distance is large [7]. The performance of narrowband communications to ultra-wideband communications in a simplistic wireless sensor network model with a view to save energy was compared. This analysis and comparison are done under various channel conditions and the author presents simulation results of these comparative studies. In [39] authors proposed a physical layer driven approach to find the best modulation technique for WSNs in a given scenario (Home Automation) of three modulations *viz.* ASK, BPSK and OQPSK as specified in IEEE 802.15.4 standard.

The author presents the best modulation strategy to minimize the total energy consumption required to send a given number of bits in energy efficient WSN scenario. In order to find the optimal transmission scheme, the overall energy consumption including both transmission and circuit energy consumption needs to be considered. Simulation results shows that for uncoded data transmission, by optimizing the transmission time and the modulation parameters, up to 60% energy savings is achievable over non optimized systems. Comparative study of band pass modulations (MFSK, MQAM, OQPSK) & derived expressions for energy consumption [40]. Then UWB modulations schemes (OOK and M-PPM) have been discussed for distances $(d) \leq 10\text{m}$. In Pass band modulations MFSK is found to be the best choice for WSN and in UWB the OOK modulation schemes are energy optimal scheme. Authors of [41] study the comparison of three M-ary modulation schemes (i.e. MFSK, MQAM, OQPSK) and optimal performance for minimize energy consumption per information bit in individual links in WSN. For analysis consider transmitted signal power and circuit power consumption. In [42] authors presented the BER performance of BPSK in AWGN by considering block codes and convolution codes. All the codes are compared on the basis of BER and energy per bit to noise ratio. M.R. Islam [43] developed an approach for selecting appropriate ECC scheme for WSNs.

2.1.2 Error Control Codes and Modulation Schemes in WSN

A survey was done on seven layers of OSI model of networking [44]. The authors had surveyed modulation schemes at physical layer and error control at MAC layer.

Modulation schemes: Simple and low-power modulation schemes need to be developed for sensor networks. The modulation scheme can either be baseband, as in UWB, or passband.

Error control: The usefulness of ARQ in sensor network applications is limited by the additional re-transmission cost and overhead. On the other hand, decoding complexity is greater in FEC, as error correction capabilities need to be built-in.

Adaptive FEC Code Control Algorithm

An Adaptive FEC technique called Adaptive FEC code control (AFECCC) was proposed in [45], which dynamically tunes the amount of FEC code per packet based on the arrival of acknowledgement packets without any specific information such as SNR or BER from receivers. The simulation experiment indicates that AFECCC performs better than any static FEC algorithm and conventional dynamic hybrid FEC/ARQ algorithms when wireless channels are modelled with two-state Markov chain, chaotic map, and traces collected from real sensor networks. Finally, AFECCC implemented in sensor motes achieves better performance than any static FEC algorithm.

Low-Density Parity-Check codes (LDPC) versus Reed Solomon (RS) Codes

Authors of [46] analyzed power optimized channel coding in WSN using Low-density parity-check code (LDPC). It observed that decoder's energy consumption increases exponentially with the number of quantization bits. They presented that high-rate Gallager codes are as energy efficient as the RS codes, which till now have been the first choice for WSNs. By exploiting the trade-off inherent in iterative decoding, the network lifetime improves up to four times with the 3–6 regular LDPC code. Hence, it is concluded that the LDPC codes are more efficient than block codes and convolutional codes. The performance analysis of ECC to reduce the BER and power consumption on different platforms was studied by [7]. Based on the study and comparison of the three

different Error Correcting Codes, (BCH, RS, and CC) it was identified that binary-BCH codes are best suitable for WSN.

Sensor Node Energy Analysis

Authors of [14], [15] have analysed the node energy variations with ECC and modulation parameters for an energy optimal node design for the nodes operating in the AWGN channel. Based on this analysis, authors calculate the per information bit node energy and this is often accustomed by selecting an “optimal” ECC and modulation scheme pair. Authors concluded that the energy optimal ECC-modulation pair selected for some specific operating conditions could save as much as 50% energy. In short, the aim is reducing the search space to find an energy optimal ECC-modulation pair for the given environment and application. For a BER of 10^{-5} and RS (31, 29, 3), out of MPSK, MQAM, and MFSK, 4-QAM is the energy optimal modulation scheme at a distance of 110 metres. Also, with BPSK modulation, RS (63, 59, 5) is the optimal ECC at 10^{-5} BER. In [43] author presented technique to finding suitable ECC for WSNs and show that the RS (31, 21) is suitable both in BER and power consumption criteria. In [47] authors investigated the use of LDPC Code for Capacity and BER Sensitive WSN at Nakagami-n Channel. The related research work of the other researchers worldwide has been analyzed and compared to obtain energy efficient modulation and ECC scheme. The Table 1.1 shows related work on modulations scheme and ECC in the field of WSNs.

Table 2.1: Summary of related work on Modulation ECC and in WSN

Sr. No.	Authors	Simulation/ Hardware Tool	Modulation Survey	ECC Survey	Energy Saving
1.	S. Chouhan <i>et al.</i> , [14], [15]	Sim- panalyzer+ MATLAB	BPSK	For BER = 10^{-5} , RS codes	Optimal (47% energy saving) at 150m distance
2.	S. Cui <i>et al.</i> , (2005) [16]	MATLAB + VHDL	MFSK for large distance MQAM for small distance	Uncoded data transmission with ARQ technique	Optimal
3.	A.Y. Wang, <i>et al.</i> , (2001), [17]	MATLAB	Non-coherent M- FSK is more energy efficient than M- PSK/M-QAM	--	Non coherent MFSK is optimal
4.	M. R. Islam (2010) [43]	MATLAB	BPSK	RS (31,21) Codes	Optimal for both in BER and power consumption
5.	G. Balakrishnan <i>et al.</i> , (2007) [7]	VLSI Tools + MATLAB	BPSK	Out of BCH, RS, Convolutional Codes,	binary BCH codes with ASIC implementatio n is Optimal
6.	H. Sharma <i>et al.</i> , (2012) [39]	Qualnet 5.2 Network Simulator	ASK, BPSK and OQPSK in Home Automation Scenario	No ECC used	OQPSK is optimal
7.	J. Abovei <i>et al.</i> , (2009) [40]	MATLAB	MFSK, MQAM, OQPSK for $d \geq 10m$ and UWB modulations (OOK, M-PPM) for $d \leq 10m$	--	In Pass band, MFSK is better for WSN & in UWB the OOK modulation is energy optimal

8.	F. M Costa and H. Ochiai (2010) [41]	MATLAB	MQAM	--	Optimal distance 10-30m
			MPSK	--	Optimal at distance 31-75m
			MFSK	--	Optimal at distance >75m
9.	I.F. Akyildiz <i>et al.</i> , (2002) [44]	Not used	Simple and low-power modulation schemes (baseband, as in UWB, or pass band)	ARQ, or simple ECC are used in WSN	Low computation complexity Modulations & ECC schemes
10.	J. Henrique Kleinschmidt <i>et al.</i> , (2009) [45]	MATLAB	--	Adaptive FEC code control (AFEC) based on ACK received	AFEC performs better than any static FEC algorithm
11.	V. Pushpa <i>et al.</i> , (2017) [42]	MATLAB	BPSK	CC codes and block codes	CC perform better than Blocks code,
12.	C. Wang <i>et al.</i> , (2010) [48]	VLSI tool	A low power 2.45GHz WPAN modulator/demodulator	--	Optimal design of Modulator/De modulator
13.	N. Sadeghi <i>et al.</i> , (2006) [49]	MATLAB	BPSK	Hamming, RS, CC, Turbo, Irregular LDPC, implementation at BER=10 ⁻⁴	Analog ECC decoders perform better than digital decoders
14.	M. Sartipi <i>et al.</i> , (2004) [50]	MATLAB	BPSK	Source & Channel coding using LDPC (R=2/3, N=1000)	LDPC codes are 45% more energy efficient than BCH codes with 2-fold energy saving

2.2 Malicious Node Detection and Prediction

Most WSN protocols, owing to the constrained resources inherent in the sensor node, assumes a significant level of trust among the communicating sensor nodes so as to eliminate the authentication overhead. This makes the risk of foes or adversaries injecting malicious (faulty) nodes into the sensor network or control the activities of existing ones. Authors in [51] presented a survey of basic methods for identifying compromised nodes. The adversary may assume responsibility for some sensor nodes and use them to infuse bogus information with the objective of misdirecting the system administrator. Thus, some risk of assailants launching an array of attacks on the sensor networks still exists [52]. A compromised or faulty SN provides forged information that may wrongly mislead the sensor network. A compromised or malicious sensor node can continuously forward wrong information to the upper layers. There have been many techniques presented in literature for detection of malicious node inside the space of the WSN. WSN may be compromised due to many reasons such as finite battery life, finite memory space, and finite computing capabilities [11], [12], [53]. It is very essential to detect the malicious node and isolate it to prevent it from generating wrong results. Ad hoc networks without a definite structure are rarely good against any types of attacks, which can lead to a node being quickly breached. In [54], authors presented a method wherein node is declared fault free, and is not a malicious node if it is treated as trustworthy by its neighbouring nodes. This method requires a minimum number of nodes nearby, which is not guaranteed in sensor networks. In [55], authors proposed a method for malicious node identification by comparing the information generated by surrounding nodes and the node itself. If the difference between the information is marginal, then the nodes are said to be trustworthy. This method gave a better result for the localized detection of malicious node which was used primarily for the detection of the malicious node. The entire sensor nodes are assigned a weight

proportional to the amount of trust and is evaluated frequently. Once the trust decreases below the threshold, the node is declared malicious and isolated. In [56], [57] authors demonstrated a method using a three-level hierarchical network with components as: Sensor Nodes (SN) whose function is to sense the parameter. SNs send its data to Forwarding Node (FN). FNs are high powered that collect data from SNs and process it and transmit to base station. This scheme is based on one critical assumption, the FNs nodes and Base station are never faulty. MATLAB simulation are presented in [58] for extensive weighted trust evaluation emphasizing on response time and detection ratio. In [59], [60] authors focused on the security issues in WSN and described the various kinds of attacks. The clustering proved a power efficient way to localize sensor nodes and increase reliability and various clustering algorithm in WSN are described in [61]. A distributed fault identification algorithm is presented in [62] to find both hard and soft faulty SN present in WSN. The algorithm is distributed, self-detectable and can detect the most common byzantine faults (the faulty node behaves arbitrarily which is also difficult to predict). Every SN collected the observed data from the neighbour's node and computes the mean to check whether faulty SN is existing or not. If a node found the presence of faulty node, then it compares observed data with the data of the neighbours and predict probable fault status. The final fault status is determined by fusing the fault information from the neighbours. In [63], [64] the authors suggested that the past value obtained from each sensor node of a network may be used as an effective and efficient measure for detecting their malicious activity using an autoregressive model. Here basically the future value (at time t) of a sensor node is predicted using the past values of its neighbouring nodes. The difference of the observed and the predicted values determine whether a node is malicious or not. In [65] the authors proposed a scheme to detect the malicious node based on their transmission time, Stop Transmit and listen (STL) method.

Here they assume that the malicious node is unaware of non-transmission time. The malicious node is detected by their neighbour node. In [66] the authors used a model to distinguish the malicious nodes in WSN through an online neural network predictor that depends on a wide span of time acquired from neighbouring nodes which prompts the detection of malicious nodes in cutting edge and thus decreases the odds of errors and processing time at the later stages. In [67], the authors proposed a Reputation Systems (RS) based on machine learning. RS offers protection against malicious activities, initiated by faulty or corrupt nodes in a network, for example they may aid in spreading of viruses or worms, or attempt attacks against known threats. In [68], SVM based framework for detecting DoS attack has been proposed. Time series prediction using SVM are discussed in [69], [70].

Detection of malicious nodes using machine learning techniques poses the following challenges:

- i) achieve dead line of real time applications.
- ii) larger data points, classification complexity and multidimensionality of future space.

The Kalman Filtering technique also used when real-time processing of data is required and the acquired data contains missing or noisy values. [71] proposed Kalman filter-based detection technique for primary user emulation attacks. KF is used for tracking and estimating the position of the primary user, then the transmitter received power is used to derive the position of the transmitter before comparing it to that estimated by Kalman filter. Secondary users may also check that the sender is a legal main recipient, or an intruder. The KF and Extended Kalman Filter (EKF) techniques are used in literature [72], [73] to address problems such as position, angle, velocity, temperature, humidity and orientation of system.

2.3 Real Time Applications

Explore some real time application of embedded system.

2.3.1 Smart Home Automation

The area of intelligent control and remote monitoring of various home appliances has been greatly enhanced. WSN is designed for remote monitoring appliances of homes, research centres, Universities, colleges, hospitals etc. Wireless technology not only helps in remote monitoring of areas where wired connection is impossible, but also economically viable for installation. Aware Home Research Initiative (AHRI) at Georgia Institute of Technology (GIT) [74], the Center for Advanced Studies in Adaptive Systems(CASAS) at Washington State University [75], AgingMo at University of Missouri [76], Place Lab at MIT [77] and Smart home Lab at Iowa State University [78], [79], are checking the activity of everyday living, enhancing the solace, and making settled mindful relative circumstances through heterogeneous sensors with cameras installed at various locations of home. In Germany, accommodation is offered after considering the nature and mental aptitude of residents, with an objective to protect and maintain living space [23]. Most researches of IOT-based homes are still in the beginning stage, and not many research trainings include viable execution [80], [81] IOT-based structures offer us responsive encompassing and remote contact examination of home vibe. The system described in [24]-[26] provides different ways to control and manage numerous home appliance such as the Global System Mobile (GSM), Zigbee, Bluetooth and Wi-Fi. The real time measurements and monitoring provides the important information that can be utilized for the automation system. It can control any change in monitoring parameter of a system in real time.

GSM based Home Automation System

GSM communication is used because it offers highly secure communication and wide coverage area. For controlling the home appliances with microcontroller PIC16F887 is used in [27]. This system is based on short message service (SMS). The SMS codes are used to control the related home appliance. The device sends the message to the user through the SMS. The system does not have any feedback system to track the device continuously. In [28] authors proposed a Machine to Machine system and communication occurs through the GSM. This system uses the SMS and attention commands. This system programmed as per the requirements of the home appliance, has the capability to control the mechanical appliances through respective sensors. There is no feedback to the user for any information. The system is totally controlled by the personal computer and the computer is active all time. This system is not a real time control system. The server at the home is based on the SMS / GPRS mobile cell module and controller [29]. This can be used by the user to monitor and control the different home appliance at the home by using the Java enabled cell phone. They transmit the command and receive the feedback from the system as the SMS strings. For hardware implementation Atmel microcontroller is used, and connected with a serial port interface RS232. The relevant data is stored in the EEPROM memory. The authentication system is based on the password. The whole system reliability depends on the SMS, the interface is pre-programmed and cannot be customized based on the devices. A voice operated control system is proposed in [26] that is used to enable or disable the home appliance remotely. An android operating system based mobile phone is used to get the voice command and convert them into text and this text message is sent via SMS to another phone through the GSM network. The user receives an alert message through feedback regarding the command. Voice command feature makes it universally accessible. It required two

mobile phones, one with user and another in proximity to the controller and can lead to additional expenses. The system presented in [27] has a GSM communication network and all peripherals are controlled by the AVR Microcontroller and is also based on SMS. Attention instructions are used to exchange with the modulator and demodulator. However, functioning within specified period is a challenge.

Bluetooth Based Home Automation

Low price, coded and efficient communication is the main feature of the Bluetooth technology. Using Bluetooth and cellular phone, authors in [80] presented a standalone Arduino Bluetooth board to control the home appliances. Designed system is cost effective and scalable allowing various devices to be controlled with minimum changes, and system is password protected. Using Bluetooth technology is to manage and control the home appliances presented in [29]. Personnel computer interface *via* Universal Serial Bus to the Bluetooth card, sensing network and a PWM circuit. The network also has a lighting sensor that can illuminates on lights when outside light is not adequate and temperature sensor also available. The main disadvantage is range of operation.

Phone Based Home Automation

A remote controller for home and office appliances by telephone is discussed in [31]. The authors suggested that the remote controller system based on Dual Tone Multi Frequency (DTMF) telephone can used to control the power supplied for remote location via telephone line. Telephone keypad is used as input devise for controller to direct data and instructional commands. In [81] the authors presented an enabling system which can be used to provide a standard framework for home automation. A home application network has the DTMF technique provide by the telephone's lines [82]. This system comprises the three main parts. DTMF receiver and the ring detector is the first components. Input

output connected unit is the second part and personal computer is the third part which provides the online access. The system has benefits of coded and standardization of the international level. DTMF tones are the same all over the world, disadvantage that the number of home appliances is restricts by the keys in the keyboard.

ZigBee and Wireless Based Home Automation

Smart energy management system for homes and buildings are proposed in [83]. The proposed system can monitor and measure electricity usage in real-time. Voice recognition-based home automation system with PIC microcontroller is proposed [84]. The system targets elderly and differently abled persons. The home automation system uses WSN with ZigBee RF modules for low power consumption resulted in higher efficiency. The system also includes security features for fire accidents at the home. In [33] the study focuses on the usages of ZigBee and WSN in smart home automation system, proposed a Simulink model of various levels of energy consumption in household electrical appliances for monitoring consumption rate numerically and graphically is designed.

Mixed Type

Automatic control of Home appliance can be obtained [26] using of GSM communication, ZigBee and Bluetooth. Android operating is used for the user application. Voice input of the user maps it to a set of textual instruction. These instructions transmit through SMS different mobiles at home. PIC controller received the instruction through the Bluetooth technology. It is named as the remote access unit. ZigBee transceiver receives the instruction from the remote-control unit. This transfers these instructions through ZigBee to the main controller. The use of multiple controllers and technologies may increase system cost. A detailed study of different technologies

that can be applied to home application appliance automation is done in [35]. It provides the basic idea how modern technology networking applied for the home appliance. Various internet protocols are used for standardization of home automation. A different alternative for home automation added with GSM communication and ZigBee is presented in [85]. It uses SMS to send instructions from long distances to the home application mobile. Implementation of the hardware using T290 i-mobile phone set, Atmega128 Microcontroller unit, ZigBee EM357 module. The controller unit deal with both the ZigBee and GSM communication networks. ZigBee system is used to communicate with the microcontroller unit. The main benefit of the network is its low cost and consumer friendliness. The added feature of this system is that it provides very good home security. In [86] the authors discussed different non-conventional network for home automation.

Table 2.2: Consolidated comparison report of all systems

System	Primary Communication	Remote access	Number of Devices	Speed	Real Time
GSM Communication	SMS	Access anyplace in the world	Unlimited	Slow due to delivery issue	No
Bluetooth	Bluetooth and Attention commands	Limited to Bluetooth range 10 meters	Unlimited	Fast due to proximity	Yes
Phone based	Phone lines	Anywhere with a phone line	12 due to 12 frequencies of DTMF	Fast	No
Zigbee	Zigbee and Attention commands	Around 10 meters	Unlimited	Fast	Yes
Wireless	RF/Other waves	Depends range and spectrum of waves used	Unlimited	Slow due to interference	Yes

There are some advantages and disadvantages of various methods explained above. The entire network has different control circuit to interface with electrical appliance. There has to be a same instruction network that will be used to issue instruction to the control the different logic circuits. The user interface is important feature of the system. This defines how user controls the system. This affects the utilization of the system. The most general types of methodologies seen from the above surveyed systems are GSM Communication, Bluetooth based, Wireless or combinations of these.

2.3.2 Auto Dipper System

Many roads are not well lit after sunset or at night time. That's why the drivers turn on their high intensity beams to improve illumination over long range. However, these beams possess a great hazard of dazzling the approaching vehicle's driver, especially if the road is one way, which is very often the case, as 26% of the national highways in India are single lane tracks [87]. Even though National Highways constitute only about 1.7% of the road network, but they carry about 40% of the total road traffic [88]. Thus, at the national highways such a situation is common sight, and the state and city road traffic are all too familiar with it as well because many people use high beams even in well-struck areas [89].

The sudden glare causes a sort of temporary blindness effect for the driver, which is termed as Troxler Effect. A glare is produced due to over exposure of the rods and cones inside the eyes. Even after the source of glare is removed, an after-image remains in eyes that creates a blind spot. Because of this temporary blindness, the driver sometime lacks their attention, resulting in accidents [90], [91]. However, some change can be brought if the headlights are intelligent enough to dip themselves, and signal the oncoming vehicle. That way at least one of the drivers would be able to see the oncoming vehicle and avert

an accident. A recent work in headlight detection through computer vision has been done by [37]. First, they identified bright blobs using thresholding and filtered them using Kalman Filter to remove nuisance light. The features extracted were classified using Support Vector Machines to decide whether to dip the beams or not. In [92] authors used multilevel thresholding to detect bright objects. The classification in this case was based on calculating the change in distance of the 'bright' objects with respect to the camera. Authors in [93] used symmetry fitting to create a bounding box over threshold frame in order to detect vehicles. In this perspective, all the work done in this field has taken thresholding as the basic step over which feature extraction and classification were performed. However, on the hardware side progress has not been made. Work in [38] suggests using LDR (Light-Dependent Resistor) based circuits to automatically dip the headlights, but this system has many inherent drawbacks. This system is dependent on the difference of light intensities. It is not accurate, since any kind of light could let it to dip the headlights. It would fail during rainy days. The headlights of approaching vehicles are considered as blobs for all frame being processed. Blobs provides a corresponding explanation of image structures in terms of regions, and hence, our algorithm shall detect and extract local features in terms of regions. Such features remain modest irrespective of obstruction, variation in observing situation or existence of clutter [94], [95].

2.4 Research Gaps

In the light of the above, it is noted that designing of wireless sensor network is recently gaining high attention. However, designing of wireless sensor network have always been sensitive to Additive Gaussian White Noise (AGWN) as discussed earlier. To resolve these issues, several energy efficient design techniques, malicious node detection and prediction methods and some techniques of real time applications of WSN have been

reported in literature but they have some limitations. In this respect, following are some technical gaps required to be resolved:

- Most of the WSN design techniques, use either modulation schemes and/or Error control codes techniques. Energy saving from these techniques is not enough. This creates an increasing need to develop an alternative energy-efficient solution to design a wireless sensor network with suitable choice of modulation scheme and error control codes.
- WSN are susceptible to the attacks such as malware, hackers and faulty hardware. In the literature, many researchers addressed these issues with the Machine Learning (Artificial Intelligence) approach. The accuracy of the earlier techniques is not good enough. There is no optimal solution for self-detection in WSN with high accuracy.
- There are so many real time applications using Embedded System are developed in literature. However, the cost and electricity consumption of existing implemented hardware is high. Hence, there are still requirement to design a compact and low-cost hardware for real time applications such as smart home automation etc.

In this thesis we address above-mentioned research gaps.

CHAPTER 3

ENERGY EFFICIENT COMMUNICATION TECHNIQUES FOR WIRELESS SENSOR NETWORKS

Any communication in the sensor node has to be made secure enough, so that the sensor node meant to receive the information should only receive it and ensure that it receives the correct information (data). To achieve this, we need modulation schemes and error correcting codes. In this chapter, we explore the modulation schemes and error correcting codes which can be used optimally for improving the energy efficiency in wireless sensor node.

3.1 Introduction

A communication system using modulation and error control coding is shown in Fig. 3.1. Here, the information source is a sensor node which measures physical quantity (e.g. temperature, light, humidity etc.) and measured data is encoded using an error control code, and transmitted using a suitable modulation scheme. At the receiver, the reverse process is performed to retrieve the data. The energy consumption of a WSN node depends on the distance between the receiving node and transmitting node, choice of Bit Error Rate (BER), modulation techniques and error control code (ECC) [95]-[97]. Authors [14], [15] have investigated node energy variations based on ECC and modulation parameters. Additive White Gaussian Noise (AWGN) channel is considered for energy-optimal node design. Transmission energy, circuit energy, transmission time

and constellation size for both uncoded and coded M-QAM and M-FSK and corresponding trade off were studied [16]. Multi-level (M-ary) modulation and binary modulation schemes were compared [17] and found that energy efficiency of M-ary is better than the binary modulation for the case with short start-up time and smaller RF output power. Author [18] have considered fading environments and addressed energy efficiency of adaptive error correction in WSN.

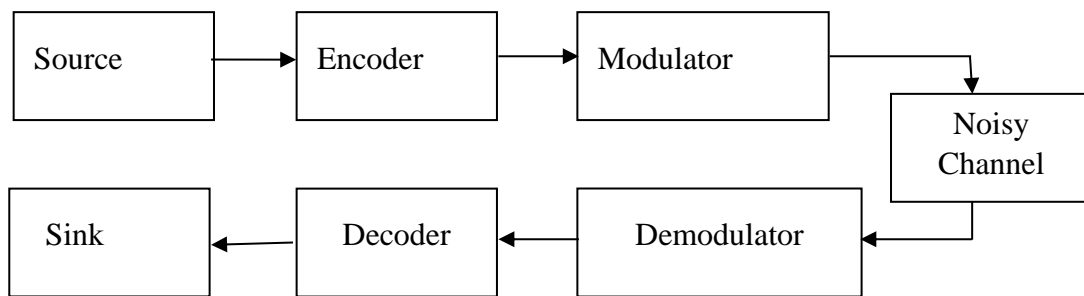


Fig. 3.1: Modulation and Error Control Codes in a Communication System

3.2 Digital Modulation and Error Control Coding (ECC) Schemes in WSN

In digital communication, the message signal contains binary data. The term digital modulation is defined as the process of varying any of three characteristics *viz.* amplitude, phase and frequency of a high frequency carrier signal as per digital message signal [96, 97]. In all of the above methods, an exclusive pattern of binary bits is assigned for every phase, frequency and amplitude for maintaining fixed bit pattern for encoding. This pattern represents specific parameters i.e. phase, frequency and amplitude. If alphabet contains $M=2^N$ alternate symbols, every symbol signifies a message consisting of N bits. If the symbol rate (also known as the baud rate) is f_s symbols/sec (or baud), the data rate is $N*f_s$ bit/sec.

3.2.1 Digital Modulation Schemes

The modulation schemes are Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK), Phase Shift Keying (PSK) and Quadrature Amplitude Modulation (QAM). Some preferable requirements from a digital transmission system [98], [99] are very high data rate, minimum transmission power and bandwidth, minimum BER (the rate at which errors occur in the transmission of digital data.), minimum interference, cost-complexity should be less. Comparison of various modulation schemes are presented in Table 3.1. Where $S_1(t)$, $S_2(t)$ are the pair of signals for used to represent binary symbols respectively, f_1 and f_2 are oscillator frequencies of upper and lower channel and R_b known as bit data rate.

Table 3.1: Comparison of various modulation techniques

Modulation Techniques	$S_1(t)$ and $S_2(t)$	Probability of Error (BER)	Band width	Complexity
Coherent FSK	$S_1(t) = A \cos 2\pi f_1 t$ $S_2(t) = A \cos 2\pi f_2 t$ ($f_1 > f_2$)	Moderate	$2 R_b + (f_1 - f_2)$	High
Non-coherent FSK	$S_1(t) = A \cos 2\pi f_1 t$ $S_2(t) = A \cos 2\pi f_2 t$	Moderate	$> 2R_b$	Low
Coherent PSK	$S_1(t) = A \cos \omega_c t$ $S_2(t) = -A \cos \omega_c t$	Low	$2 R_b$	High
Non-coherent PSK	$S_1(t) = A \cos \omega_c t$ $S_2(t) = -A \cos \omega_c t$	Low	$2 R_b$	Low
Coherent ASK	$S_1(t) = A \cos \omega_c t$ $S_2(t) = 0$	High	$2 R_b$	High
Non-coherent ASK	$S_1(t) = A \cos \omega_c t$ $S_2(t) = 0$	High	$2 R_b$	Low

3.2.2 Error Control Coding Schemes in WSN

The signal may be corrupted during transmission due to noise and may cause error in the received data. Using coding techniques such errors can be detected and sometimes corrected. Error Control Coding (ECC) schemes are usually of two forms [100], [101] as follows:

- (i) Error detection with Automatic Repeat Request (ARQ).
- (ii) Forward Error Correction (FEC).

According to first scheme, whenever error occurs, a request of retransmission is sent back to the transmitter. In case of second scheme, the errors are detected and corrected at the receiver end using suitable coding techniques.

Some basic terminology and definitions used in ECC are as follows [100]:

Minimum Distance (d_{\min}): The minimum distance between two code words is expressed as the bit distance in which they can diverge from each other. For the (n, k) block code, the minimum distance (d_{\min}) follows the inequality:

$$d_{\min} \leq n - k + 1 \quad \dots(3.1)$$

For example, a $(7, 4)$ hamming code has minimum distance $d_{\min}=7-4+1=4$ bits i.e. two 7-bit hamming codes can differ up to 4 bits.

Coding Gain (CG): For a given error probability, the reduction in E_b/N_0 achieved by an ECC scheme as compared to the E_b/N_0 of uncoded data transmission is known as coding gain. Where E_b is transmitted signal energy per bit and N_0 noise power spectral density.

The coding gain is generally expressed in dB, as

$$CG = \left(\frac{E_b}{N_0} \right)_u (dB) - \left(\frac{E_b}{N_0} \right)_c (dB) \quad \dots (3.2)$$

where, $(E_b/N_0)_u$ and $(E_b/N_0)_c$ are called Signal to Noise Ratio (SNR) of uncoded and coded system respectively.

Crossover Distance ($d_{\text{crossover}}$): An ECC scheme's Coding Gain (CG) [102] vary with distance (in meters) resulted in crossover distance ($d_{\text{crossover}}$) refers to the distance at which an ECC scheme is energy efficient compared to other ECC schemes or uncoded data transmission. Thus, the coding gain starts to attain at crossover distance.

Information Capacity Theorem: The channel capacity of a channel whose bandwidth B in Hz, interference by AWGN noise of Power Spectral Density (PSD) equals to $N_0/2$ and limited in bandwidth to B [98] is shows as

$$C = B \log_2 \left(1 + \frac{P}{N_0 B} \right) ; \text{bits per second} \quad \dots (3.3)$$

Where, C= Information channel Capacity, bits/sec; B=Channel Bandwidth, Hz; P=Signal Power, W; N_0 =Noise Power, W.

The minimum acceptable value of BER for multimedia applications is 10^{-6} and for data communication is 10^{-9} [103]. An energy efficiency analysis of Adaptive Error Correction in WSN is investigated [18] which shows the number of redundant bits can be adjusted as per the noise conditions in the channel leading to saving in transmission energy.

3.2.3 Types of Error Control Codes

Classification of various Error Control Codes in WSN are presented in Fig. 3.2. Forward Error Correcting (FEC) codes are classified in two categories i.e. Linear Block Codes (LBC) and Convolution Codes (CC). The former category is further sub-divided into Cyclic and Iteratively Decoded Codes (IDC).

- (i) Hamming Code, Bose–Chaudhuri–Hocquenghem (BCH) Codes, Reed Solomon (RS) codes belong to Cyclic Codes and have Codeword length (n) and is it (n-k) parity bits, where k message bit.

(ii) Turbo Codes, Low Density Parity Check (LDPC) Codes with Sum Product Algorithm (SPA) decoding fall under iteratively decoded codes.

(iii) Convolution Codes (CC) – code rate $R = k/n$.

The (RS) code [98] are nonbinary cyclic code with ‘m’ bit symbols (where $m > 2$). An RS (n, k) code on m-bit symbol exists for entirely ‘n’ and ‘k’ for which

$$0 < k < n < 2^m + 2 \quad \dots (3.4)$$

Where ‘k’ shows number of message symbols being encoded, ‘n’ shows total number of codeword length. The equation for defining the RS (n, k) code with an error correcting capability (t) is

$$(n, k) = (2^m - 1, 2^m - 1 - 2t) \quad \dots (3.5)$$

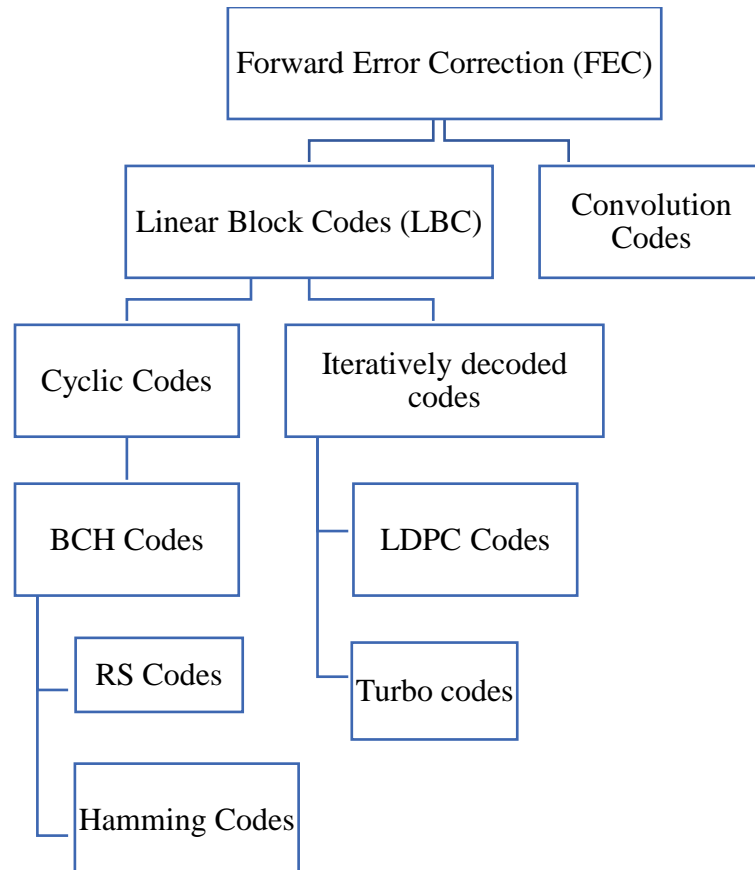


Fig. 3.2: Error Correcting Codes (ECCs) in WSN

For example, if $m=3$ and $t=1$, the value of (n, k) is RS (7, 5) codes. The RS code is defined as RS (n, k) with s -bit symbols [100]. This ensure that the encoder takes ‘ k ’ data symbols of every ‘ s ’ bits and sums parity symbols to construct a codeword for ‘ n ’ symbol. The parity symbols of s bits are ‘ $n-k$ ’. The RS decoder will correct up to t symbols in a codeword, where $t = (n-k)/2$ and includes errors. The codeword of RS code is explained in Fig. 3.3. This is considered as a systematic code because the data remains unchanged and the parity symbols are involved. The RS code encoder differs from a binary encoder, it operates on multiple bits instead of individual bits. The RS (n, k) code is used to encode m -bit symbol into blocks containing of $n = 2^m - 1$ symbol, where $m \geq 1$.

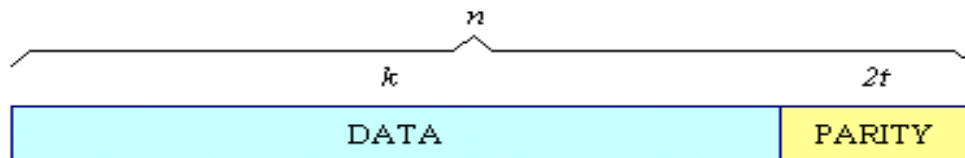


Fig. 3.3: Codeword for RS code with k data and $2t$ parity bits

Thus, the encoding algorithm extends sequence of k symbols to n symbols by addition of ‘ $n-k$ ’ redundant symbols. The parameters of RS (n, k) code with error correcting capability (t) are summarized in Table 3.2

The RS code block length is lesser than one of the sizes of a code symbol, and the minimum distance is one greater than the number of parity check symbols. The RS codes make efficient use of redundancy, block lengths and size of symbols. It can be readily changed to accommodate a wide range of message size.

Table 3.2: Parameters of Reed Solomon (RS) Code

Block Length	$n=2^m - 1$ symbol
Size of Message	k symbols

Error Correcting Capability	$(n-k)/2 = t$ symbols
Minimum distance	$d_{\min} = 2t+1$ symbol

Moreover, RS codes offer a variety of code rates to optimize performance. Finally, efficient decoding techniques are available with RS codes, which is one more reason for their wide applications (e.g. CDs, wireless communication, mobile communication and satellite communication, etc.).

3.3 System Design Methodology

The factors on which energy consumption of a sensor node depends are internodes distance (d), preferred BER, modulation techniques and ECCs [45]. Figure 3.4 describes the exploration method of WSN for designing an energy-efficient network with various design parameters. The deployment range is guided by specified application with the parameters such as area under surveillance, number of nodes to be deployed, network topology for efficiency, minimum power consumption and channel conditions. The required Quality of Service (QoS) and SNR are the constraints to be maintained. The appropriate modulation scheme and error correcting codes can be selected based on the application requirements. The selection process is based on minimum energy consumption, which is calculated by an energy simulator for all probable combinations of modulation schemes and error control codes. The optimal combination of modulation schemes and ECC vary with applications.

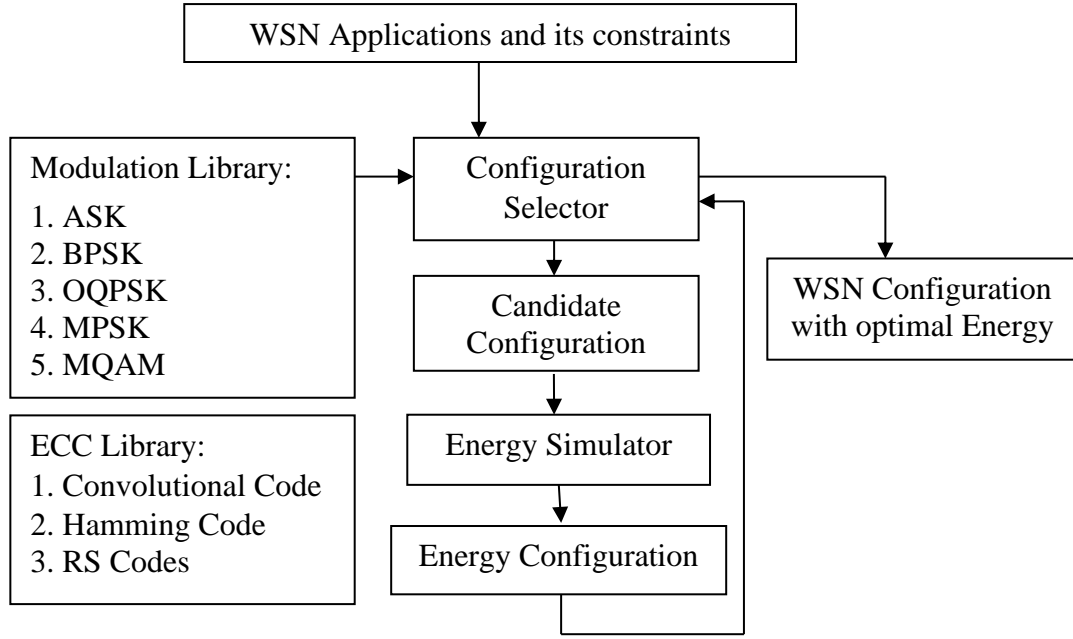


Fig. 3.4: System design methodology for finding energy optimal ECC-modulation pair

A detailed exploration system Fig. 3.5 is proposed to investigate the design space for energy-optimal ECC for a sensor node. The combination of optimal ECC and modulation method is selected on account of the node energy per bit for the candidate configuration. The energy model of the sensor node is used to measure the energy of the sensor node per bit. The key components of the energy in a sensor node has been identified to develop the sensor node energy model. In any sensor node, energy is consumed by the sensing unit, power supply unit, the computation unit, and the radio unit. In general, the energy consumption depends mainly computational unit and radio unit. In the computation unit, energy is consumed in execution of encoding and decoding of information bits. The energy of radio unit refers to the energy consumption of the signal while transmitting the encoded data and energy consumed in the circuit components of the radio unit. The Radio Energy Model (RadioEM) and the Computation Energy Model (CompEM) are the two main components of this design space exploration agenda [14], [15].

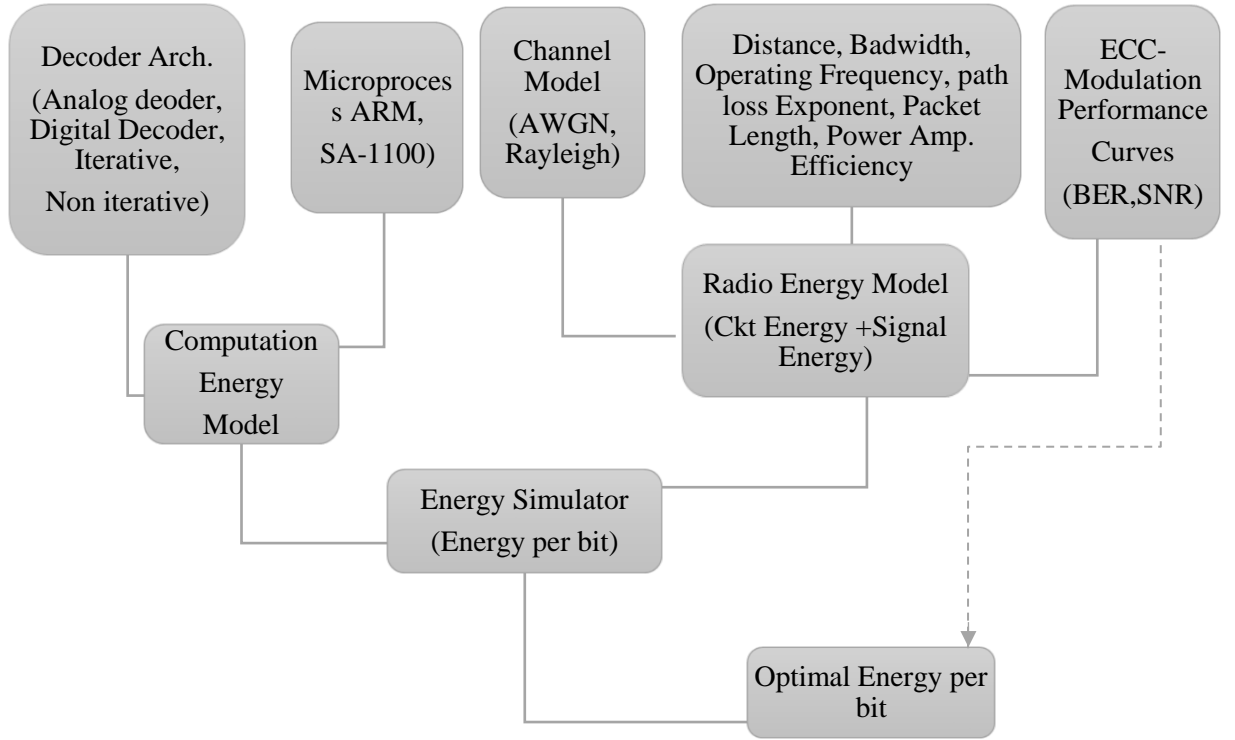


Fig. 3.5: Block diagram for WSN design exploration agenda

3.4 Energy Model of Sensor Node

In any sensor node, energy is consumed by the power supply unit (filter and regulator), the sensor unit, the computation unit and the transceiver (radio) unit. The Radio Energy Model (RadioEM) and the Computation Energy Model (CompEM) are the two major modules of this design space exploration agenda [14], [15].

Radio Energy Model: For a SN the energy can be calculated by using the basic formula [Energy (J) = Power Consumed (W or J/s) x Time period (s)]. The component which contributes to the variation in energy consumption of a radio energy model are energy consumed in transmitting the signal and energy consumed by the radio circuit [104], [105]. These two components are incorporated into the energy model. The radio energy E_{radio} per bit, in transmitting L bits, can be described as

$$E_{radio} = \frac{P_{on}T_{on}}{L} \quad \dots (3.6)$$

where, P_{on} denotes energy consumed by the node while transmitting, receiving and being in idle mode and T_{on} is transceiver on time. The power spent in radio during ON mode is the summation of is power consumption transmitting signal (P_{sig}) and total power consumption of circuit ($P_{ckt_tot.}$). Thus, the consumption of radio energy is

$$E_{radio} = \frac{(P_{sig} + P_{ckt_tot.})T_{on}}{L} \quad \dots (3.7)$$

Transceiver Circuit Energy Model: The key components of a typical transmitter circuit are Digital-To-Analog Converter (DAC), Low-Pass Filter (LPF), mixer, frequency synthesizer (FS), power amplifier (PA), and band-pass filter (BPF). The receiver circuit components are mainly BPF, Low-Noise Amplifier (LNA), mixer, Freq. Synthesizer, Intermediate-Frequency Amplifier (IFA), LPF, and Analog-To-Digital Converter (ADC). Circuit power consumption P_{ckt_tot} is contributed by the Power Amplifier (PA) power (P_{PA}) and rest of the circuit elements power (P_{ckt}) of the transceiver circuit.

$$P_{ckt_tot} = P_{PA} + P_{ckt} \quad \dots (3.8)$$

$$P_{ckt} = P_{DAC} + 2P_{LPF} + 2P_{FS} + 2P_{BPF} + P_{LNA} + P_{IFA} + P_{ADC} \quad \dots (3.9)$$

where, P_{DAC} , P_{LPF} , P_{FS} , P_{BPF} , P_{LNA} , and P_{IFA} represent the power consumptions in DAC, ADC, LPF, FS, BPF, LNA, and IFA respectively. The ratio of RF output power to the DC input power is known as drain efficiency (η) of PA. Power consumption in PA related to transmit signal power as $P_{PA} = \alpha P_{sig}$, where, constant α relates to η with $\eta = 1 / (1 + \alpha)$.

Computation Energy Model: The total computation energy per bit E_{comp} is

$$E_{comp} = \frac{E_{enc} + E_{dec}}{L} \quad \dots (3.17)$$

where, E_{enc} represents as encoder computation energy and (while) E_{dec} corresponds to as decoder computation energy. This job is performed by the processor unit in the MICAz sensor node

Transmit Signal Energy Model: The power needed for transmitting L bits can be represented as

$$E_{radio} = \frac{((1+\alpha)P_{sig}+P_{ckt})T_{on}}{L} \quad \dots (3.10)$$

Signal power required in the free space can be expressed by Friis transmission equation [99] given by (3.11)

$$P_{sig} = \left(\frac{4\pi}{\lambda}\right)^2 d^n \frac{P_r}{G_t G_r} \quad \dots (3.11)$$

where, d denotes the distance between transmitter and receiver; λ denotes transmitted signal wavelength; G_t and G_r are the antenna gains of transmitter and receiver respectively; and n is known as the path loss exponent. The received power is expressed as

$$P_r = SNR_{uncoded} bB \frac{N_0}{2} NF \quad \dots (3.12)$$

Where, $SNR_{uncoded}$ is the SNR for uncoded transmitting data, b knows as number of bits per modulation symbol, B denotes bandwidth, $\frac{N_0}{2}$ known as noise spectral density for the AWGN channel and NF is express as receiver noise figure. The received power of coded data is

$$P_r = SNR_{coded} bB \frac{N_0}{2} NF \quad \dots (3.13)$$

where, SNR_{coded} is express as SNR per bit for coded data transmission. The received power can be stated in terms of coding gain CG as

$$P_r = \frac{SNR_{uncoded}}{CG} bB \frac{N_0}{2} NF \quad \dots (3.14)$$

The node energy consumed per information bit for the coded system is the sum of E_{radio} and E_{comp} . Using (3.10), the node energy for the coded system is defined as

$$E_{node_coded} = \frac{(1+\alpha)P_{sig}T_{on}+P_{ckt}T_{on}\frac{N}{K}LE_{comp}\frac{N}{K}}{L} \quad \dots(3.15)$$

Where, N denotes as encoded bits corresponding to the K data bits. For RS codes, N and K characterize as number of symbols and it can correct up to t symbols, where $K = (N - 2t)$. RS code is expressed as RS (N, d_{min}) , where d_{min} known as the minimum distance of the code, $d_{min} = (2t + 1)$. Thus, in RS codes $N/K = N/(N - 2t)$. The node energy per information bit for the uncoded system is specified by

$$E_{node_uncoded} = \frac{(1+\alpha)P_{sig}T_{on} + P_{ckt}T_{on}}{L} \quad \dots (3.16)$$

Crossover Distance: Coding gain vary with distance, the distance at which an error control scheme become energy efficient is called crossover distance [14]. At crossover distance, (d_{xover}), for the same Bit Error Rate, the consumption of node energy of the uncoded and coded systems is equal, i.e.,

$$E_{node_uncoded} = E_{node_coded} \quad \dots (3.18)$$

For distances less than the crossover distance, $E_{uncoded} < E_{coded}$, i.e., use of ECC is not energy efficient. The relationship for d_{xover} from above the model as

$$d_{xover} = \left(\frac{P_{ckt}T_{on}\left(\frac{N}{K}-1\right) + LE_{comp}\frac{N}{K}}{\left(\frac{4\pi}{\lambda}\right)^2 \frac{(1+\alpha)SNR_{uncoded}}{2G_rG_t} bBN_0NFT_{on}\left(1-\frac{1}{CG}\right)} \right)^{1/n} \quad \dots (3.19)$$

The circuit energy, signal energy, and computing energy all have a different effect on crossover distance. Where n is path loss exponent and take 2 for free space [103]. From (3.19) it is clear that if radio circuit energy and computation energy decreases, then crossover distance decrease and ECC becomes feasible at a lower distance. For An ECC, if change the constellation size by b then d_{xover} depends on coding gain CG and bT_{on} . Effect of T_{on} and CG are different with different modulation schemes. Hence the error-correction capability varies with different schemes. We can analyse the combination of modulation schemes and ECC parameters by the code word length N and error-correcting capability t for energy consumption.

Final Node Energy Equation: For coded system, the node energy per bit (E_{node_coded}) is the summation of radio energy and computation energy. Using (3.18) and equation (3.24)

$$E_{node_coded} = \frac{(1+\alpha)P_{sig}T_{on} + P_{ckt}T_{on}\frac{N}{K} + LE_{comp}\frac{N}{K}}{L} \quad \dots (3.20)$$

Figure. 3.6 describe power consumption of a typical WSN node in several sub-systems and modes of operation [104]-[106] namely transmitter, receiver, idle and sleep. From Fig. 3.6, it may be noted that, the highest amount of energy is consumed in communication subsystem (Transmit-Receive mode) as compared to other subsystems or modes of operation in the sensor node. By using optimal combination of modulation schemes and error correcting codes, we can make WSN energy efficient.

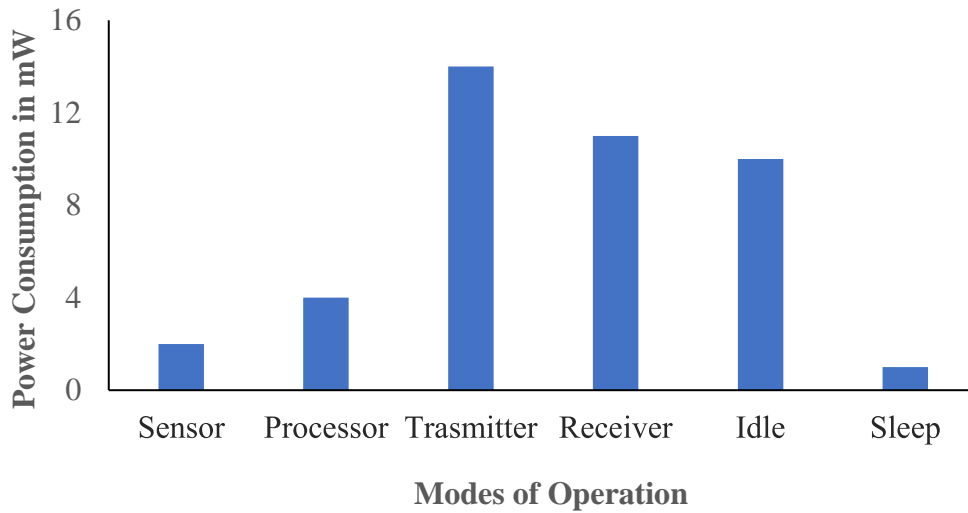


Fig 3.6: The consumption of power in SN for various modes of operation

3.4.1 Variation of Signal Energy with ECC and Modulation Techniques

In this section, the effect of variation of codeword length N , number of bits per modulation symbol (b) for code error correcting capabilities (t) on signal energy is discussed)

- i) Variations in Signal Energy with respect to Codeword length N and Number of bits per Modulation Symbol b while keeping Error Correcting Capability t constant: For

constant t as increase codeword length N , in equations shown in Table 3.3 SNR_{coded} , term $N/(N-2t)$ reduces and value of $(erfc^{-1}(\cdot))$ term rises (Fig.3.13). Thus, the signal energy is optimum for a particular N . For higher values of t along with b , the signal energy is minimized for a higher value of N .

- ii) Variations in Signal Energy with respect to Error Correcting Capability t and Number of bits per Modulation Symbol b while keeping Codeword Length N Constant: The effects of the modulation and ECC parameters on the transmit signal energy is analyzed.

Using (3.11) and (3.13), the transmit signal energy $E_{sig} = P_{sig}T_{on}$ can be written as:

$$E_{sig} = C_1 SNR_{coded} b T_{on} \quad \dots (3.21)$$

where, C_1 kept constant w.r.t the ECC and the modulation scheme and express as

$$C_1 = \left(\frac{4\pi}{\lambda}\right)^2 d^n \frac{1}{2L G_r G_t} B N_0 N F \quad \dots (3.22)$$

Now, the value of E_{sig} for three modulation techniques along with RS codes in which $N/K=N/(N-2t)$ is evaluated as follows in Table 3.3.

Table 3.3: Formulas expressed for T_{on} , SNR_{coded} and E_{sig_norm}

Modulation scheme	T_{on}	SNR_{coded}	E_{sig_norm}
MPSK Modulation	$\frac{L}{bB}$	$= \begin{cases} \frac{N}{N-2t} \frac{(erfc^{-1}(2p_s))^2}{b \left(\sin\frac{\pi}{2b}\right)^2}, & \text{otherwise } b=1 \end{cases}$	$= \begin{cases} \frac{N}{N-2t} \frac{(erfc^{-1}(2p_s))^2}{b \left(\sin\frac{\pi}{2b}\right)^2}, & \text{otherwise } b=1 \end{cases}$
MQAM Modulation	$\frac{L}{2bB}$	$= \frac{N}{N-2t} \frac{2(2^b-1)}{3b} \left(erfc^{-1} \frac{p_s}{2 \left(1 - \frac{1}{\sqrt{2^b}}\right)} \right)^2$	$= \frac{N}{N-2t} \frac{2(2^b-1)}{b} \left(erfc^{-1} \frac{p_s}{2 \left(1 - \frac{1}{\sqrt{2^b}}\right)} \right)^2$
MFSK Modulation	$\frac{2^b L}{bB}$	$\leq \frac{N}{N-2t} \frac{2}{b} \left(erfc^{-1} \left(\frac{2p_s}{2^b-1} \right) \right)^2$	$\leq \frac{N}{N-2t} \frac{2}{b} \left(erfc^{-1} \left(\frac{2p_s}{2^b-1} \right) \right)^2$

where, p_s denotes, channel symbol error probability corresponding to the desired coded symbol error probability (p_{es}). It can be calculated while calculating the coding gain for different RS codes with different modulation techniques.

3.4.2 Variations of Node Energy with ECC and Modulation Parameters

(a) Constellation Size

Consumption of Node energy depends on the constellation size of a modulation techniques in two ways. When the constellation size of the uncoded signal is increased, the required SNR per bit is decreases. On the other hand, for a coded signal with an increased constellation size, a large SNR is needed to maintain the desired BER. For large distances ($d > 90m$) on increases the Constellation size (b) the consumption of node energy also increases & vice versa (Fig.3.15(a)). This, in turn, affects the coding gain of ECC. Therefore, when the size of constellation is changed, the node energy with the same ECC changes (increases for $d > 90m$ and remains constant for $d < 30m$). It means for very small distances ($d < 30m$) ECC loses its significance and hence, no coding gain is achieved.

(b) ECC Parameters

Various RS codes are designed by doing variations in code word length N and error-correcting capability ' t '. The normalize signal energy with an RS code ($N = 31$) is plotted against varying ' t ' at distance 100m. The node energy is optimum for a particular ' t '. The node energy of the coded system can be calculated using (3.11), (3.13) with (3.15) which results in the following equation

$$E_{node_coded} = C_2 d^n \frac{SNR_{uncoded}}{CG} b T_{on} + E_{comp} \frac{N}{K} + P_{ckt} T_{on} \frac{N}{KL} \dots (3.23)$$

$\xleftarrow{\hspace{1.5cm}} \hspace{0.5cm} \xrightarrow{\hspace{1.5cm}}$

Signal Energy
Comp Energy
Ckt Energy

where,

$$C_2 = \left(\frac{4\pi}{\lambda}\right)^2 \frac{(1+\alpha)}{2LG_rG_t} BN_0NF \quad \dots (3.24)$$

where, C_2 is kept constant for various ECCs and modulation techniques. The $SNR_{uncoded}$ can be calculated using equations in Table 3.3 SNR_{coded} by replacing the ratio of $N / (N - 2t)$ with unity. In (3.23) total node energy is expressed as the summation of three energy components that is the signal energy, the computation energy, and the circuit energy, respectively. Involvement of every energy component to the node energy vary with the distance.

3.5 Experimental Setup and Simulation Results

The energy consumption of a wireless sensor node is a complex function of internodes distance, desired BER, channel conditions, operating frequency, modulation schemes, and ECCs. In this section, following two scenarios are consider:

3.5.1 ZigBee Home Automation Scenario in Qualnet 5.0 Simulator

In scenario 1, IEEE 802.15.4 standard's three modulation schemes (ASK, BPSK, OQPSK) [107] have been taken with fixed distance of internodes, desired BER, channel conditions, operating frequency (without ECC) and simulated in Qualnet 5.0 Simulator [108] them on a home automation scenario one by one and calculated entire energy consumption by the network's nodes. Then this work is extended by analysing the impact of different parameters on which node energy depends like internodes distance, desired BER, channel conditions & operating frequency.

3.5.2 Implementation of the WSN Node Energy Model Equations in MATLAB

In scenario 2, the WSN node energy equations have been simulated on MATLAB command window to obtain the results [108]. Then this work has been extended by analysing the impact of different parameters on which node energy depends like internodes distance, desired BER, channel conditions & operating frequency. Therefore, using this framework, the consumption of energy in a sensor node with and without using ECC and with different modulation techniques have been explored and analyzed. Several configurations of Hamming code, RS code, and Convolution Code are considered. In this section, the exploration results of node energy for different ECCs and modulation schemes have been presented. The ECC with minimum energy in a given set of ECC's is referred to as the energy-optimal ECC. Simulation parameters of Qualnet network simulator and MATLAB are presented in Table 3.4.

Table 3.4: Simulations Parameters

Qualnet Network Simulator [107]		MATLAB [108]	
Parameters	Values	Parameter	Values
Radio Type	802.15.4 Radio	Power consumption of freq. Synthesizer (P_{FS})	13.7 mW
Transmission Power (dBm)	15.0	Power consumption of LNA (P_{LNA})	0.55 mW
Model of Packet Reception	PHY 802.15.4 Reception Model	Power consumption of Band Pass Filter (P_{BPF})	6.12 mW
Antenna Gain (dB)	0.0	Power consumption of IF Amp. (P_{IFA})	0.2 mW
Antenna Height (meters)	1.5	Power consumption of LPF (P_{LPF})	0.29 mW
Antenna Efficiency (dB)	0.8	Power consumption of ADC (P_{ADC})	4.1 mW

Antenna Mismatch Loss (dB)	0.3	Power consumption of DAC (P_{DAC})	55 mW
Antenna Cable Loss (dB)	0.0	α	1.9
Antenna Connection Loss (dB)	0.2	G_r, G_t	1 W
Antenna Model	Omni directional	n	4
Temperature (°K)	290.0	N_0	4×10^{-21} W/Hz

3.5.3 Simulation Results

A. Comparison of Different Modulation Techniques

In this sub-section, the performance of modulation techniques is compared using the equations and summarized in Table 3.5. The BER is plotted in Fig. 3.7 to 3.9 for various modulation techniques. Following are the observations:

- The BER for all the systems reduces monotonically with raising E_b/N_0 values; the defining curves have a similar shape as a waterfall (Fig. 3.7).
- For any value of E_b/N_0 value, coherent binary PSK, QPSK, and MSK, OQPSK and QAM generates a small BER than any other modulation technique (Fig. 3.7).
- Coherent binary PSK and DPSK require an E_b/N_0 value of 3 dB, less than the corresponding values for conventional coherent binary FSK, so that the same bit error rate can be realized. (Fig. 3.7)
- At higher values of E_b/N_0 , DPSK performs almost as well (around about 1 dB) as coherent binary PSK and conventional coherent binary FSK, respectively, for the same bit rate and signal energy per bit.

- (e) In coherent QPSK, two orthogonal carriers are used, $\sqrt{2/T} \cos(2\pi f_c t)$ and $\sqrt{2/T} \sin(2\pi f_c t)$, where the f_c represents carrier frequency and is an integer multiple of the symbol rate $1/T$ with this two independent bit streams can be transmitted simultaneously and then detected in the receiver.
- (f) The MSK technique differs from its counterpart, the QPSK [15] in that its receiver has a memory. In particular, the MSK receiver makes decision on the basis of observations over two consecutive bit intervals.
- (g) The E_b/N_0 also increases as the value of M increases. Practically, we don't use value of $M > 8$ in wireless communication. (Fig 3.8)
- (h) In Fig. 3.9 on increasing the modulation order of PSK scheme, we have observed the signal energy follows the same pattern, whereas the signal energy level rises.

Table 3.5: BER of various modulation Schemes [100]

Sr. No.	Modulation Scheme	Bit Error rate (BER)
1.	Coherent ASK	$Q \left[\sqrt{\frac{A_c^2 T_b}{4N_0}} \right]$
2.	Coherent binary PSK Coherent QPSK Coherent MSK	$\frac{1}{2} \text{erfc}(\sqrt{E_b/N_0})$
3.	DPSK	$\frac{1}{2} \exp(-E_b/N_0)$
4.	Coherent binary FSK	$\frac{1}{2} \text{erfc}(\sqrt{2E_b/N_0})$

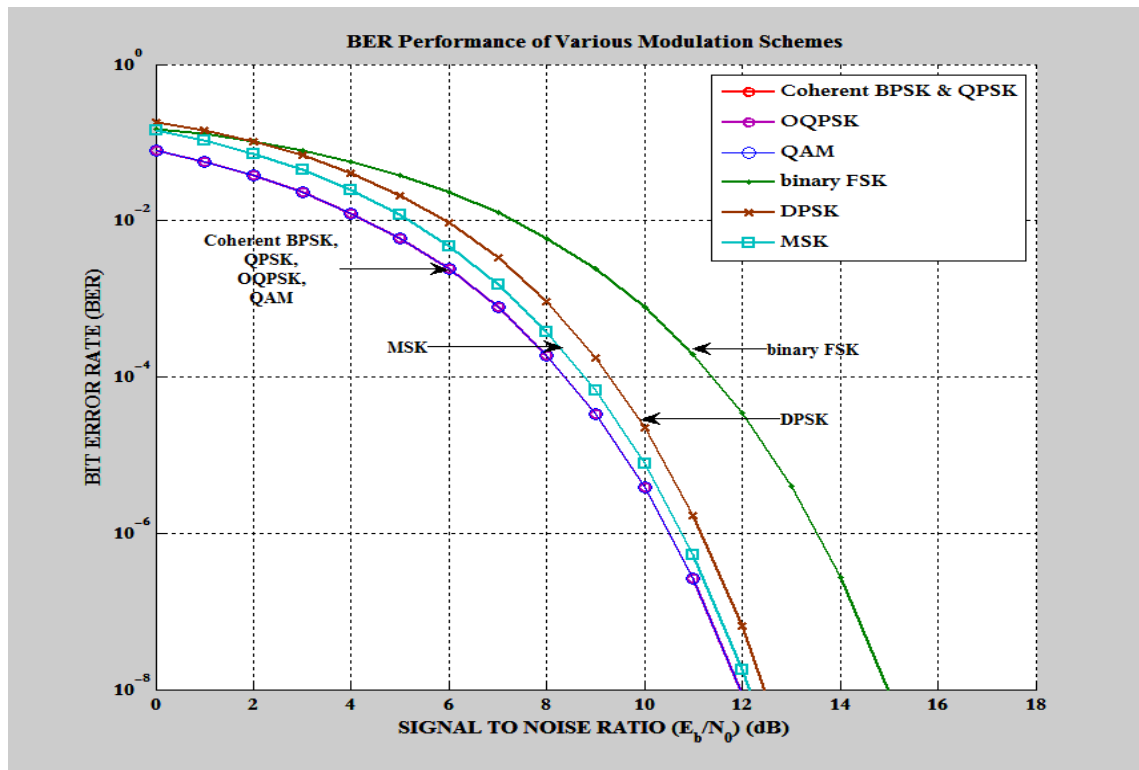


Fig. 3.7: BER performance of various Modulations schemes

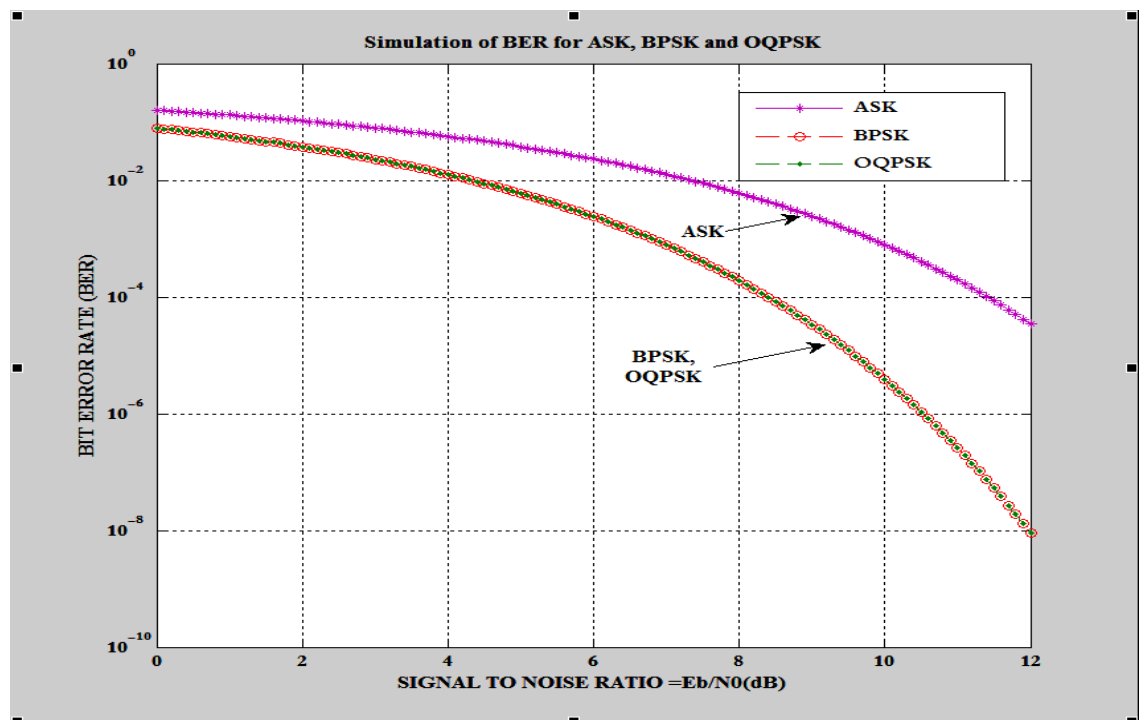


Fig. 3.8: Simulation Results ASK, BPSK and OQPSK of in MATLAB

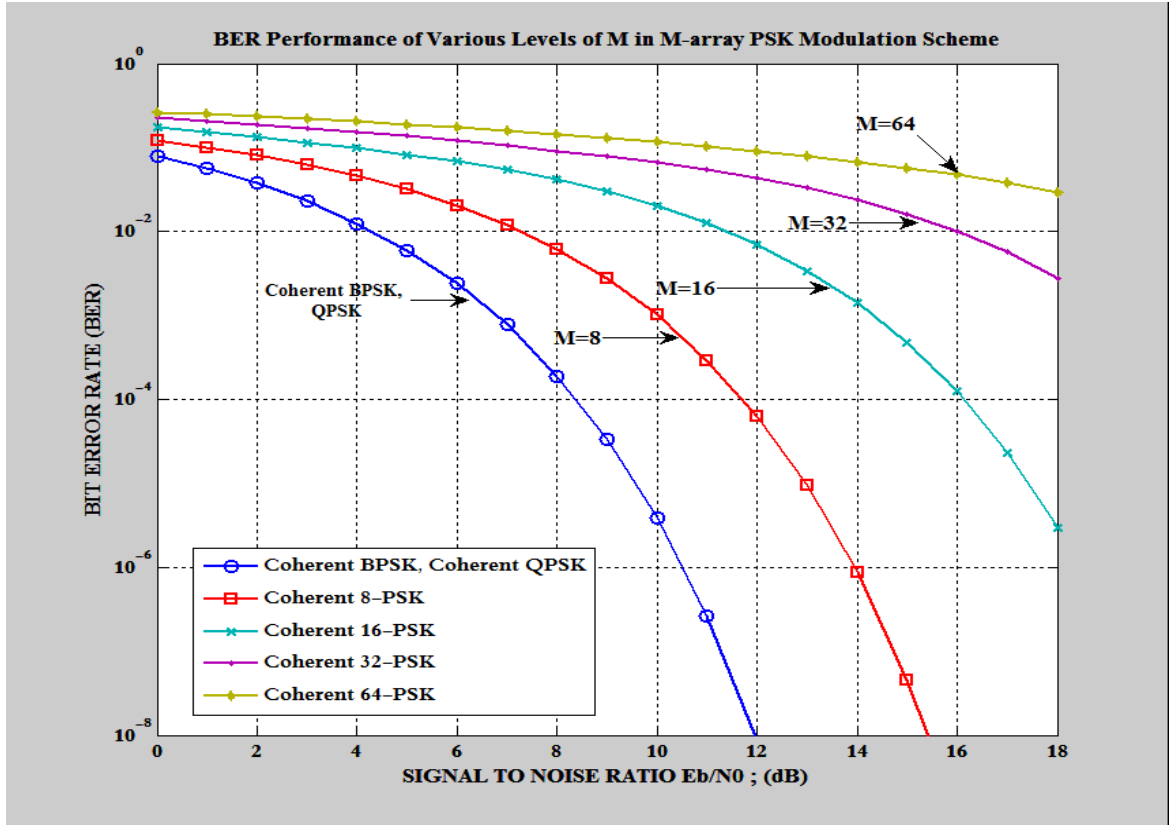


Fig. 3.9: BER performance of M-array PSK

B. Comparison of Different ECC Techniques (Performance Measure)

Here we have taken various ECC of some general values of Codeword length (N) and Message Length (K) as available in literature and in simulation tools (MATLAB). The Fig. 3.10 indicates the RS (511,479) code has optimum energy consumption (7dB) with respect to minimum BER performance curve (i.e. between $10^{-1} - 10^{-2}$). Though the CC - Hard (7, [171], [133]) has smaller value E_b/N_0 ratio (dB) its BER is lies between 10^{-1} to 10^0 which is larger than RS code BER value. Therefore, in this analysis our result is RS (511,479) codes have optimum energy consumption with good BER values.

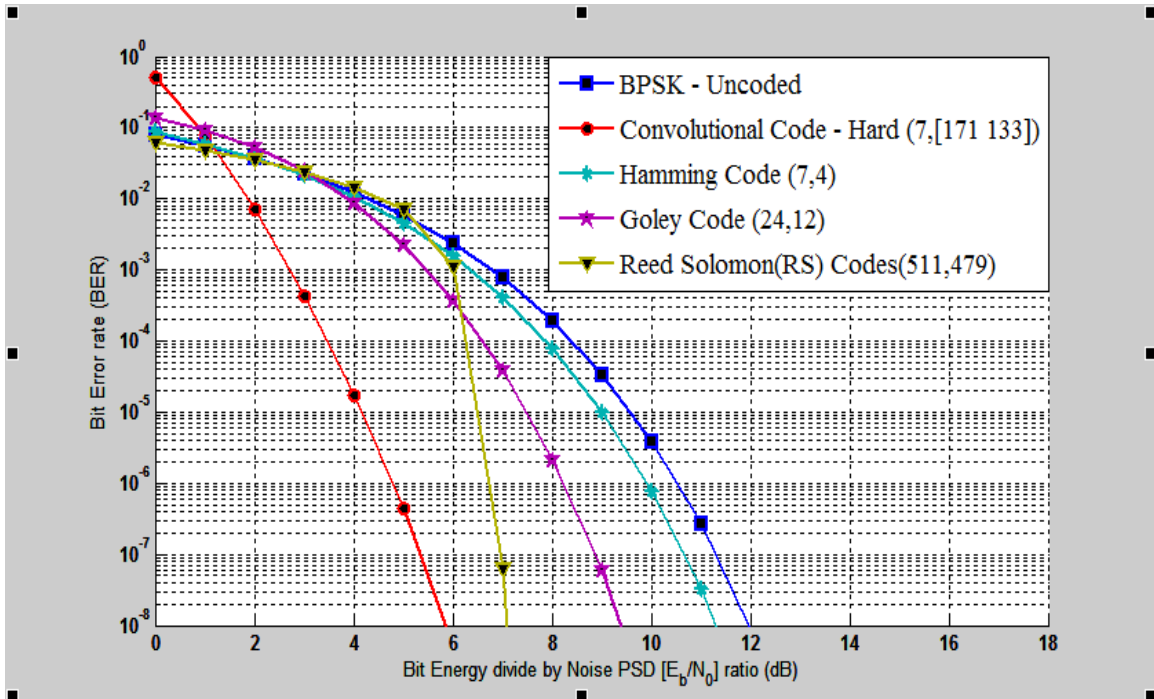


Fig. 3.10: BER performance of BPSK with uncoded and with various ECC

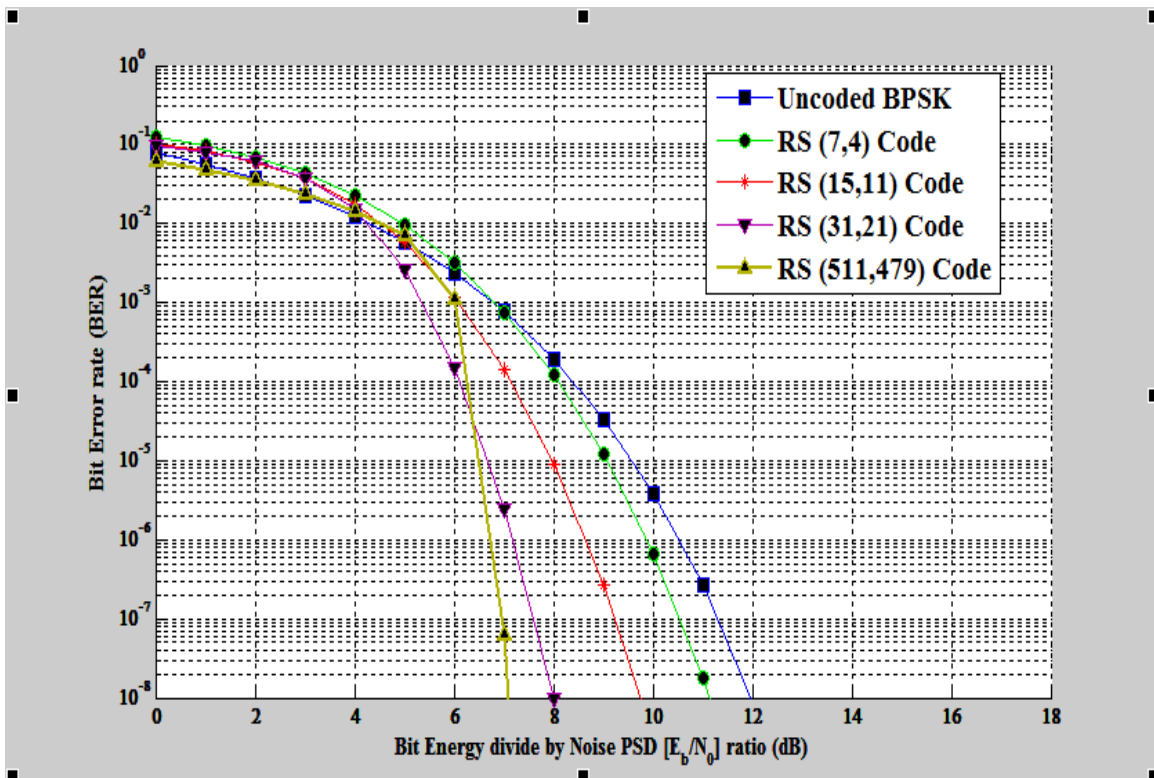


Fig. 3.11: BER performance results of BPSK using different RS Codes

Fig. 3.11 shows the RS codes (N=511, K=479) has optimum energy consumption (7dB) with respect to minimum BER performance curve (between 10^{-1} – 10^{-2}). Here various values of Codeword length (N) and Message Length (K) for RS codes are taken and compared which gives results as RS (511,479) codes has optimum energy consumption with good BER values.

C. Energy Analysis using Qualnet Network Energy Simulator Results

Energy Consumption by SNs in network setup of Home automation in transmit, receive and idle modes using modulation techniques i.e. ASK, BPSK and OQPSK are obtained through Qualnet Network energy simulator and observations are placed in Table 3.6. The same is pictorially presented in Fig. 3.12.

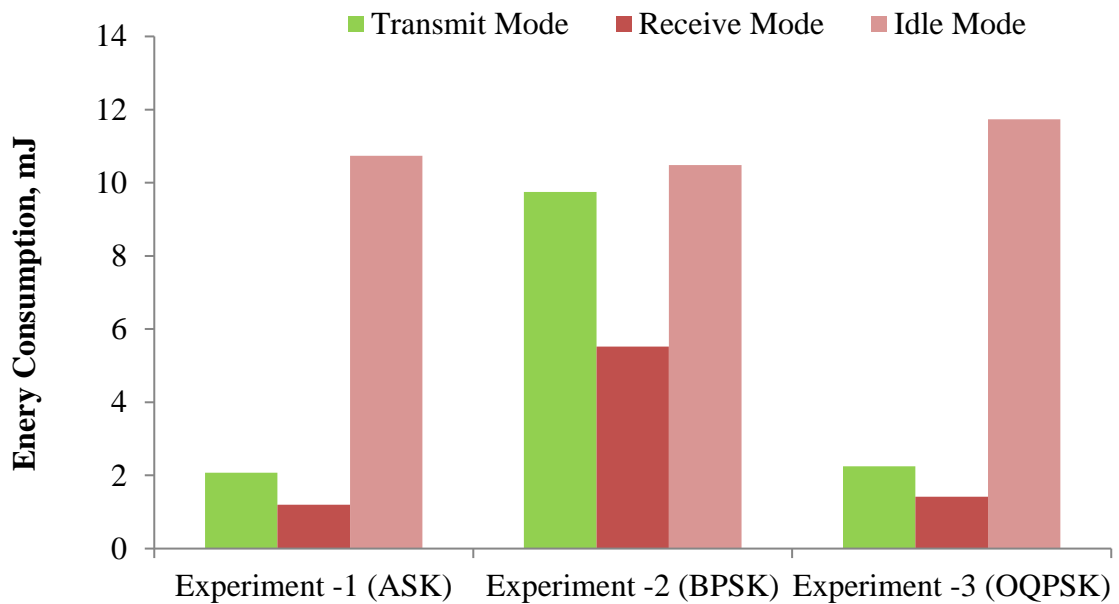


Fig. 3.12: Simulation results of energy consumption in transmit, receive and Idle modes

Table 3.6: Simulation results in Qualnet for energy consumption in sensor nodes

Exp. No.	Modulation techniques	Transmit Mode (mJ)	Receive Mode (mJ)	Sleep Mode (mJ)	Idle Mode (mJ)	Total Energy Consumption in all Modes (mJ)
1	ASK	0.071233	0.203	0	10.739	11.013233
2	BPSK	0.374523	1.254	0	10.487	12.115523
3	OQPSK	0.072504	0.215	0	10.736	11.023504

It is clear, from Table 3.6 that the ASK is consuming smallest power in all three modes as compared to BPSK and OQPSK (uncoded data transmission). But as we know that the Noise has high effect on ASK modulated data packets therefore unwillingly, we have to leave the ASK from our choice for WSN and to choose the second smallest energy consumption modulation scheme i.e. OQPSK for WSNs.

In digital Communication, ASK has very high noise interference such that in some cases, we need to retransmit each packet twice. Therefore, practically ASK is never used in digital wireless communication. The PSK has very high noise immunity (very small noise interference). Therefore, BPSK and QPSK are widely used in all practical cases.

D. Energy Analysis using MATLAB Results

Fig. 3.13 shows variations in Normalised Signal energy in with 4-QAM & 4-PSK w.r.t varying Code word Length (N) with constant error correcting capability ($t=4$) at distance $d=100\text{m}$. It is observed, the energy consumed is higher in 4-QAM as compared to QPSK for a value of RS codeword length ($N=20$ to 120).

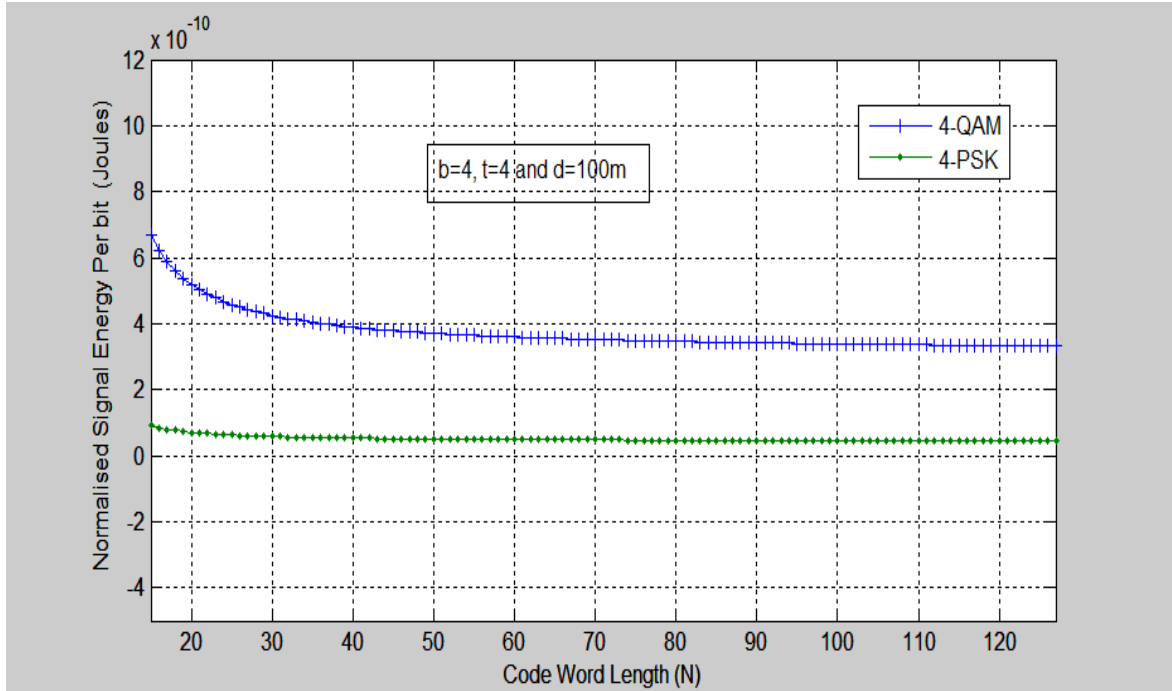


Fig. 3.13: Normalised signal energy of 4-QAM and 4-PSK w.r.t code word length (N)

Variations in Normalised Signal Energy in with 4-QAM, 4-PSK and 4-FSK w.r.t. constant Code word Length ($N=31$) and varying error correcting capability ($t=1$ to 10) at constant distance ($d=100\text{m}$) are presented in Fig. 3.14. It is observed that the energy consumed is lower in 4-PSK as compared to 4-QAM and 4-FSK for any value of RS codeword length ($t=1$ to 10).

The overall effect of varying N and t on the signal energy is shown in Fig. 3.13 and Fig.3.14. When the modulation techniques differ from BPSK to QPSK, the signal energy follows same patterns, except that the level of signal energy rises.

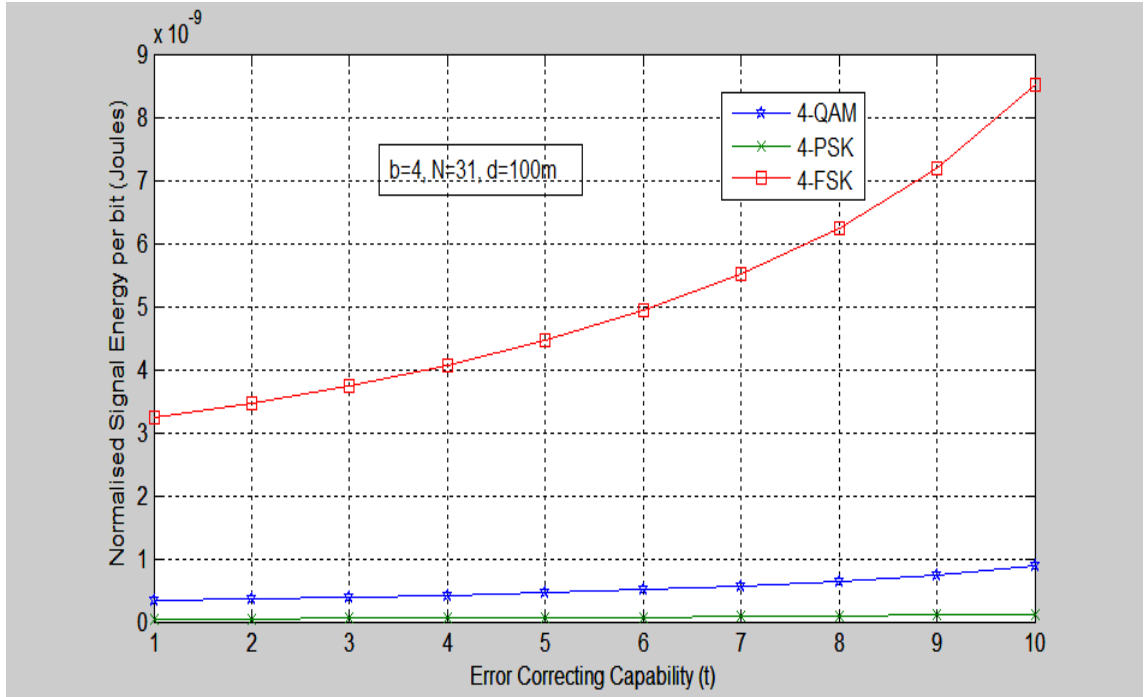


Fig. 3.14: Normalized signal energy of 4-QAM, 4-PSK and 4-FSK w.r.t Error Correction Capability (t)

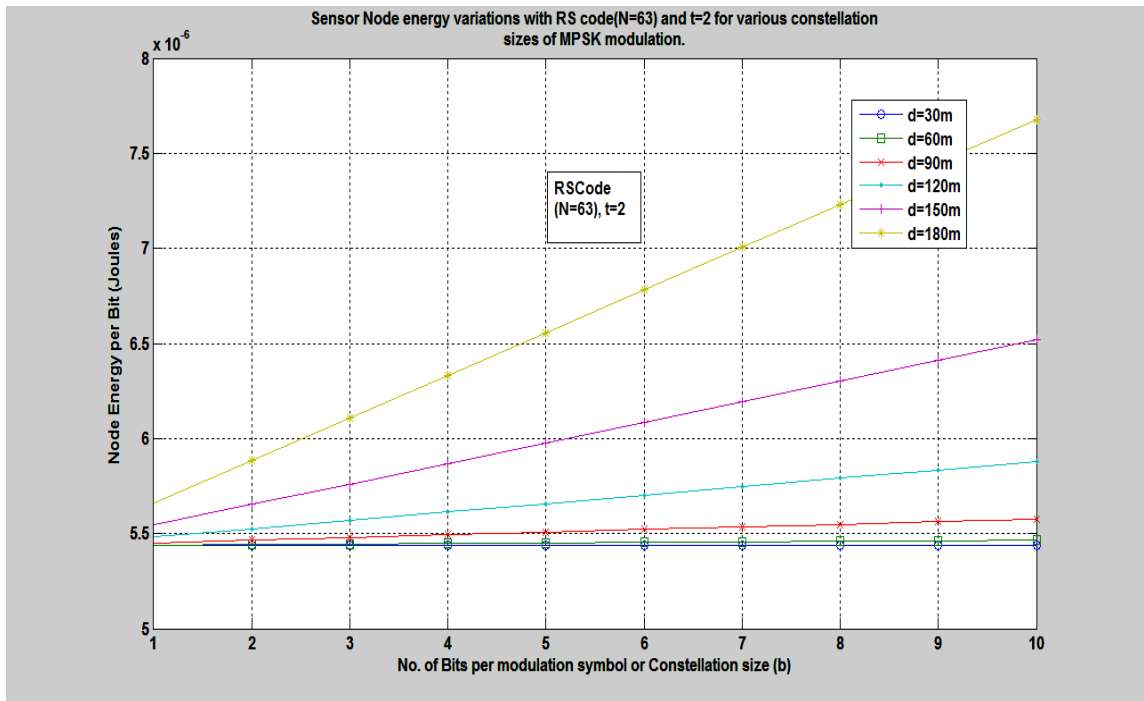


Fig. 3.15 (a): Variations of sensor node energy with RS code (N=63) and t=2 for varying constellation sizes of MPSK Modulation at different distance (d)

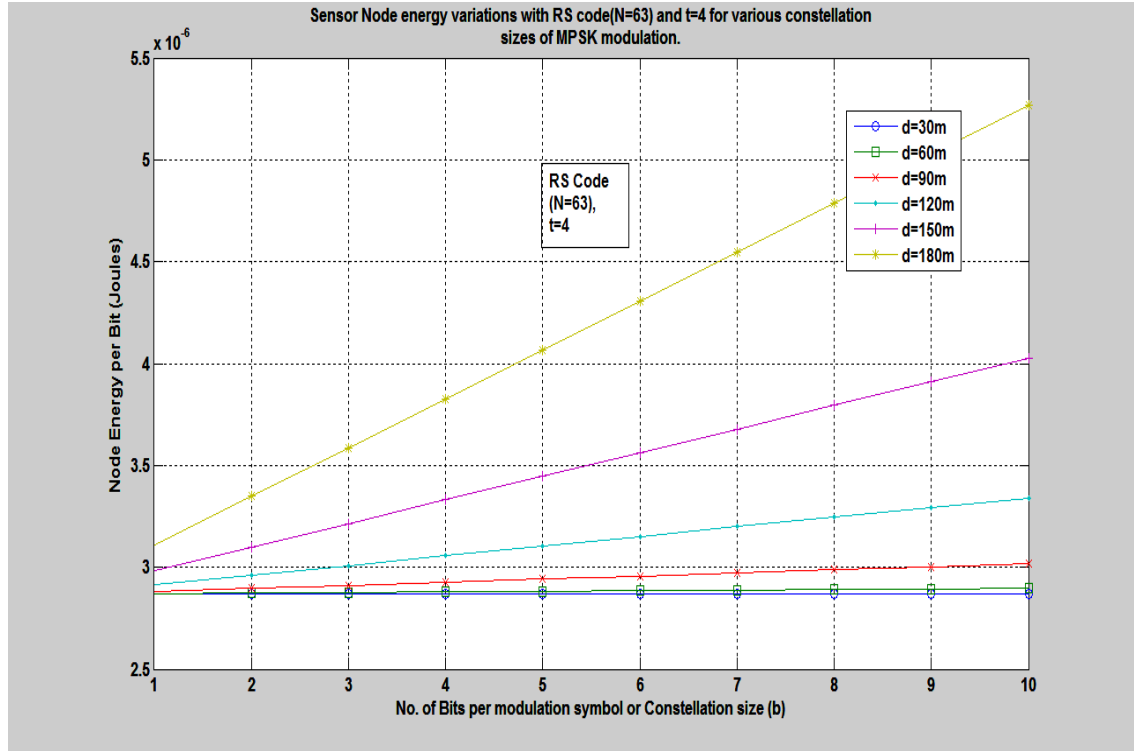


Fig. 3.15 (b): Variations of SN energy with RS code(N=63) and t=4 for varying constellation sizes of MPSK Modulation at different distances (d)

In Fig.3.15 (a) at an internodes distance of 180 m, for $N=63$, $t = 2$ and $b=2$ the node energy is $E_1=5.75 \times 10^{-6}$ J as compared with Fig. 3.15 (b) at 180m, $N=63$ and $t=4$ the node energy is $E_2=3.40 \times 10^{-6}$ J. Hence, in BPSK, as ECC capability increases the energy consumption is decreased ($E_{\text{saving}} = E_2 - E_1$) i.e. 2.35×10^{-6} J per bit (or 40%) of energy is saved.

Table 3.7: MATLAB simulation results for RS (N=63) code with t=2 and t=4

Distance (d)	MPSK (b=2 i.e. BPSK)	Node Energy(E_1) per data bit (μ J) at (t=2)	Node Energy(E_2) per data bit (μ J) at (t=4)	Node energy saving (μ J) $E_1 - E_2$	Node energy saving (%) $= (E_1/E_2) \times 100$
30	2	5.38	2.79	2.60	47%
60	2	5.41	2.81	2.60	48%
90	2	5.42	2.85	2.57	47%
120	2	5.52	2.92	2.60	47%
150	2	5.54	3.20	2.34	42%
180	2	5.75	3.40	2.35	40%

3.6 Conclusion

This chapter describes the method for exploring different ECCs based on their energy consumption for sensor nodes have been proposed. For this exploration, proposed an integrated framework that computes the radio energy and the computation energy. Several configurations of Hamming codes, RS codes, and CCs have been examined using this framework. The results clearly show that energy trade-offs in radio and computation energies save up to 60% energy of the sensor node. Application-defined parameters such as internode distance (d) and path loss exponent (n) also play's a significant role in selecting the energy efficient ECC. Furthermore, varying the error-correcting capability (t), code word length (N), and modulation parameters affect the choice of the optimal ECC. The analysis presented in the chapter reduces the search space by eliminating many of the available ECCs and modulation variants, and the optimal energy consuming ECC-Modulation configuration for the sensor node is obtained. Simulation results show that in certain operating conditions, sensor node with RS codes and BPSK modulation consumes the optimal energy. Furthermore, the optimum energy pair can be found among various modulation schemes, according to the design requirements. We find at distance $d = 60\text{m}$ an optimal ECC-modulation pair RS ($N=63$) code with $t=4$ and BPSK modulations schemes give 48% energy savings.

CHAPTER 4

MALICIOUS NODE DETECTION AND PREDICTION

The WSN applications in general covers, supervising and tracking of surveillance area and events, respectively. The former keeps an eye on the environment but transmission is only triggered if a previously defined event trapped. The latter watches a process and keeps reporting the status of such a process. Examples include forest fire monitoring which monitors an event of fire, power and water meters which tracks energy and water usage in households etc. Due to very constraint resources in the sensor nodes, most of the WSN protocols, shows a great value of trust between the nodes which are communicating so as to reduce the phenomenon of the authentication overhead. This on the other hand causes the danger to introduction of malicious nodes to the WSN or alter the operation of existing ones. The unfavourable environment might take some sensor nodes into their control and use them to introduce wrong data with the only aim of affecting the network operator. Consequently, there is a risk of an attacker launching an array of attacks in the sensor network [109]. According to [22] the most dangerous attack in WSN is the insertion of the malicious node as it can destroy the whole network. In this chapter, we discuss about detection of malicious nodes and how we can protect the network from such adversaries.

In this chapter, we propose an enhanced malicious node detection scheme using Cluster Based Weighted Trust Evaluation (CBWTE), Support Vector Machine (SVM) methods.

The malicious node detected can be isolate by analysing the prediction time, detection ratio and classifying by SVM method with Auto Regression (AR) prediction. We also include detection of Byzantine Attack using Extended Kalman Filter (EKF) method.

4.1 Weighted Trust Evaluation

Weighted Trust Evaluation (WTE) based scheme is a light weighted algorithm used to detect and subsequently isolate malicious nodes by monitoring their reported data in WSN. Earlier Researches employed and demonstrated this method using a three-layer hierarchical sensor network. In hierarchical topology, when root node fails, entire network crashes and it's difficult to configure. The components of the three-layer hierarchical network architecture are [56]:

- a) Sensor Nodes (SNs): These are low power devices with limited functionality. SN's are the first in a layer that collects information from the environment and sends it to its Forwarding Node (FN).
- b) Forwarding Nodes (FNs): These are comparatively high power-operating devices which collect data from SN's aggregate and forward it to the next level Base Stations.
- c) Base Stations (BS): These act as upper layer FN, which collects data from the lower level FNs. This layer is also known as Access Points (AP) since they verify the data from the previous layer and route data between wireless and wired network.

4.1.1 Operation of Weighted Trust Evaluation

Previous schemes were based on two assumptions; first, the FNs and BSs have trusted nodes that cannot be compromised by an attacker since once an adversary seizes control of the BS then they can launch any possible attack in the sensor

network. Another critical assumption was that the normal nodes (working in proper condition) in the sensor network exceeds in number than the compromised nodes. Otherwise, the scheme may misidentify a normal node as compromised nodes increasing false positives. The proposed Random Deployment (RD) and Cluster Based Weighted Trust Evaluation (CBWTE) intends to detect and isolate malicious FNs in the sensor network instead of assuming that they won't be compromised by adversaries. Weighted Trust Evaluation is aims to detect all the SNs as well as FNs which are attacked or been non-working due to natural weathering conditions under hostile environment.

4.1.2 Network Model and Topology

The WSN is used for environmental monitoring of air pollution system comprises the SN's that are scattered over all the field. These SN's are composed of sensing elements that monitors and detect the concentration of pollutant in the environment and are connected to the respective cluster heads (CH) *via* a wireless link. The collected readings from each individual node are processed by CH and transmits to the Base Station through FN.

A hybrid cluster network architecture is shown in Fig. 4.1 which is combination of star, mesh and ring topology. Such topologies are used to improve the flexibility of the network for maintaining reliability by taking into account the available resources [110] as discussed below:

- Star topology is scalable and reduces power consumption.
- Mesh topology ensures efficient communication.
- All CH are connected directly to the FN which serves as a link from wireless

to wired network i.e. to the outside world. Fig.4.1 display the overall WSN architecture employing hybrid network topology.

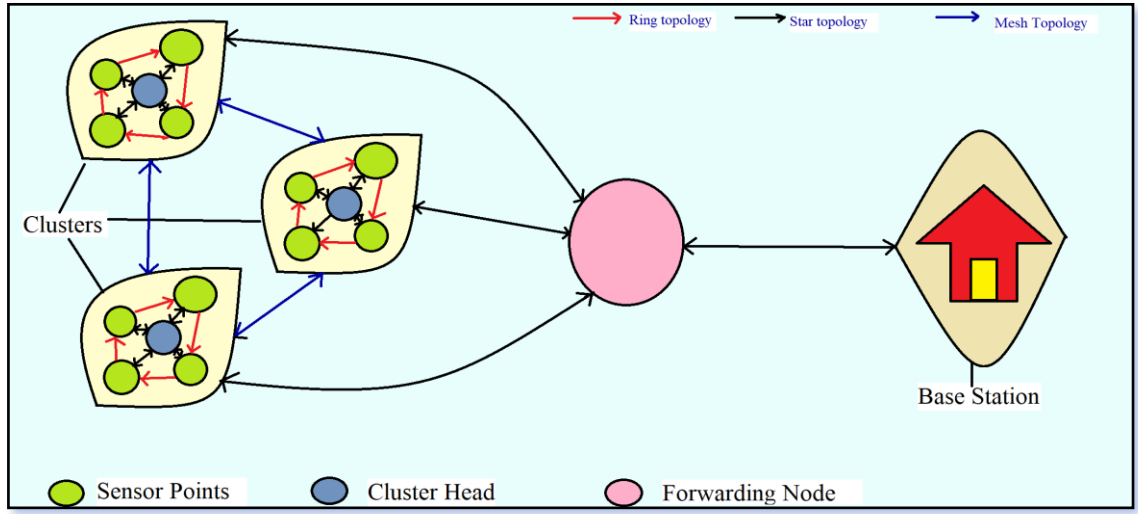


Fig. 4.1: Hybrid Topology

Cluster Based Weighted Trust Evaluation (CBWTE) method for malicious node detection is done in two steps:

- i. Error Detection
- ii. Weight Modification

4.1.3 Error Detection

Each CH maintain the trust among with SN's associated with it. The trust value (V_w) lies in the range (0 to 1) and is initialized to 1 for each SN. The weight represents the SN's trustworthiness or dependability. The SN with a higher weight is more trustworthy. Updating the trust values is important to maintain the fidelity of the readings obtained from the SNs. To determine the non-erroneous node the weighted threshold value should be greater than the minimum threshold value.

$$V_{th} \leq V_w \quad \dots (4.1)$$

$$V_w \leq \frac{M-|D|}{M} \quad \dots (4.2)$$

where, V_{th} is minimum threshold weight and V_w denote as the weighted threshold. ‘M’ represents the average or mean value of the sensor at a point and is the user specific attribute. D is the deviation from the mean value (M) of sensor node and its dependent on measured value. Its value can be determined as:

$$D = M - I \quad \dots (4.3)$$

where, ‘I’ the measured value

In a rainforest, let us assume that there exist temperature variations from 22 to 31°C then the mean value (M) is 26.5°C. Let measured value of temperature at any moment be ‘I’ and if it is 35°C, the estimated threshold value will be:

$$V_w = \frac{26.5 - |26.5 - 35|}{26.5} \quad \dots (4.4)$$

V_w is 0.679. If the minimum threshold V_{th} is set to 0.7, then $V_{th} \leq V_w$ is not satisfied. Thus, the related SN is a suspicious node.

4.1.4 Weight Modification

If the SN is detected as suspicious node, then the weight will be reduced according to the (4.5)

$$W' = W + F \times W \quad \dots (4.5)$$

where W' and W modified weight and current weight respectively and F is the weight penalty factor.

4.2 Cluster Based Weighted Trust Evaluation

This section introduces a Cluster Based WTE (CBWTE) method to detect malicious sensor nodes and malicious CHs. This method performs in less Detection time, high Detection Ratio and low Misdetection Ratio. Detection time is the time taken by a

SN to receive input from the surroundings, followed by forwarding to CH and detect malicious node. The trustworthiness of the SN's can be calculated by implementing the proposed algorithm which is explained in subsection 4.2.1 and also presented in the form of flow chart in the Fig. 4.2.

Suppose there are total 'n' SNs spread randomly in the area of action, a few of them are selected as the FN while the rest act as ordinary SN's. These SN's organize themselves to form an operational clustered network.

4.2.1 Algorithm

The algorithm comprises of two phases:

- i) Deployment phase
- ii) Computation and Transmission phase

(i) Deployment Phase

Step 1: 'n' number of SNs randomly deployed over an area under surveillance.

Step 2: Clusters are generated by dividing the area into four segments.

Step 3: The SN's send data to the CH that lies in their respective segments.

(i) Computation and Transmission Phase

Step 1: SN in a cluster transmits the sensed data to the FN.

Step 2: FN collects and stores all the data sent by the SN's lying under respective FN.

Step 3: FN implements the Clustered WTE algorithm and assign weights to the normal SN

- Step 4: The weighted value is compared with the values of the respective SN's.
- Step 5: The weights of the nodes whose values does not lies in range of deviation are reduced until their values are below the minimum threshold value set by user.
- Step 6: When the value of weight is less than the minimum weighted threshold, they are detected as malicious nodes.
- Step 7: The FN that do transmit during the rest time (non-transmission time) is separated as malicious.

4.2.2 Simulation and Modelling

The detection and isolation of malicious nodes is a continuous process. The response data of events triggered in the network is generated. This data is used for identifying malicious node.

The simulation methodology for evaluating and analysing malicious node detection and isolation scheme is done under different conditions. These conditions are as follows:

- i) The sensor nodes are randomly deployed.
- ii) The surveillance area is divided into segments which communicate through cluster heads.

Simulation parameters used for malicious nodes detection in CBWTE deployment are given in Table 4.1.

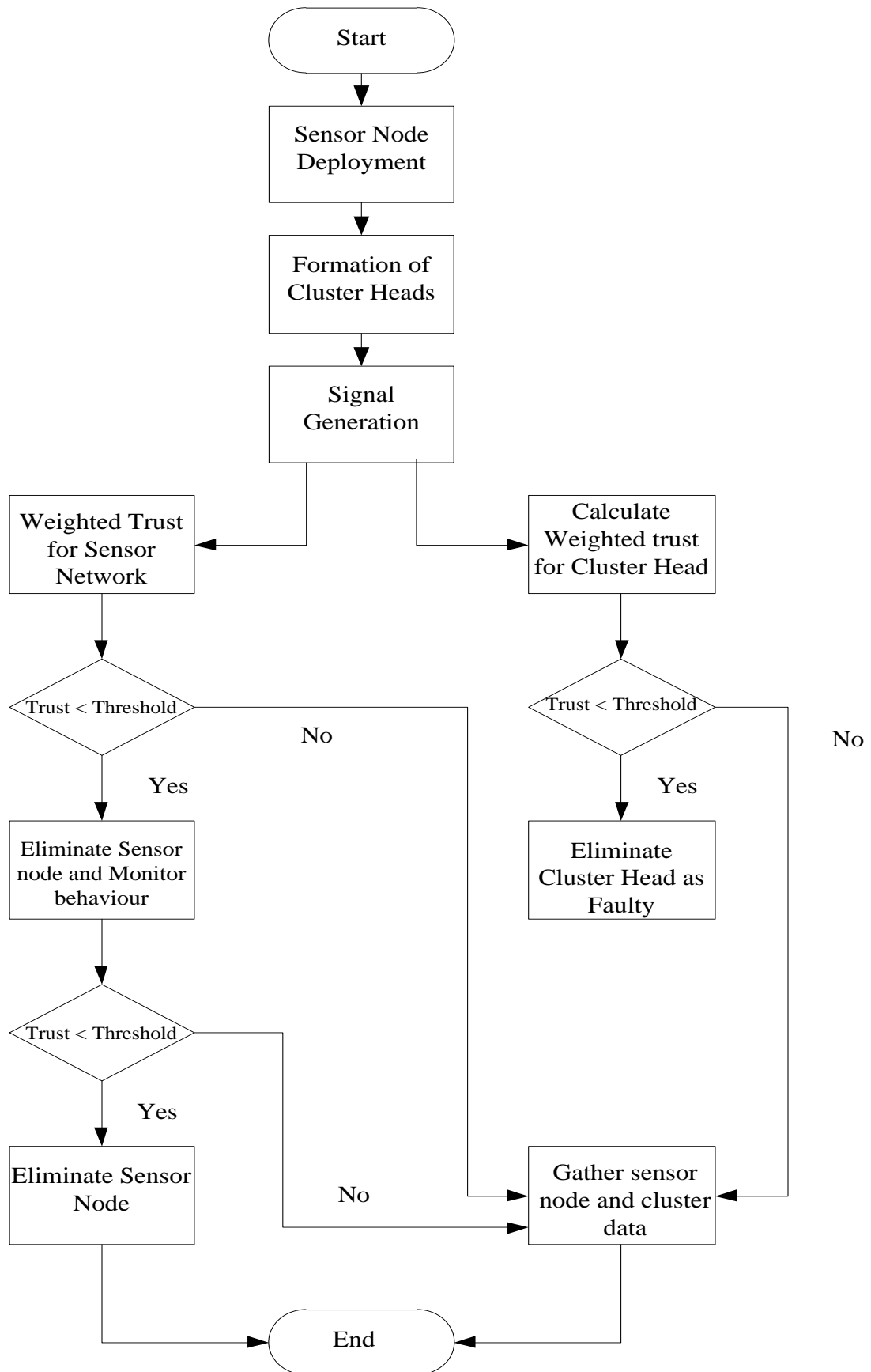


Fig. 4.2: Flowchart for Cluster Based WTE

Table 4.1: Simulation Parameters for CBWTE

Minimum threshold weight	0.7
Number of clusters	4
Number of repetitions of samples	5
Simulation Area	100x100 m ²
Sensor Nodes in field	100
Weight Penalty Factor	20%
Malicious nodes at deployment	20%

Random Deployment of Sensor Nodes

100 SN are spread randomly in the area with a dimension of [100x100 m²], the simulation is as shown in Fig. 4.3. Simulation are done in MATLAB

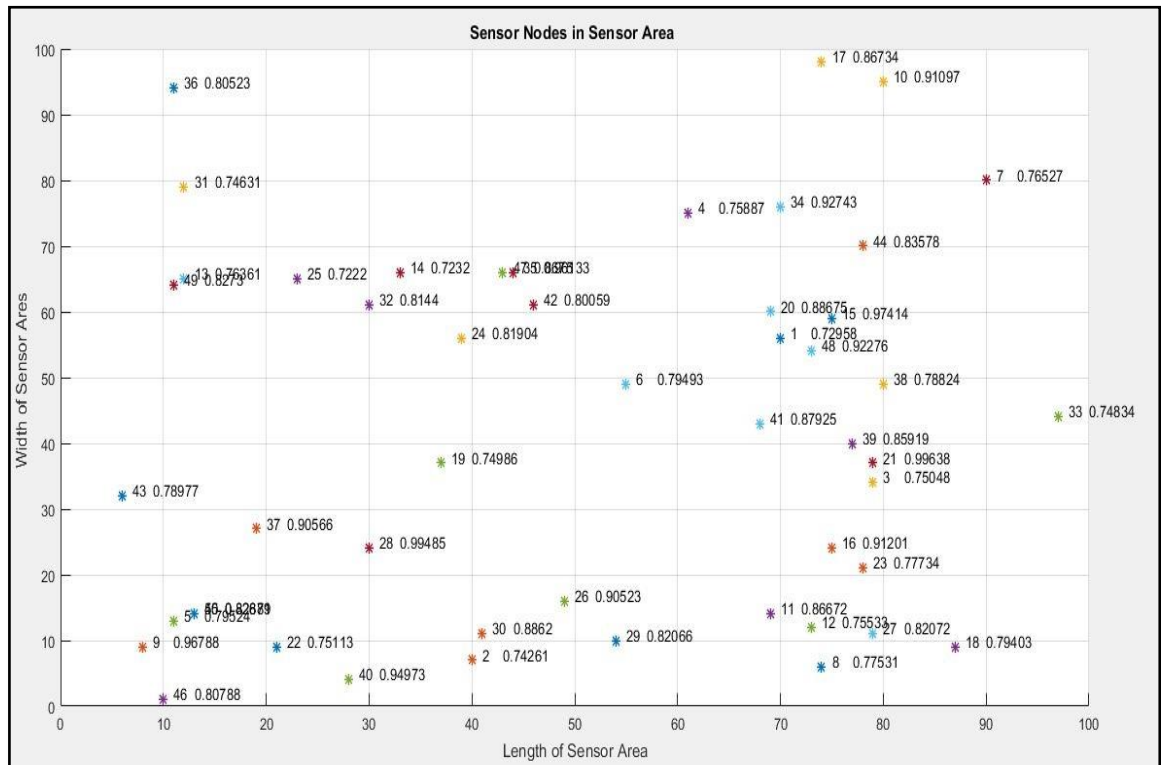


Fig. 4.3: Random deployment of SN in an area

Cluster Based Deployment

The sensors are grouped in clusters and the weighted trust evaluation algorithm performs over it. As shown in Fig. 4.4, the malicious nodes are displayed in respective clusters.

Performance Parameters

The performance parameters of Random Deployment and Cluster-Based WTE Deployment of SN may be measured in terms of:

- (i) Detection Time
- (ii) Detection Ratio

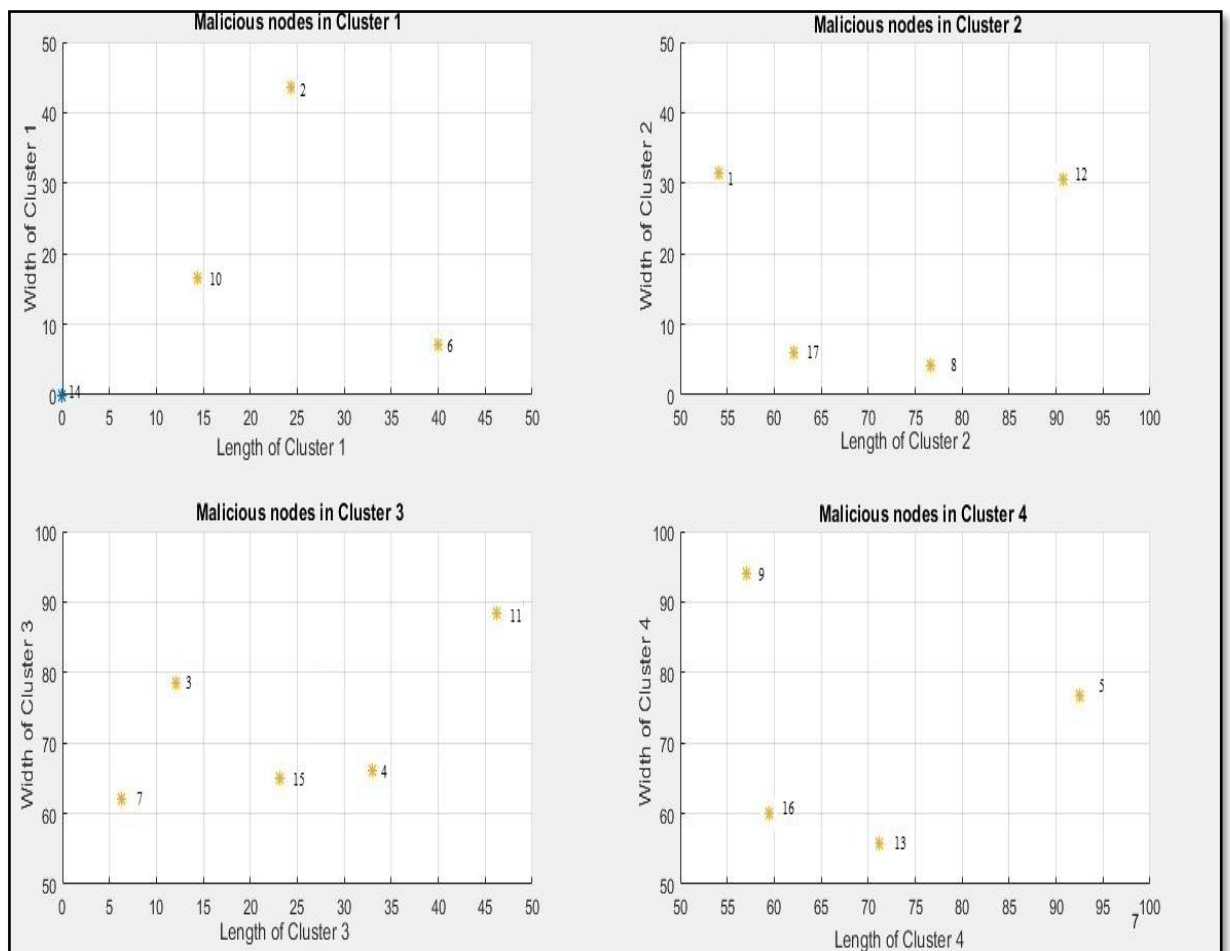


Fig. 4.4: CBWTE deployment of SN in an area

Detection Time

This process of deployment is repeated five times and detection time for Random and Cluster-Based Deployment are presented in Fig. 4.5 and 4.6, respectively. The detection time is observed to be more in Random Deployment and then Cluster Based Deployment.

Detection Ratio

Detection Ratio (DR) refers to the ratio of malicious nodes (MN) that are correctly detected to the total number of malicious sensor nodes (m) present in the clustered network (set at the time of deployment). Let, the percentage of malicious nodes (MN) at time of deployment, is set to 20% i.e. $=0.2$.

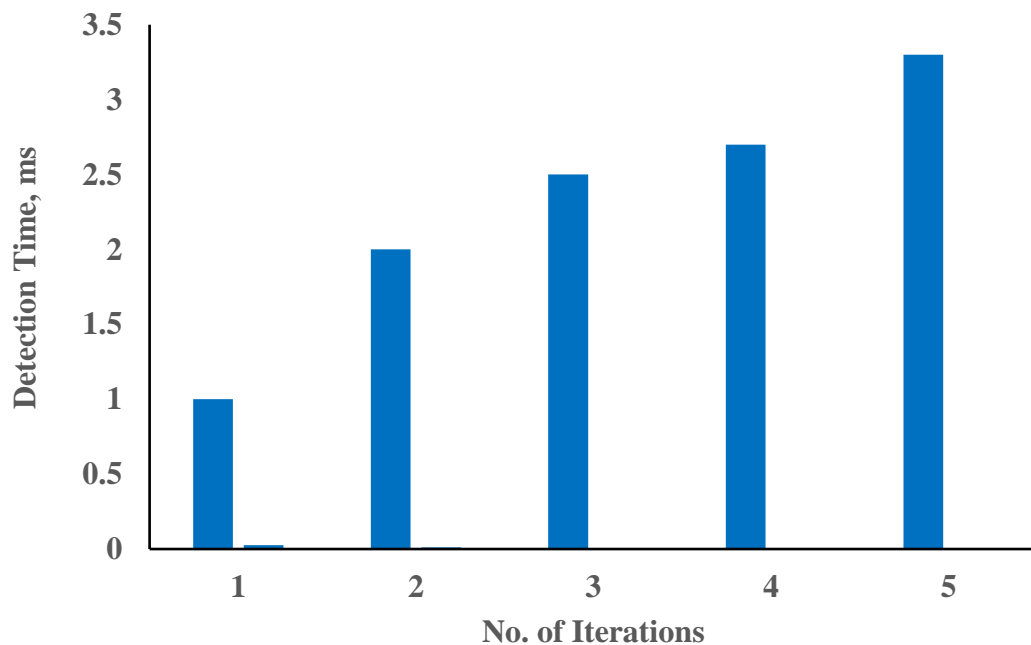


Fig. 4.5: Detection time for random deployment

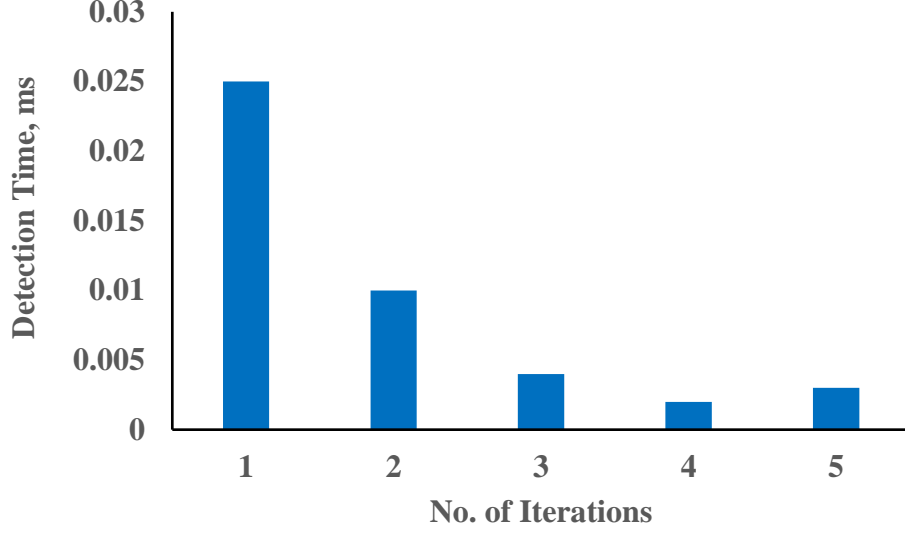


Fig. 4.6: Detection time for Cluster Based deployment

This implies that:

$$MN = m * n \quad \dots (4.6)$$

where, n is total the number of deployed SNs. Assume $n = 100$

Thus, $MN = 0.2 * 100 = 20$

Suppose, cluster head (CH) is also malicious (M_CH).

$$M_CH = m * (p * n) \quad \dots (4.7)$$

where, p is the percentage of CH in the network, we consider here 4 cluster segments and each segment has one CH. i.e.

$$p = \frac{\text{Number of CH}}{100} = 0.04$$

Assume that 20 per cent of CH are malicious, so number of malicious CH is given by

$$M_CH = 0.2 * (0.04 * 100)$$

which results in 0.8 thus near to 1. Thus, it is safe to assume that 1 CH faulty. Table 4.2 shows the DR while increasing the number of malicious nodes.

Table 4.2: Results of CBWTE method for Detection Ratio *vs* nodes

Parameters	Total Malicious Nodes (At deployment) out of 100			
	20	40	60	80
Detected Malicious Nodes (Simulation) including CH	18	33	38	29
Detection Ratio (DR)	0.9	0.83	0.63	0.36

The number malicious nodes can be calculated as

$$m * (n - (p * n)) \quad \dots (4.8)$$

$$\text{i.e., } 0.2 * (100 - (0.04 * 100)) = 19.2$$

The number of detected malicious node is 17 out of the 19 (through simulation) that had been set as malicious whereas, all the malicious cluster heads are detected by the method.

$$Detection\ Ratio(DR) = \frac{Number\ of\ correctly\ detected\ MN}{Total\ Number\ of\ MN} \quad \dots (4.9)$$

$$\text{i.e. } DR = \frac{17+1}{20} = 0.90$$

Detection Ratio w.r.t Number of Malicious nodes

The graph between Malicious Nodes and Detection Ratio for cluster-based deployment is shown in Fig. 4.7. An inverse relation between the detection ratio and malicious nodes were observed from the Fig. 4.7 i.e. detection ratio decreases with the increase in number of malicious nodes.

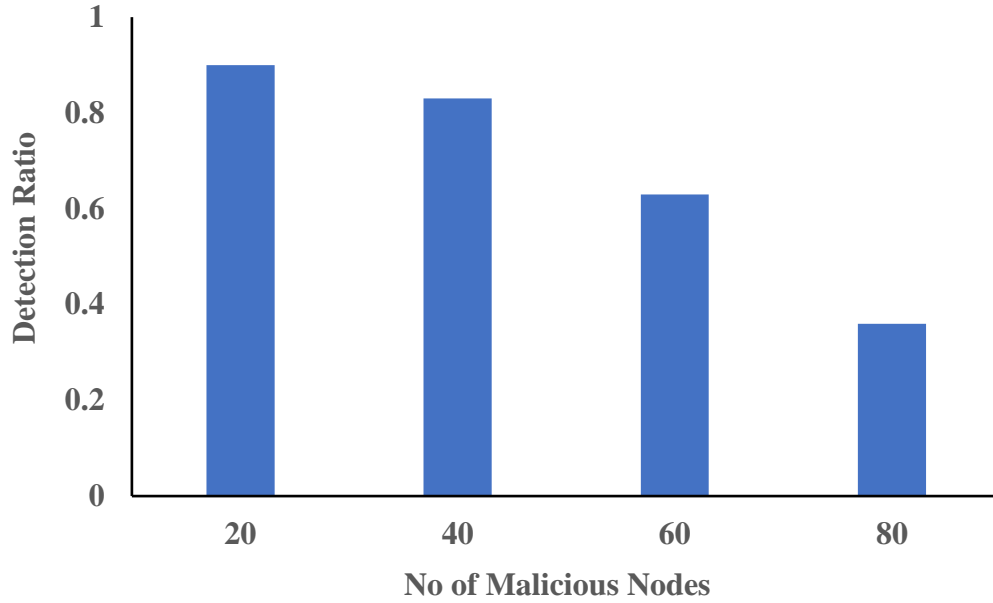


Fig. 4.7: Detection Ratio vs Malicious Nodes (CBWTE Method)

4.3 Malicious Node Detection in WSN Using Support Vector Machine: (A Machine Learning Approach)

So far, lot of research work have been done for detection of malicious nodes in WSN. The main challenges in detection of malicious nodes, using machine learning techniques are:

- i) achieve dead line of real time applications
- ii) larger data points
- iii) classification complexity and multidimensionality of feature space.

In this section, we propose SVM based detection of malicious node. There are two main reasons for using SVM, one is speed and the other is scalability [111]. It can learn a larger set of patterns as compared to neural network. It does not depend on number of data points and the classification complexity. It also does not depend on the dimensionality of the feature space. With this motivation, we use SVM to detect the malicious node from

the data gathered by neighbouring nodes. Hence, the Malicious Node Detection Strategy is proposed to address the above challenges.

4.3.1 Malicious Node Detection Strategy

For efficient detection of malicious nodes, we chose a topology having following characteristics.

- a) In case of a static sensor network, each SN should be empowered for self-localisation [12], no matter whether they are installed physically or through aerial scattering. After these SN are deployed in the field, a one-time authentication procedure is adopted for ensuring the same.
- b) These SNs are equivalent to the current generation SN, e.g. the Berkeley MICA2 motes in respect to memory, communication and computation facilities.
- c) We assume that the base station is safe and will not undergo any attacks.

A regression based SVM is proposed for malicious node detection and prediction of a SN for protecting it from adverse effects.

Methodology

The working of proposed model using a binary classification problem is illustrated in [112]-[115], [117]. The aim of SVM is to determine a decision boundary that maximises the margin between different classes. For solving a classification problem, the approach is to find a hyperplane which can separate data linearly with minimum error. The SVM then attempts to align the decision boundary in such a manner that maximises the separation between the boundary and the closest data point in each class. Fig.4.8. The concept of maximal margin is used to attain better classification of new data (generalization). The hyperplanes are defined by the vectors which are known as

the support vectors. Once the support vectors are selected, the rest of the data can be discarded. Thus, SVM uses the strategy of keeping the error fixed and minimizing the confidence interval. Its aims in finding the optimal hyperplane that separates data of classes and use for many machine learning tasks as pattern recognition, object classifications and time serise prediction, regression analysis.

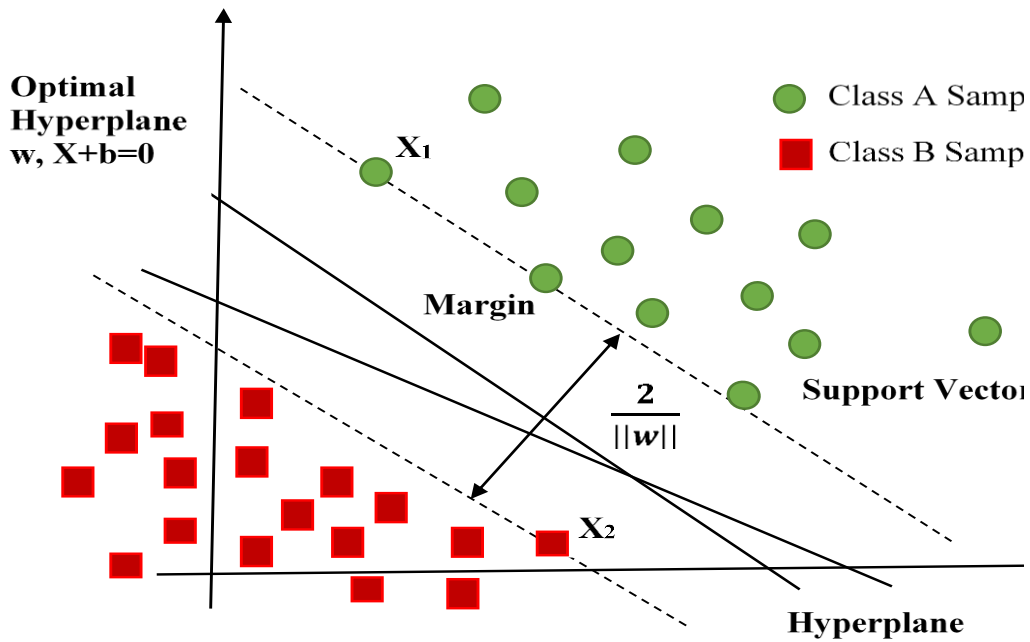


Fig. 4.8: Support Vector with Maximal Margin

The principle of this technique consists in defining a decision function

$$f : X \rightarrow \{-1, 1\}$$

while having sample set of data

$$\{(x_i, y_i); x_i \in X \text{ and } y_i \in \{-1, 1\}\} \quad \dots (4.10)$$

For each new point, $x \in X$, this decision function allows to predict its belonging to the right class (-1 or $+1$). At initial stages, tested only for binary classification of data later on the implementation are proposed and then it got tested for classification of problems that includes many levels of classes as an extension.

Suppose, there is dataset of two classes of samples, in which each sample is denoted by x_i with the corresponding class label y_i ; i.e.,

$$x_i \in R^n, \quad y_i \in \{-1, 1\}, \quad i = 1, 2, 3, \dots, N \quad \dots(4.11)$$

Here, x_i is a n-dimensional vector with corresponding y_i equal to 1 if it belongs to a positive class or -1 for negative. Let the binary classification data points be

$$D = \{(x^1, y^1), \dots, (x^l, y^l)\}, \quad x \in R^n, y \in \{-1, 1\} \quad \dots(4.12)$$

where, y is a binary value representing the two classes, x is input vector and l = the number of training sets.

As explained already, there are a number of hyperplanes that can separate these two set of data and the problem is to find out the one with the largest margin. The support vector classifiers are based on the class of hyperplanes (boundary line),

$$(w \cdot x) + b = 0, \quad w \in R^n, b \in R, \quad \dots(4.13)$$

where, w = the boundary, x = the input vector, and b = the scalar threshold.

To remove redundancy, the hyperplane is considered in canonical form and is defined by a unique pair of values (w, b) at the margins satisfying the conditions:

$$(w \cdot x) + b = 1, \quad \dots (4.14)$$

$$(w \cdot x) + b = -1, \quad \dots (4.15)$$

The quantities w and b will be scaled for this to be true, and therefore the support vectors correspond to the extremities of the data. Thus, the decision function that can be used to classify the data is:

$$y = \text{sign}((w \cdot x) + b). \quad \dots (4.16)$$

Thus, a separate hyperplane in canonical form must satisfy the following constraints [114]:

$$y_i[(w \cdot x_i) + b] \geq 1, \quad i = 1, \dots, l. \quad \dots (4.17)$$

There can be many possible hyperplanes that can separate the training data into the two classes. However, the optimal separating hyperplane is the unique one that not only separates the data without error but also maximizes the margin. This means that it should maximize the distance between the closest vectors in both classes to the hyperplane. This margin (ρ) is the sum of the absolute distance between the hyperplane and the closest training data points in each class.

This distance $d(w, b; x)$ of a point x from the hyperplane (w, b) [115] is:

$$d(w, b; x) = \frac{|(w \cdot x_i) + b|}{||w||}. \quad \dots (4.18)$$

Thus, the sum of the absolute distance between the hyperplane and the closest training data points in each class i & j and the ρ is calculated as given in (4.19).

$$\rho = \min \frac{|(w \cdot x_i) + b|}{||w||} + \min \frac{|(w \cdot x_j) + b|}{||w||} = \frac{2}{||w||} \quad \dots (4.19)$$

The optimal hyperplane, with the maximal margin of separation between the two classes can be uniquely constructed by solving a constrained quadratic optimization whose solution is in terms of a subset of training patterns that lie on the margin. The solution of convex optimization problem using Lagrange multipliers [115].

$$\left. \begin{aligned} \max L(\alpha) &= \sum \alpha_i - \frac{1}{2} \sum_{j=1}^n \sum_i^n \alpha_i \alpha_j y_i y_j K(x_i x_j) \\ \text{Subject to } \sum_i^n \alpha_i y_i &= 0 \text{ and } 0 \leq \alpha_i \leq C \quad \forall \quad 1 \leq i \leq n \end{aligned} \right\} \quad \dots (4.20)$$

where α_i is the Lagrange multiplier, $K(x_i x_j)$ denotes the kernel function (e.g., linear, polynomial, radial basis). The trade-off marginal maximization and error minimization denoted by the constant C [114]. In the proposed model, Support Vector Classification has been used to obtain the prediction speed by using Radial Basis Kernel

function. The desired values have been obtained by means of trial and error method. For carrying out this research work, the SVM toolbox for MATLAB has been used. The results would be calculated by solving (4.20).

$$w_{\alpha} = \sum_{i=1}^n \alpha_i y_i x_i \quad \dots (4.21)$$

Finally, the decision function is given by:

$$f(x, a, b) = \{\mp 1\} = \text{sign}(\sum_{i=1}^n y_i \alpha_i K(x_i x_j) + b) \quad \dots (4.22)$$

The SVM constructs a decision boundary by extracting the support vectors that lie nearest to the class boundary. In this way, optimal separations of data pertaining to different classes is achieved. SVM employs a linear separating hyperplane in order to create a classifier with a maximal margin. After the completion of this step, the SVM obtains an optimal hyperplane that is linear for the given features space [115] [116].

SVM transform the data into a high-dimensional feature space by employing a non-linear mapping. The process flow block diagram illustrated in Fig. 4.9.

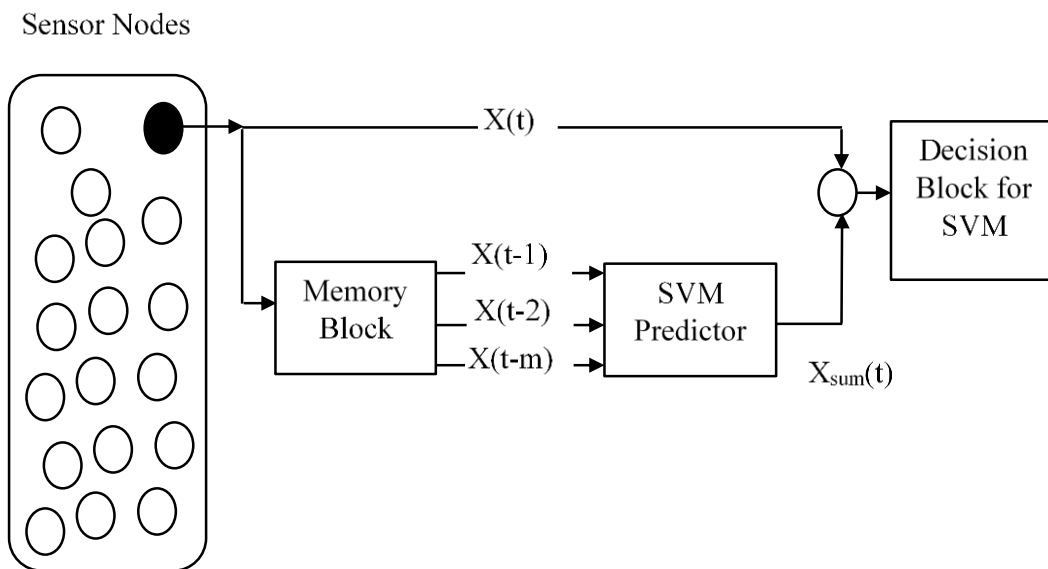


Fig. 4.9: Block diagram of the process of SVM

Flow Chart: The basic flow chart of the algorithm is shown in Fig. 4.10 and the steps are briefly described below:

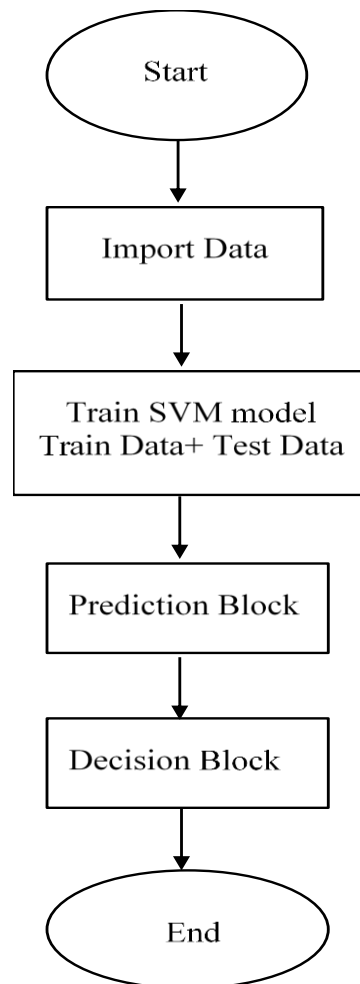


Fig. 4.10: Flow chart for SVM

Step 1: Node Data for various instances is imported for further processing through a MATLAB script.

Step 2: Training of SVM modes constitute two parts, first is used as training data and other is to test data. Training data is randomized 80 % of the total data that would be fed into the predictor block to predict the remaining 20% test data.

Step 3: The Prediction Block predicts the value for 20% test data and forwards the predicted value to the decision block.

Step 4: Decision block calculates the difference between actual and predicted values.

If the deviation of predicted value from the actual value is more than a certain point then the node is termed as malicious node.

4.3.2 Simulation Results

The labelled dataset used in this work is taken from [117], [118] which provide a WSN dataset collected from a simple single-hop and a multi-hop WSN deployment using Telos B motes. The data consists of humidity and temperature measurements collected during 6-hour period at intervals of 5 seconds. Label '0' denotes normal data and label '1' denotes an introduced event. In this case steam from hot water is introduced to increase the humidity and temperature.

The detection algorithm using SVM was implemented during simulation for monitoring SNs. The simulation parameters used in the proposed model is presented in Table 4.3.

Table 4.3: Simulation Parameters for SVM

Parameters	Values
Training Data	80% of Input Data
Test Data	20% of Input Data
Kernal Function	Radial Basis Function (RBF)
Mu	46.6506
Sigma	4.3995

The above mentioned field parameters are used in the simulation of SVM evaluation. We have used multi-hop data for simulation. The 80% of multi-hop data is used for training and remaining 20% data for test. Randomly 80% data goes into training and remaining data is used for prediction with every execution.

i) Error Detection and Prediction

The model was run for five iterations of sample data. A comprehensive result of simulation with SVM method in terms of Predicted label and True label of data and their comparison are presented in Fig. 4.11.

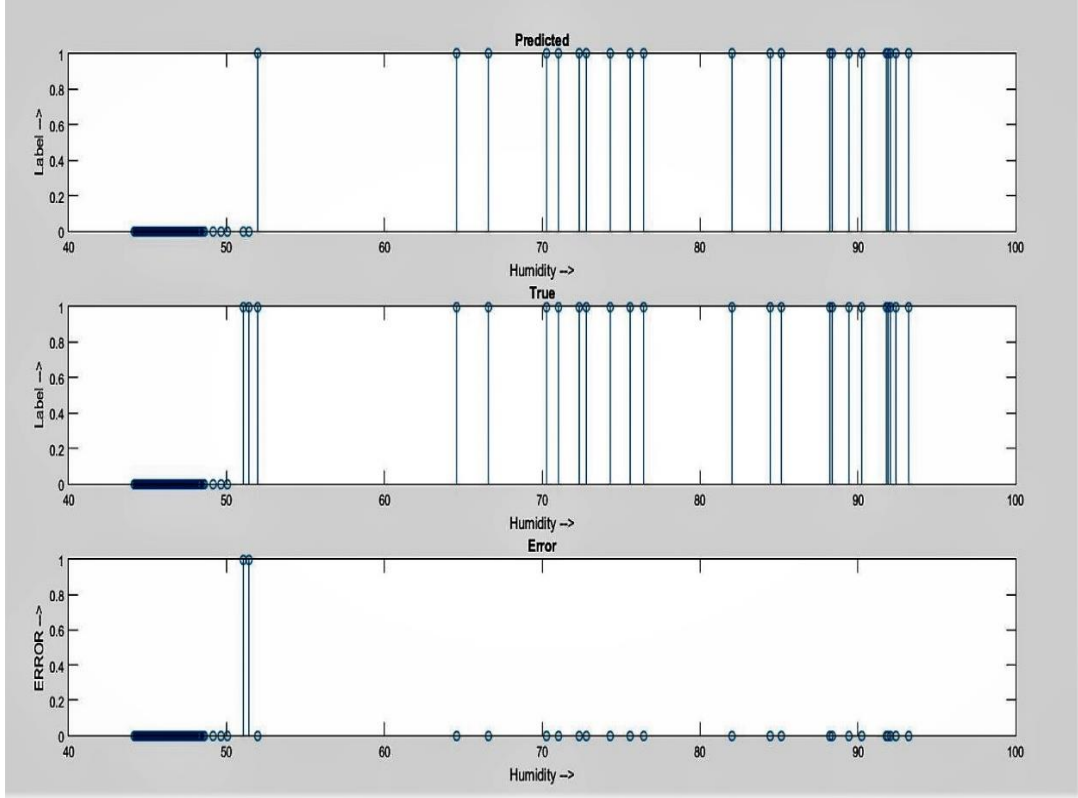


Fig. 4.11: Simulation of SVM model for Predicted label and True label of data and Error Detection

In Predicted and True graph, the Label '0' represents "True Reading" whereas Label '1' represents "Malicious Reading". However, in ERROR graph '0' represents "No Error" and '1' represents "Error" in prediction. A plot of error instances detected when original data (with noise) is compared with the predicted data in Fig. 4.12.

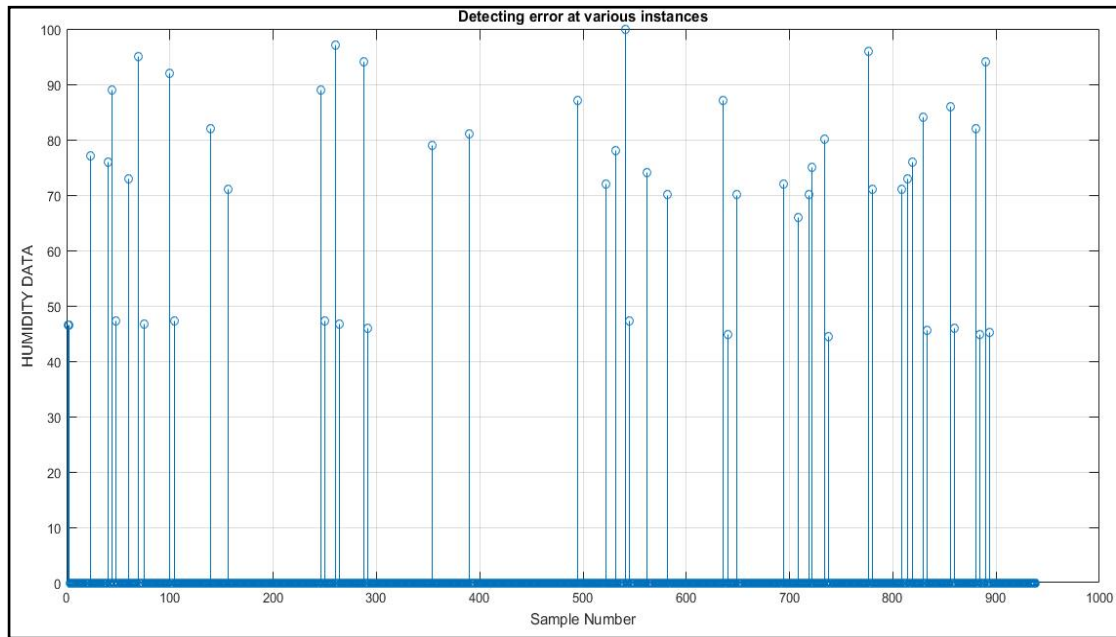


Fig. 4.12: Detecting Error Instances by Comparing Original (with noise) and Predicted Signal

(ii) Performance Parameters

To get better overview of the result, five iterations of test data are analyzed for each performance parameter. The performance parameters that observed in the study are: Prediction Time, Detection Ratio, Misdetection Ratio and Accuracy.

Prediction Time

Prediction time of the data is calculated on the basis of five iterations of sample data that have additional noise induced at 70 random instances in test data. Prediction Time is the time taken by the code to calculate the predicted value at all instances shown in Fig. 4.13.

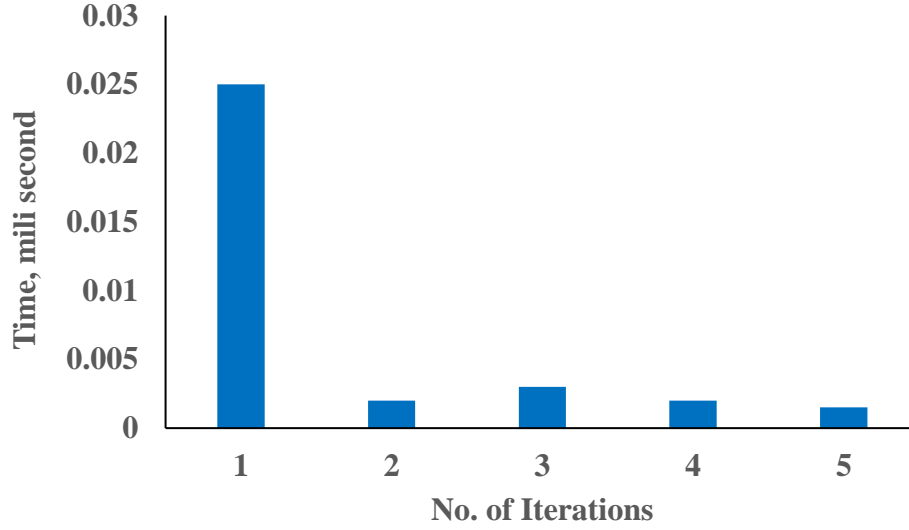


Fig. 4.13: Prediction time for SVM

Detection Ratio (DR)

Detection Ratio (DR) is defined as the number of faulty instances predicted out of total number of faulty instances. The expression of DR is given as follows:

$$DR = \frac{\text{Malicious instances predicted}}{\text{Total number of malicious instances}} \quad \dots(4.23)$$

Detection ratio is calculated in samples with five iteration. It is observed from the Fig. 4.14 that when there was no noise induced the detection ratio was almost 100% since the number of faulty instances were very less.

Misdection Ratio

Misdection Ratio (MDR) is defined as the ratio of number of malicious instances prediction failures to the total number of malicious instances. The expression of MDR is given as follows:

$$MDR = \frac{\text{Malicious instances prediction failures}}{\text{Total number of malicious instances}} \quad \dots(4.24)$$

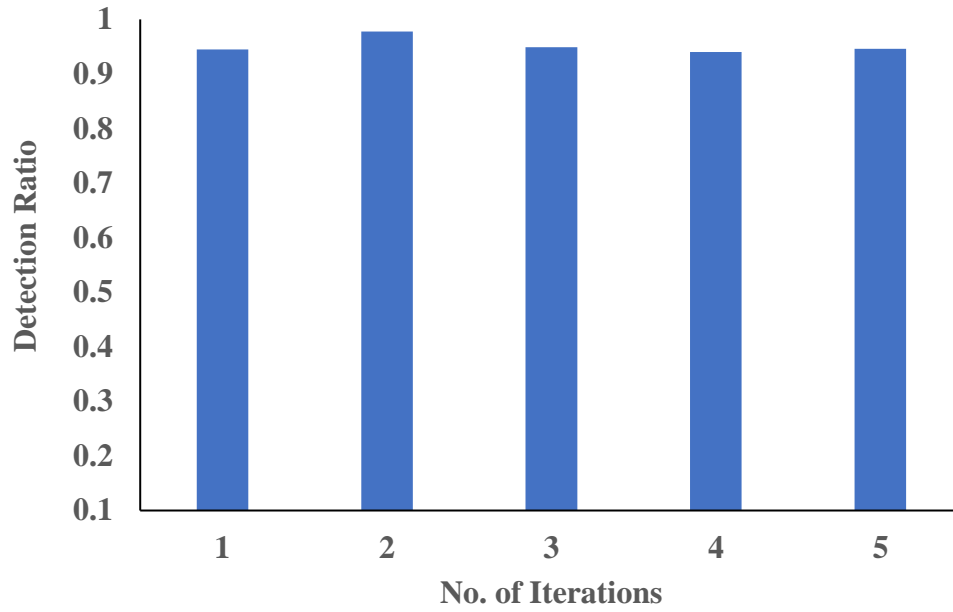


Fig. 4.14: Detection ratio for SVM

Five iteration of data were carried out for determination of misdetection ratio and the same is presented in Fig. 4.15.

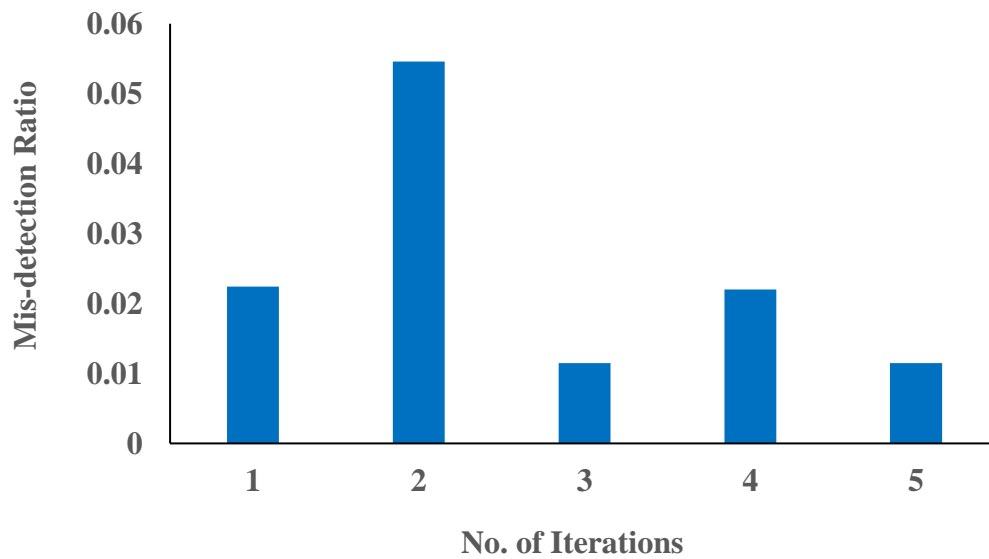


Fig. 4.15: Mis-detection ratio for SVM

(i) Accuracy

The accuracy of the malicious instances was analysed and is presented in Fig.4.16.

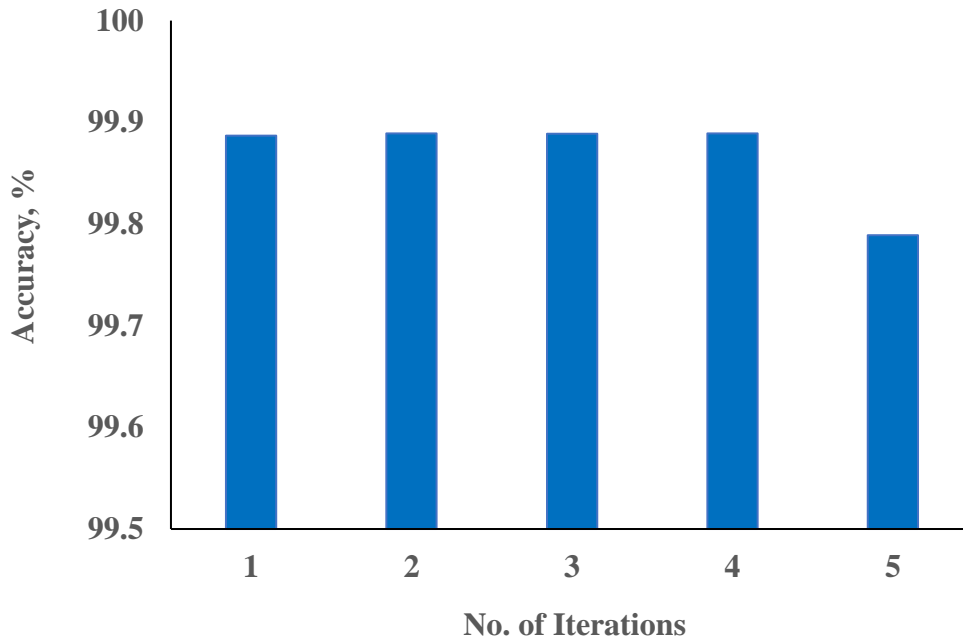


Fig. 4.16: Accuracy for SVM

The samples were iterated five times to calculate the accuracy of data. The average accuracy of five iterations is observed to be = 99.87%.

4.3.3 Comparison of SVM and AR for Performance Parameters

The Algorithm has been implemented and scripted in MATLAB. The simulations were carried out to achieve performance parameters like Prediction Time, Detection Ratio and Accuracy. The results obtained in section of 4.2 and 4.3 are compared with method Auto Regression. The results are presented in Fig. 4.17 to 4.19.

Detection Ratio between AR and SVM.

In SVM and Auto Regression prediction, the relative graph of detection ratio between AR and SVM prediction is developed and shown in Fig. 4.17.

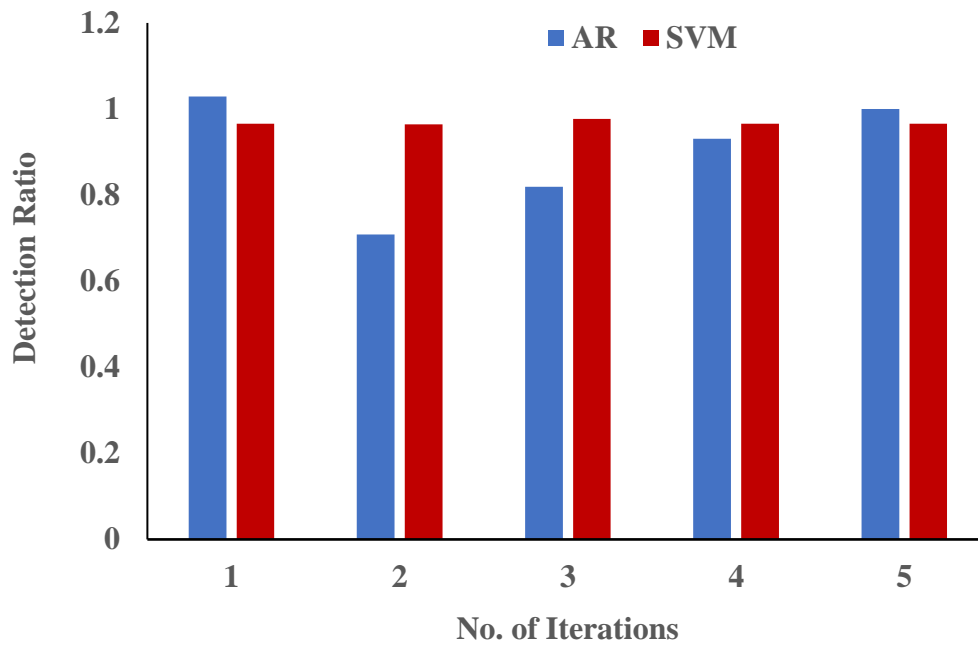


Fig. 4.17: Detection Ratio of AR and SVM prediction

The code was run for five iterations as shown in the above Fig. 4.17. It is interesting to note that the DR in case of AR prediction is observed to be more than '1', normally detection ratio cannot be greater than '1'. This happens because addition of noise in system makes prediction even more unstable and due to induced erroneous instances, the total number of unpredicted instanced become more than they should be, so the linear AR predictor predicts more number of erroneous instances that were actually there, thus making DR more than unity. Thus, SVM is better in detecting erroneous instances than AR predictor and it provide more uniform results.

Accuracy and RMS Accuracy of Prediction between SVM and AR

Accuracy and Root Mean Square (RMS) accuracy of prediction was obtained by five iterations of codes and are shown in Fig. 4.18 and Fig. 4.19, respectively.

It is clear from the Fig. 4.18 and 4.19 that SVM method proved to be better for Prediction of malicious instances since, the value of RMS accuracy of prediction is 99.57%. However, in case of AR prediction, the RMS accuracy is 93.31%, though it itself is a

good value. While comparing SVM and AR prediction, the AR lags behind in terms of accuracy.

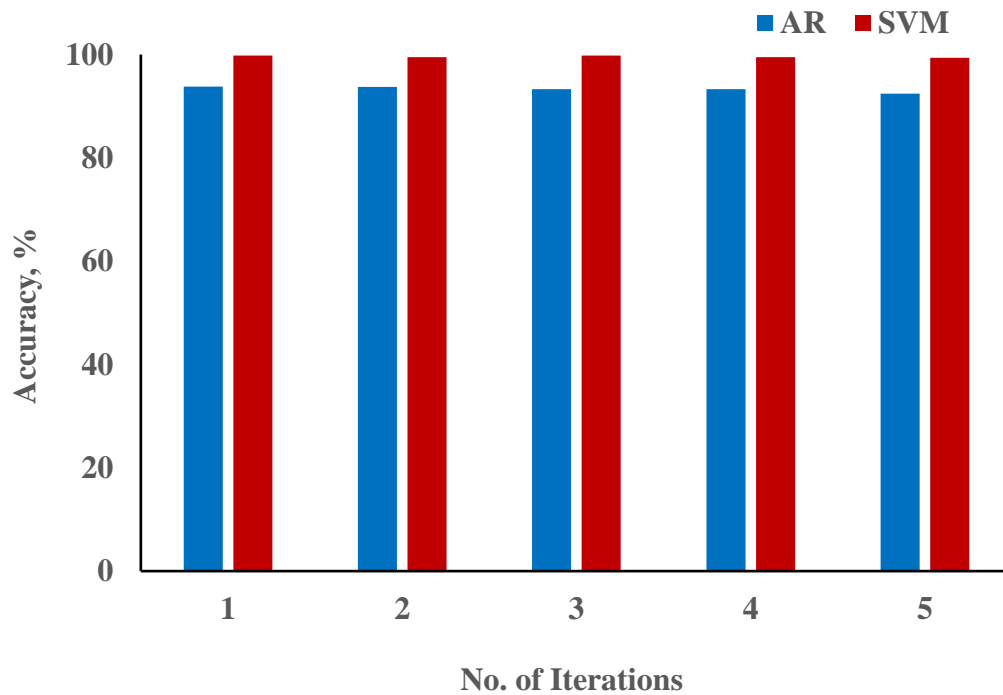


Fig. 4.18: Accuracy for AR and SVM Prediction

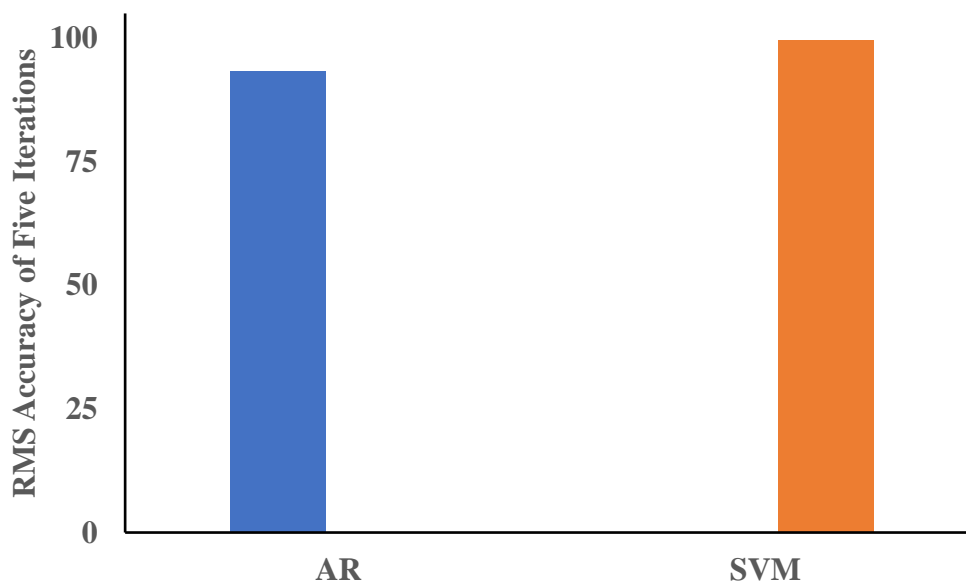


Fig. 4.19: RMS Accuracy for AR and SVM Prediction

The low implementation cost makes CBWTE an ideal choice for monitoring of the agricultural activities, environmental monitoring etc. This method can be used in

different fields/ares where high detection ratio or accuracy is not required. The CBWTE method is easier to implement since sensor nodes are randomly deployed over the field. The prediction time is least for SVM method with high detection ratio and accuracy. Though, the introduction of Prediction and Decision blocks in algorithm makes it slightly costly but it is good for industrial monitoring, defense monitoring, medical monitoring, where the accuracy is most important with negligible lag. The example of industrial monitoring, immediate detection and prediction without any delay for leakage of any toxic gas in any organization.

Also, unlike AR prediction, there is no trade of between prediction time and accuracy in SVM and both the parameters achievable at same time, so SVM is a better option where accuracy and prediction time both are must.

4.4 Extended Kalman Filtering (EKF) Technique to Detect Byzantine Attack in a WSN

Detection and isolation of malicious or malfunctioning nodes in border surveillance is a major security issue. It is crucial that these nodes be detected and excluded in the sensor network to avoid catastrophic decision being made as a result of falsified information injected by the adversary as well as prevent an array of attacks that can emanate from malicious nodes. Some of the attacks that can emanate from malicious nodes include sinkhole attacks, black hole attack, wormhole attack, Sybil attack, HELLO flooding attacks, Denial-of-Service attacks and Byzantine attack [119]. These necessitate that their detection and isolation be given top priority as malicious nodes can send erroneous or falsified report (Byzantine attack) to the base station leading to a

disastrous decision; such as, in a surveillance WSN a misleading report about the enemy operations may result to extra casualties.

4.4.1 Byzantine Attack Detection Strategy

Byzantine attack is one of the insider attacks in mobile *ad hoc* network. Compared to other attacks it is difficult to predict. These are more hazardous than outsider attack and it is too difficult to trace and mitigate such attacks as they are active members of the network. These attacks are also known as byzantine attacks. Once the active set of insider nodes in the network will get corrupted by the attacker the whole network will be controlled by the attacker and further secured data transmission become impossible [120]. This is very dangerous in case of mobile devices used in medical application for transferring patient reports. A Byzantine attack can prevent the route establishment by dropping the route request or response packets. In this attack a single node or group of nodes acts together to generate loops, forward packets through arbitrary paths or drop the packets selectively resulting in disrupt or deteriorate the routing services and network performance.[121], [122].

In order to assure a high grade of efficiency for our malicious node detection strategy we chose a topology for the sensor network having the following attributes:

- Assume the sensor network to be static with each SN having knowledge of its own location.
- All SNs have similar properties like computational and communication capabilities and power resources, e.g. the Berkeley MICA2 motes. Every node has its own storage capability to perform communication with others of the network.
- The base station, sometimes called access point, acting as a controller and as a key server, is assumed as a laptop class and having infinite power. Further, also assume

that the base station will not be compromised.

The measured values provided by each sensor present a strong deterministic component rather than a truly random (stochastic) one (e.g. wind speed or temperature measurements in different locations). In this case there exists a correlation between past values and the current one.

So, to overcome the SNs from getting trapped by the adversary/attackers, a strategy to handle Byzantine attack in sensor network is proposed. It is based on Extended Kalman Filter (EKF) technique weighted moving average technique and seasonality factor. Theoretical estimation for each observation is calculated using three points moving average of past three predictions. We have also considered biasing effects of seasonal variation in data to get a final forecast. The estimated value by proposed algorithm is compare with the actual observed value. If the difference between the estimated value and the actual observed value is very high then the node is malicious and is under Byzantine attack. Then necessary action takes to protect the node.

4.4.2 Extended Kalman Filter (EKF)

The filter is named after R. E. Kalman, one of the primary developers of its theory. The Kalman Filter (KF) has numerous applications in technology. The KF is a widely applied concept in time series analysis used in fields such as signal processing, econometrics, robotic motion planning and control, and they are also sometimes included in trajectory optimization. The KF technique is used when real time processing of data is required and the acquired data contains missing and noisy values. It is a stochastic optimization algorithm which uses an error signal to adjust the transfer function, it is also known as a self-adjusting filter [123]. The KF gives a better prediction of the target's future position by balancing between the measurement and estimated values. It gives more weight to

the components which contains relatively less error and produce a better result than either estimation or measurement can produce. It also estimates the effect of white noise in the results [124]. Ideally, the estimator is quite similar to a quadratic estimation error function. The KF essentially uses two models for determining the state of a dynamic system, namely, observational and dynamic model. In the observational model, the relation between data directly acquired from sensors and the state vector. The dynamic model is essentially a mathematical model of the system and it is used to determine a theoretical estimation of the state vector. The KF uses inputs from the two models to make a time phase update and a state phase update, thereby, adjusting Kalman filter gain and predicting the subsequent state of the dynamic system. The Extended Kalman Filter (EKF) is developed to address the filtering problem in the non-linear systems [125]. The EKF gives an approximation of the optimal estimate. The non-linearities of the system's dynamics are approximated by a linearized version of the non-linear system model around the last state estimate. No of research studies shows the use of KF and EKF techniques in a wide variety of problems such as determining position, angle, temperature, humidity and orientation of the system [126]. The algorithm is recursive, can be run in real time, using only the present input measurements and the previously calculated state and its uncertainty matrix; no additional past information is required.

4.4.3 Time Series Prediction using EKF for Malicious Node Detection and Byzantine Attack

The KF is a self-adjusting filter which utilizes measurement and estimation to predict future values. Linear stochastic difference equation is used to determine the state X_k of the dynamic system [127]. The discrete data linear filtering problem is resolved by the

KF with the help of a recursive solution. Following linear stochastic difference equation governs the state $x \in R^n$ of a discrete-time controlled process:

$$X_k = Ax_{k-1} + Bu_{k-1} + w_{k-1} \quad \dots (4.25)$$

With a measurement i.e., $z \in R^m$

$$Z_k = Hx_k + v_k \quad \dots (4.26)$$

where, Z_k measurement vector, u represent input, random variables, w_{k-1} correspondence to process noise, v_k as measurement noise and A is transition matrix, B represents control matrix and H is measurement matrix.

Let us suppose that random variables are independent, white and with normal probability distribution.

$$P(w) \cong N(0, Q) \quad \dots (4.27a)$$

$$P(v) \cong N(0, R) \quad \dots (4.27b)$$

where Q as process noise covariance and R as measurement noise covariance.

The association between previous time step $k-1$ and current state k is determined by $n \times n$ (square) matrix A in difference (4.25) even without either a driving function or process noise. The relationship between control inputs $u \in R^1$ to state X can be assessed by matrix B , the matrix H ($m \times n$) relates to measurement z_k .

A priori and posteriori error are represented, respectively as

$$P_k^- = E[e_k^- e_k^{-T}] \quad \dots (4.28)$$

$$P_k = E[e_k e_k^T] \quad \dots (4.29)$$

The time update phase functions as a predictor and measurement update phase as a connector.

Moving Average method and Seasonality Factor

In statistics, a moving average is a calculation to analyze data points by creating a series of averages of different subsets of the full data set. It is also called a moving mean or rolling mean and is a type of finite impulse response filter. Its variations include: simple, and cumulative, or weighted forms.

In this case we have used weighted moving average method to calculate the estimate of the quantity in time update equation.

$$\hat{x}_{\bar{k}} = \frac{A\hat{x}_{k-1} + B\hat{x}_{k-2} + C\hat{x}_{k-3}}{(A + B + C)} \quad \dots (4.30)$$

We are taking three previous values to calculate the current value by weighted moving average method. The value of constant parameters A, B and C are data dependent and unique for each dataset.

Seasonal component stands for some periodic fluctuations in data. For example, number of logins in night hours is constantly smaller than in day hours, as well as number of logins in weekdays is larger than on weekends. To take account the seasonality factor and make our prediction better we are modifying the output of Kalman filter. We are multiplying the estimated value by the Kalman filter by average of the ratio of predicted value of the Kalman filter to the measured value given by the sensor. By this, we can take account of the seasonality factor and predict our result more accurately.

$$P_{\bar{k}} = P_k \frac{1}{T} \sum_{j=1}^T \frac{P_j}{z_j} \quad \dots (4.31)$$

where, $P_{\bar{k}}$ represents predicted value, T is period of seasonal variation i.e. number of samples after same variation occurs. We are basically multiplying the

predicted values with a seasonality factor which is, an average of ratios of predicted value to the measured value.

In time update phase equations are given by:

$$\hat{x}_{\bar{k}} = \frac{A\hat{x}_{k-1} + B\hat{x}_{k-2} + C\hat{x}_{k-3}}{(A + B + C)} \quad \dots (4.32)$$

$$P_{\bar{k}} = \frac{A^2\hat{P}_{k-1} + B^2\hat{P}_{k-2} + C^2\hat{P}_{k-3}}{(A^2 + B^2 + C^2)} \quad \dots (4.33)$$

Measurement update phase equations are given by:

$$K_k = P_{\bar{k}}^- H^T (H P_{\bar{k}}^- H^T + R)^{-1} \quad \dots (4.34)$$

$$\hat{x}_k = \hat{x}_{\bar{k}} + K_k(z_k - H\hat{x}_{\bar{k}}) \quad \dots (4.35)$$

$$P_k = (I - K_k H) P_{\bar{k}} \quad \dots (4.36)$$

Once we have obtained prediction results, we treat our prediction for seasonal variation using seasonality factor (4.31).

4.4.4 Working

The working of the scheme is as follows: whenever a node gets compromised by an attacker, it will start behaving unnaturally i.e. it will either transmit no data, false data or send data at irregular intervals. Whenever this occurs, the base node will register this behaviour and the predictions from the KF starts deviating by a large margin from the measured value, this anomaly can easily be detected by taking the difference of measurement w.r.t prediction and hence, malicious behaviour can be detected and reported at the same time.

$$e_k = |P_k - z_k| \quad \dots (4.37)$$

If $e_k > v_{th}$ (malicious behaviour) else, non-malicious, where v_{th} Error threshold.

If the error is greater than the threshold set initially, then that sensor node will be marked as malicious in the database of the WSN base station. It considers the error threshold as $2\sigma_i$, where σ_i is i^{th} standard deviation of seasonality factor.

4.4.5 Simulation Results

The scheme is tested by simulating a network of eight sensors using MATLAB. We have taken Air Quality Data from UCI Machine Learning Repository [118] which is freely accessible in the public domain. The ICA method was applied to the 6394 measurements on hourly averaged concentrations. We picked 168 continuous data points of 8 sensors and modified the data at some points and added false value which corresponds to the Byzantine Attack. Then we performed the simulation and ran our algorithm on the modified dataset. The results are shown in Fig. 4.20 -Fig. 4.25. Then the parameters such as misdetection, correct detection, and undetected points are calculated and the results are summarized below. Here we have shown the performance of our algorithm running on six sensors namely PT08.S1(CO), C6H6(GT), PT08.S2(NMHC), PT08.S3(NO_x), PT08.S4(NO₂) and PT08.S5(O₃).

The data description is as follows:

1. PT08.S1 (tin oxide) hourly averaged sensor response – PT08.S1(CO)
2. True hourly averaged Benzene concentration in microg/m³ – C6H6(GT)
3. PT08.S2 (titania) hourly averaged sensor response– PT08.S2(NMHC)
4. PT08.S3 (tungsten oxide) hourly averaged sensor response – PT08.S3(NO_x)
5. PT08.S4 (tungsten oxide) hourly averaged sensor response – PT08.S4(NO₂)
6. PT08.S5 (indium oxide) hourly averaged sensor response – PT08.S5(O₃)
7. Relative Humidity (%) – RH
8. Absolute Humidity – AH

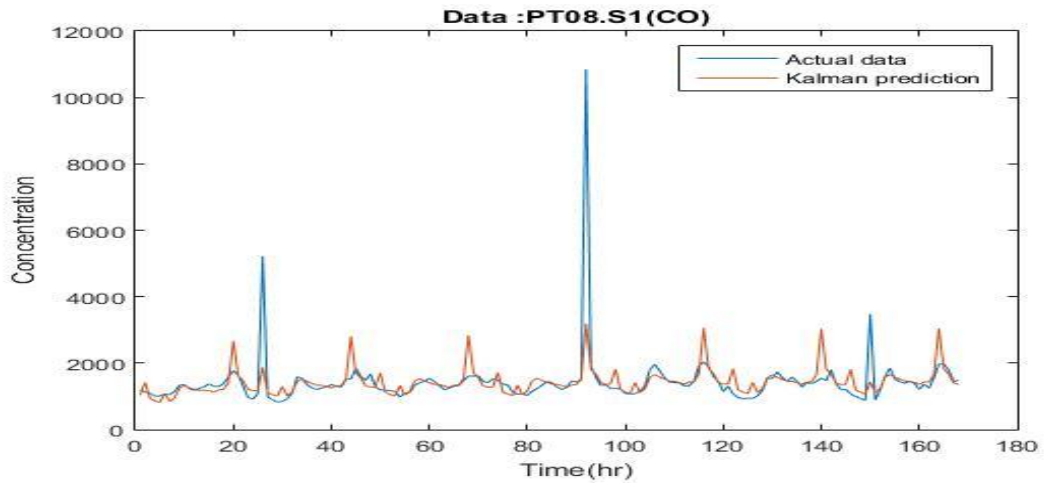


Fig. 4.20: Kalman Filter response for PT08.S1(CO) data sample size 168 data points i.e. 1-week

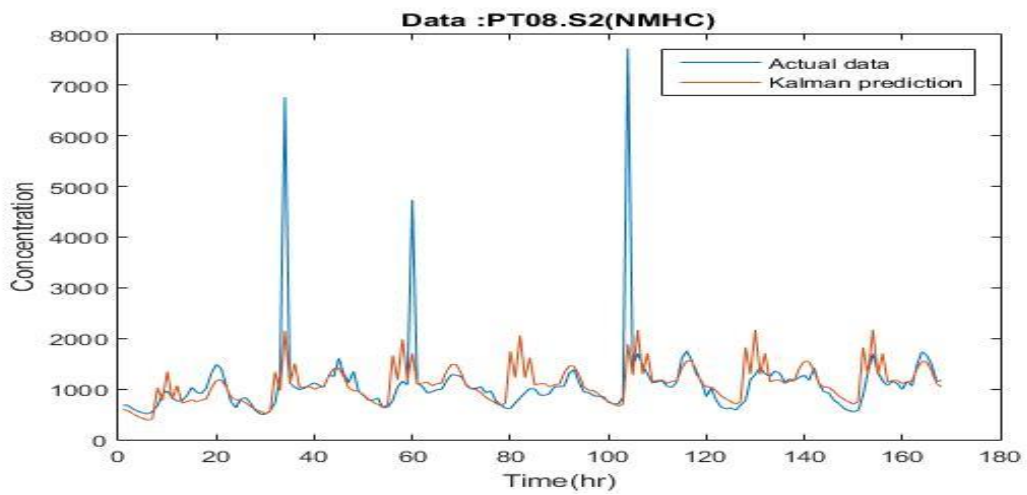


Fig. 4.21: Kalman Filter response for NHMC(GT) data sample size 168 data points i.e. 1-week

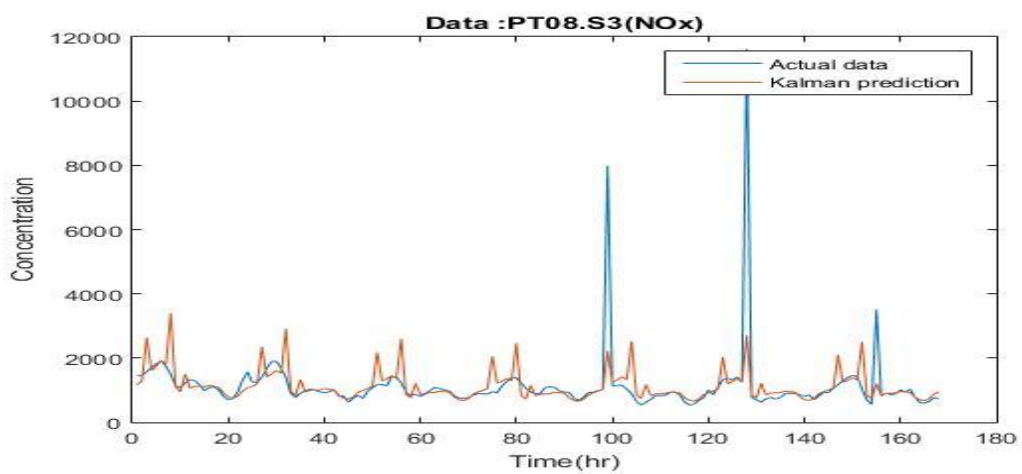


Fig. 4.22: Kalman Filter response for PT08.S2(NMHC) data sample size 168 data points i.e. 1-week

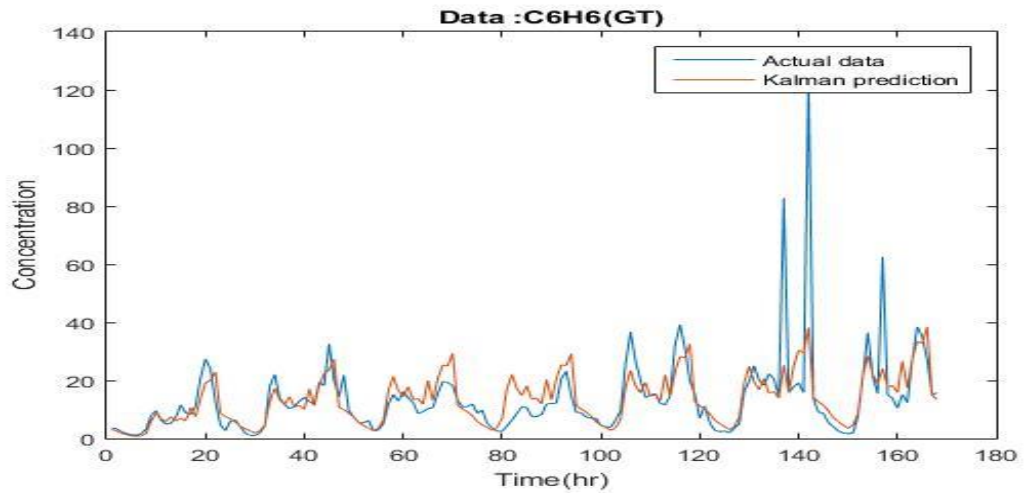


Fig. 4.23: Kalman Filter response for C6H6(GT) data sample size 168 data points i.e. 1-week

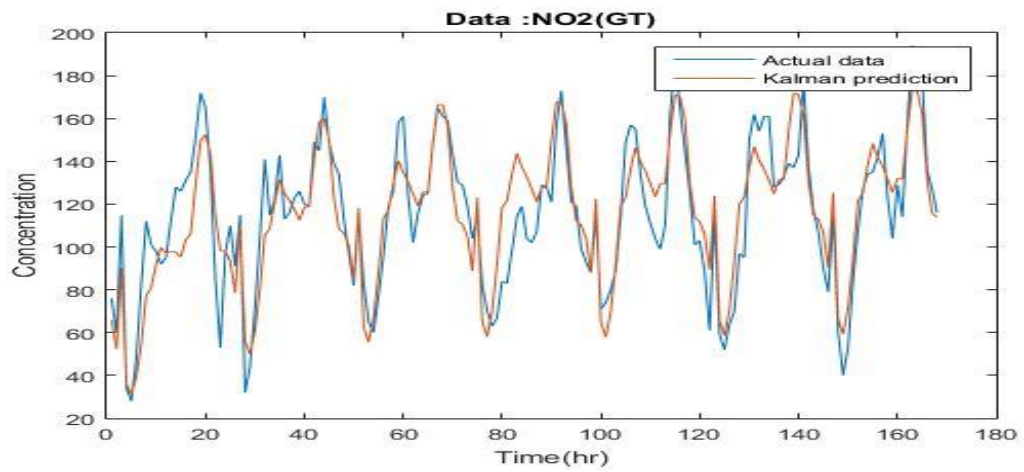


Fig. 4.24: Kalman Filter response for PT08.S4(NO₂) data sample size 168 data points i.e. 1-week

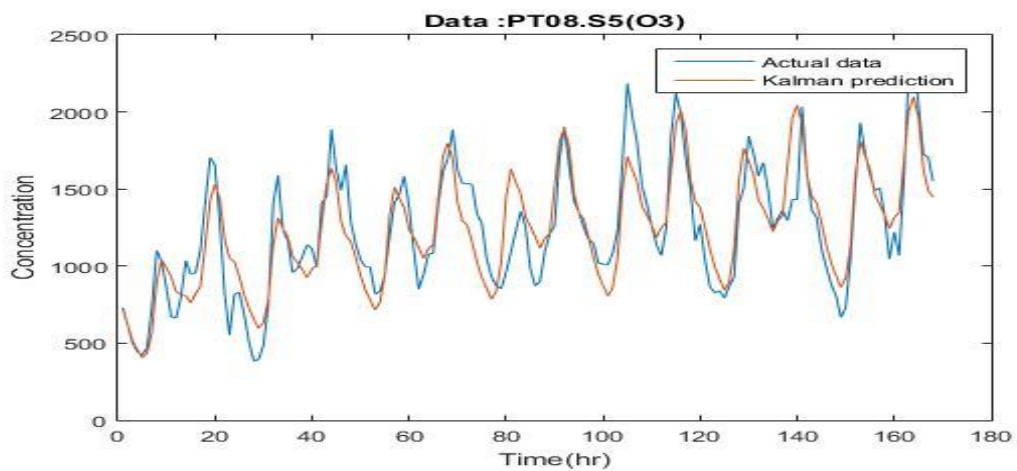


Fig. 4.25: Kalman Filter response for PT08.S3(O₃) data sample size 168 data points i.e. 1-week

The performance analysis of simulation of EKF method results for first 24 data points out of 168 data points (1-week data) are presented in Table 4.4.

The parameters used in Table 4.4 carry the following meanings, AM denotes the number of actual malicious nodes, MD denotes the number of nodes that were detected malicious by the algorithm, CD denotes the number of nodes that were correctly identified as malicious, UD denotes the number of nodes which were, in fact, malicious but goes undetected by our algorithm, MiD represents the number of nodes which were wrongly detected as malicious.

Table 4.4: Performance analysis of simulation results for first 24 data points out of 168 data points

Time (Hours)	AM	MD	CD	UD	MiD
1	1	0	0	1	0
2	0	2	0	0	2
3	0	1	0	0	1
4	0	1	0	0	1
5	0	1	0	0	1
6	0	0	0	0	0
7	0	1	0	0	1
8	0	1	0	0	1
9	1	2	1	0	1
10	0	1	0	0	1
11	0	2	0	0	2
12	0	2	0	0	2
13	0	2	0	0	2
14	0	2	0	0	2
15	0	3	0	0	3

16	0	3	0	0	3
17	0	3	0	0	3
18	0	4	0	0	4
19	0	0	0	0	0
20	0	0	0	0	0
21	0	1	0	0	1
22	1	2	1	0	1
23	0	1	0	0	1
24	0	1	0	0	1

The results found out using EKF with the treatment of prediction results with seasonality factor further enhanced the performance and thus resulted in better tracking of data. Figure 4.26 shows the Detection Accuracy and Misdetection Ratio.

The calculation for Detection Accuracy and Misdetection Ratio is as follows:

$$DDR_j = \frac{1}{N} \sum_{i=1}^N \frac{CD_i}{MD_i} \quad \dots (4.38)$$

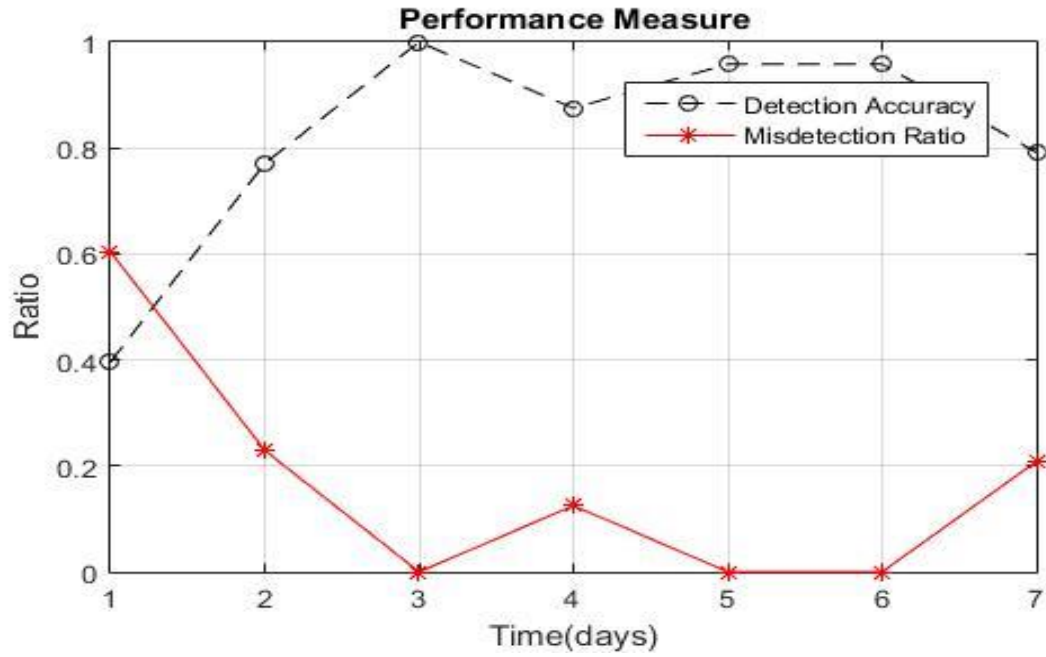


Fig. 4.26: Performance of EKF on 168 data points, distributed over a period of 7 days

$$DMDR_j = \frac{1}{N} \sum_{i=1}^N \frac{MiD_i}{MD_i} \quad \dots (4.39)$$

$$ODR = \frac{1}{M} \sum_{j=1}^M DDR_j \quad \dots (4.40)$$

$$OMDR = \frac{1}{M} \sum_{j=1}^M DMDR_j \quad \dots (4.41)$$

Where, DDR = Daily Detection Ratio, DMDR = Daily Misdetecion Ratio, ODR = Overall Detection Ratio, OMDR = Overall Misdetecion Ratio, N = No. of samples in a day, M = No. of Days.

Table 4.5: Performance Measure for EKF

Performance Measures	Ratio
Detection Accuracy	0.8333
Misdetecion Ratio	0.1667

4.5.6 Conclusion

The simulation results of proposed scheme show that the malicious nodes were detected successfully with high detection ratio and low misdetection ratio. The scheme gives an accuracy of 83.33% and misdetection ratio 16.67% over 168 data points. The EKF technique utilizes a weighted moving average to update estimation and estimation error, thereafter uses seasonality factor to improve the prediction. The scheme thus takes non-linearity in the account and improves upon the novel-KF prediction. It suitably tracks the data given to it, with consideration of seasonality factor; data tracking is further enhanced.

CHAPTER 5

REAL TIME APPLICATIONS

In the previous chapters, we have proposed an energy efficient and malicious node detection & prediction technique for designing a WSN. Various researches discuss the design issues related with implementation of WSN based on Zigbee module. One of the applications of WSN are home monitoring and automation. The main task is to remotely operate various home appliances like AC, fridge, fans, lights etc. The design of an embedded system which improves the energy consumption rate has been proposed in [31]. The usages of ZigBee and WSN in smart home automation system is presented in [84]. Generally, the data generated by sensors for home automation is irregular, complex and unorganized. In this chapter, we have described the implementation of home automation and an automatic dipper system. The proposed home automation system is low-cost, compact, and flexible. Such systems reduce energy consumption thereby reducing carbon footprint.

The chapter is organized as follows: Section 5.2 presents the hardware implementation of home automation system. The validation and measurement of the implemented hardware is presented in section 5.3. Section 5.4 presents the hardware implementation of automatic dipper system. Section 5.5 presents the measurement results of automatic dipper system. Section 5.6 summarizes the findings of the work in this chapter.

5.1 Home Automation System Configuration

The proposed system has been designed for remotely monitor and control the connected household appliances and measure their electrical parameters. The system is easy to

model and implement. It is also user-friendly. Figure 5.1 shows the description of the designed and developed system.

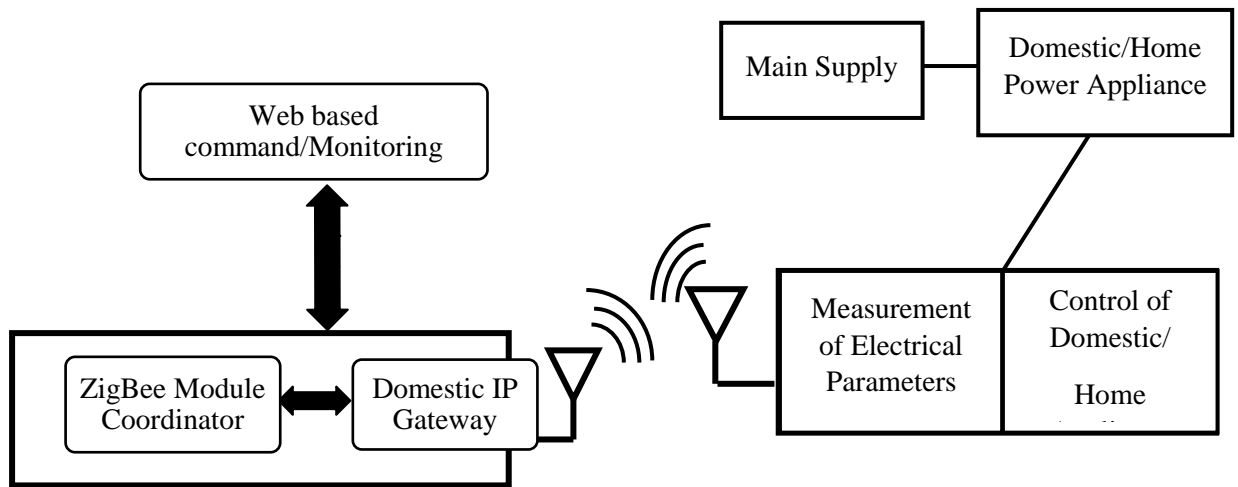


Fig. 5.1: Functional block diagram of the system configuration

The electrical parameters of home appliances were measured by interfacing with fabricated sensing modules. The functional details of the designing and developing of the sensing modules are described in the sections below:

- Master Unit
- Slave Unit

The sensors' output signals are integrated and connected to Microcontroller and ZigBee module for wireless data transmission of electrical parameters. The ZigBee module and microcontroller are interfaced with several sensing devices and are inter-connected to a centralized ZigBee coordinator in mesh topology for reliable reception of data. The maximum range between neighbouring ZigBee nodes is less than 10m. Hopping technique of the mesh topology is used for reliable fusion of sensor data. The entire hardware system consists of two parts, one is Master unit and another Slave unit.

5.1.1 Master Unit and its Operation

The microcontroller ATmega 328P based on Audrino Uno is interfaced with the Wi-Fi Module and the Zigbee Module through level shifter. Figure 5.2 shows the functional block diagram of Master Unit. Microcontroller is also interfaced with the SD card, Real Time Clock (RTC) Module and Liquid Crystal Display (LCD).

The microcontroller ATmega 328P is the main controlling device that communicates with Wi-Fi, Zigbee module through level shifter, SD card module, RTC module and LCD. It generates and receives the command to /from the unit. The Wi-Fi is a password protected wireless communication medium. After connecting to internet, Wi-Fi communicates with microcontroller and User-1 (Website Based). The Wi-Fi, ZigBee and Microcontrollers operate at different voltage levels. Thus, Level Shifter is used to convert one voltage level to another suitable voltage level.

The Coordinator ZigBee Module communicates with Master Microcontroller and Slave ZigBee module. SD card module stores the data of each connected device with slave unitlike voltage, current and power. To know the timing of each log, time stamping is required. So RTC module is used to generate time stamping for each log.

The LCD display existing position of device (ON/OFF), current, voltage and power of each device. The device status is displayed on the LCD as either 0 or 1. 0 signifies the OFF position of device and 1 signifies the ON position of device.

The voltage regulator LM2596 and LM1117 is used to generate 5V and 3.3V fixed supply, respectively. The 5V supply is used to operate Microcontroller, Level Shifter, RTC, SD and LCD. ZigBee, Level Shifter and WI Fi module run with 3.3V power supply.

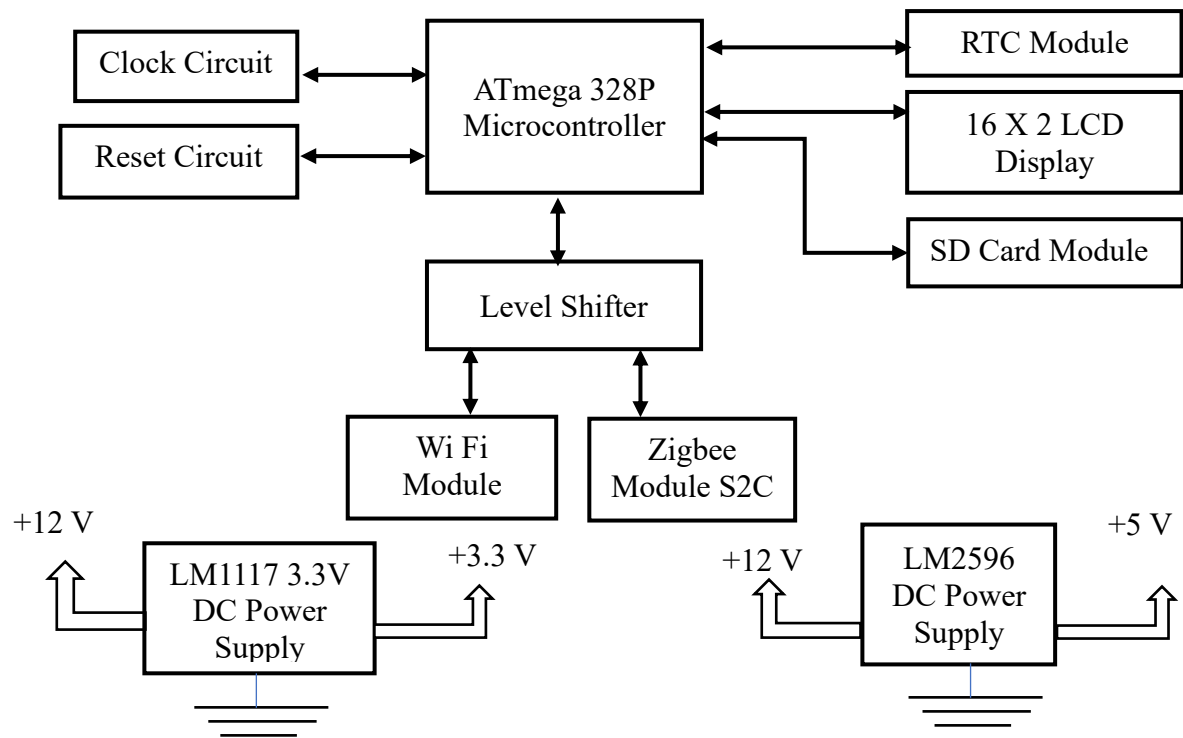


Fig. 5.2: Block diagram of Master Unit

5.1.2 Slave Unit and its Operation

The block diagram of the Slave Unit is presented in Fig. 5.3. Microcontroller has been interfaced with voltage sensor, current sensor, switching circuit, ZigBee module, Temperature sensor, Power cut-off circuit.

Microcontroller is core controlling device which communicate with voltage, current sensor, switching circuit, ZigBee module, temperature sensor, and power cut-off circuit. It generates and receives the command to /from the unit. The 220 V supply is stepped down to 12 V and further it is reduced by a voltage divider circuit. This analog signal is converted into digital signal by the ADC and is fed to the microcontroller. The microcontroller will display it on the LCD of Master Unit. Current sensors (ACS712) are positioned in series of Loads/Devices. Current sensors are interfaced with Microcontroller and is displayed on the LCD of Master Unit. The temperature of Slave

Unit area is measured by temperature sensor (LM35) and is displayed on the LCD of Master Unit. In switching circuit, Solid State Relay (SSR) is used to ON/OFF the devices. Microcontroller sends a signal to SSR for switching purpose. sensors.

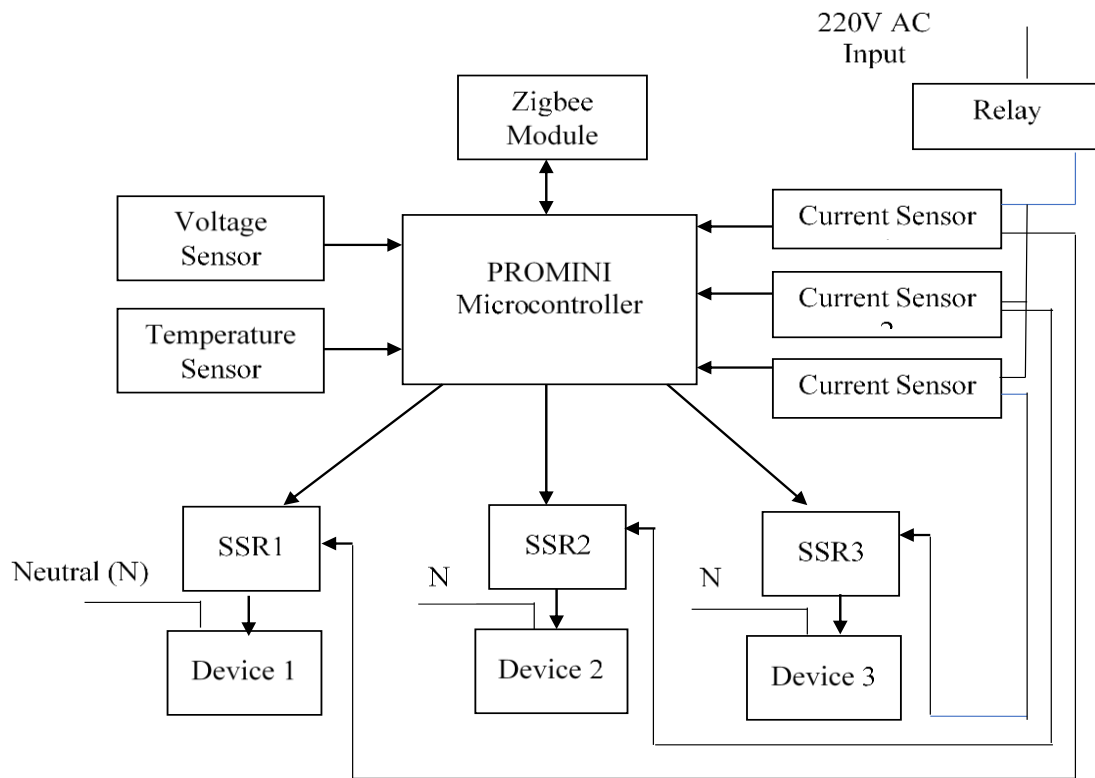


Fig. 5.3: Block diagram of Slave Unit

SSR consist of Opto-coupler and the Triac. Slave Zigbee Module communicates with Slave Microcontroller and Coordinator Zigbee module. It receives voltage, current, temperature and status of each device from the Slave Microcontroller. It also receives the ON/OFF instruction from the coordinator ZigBee. It sends the received slave microcontroller data to coordinator ZigBee and Coordinator ZigBee data to slave Microcontroller. LM7805 and LM1117 voltage regulator are used to generate fixed 5V and 3.3V supply respectively. 5V DC is required to operate the microcontroller, current sensor and SSR, 3.3V DC is used to operate the Slave ZigBee.

5.1.3 Working of the Proposed System

Web pages were also developed for complete operation of the system. The web page name is User/Admin login page, User web page/Admin web page. In starting, Login user ID and Password entered in the web login page. User web page will be opened after authentication of user ID and password. First, the status of the connected devices is checked in user web page. Thereafter the user presses the ON switch of a device, then command through MQTT reaches to Wi-Fi module, if Wi-Fi module is connected to authorize internet connection then Wi-Fi forward this command to Microcontroller, which sends a signal to coordinator Zigbee module (Master), coordinator Zigbee further sends command to Slave Zigbee. Then, Slave Zigbee send a command to Slave microcontroller, the microcontroller generates a trigger command to SSR, and device1 will activate. Voltage sensor and current sensor are interfaced with slave microcontroller which senses the voltage and current and sends to Slave Zigbee. The Slave ZigBee subsequently sends status of devices and sensed voltage and current to the Master controller. These signals are finally sent to LCD for displaying the status of devices, voltage, current and power of each device. The sensed data is also displayed on the user web page for monitoring and control the devices.

A SD card is used to store information that comes from Master Microcontroller. The stored data is used to data analysis for Load Management and other uses.

A scheme has been setup where the system figures out the peak hour of electricity usage and it accordingly controls power consumption at home by switching off the unimportant appliances. The system is connected to the mains (220- 240 V, 50 Hz) through monitoring circuit.

5.1.4 Electrical Parameters Measurement

This sub-section describes the measurements of various electrical parameters such as voltage, current and power.

Voltage measurements

The input (230–240 V) of ac input supply is stepped down to 12 V rms AC signal. The stepped down voltage is then rectified and to get a ripple free DC voltage, the rectified voltage is passed through a capacitor filter. Once the DC signal is obtained it is given to a voltage divider circuit which brings down the voltage to the level of microcontroller. It is important to note that this voltage is linearly proportional to input voltage. The scaling of the signal is found through voltage divider and transformer step down ratio. The actual voltage is thus

$$V_{\text{actual}} = V_m * m_1 \quad \dots (5.1)$$

where, V_{actual} is actual input voltage, V_m is measured voltage and m_1 represents the proportionality factor.

Current measurement

The current sensor ACS712 is used to sense the current. Compact size and fully encapsulated PCB mounting are the main features of this sensor. Schematic diagram of Slave unit for current measurement is presented in Fig.5.8. The three current sensors were used in Slave Unit for current measurement, one in the range of 0-5A and other two were in the range of 0-20A. It is also important to note that the circuit has filter that reduces the noise.

For Current,

$$I_{\text{(actual)}} = V_m * m_2 \quad \dots (5.2)$$

where, I is the actual current and m_2 scaling factor. Different values of m_2 should be used for two different current sensors. It is important to note that 1st sensor is used for appliances with a combined power rating of 1000 Watt and the 2nd sensor is used for appliances with power rating between 0 to 4000 Watts. We intend to provide outlets of two different loads at same sensing node that is why we have used two different sensors.

Power measurement

The power of a single-phase ac circuit is calculated by multiplying RMS voltage and RMS current by the power factor. Power factor is $\cos\phi$ (the phase angle of voltage and current).

$$P_{\text{(actual)}} = V_{\text{(rms)}} * I_{\text{(rms)}} * \cos\phi \quad \dots (5.3)$$

The power consumption depends on property of connected load. Under varying in load conditions (Capacitive, inductive or resistive), the current signal may not be pure sinusoidal in nature. The non-sinusoidal nature, difficulty in eliminating noise and identification of zero crossing are the main challenges in accurate power measurement. Hence, we use correction factor for calculating power consumed.

The correction factor is the ratio of actual power to measured power. The system has been tested on many household electrical appliances and the results are shown in the result sections.

5.1.5 Control of Electrical Home Appliances

To give flexibility to consumer in controlling the device triac-BT139 along with intelligent metering system has been used for switching device ON/OFF. Our system is unique from other similar literature because of its controlling feature. The user can turn the device off /on in three different ways:

Automatic

It can be programmed in such a way that it can automatically scan webpage of electricity distributor of the particular user to get the tariff rate of electricity. The system has the capability of deciding the peak hour and accordingly it will switch off or switch on the connected device, giving user some sort of automation.

Manual

The user is provided with a manual control of system. An ON/OFF switch is directly provided to user to control the system at his/her own wish. This actually gives power to user to bypass the automatic control. Our system is designed in such a way that a manual command will always override the automatic command.

Control Remotely

The users can control system remotely through a webpage or even from an app. This is pretty useful for users who often forget to switch Off their electric appliances before stepping out of home. The webpage will show the user about the current status of appliance and the user can turn the appliance ON/OFF from the webpage.

5.1.6 Data Storage

Data information such as time, source address and channel and sense data are stored in database. Every time a packet is received a row gets added to the table. Hence samples get arranged by sensor node, time and sensor channel. C language has been used here for programming packet transformations, data transmission, packet reception and data storage. The web interface is developed using PHP and Java script.

5.1.7 Hardware Component Description

The entire system has been designed and developed using Master and Slave Units. The Hardware used in the Master and Slave Unit has been described below:

- AVR ATmega328P Microcontroller working on Arduino UNO Platform
- Wi-Fi Module - ESP 8266
- ZigBee Module 2C
- DC-DC Converter - LM 2596
- Voltage Regulator - LM 7805 & LM 1117
- Triac with optocoupler - BT139
- Current Sensor - ACS712
- Micro SD card Module
- RTC - DS 1307 module
- Level Shifter
- 16 x 2 LCD MATRIX
- Temperature sensor - LM 35

Microcontroller (ATmega328/P)

It is an 8-bit, CMOS based low power microcontroller. It is designed and developed using on Reduced Instruction Set Complex (RISC) architecture. It has 32 general purpose register, all are 8-bit register. The throughput is 20 MIPS at 20 MHz's. It has 2 cycle multipliers on the chip. It can execute powerful instruction in a single clock cycle. It has Electrical Erasable Programmable Read Only Memory (EEPROM) and Internal Static Random-Access Memory (SRAM) of sizes 1 KB and 2 KB. It works on +5V DC. It has Digital input/output Pin is 14 and Analog input Pin is 6. DC current per

input/output is 40 mA. Its clock speed is 16 MHz's. Arduino is free electronics prototyping platform based on easy to use software and hardware. It has the ability of sensing the surrounding by receiving input data from several sensors and it can reflect output using control motors, lights, and actuators. With the support of Arduino programming language and development environment microcontroller was programmed. Fig. 5.4 show the pin diagram of microcontroller.

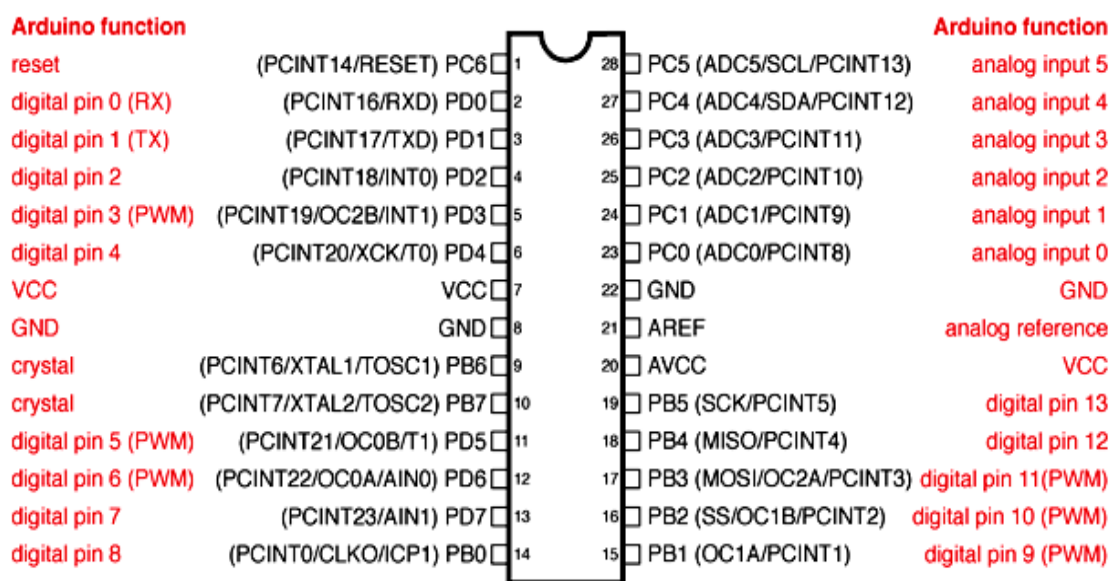


Fig. 5.4: Pin diagram of the UNO along with mapping of Atmega328 pin

Module of ZigBee (S2C)

Zig Bee Module (S2C) is a 20 Pin IC module which is mounted on IC base. It works on 3.3V DC supply. The ZigBee Series 2 OEM RF modules were engineered to operate within the ZigBee protocol and support the unique need of low cost, low-power wsn. It requires minimal power and provide reliable delivery of data between remote devices and operate within the ISM 2.4 GHz frequency band. ZigBee module key features are low power, cost wise low, performance wise high, advanced security and networking, easy to use.

Module of Wi-Fi (ESP8266)

Wi-Fi (ESP8266) module is a small size, low power, 32-bit microcontroller unit. It is wireless, System on Chip (SOC) module with high integration. It has 10-bit ADC Integrated, TCP/IP protocol stack Integrated. It supports antenna diversity, 80 MHz and 160 MHz clock speed. The IEEE802.11 b/g/n standard is used in this module. This module can be used as a separate network controller or the add-on modules in existing network. It is designed for power and space limitation mobile platform designers. It gives incredible capacity to implant Wi-Fi abilities inside different frameworks, or to work as an independent application, with the most reduced cost, and insignificant space necessity. At the point when ESP8266EX has the application, it boots up and straight forward from an outer blaze.

Switching Regulator (Step-Down) (LM 2596)

The LM2596 is a step-down switching regulator, monolithic integrated circuit, known as buck converter. It is suitable for easy and convenient design of step-down switching regulator. It can drive up to 3A load current with excellent with high efficiency. The desired output can be adjusted by variable potentiometer. It is a SMPS (switch-mode power supply). It works at a switch frequency of 150 kHz in this way permitting smaller size filter component than what might be required with lower frequency switch regulator.

Voltage Regulator

Two types of voltage regulator used. AMS1117 for fixed at 3.3 volts and LM 7805 for fixed at 5V. The AMS1117 devices are pin compatible with other three-terminal SCSII controllers and are offered in the position of safety surface mount SOT-223 bundle, in

the 8L SOIC bundle and in the TO-252 (DPAK) plastic bundle. It is available in many models for fixed and adjustable voltage requirements. It can deliver maximum current of 1A and output voltage can vary from 1.5V to 5V. here it uses for fixed 3.3V. It has a low drop out voltage of 1.3V when operating at maximum current. Current cut off is set to limit the worry under over-burden conditions on both the controller and power source hardware.

LM7805 IC a member of 78xx series of fixed linear voltage controller. The voltage source in a circuit may have variances and would not give the settled voltage yield. The voltage controller IC keeps up the yield voltage at a steady esteem. The xx in 78xx demonstrates the settled output voltage it is intended to give. 7805 gives +5V managed control supply. Capacitors of appropriate values can be associated at input and output pins relying on the particular voltage levels.

Module of Triac (MOC3061 BT139 600V 16A)

MOC3061 Triac Module has the ability to control AC related applications using Arduino, PIC or any other microcontroller. There are one/two directs as specified in the thing portrayal and single/both channels can be utilized all the while. In this module Triac is operated through optocoupler MOC3061.

Module of Current Sensor (ACS712)

The ACS712 current sensor uses indirect sensing method to calculate the current and operates at 5V. To sense current a linear, low offset Hall Sensor circuit is used. This sensor is placed at the surface of IC on copper conduction path. When current flows, it generates a magnetic field, which is sensed by Hall effect sensor, and used to measure current. It can sense AC or DC current accurately in commercial, industrial and communication applications. The main uses include load detection and motor control

management, SMPS, and overcurrent fault protection. It does not require any other isolation techniques. It has nearly zero magnetic hysteresis and small-noise analog signal path. Filter pin is used to set the device bandwidth. The output rise time is 5 microseconds in respect to step input current. The bandwidth is 80KHz. It operates on +5V DC and minimum isolation voltage is 2.1 KVRMS. The output voltage proportional to AC or DC currents. The output sensitivity is from 66 to 185 mV/A.

Liquid Crystal Display (LCD)

An LCD display of 16x2 is very common module and it is used in displaying data of various circuit and devices. Its chosen over multi segment LED and seven segments display, easily programmable, no limitations displaying special character, animation, economical and so on. There are two such lines by which 16 characters per line can be displayed in a 16x2 LCD. Command and Data register are used in this LCD. Command register is used for insert a special command and Data register is used for insert a Data into LCD. Like move to line one character, setting up the cursor, clear screen, etc

Micro Storage Device (SD) Breakout Board

The micro SD device is used to store the data of the events. It is a user-friendly device. Connect DI to pin 11, DO to pin 12 and CS to pin 10, CLK to pin 13 with Arduino. Level shifting is used instead of resistors minimize problems, and fast read/write access. 5V and 3V regulator offers 150mA onboard for power-hungry cards. Pins no. 3 or 4 is used to read and write, storage is 2Gb. When read/write operation carried out LED glow. SD card can be insert/remove easily by Push-pull sock. Fig. 5.5 show the Micro Storage breakout board of Arduino.

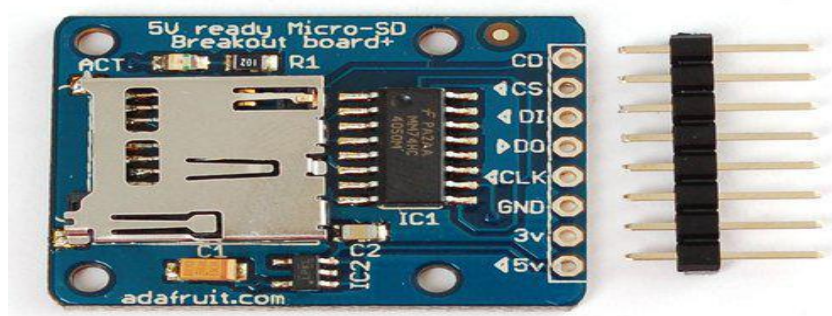


Fig. 5.5: Micro storage breakout board of Arduino

Real Time Clock (DS 1307)

It is serial real time clock which is full Binary-Coded Decimal (BCD), calendar / clock plus 56 bytes of Non-volatile Static Random-Access Memory (NV SRAM), low-power. Data and address are sent serially through two wire, bi-directional bus. It provides hours, minutes, seconds, date, month, day, and year information. The month end date is adjusted automatically for months with fewer than 31 days, including for leap year corrections. The clock can set in either the 12-hour or 24-hour format with A.M/P.M indicator. The RTC can sense power failure and switch to battery supply automatically. Operating temperature range for industry from -40 to +85 degree Celsius. With oscillator running, consumes less than 500nano Ampere in battery backup mode.

Level shifter

Level shifter is used to connect devices of different digital voltage levels. For example, connecting an Arduino (5V device) to an ESP8266 (3.3V device). A level shifter is used to interface two circuits, operating on different voltage level. For Level shifter module operation, two power supplies are required, high and low voltage source. HV pin of level shifter is connected with high voltage and LV pin of shifter is connected with low voltage supply. Both Ground pin of (LV and HV) shifter is connected with supply ground. If we have to connect the Microcontroller (+5V signal) and Wi Fi (ESP8266) (3.3V signal) with level shifter than HV pin of shifter is connected with +5V and LV

pin is connected with +3.3V. Ground pin is connected with supply ground. Convert 4 pins on the low side to 4 pins on the high side or vice versa.

Temperature Sensor (LM 35)

For temperature measurement, LM35 IC is used in the slave module. The LM35 series are very precise temperature sensors. Its output voltage is directly proportional to temperature in degree Celsius. The LM35 has a very important characteristics that its output comes in directly degree Celsius ($^{\circ}\text{C}$), while many other temperature sensors, output comes in Kelvin. it does not require any calibration externally because it is factory calibrated IC. The sensor can measure temperature within range from -55°C to 150°C . The accuracy of temperature measurement of the sensor is $\pm 1/4^{\circ}\text{C}$ at room temperature however, it is $\pm 3/4^{\circ}\text{C}$ when temperature range from -55 to $+150^{\circ}\text{C}$. The LM35 is precise inherent calibration, low output impedance and linear output creates interfacing to control circuitry especially easy or readout. It operates with single power supply and draws $60\text{ }\mu\text{A}$.

5.1.8 Complete System Work Description

The entire work is divided into 2 main parts (Master and Slave) and we designed the system accordingly.

Master Unit Section

In Master Unit, many components are used like Power Module, Microcontroller, Wi-Fi, LCD, Real Time Clock (RTC), SD Module and Level Shifter. All the components were assembled and soldered according circuit diagram as is shown in Fig 5.6 and interfaced with each other as per schematic of Master Unit as shown in Fig 5.7.

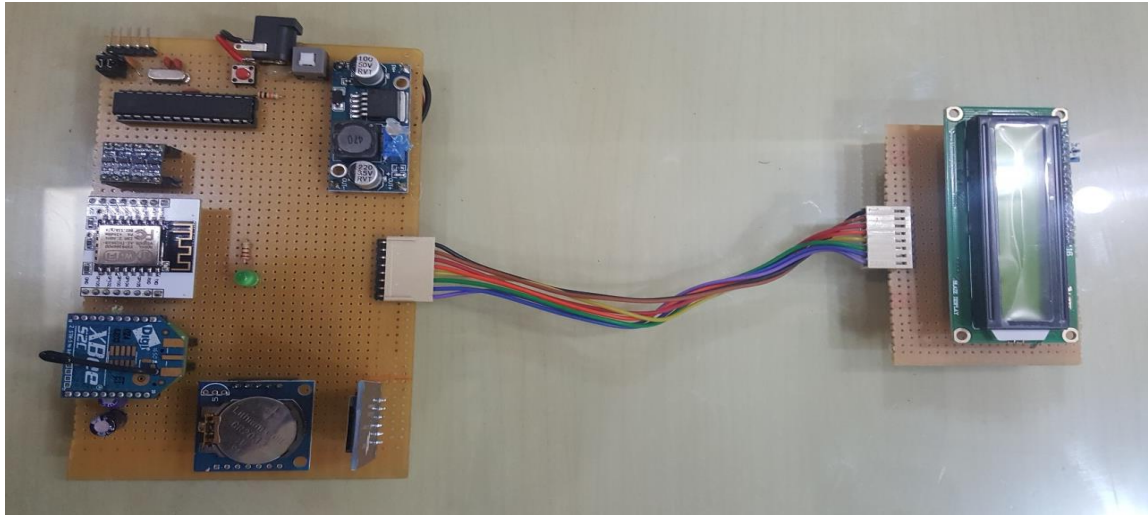


Fig. 5.6: Master Unit Hardware

Hardware Design of Master Unit and its Power Supply Requirement

Master unit module needs two different power supplies (5V and 3.3V). 5V power supply has been used for microcontroller, RTC, SD module, LCD and LM 1117. Power supply of 3.3V has been used for Wi-Fi, Zigbee Module and Level Shifter. Fixed 5V generated by using LM 2596 Step down Power Module DC-DC converter. The range of input voltage is 4.2V-40V and output voltage is 1.25V-7V, which are continuously adjustable, through potentiometer and get the output voltage of 5 volts. Potentiometer was fixed so that output remains constant during the operation. The input voltage must be 1V higher than output voltage. LM 1117 low drop out voltage regulator IC is used for generating fixed 3.3V. In this IC, three pins are used for Input, Output and Ground. 5V is applied at Input and fixed 3.3V is received at output of the regulator.

Microcontroller (ATmega 328P)

ATmega 328P Microcontroller has been used in the master and slave unit of the module. In master unit, basic Arduino platform was used for the functioning of the microcontroller. Minimum circuit which is required for the functioning of the

Microcontroller (ATmega 328P) includes crystal oscillator circuit and Reset circuit. It is a 28 Pin IC which has an internal clock generation circuit but for more accuracy external clock generation circuit has been used.

Reset function is also a critical and important feature of the microcontroller which is useful under various operations. 16 MHz Crystal oscillator was mounted and soldered between the Pin no. 9 and 10 and two capacitors of 33 pF were mounted and soldered at pin no 9 and 10. One end of capacitors was grounded. Ground and 5V output was provide to Reset and Oscillator circuit.

A 16 x 2 LCD was used for displaying of various parameters like Voltage, Current, Power status of all the connected appliances and Temperature during the operation. LCD is interfaced with microcontroller. Microcontroller sends data to LCD for displaying these parameters. 5V DC was supplied to pin no. 1 and pin no 2 was grounded. Pin no. 3 was used for contrast that can be adjusted with 10 K Ω variable resistance.

The Wi-Fi Module (ESP 8266) is used for internet connectivity to the Master module. The Wi-Fi Module was programmed separately to connect to a particular SSID/Password. It was integrated with the system to works at 2.4GHz that requires 3.3V DC for operation of Wi Fi module. This is 16 Pin Unit which was mounted on IC base and it only 4 Pins were used for the operations such as supply (Vcc), Ground, transmission (Tx) and reception (Rx). Theses pins were connected as Pin no. 8 was supplied 3.3V, pin no. 16 was grounded, pin no 9 and pin no. 10 was connected for Tx and for Rx, respectively. Further, LV1 & LV2 of Level Shifter were connected with Wi-Fi Module and HV1 & HV2 of Level Shifter were connected with pin no. 2 (Rx) and pin no. 3 (Tx) of microcontroller.

In this master unit, ZigBee is programmed to communicate with the Microcontroller with ZigBee in slave circuit. Here, only 4 pins out of 20 are used for data transfer and

to provide the voltage to the module. It communicates with the microcontroller. It was configured as per the system requirements i.e. 3.3V DC was connected to pin no.1, pin no. 10 was grounded, the pin no 2 (Dout) and 3 (Din) of ZigBee's were connected with LV3 and LV4 of Level Shifter. HV3 and HV4 of Level Shifter was connected with pin no. 15 and 16 of the Microcontroller.

As discussed above, the Level shifter is used to convert voltage level of 3.3V into 5V and vice versa. This supplies the different digital voltages to the Microcontroller, Wi-Fi and ZigBee as per their requirement to operate. Level Shifter Module has been mounted and soldered as per schematic diagram of master unit shown in Fig. 5.7. The LV and HV were connected to supply with 3.3V and 5V, respectively and Ground was connected to respective LV and HV. The LV1 and LV2 were connected with Wi Fi module. LV3 and LV4 were connected with ZigBee module. Pin no. 2, 3, 15 and 16 of microcontroller were connected with HV1, HV2, HV3 and HV4 of level Shifter, respectively.

To store the events with their real time instants can be done using RTC and SD Card as discussed above. In this master unit an RTC and SD module were mounted and soldered as per schematic diagram of master unit shown in Fig. 5.7.

5.1.9 Slave Unit Section

In Slave Unit, number of components were used like power supply, Triac module with opto-coupler, microcontroller, current sensor, voltage sensor, LCD and ZigBee module. All these components were mounted and soldered as per schematic of Slave Unit in Fig 5.8.

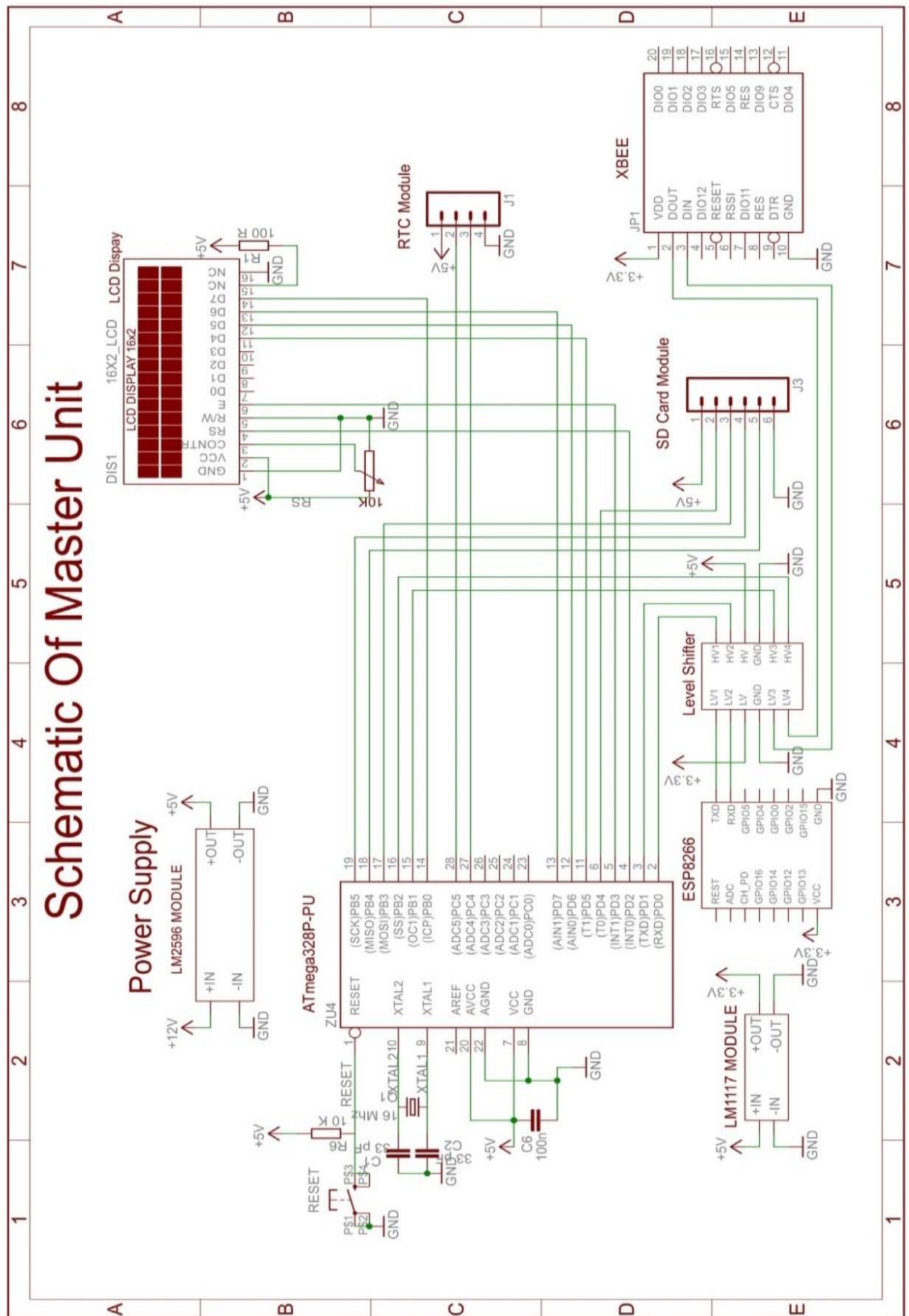


Fig. 5.7: Schematic of Master Unit

The description of work done is as given below:

Hardware Design of Slave Unit and its Power Supply

Power supply was designed as per the current and voltage requirements of the Slave Unit. Figure 5.9 shows the hardware of the Slave Unit and accordingly all components were assembled and soldered. Various supplies 5V/3.3V were generated using a transformer and rectifier using different regulators. In master unit, we have used two power supply 5V and 3.3V. Power supply of 5V has been used for microcontroller, Relay module, Current sensor and LM1117. Power supply of 3.3V has been used for ZigBee Module. LM 1117 low drop out voltage regulator IC was used for generating fixed 3.3V. In this IC, three pins are used for Input, Output and Ground. A DC supply of 5V was applied at input and fixed 3.3V output was obtained.

Voltage Sensor

In voltage sensor, the input voltage is measured and displayed at the LCD and web page. For this purpose, a 12V transformer converts 240V AC voltage into 12V AC which is fed to the voltage divider circuit. The output of voltage divider is fed to the microcontroller. Microcontroller senses, this voltage using appropriate multiplication factor the actual input voltage is monitored on the display. 12V transformer was fed to voltage divider circuit, for designing it use $10K\Omega$ and $1K\Omega$ resistance. The output of voltage divider was fed to microcontroller. Microcontroller has inbuilt ADC to sense the voltage. Sensed voltage by Microcontroller is displayed at LCD with incorporating appropriate multiplication factor. This voltage is also displayed at the web page.

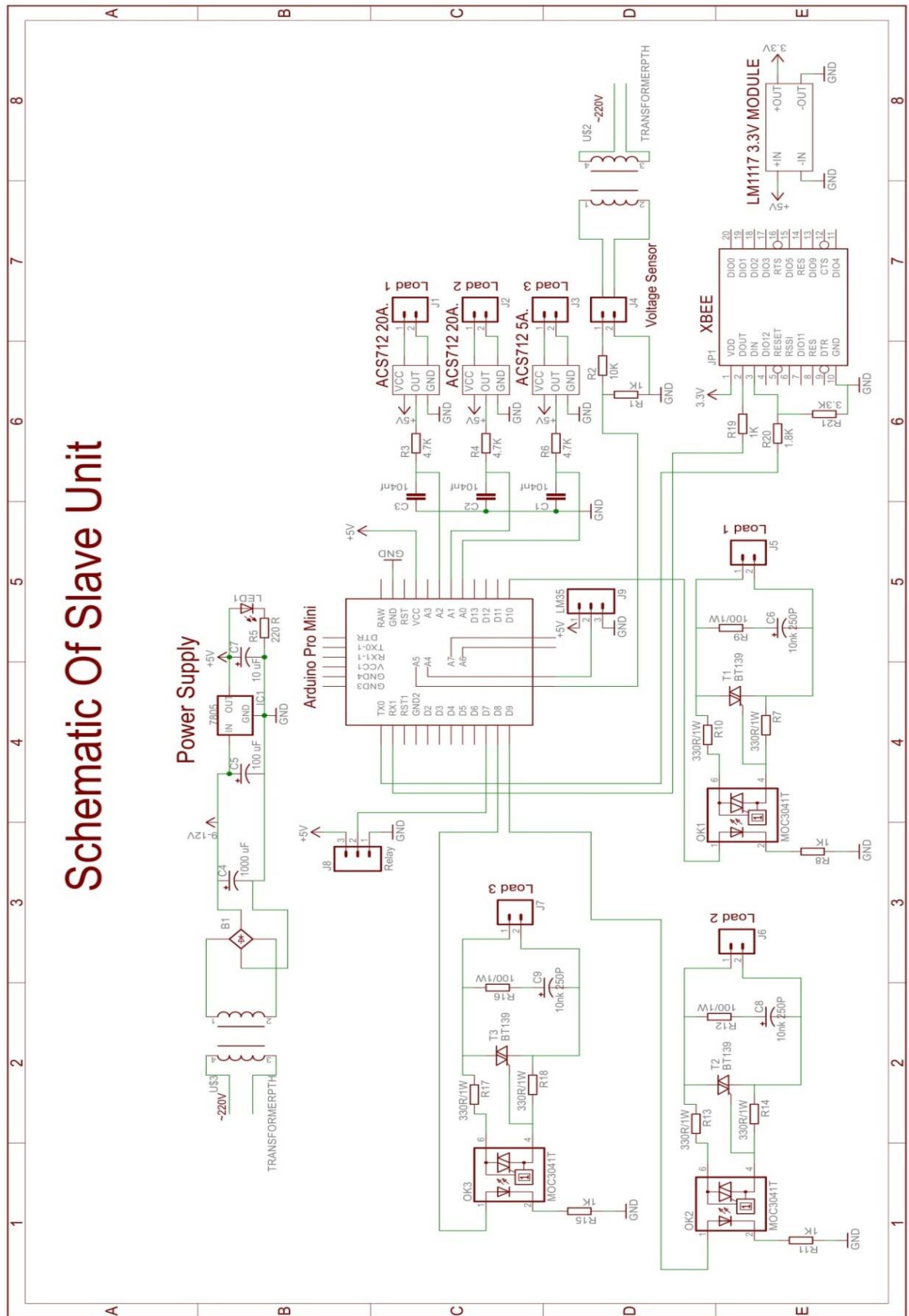


Fig. 5.8: Schematic of Slave Unit

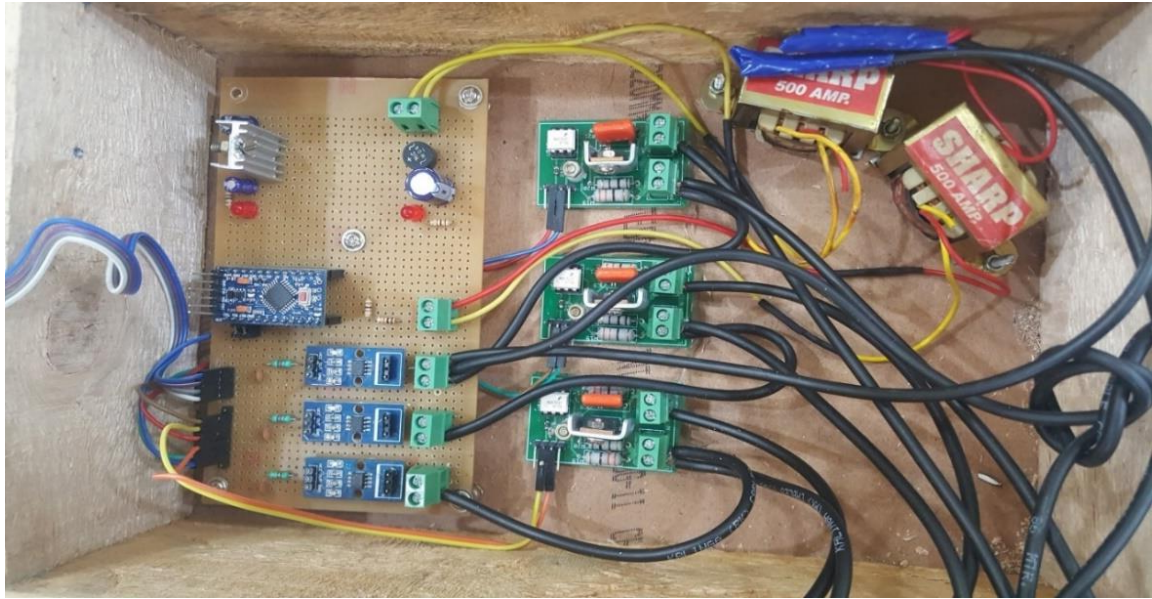


Fig. 5.9: Slave Unit Hardware

Current Sensor

ACS712 is a current sensor which is used to measure the load current. To measure the current of each appliance, each load was connected via an invasive current sensor (ACS712) and its value was measured using ADC of the Microcontroller, two different rating Current sensors were used (5A and 20A). Current sensor was placed in line with the load. The output of current sensor is in millivolt range which is fed to ADC of Microcontroller. In the 5A current sensor, 1A current corresponds to 185mV. In the 20A current sensor, 1A current corresponds to 100mV. These respective mV values are sensed with the microcontroller. For displaying the Actual Load current these are multiplied with their appropriate multiplication factor. Actual Load current value is displayed on the LCD of Master unit and web page.

Switching Circuit

For switching On/OFF to the connected appliance, switching circuit was implemented using Solid State Relays based on TRIAC BT139 and opto coupler (MOC 3041). Once

the switching has been tested, we added Sockets with the switches for demonstrating the switching of loads properly. Three switching circuits were placed before the loads. The inputs of optocoupler (MOC 3041) were connected through microcontroller D8, D9, and D10. Microcontroller gives the command to optocoupler, which triggers the Triac. After this operation the main supply extended to the load.

ZigBee Module was mounted and soldered as per schematic diagram given in Fig. 5.8.

In this unit a temperature sensor (LM35) was mounted and soldered as per schematic diagram given in Fig. 5.8. for sensing the temperature of slave unit area.

Cut off Circuit

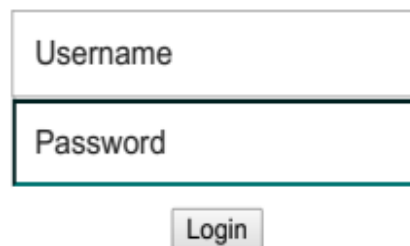
In case of any emergency or such requirement, if we have to switch off the all appliances there is an option for doing the same. This can be done by switching off the supply of slave circuit. Relay has been used to cut off the supply of slave switching unit and the cut off signal is generated by the Master unit. Master unit generates the cut off signal, Slave controller receives the signal through the Zigbee communication. Slave Microcontroller send signal to relay. Relay will be activated and supplies will be interrupted.

5.1.10 Web Pages Development

For remotely control and monitor of electrical appliances, the three web pages have been developed using HTML, Java script, PHP. Login Web page has been developed for secure login in the internet for user and Admin. For login, user name and password is required. Figure 5.10 has been given below for login the user or Admin.

Welcome to IOT Load Monitor & Control

Enter Username and Password



A login form consisting of two stacked text input fields. The top field is labeled 'Username' and the bottom field is labeled 'Password'. Below the fields is a button labeled 'Login'.

Click here to clean [Session](#).

Fig. 5.10: Login page of user

The user name and password are entered in the login page of the user/Admin. Here two pages were developed for Appliance user and Admin. Appliance user can control and monitor all appliances which are connected through the developed Slave system. But admin can only monitor and ON/OFF all the appliances at a time in emergency condition. The new page will open only after entering the correct user name and password. In this page, it has been shown in Fig. 5.11 that three electrical appliances can be operated remotely. We also measure the voltage, current and power of each appliance and temperature of Slave unit. Every status symbol represents its corresponding appliance condition. Here status symbol colour is blue, which indicates Master unit is not connected with internet, so we cannot operate or monitor the appliances until master

unit is not connected with the internet. When Master unit is connected with internet the colour of status symbol will change to Red or Green. Red indicates particular appliance is OFF. Green indicates particular appliance is ON.

7/30/2019

homeautomation1.esy.es/user1.php

User 1 Access Panel

Control

Device 1 :

Device 2 :

Device 3 :

Monitor

Voltage : --- V

Temp : --- degC

Current(Device1) : --- mA

Power(Device1) : --- W

Current(Device2) : --- mA

Power(Device2) : --- W


Current(Device3) : --- mA


Power(Device3) : --- W


Current(Total) : --- mA

Power(Total) : --- W

Status

Device 1 : 

Device 2 : 

Device 3 : 

Click here to clean [Session](#).

Fig. 5.11: Webpage of monitor and control of devices

In Fig 5.12 Admin Webpage has been shown. It comes after entering the Admin user name and the related password. In this admin webpage total voltage, current, power of all connected home appliances and temperature of Slave unit is monitored, moreover check the position of each device by the colour. Blue colour implies Master unit is not associated with the web. Red colour shows that appliance in OFF condition. Whereas Green colour of status appear device in ON condition. Here Admin can OFF or ON the all the devices within the crisis or as per requirement.

Admin Access Panel

Room 1

Monitor


Voltage : --- V


Current : --- mA


Power(Total) : --- W

Temp : --- degC

Status

Device 1 : 

Device 2 : 

Device 3 : 

Control

Room 2

Monitor


Voltage : --- V


Current : --- mA


Power(Total) : --- W

Temp : --- degC

Status

Device 1 : 

Device 2 : 

Device 3 : 

Control

Fig. 5.12: Webpage of Admin

5.1.11 Result and Discussions

The system designed here is best suited for smart home. We have tested our system on loads like AC, geyser, television, refrigerator, water kettle, toasters, microwave oven etc. However, any electrical appliance can be connected with a maximum load of 4000W. Monitoring and measurement of electrical parameters was tested using the system developed, shown in Fig. 5.13. AC was connected to Device 2 position. The AC was operated remotely through internet (webpage). When AC operated, the status of Device 2 was changed from Red to Green. The web page also shows the input voltage 228V, current drawn by AC 6284 mA, power consumption 1435W and temperature of slave unit is 30 °C.

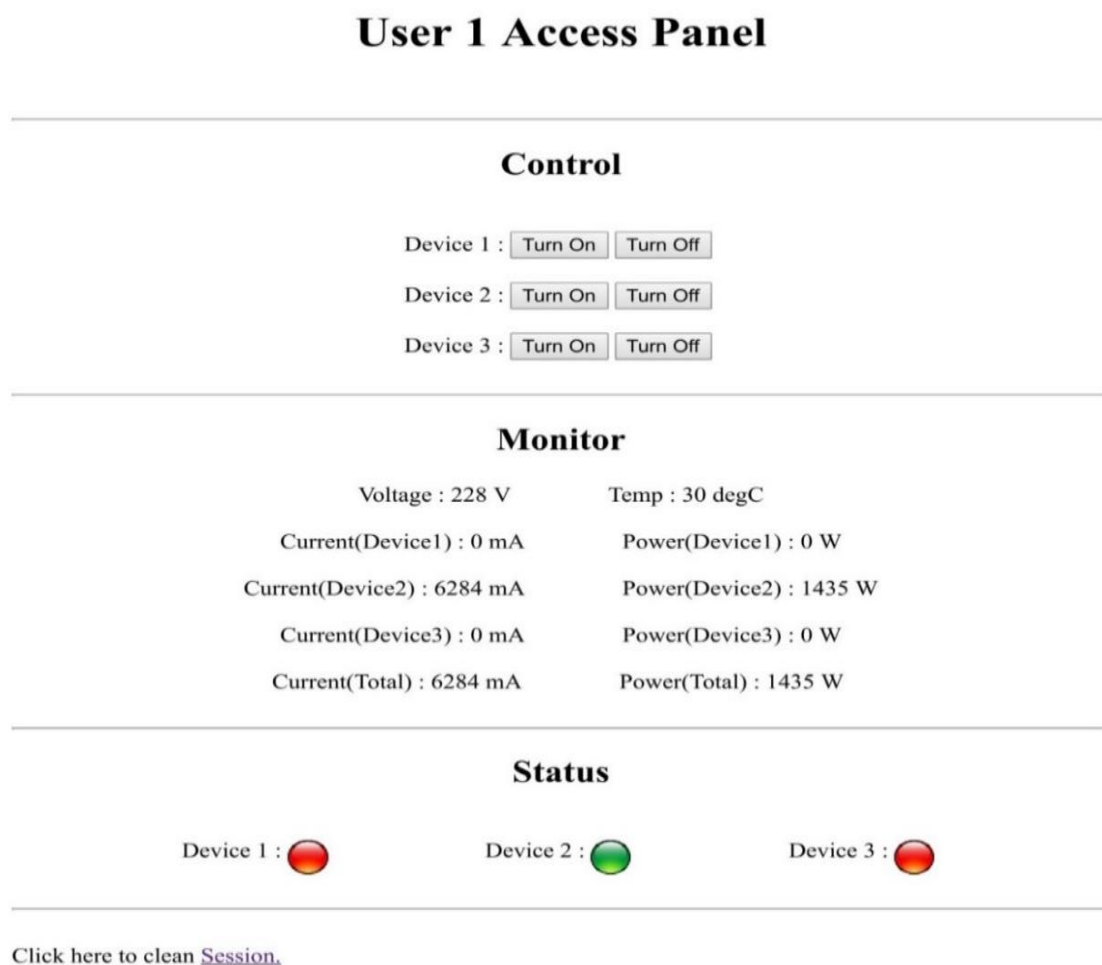


Fig. 5.13: Controlling and monitoring of AC

Electrical parameters of Electric Iron operation and monitoring was tested using developed system and the same are shown in Fig. 5.14. The Electric Iron was connected to Device 3 position. The Iron was also operated remotely through internet (webpage). When Iron operated, the status of Device 3 was changed from Red to Green. The web page also shows the input voltage 229V, current drawn by AC 496 mA, power consumption 1139W and. temperature of slave unit is 30 °C.

User 1 Access Panel

Control

Device 1 :


Device 2 :


Device 3 :


Monitor

Voltage : 229 V	Temp : 30 degC
Current(Device1) : 0 mA	Power(Device1) : 0 W
Current(Device2) : 0 mA	Power(Device2) : 0 W
Current(Device3) : 4960 mA	Power(Device3) : 1139 W
Current(Total) : 4960 mA	Power(Total) : 1139 W

Status

Device 1 : 

Device 2 : 

Device 3 : 

Click here to clean [Session](#).

Fig. 5.14: Controlling and monitoring of Electric Iron

Three Devices were connected with the developed system for controlling and monitoring of electrical parameters of Water cooler, Refrigerator and Electric Iron. All

the three devices connected respectively at Device 1, Device 2 and Device 3. All the devices were operated remotely through internet (webpage). When Device 1 (Water Cooler) operated, the status of Device 1 was changed from Red to Green. The web page also shows the input voltage 243V, current drawn by Water cooler as 1131mA, power consumption as 275W and temperature of slave unit is 30 °C. When Device 2 Refrigerator operated, the status of Device 2 was changed from Red to Green. The web page also shows the current drawn by refrigerator as 1482mA and power consumption as 361W. When Device 3 (Iron) operated the status of Device 3 was changed from Red to Green. The web page shows the current drawn by Iron 496mA and power consumption 1233W. Fig. 5.15 shows the different electrical parameters of operation and monitoring when all the three home appliances were tested at the same time.

User 1 Access Panel


Control


Device 1 :
 Device 2 :
 Device 3 :


Monitor

Voltage : 243 V	Temp : 30 degC
Current(Device1) : 1131 mA	Power(Device1) : 275 W
Current(Device2) : 1482 mA	Power(Device2) : 361 W
Current(Device3) : 5059 mA	Power(Device3) : 1233 W
Current(Total) : 7673 mA	Power(Total) : 1871 W

Status

Device 1 : 

 Device 2 : 

 Device 3 : 

Click here to clean [Session](#).

Fig. 5.15: Controlling and monitoring of three Devices

The total current and power consumption of all devices was calculated and are presented in Table 5.1. The perusal of Table 5.1 revealed that the total current and power consumption is 7673mA and 1871W, respectively consumed by all the home appliances.

Table 5.1: Power consumption of different home appliances determined by the system

Device	Status	Current, A	Power consumption, W
1 (Water Cooler)	ON	1.131	275
2 (Refrigerator)	ON	1.482	361
3 (Electric Iron)	ON	5.060	1233
Total	All devices were ON	7.673	1871

The system also give warning regarding failures. We have designed the system in such a way that it would automatically sense the peak hour of power consumption and it would automatically turn off the devices. The system has been tested on many household electrical appliances and the results are shown in Fig. 5.13 to 5.15. The accuracy of the developed system was calculated and found that the system is having more than 99% accurate.

To log time, we have used SD card module. Electrical or Electronics appliances generate lots of data. This data corresponds to power consumption by different appliances. The data need to be stored for further use and processing so these are stored in SD card and can be accessed by user using graphic user interface.

The sensors pick the data and it calculates the value of temperature, current and voltage. These values are converted to digital form and is passed on to Coordinator. Computer receives data through Wi-Fi and calculates the power consumed by the appliances. It is also worthwhile to note that we have used C programming to process the data.

Errors are inevitable. It can occur from wrong sensing of voltage, wrong sensing of current or even from analog to digital converter. Our system is capable of handling errors. It can even warn users about the failures. We have designed the system in such a way that it would automatically sense the peak hour of power consumption and it would automatically turn off the devices which are not in use at that particular time and a notification will be sent to the user. If user wishes to turn it back on, he/she would be able to do it. ZigBee has been put with IPv6 networking. It has been used to get best performance while handling things remotely.

5.2 Auto Dipper System

These are situations when a sudden come from oncoming vehicles on single lane roads and hinder impair drivers' vision, causing an inconvenience or in worse case results in accident. Mostly, this condition arises due to the negligence of duty by driver to dip headlight whenever not required.

Thus, an automated system which can detect high beam is proposed. This system dips down the headlights as a response to the signal of the oncoming vehicles. The headlights should remain dipped for a short period of time and if necessary, again can be turned to high beam.

A camera-based headlight detection for automatic dipping is proposed in this work. The camera takes live video feed, process it in real time to differentiate and detect oncoming vehicles with high beam. An interrupt is generated on detection of high beam to dip the headlight of the vehicle

The proposed solution works in two phases: video processing to detect the intensity of light from oncoming vehicle and generation of interrupt to dip the headlight.

5.2.1 Video Processing for Head Light Detection

The camera placed on vehicle will be continuously recording. From the video, we have to detect headlight. The headlights are detected by converting the RGB frame to greyscale and cropping it at appropriate level. Then next comparison with threshold is done which define the overall region of interests. The desired features were extracted using Maximal Stable Extremal Regions (MSER) blob detection method. Frames of interest, where the returned MSER regions were indicative of a high beam headlight, on successful detection would trigger an interrupt to the circuit to dip the high beams.

We used Sony DSC W-630 digital camera for video recording. Video recording was done by placing camera at the dashboard of “Honda Amaze” (“dash cam”) with a smaller aspect ratio and bit rate for reducing computation complexity while preserving color space. After the detection of frame of interest, the headlights are dipped and will remains dipped for 20 seconds. The process is explained using the block diagram shown in Fig. 5.16.

Video Processing

It is important to realize the nature of video which is taken by camera. The captured video is likely to include most road scene with headlights, street lights, traffic and dividers and may be fog, rain and snow. The following features along with their nature in the expected video were considered:

- The oncoming high beam highlight is key part of the video to be analyzed.
- Among other surrounding features, the head light will be more prominent and differentiated.
- They can be viewed as elliptical region with very high light intensity concentrated thickly and slowly fading with radial distance around the centre.

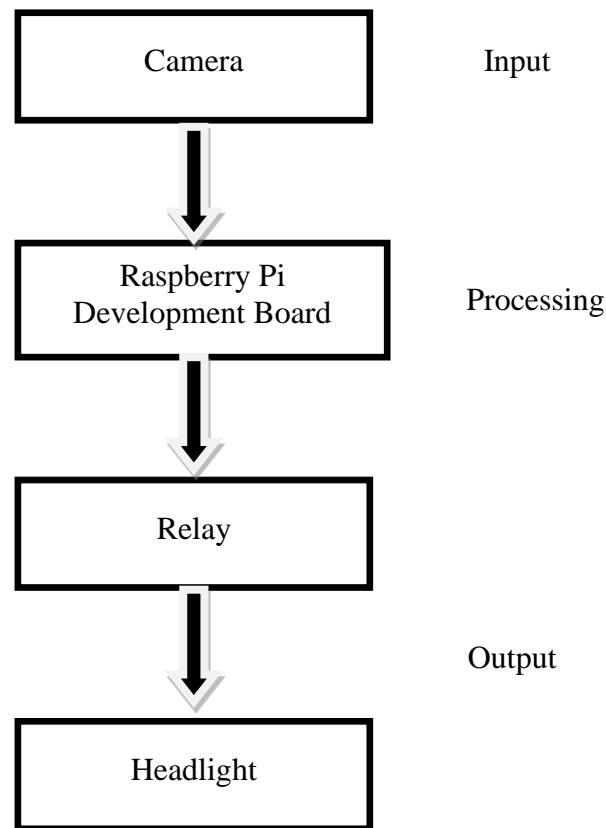


Fig. 5.16: Flow chart of the System

- Bright reflection from stationary object can also provide a very similar picture and therefore, these cases need to be filtered out.

The headlight of oncoming vehicles is detected using ‘Blobs’. It provides a complementary region-specific description of the image structure, and can be used to detect and extract local features. These features remain unaffected irrespective of occlusion, change in visual conditions or clutter [94], [95].

5.2.2 Algorithm

Since we are primarily interested in high intensity region, working with Grayscale image, also known as Intensity image, could be efficient and convenient. These can be easily obtained from a true-colour RGB image represented by a triplet (R, G, B) using the relationship through a simple conversion (Luma conversion) [128], [129].

$$\hat{Y} = 0.2989 * R + 0.5870 * G + 0.1140 * B \quad \dots (5.4)$$

To isolate desired features and make it is easier to detection, we would first suitably crop and threshold the image in order to eliminate the irrelevant component which would never result in favour after processing.

General observation revealed that the nearest street light at any point of time was never below 30 per cent of the top image height (aspect ratio of original frame has 16:9), whereas the oncoming vehicles were always below that bar (see in cropping). So, before it is processed, we decided to crop each frame from the top by 30 per cent to prevent the detection of street light.

a) Cropping at 30 per cent

Figure 5.17 show the surface of road, represents by XY, where

O: camera elevation 'e' from the ground,

OAB: captured region by camera,

α : camera acceptance angle,

R: expected image range, and

PQ: farthest visible image of street light, and

e: camera elevation.

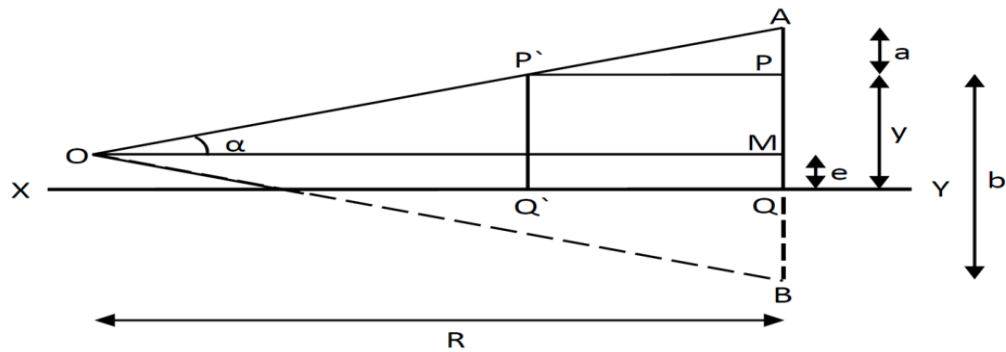


Fig. 5.17: Field of view of camera for cropping 30% of image

In region ΔOAB

$$\tan \alpha = \frac{\frac{a+b}{2}}{R} = \frac{a+b}{2R} \quad \dots (5.5)$$

Also,

$$y = e + \left[\frac{a+b}{2} - a \right] = e + \frac{b-a}{2} \quad \dots (5.6)$$

From (5.5)

$$a = 2R \tan \alpha - b$$

Or

$$a/b = \frac{2R \tan \alpha}{b} - 1 \quad \dots (5.7)$$

Assuming $t = a/b$, (5.7) may be rewritten as

$$t = \frac{2R \tan \alpha}{b} - 1 \quad \dots (5.8)$$

Rearrange the (5.5) and (5.6)

$$a + b = 2R \tan \alpha \quad \dots (5.9)$$

$$-a + b = 2(y - e) \quad \dots (5.10)$$

Adding the (5.9) and (5.10) then

$$b = R \tan \alpha + y - e \quad \dots (5.11)$$

Using the value of (5.11) in (5.9) then

$$t = \frac{2R \tan \alpha}{R \tan \alpha + y - e} - 1 \quad \dots (5.12)$$

Considering the values $e = 1\text{m}$, $y = 8\text{m}$, $\alpha = 16^\circ$, $R = 45\text{m}$, $t = 0.2966 \cong 30\%$.

The values of 'e' and α are measured precisely and the value of R and y measured approximately.

a) Thresholding at ~78 per cent

In standard headlight (Halogen light lamps) [133] the red colour intensity (645nm) as the maximum, blue colour intensity (440 nm wavelength) as the lowest and green colour intensity (510 nm wavelength) as moderate intensity [131],[132].

Any faint light from outside sources will have highest (100 per cent) intensity of red colour, minimum (25 per cent) of blue colour intensity and moderate (75 per cent) of green colour intensity. It translates into a limiting case of RGB (255, 192, 64) as the criterion for detecting headlights through its colour. So, using Luma conversion [129] in grayscale.

Using (5.4)

$$\begin{aligned}\hat{Y} &= 0.299 * 255 + 0.587 * 192 + 0.114 * 64 \\ &= 198.165\end{aligned}$$

Because 255 is the highest intensity, $Y/255 = 77.71$ per cent is the point at which choose the threshold to exclude all those sources that are not sufficiently intense to measure themselves as significant visible headlight. Since all intensities are not relevant, thresholding [133] at approximate 78 per cent showed that most of distant and faint sources were removed and only those were retained whose brightness was significantly high or dazzling and straining to drivers' eyes. These would naturally include all the high beam (especially most central region of their brightness) and bright lights (if any, including reflections or taillights).

We used the Maximal Stable External Regions (MSER) algorithm is based on the idea of taking regions that stay almost the same through a wide range of thresholds [134] as it detects (based on watershed algorithm this thresholding will be done on top of previous one, and so, it will refine results even more), the oncoming high beams will be quickly and distinctly identified by the MSER algorithm, thus successfully providing with the desired results. Another popular algorithm for such a purpose is Lindeberg's watershed-based grey-level blob detection algorithm [135]. However, MSER was more suited for our purpose since image descriptors in MSER remain robust under perspective transformations [136], [137]. This would allow our system to detect dazzling high beams from any part of the oncoming road.

MSER Algorithm

The steps MSER extraction as follows:

- Sweep threshold of intensity from black to white, performing a simple luminance thresholding of the image.
- Extract related components "Extremal Region".
- Finding a threshold when an extremal region is "Maximally Stable" i.e. the local minimum of relative growth of its square. Due to discrete nature of the image the region below or above may be coincide with the actual region, in which case the region is always considered to be maximum.
- Descriptors of those regions keep as features.

However, even if an extremal region is Maximally Stable, it could be rejected if:

- It's too large (there is a Maximum Area parameter)
- It's too small (there is a Minimum Area parameter)
- It's too unstable (there is a Maximum Variation parameter)

- It's too similar to its parent MSER.

The salient features of the algorithm are:

- MSER performs good on images contain homogeneous regions with distinguishing boundaries.
- Its works good for small regions.
- It does not work well with any motion blur images.
- The smart implementation makes it one of the fast region detectors.

After getting the desired frame, MSER features were detected using several parameters. These parameters help to decide which potential candidates are indeed maximally stable, are discussed below:

Region Area Range

This defines a range of area for detected regions that will be considered. It would thus remove stray reflections, both small and large, which may arise from nearby cars.

Threshold Delta

To detect a stable region, the MSER detector incrementally steps through the range of intensity of the input image. This parameter specifies the number of increments that the detector tests for stability. For a large delta will get less regions.

For every region whose “White” (remnant) area at threshold T is given by Size (T), Variation is measured of every pixel in “delta” steps

$$V(T) = \frac{\{size(T) - size(T - delta)\}}{\{size(T - delta)\}} \quad \dots(5.13)$$

If the variation for a pixel is a local minimum of a variation, is $V(T) > V(T - 1)$ and $V(T) > V(T + 1)$, then the region is maximally stable. This expression for determining

of variation is found in Open CV and MATLAB implementation of MSER as it speeds up extraction process

$$V(T) = \frac{\{size(T + \delta) - size(T - \delta)\}}{\{size(T)\}} \quad \dots (5.14)$$

Maximum Variation

If a region is maximally stable, it can still be rejected if the regions' Variation is bigger than this parameter. Smaller this value, Lesser the regions.

5.2.3 Hardware Implementation

Since the goal is to build a standalone device that can be installed in a vehicle, so for this select Raspberry Pi development board, and interface with USB webcam for taking input. Raspberry Pi run in OpenCV, and processing to generate a trigger. Once trigger is generated, the script sends command to the GPIO pins to turn OFF the LED corresponding to high beam (we chose two separate LEDs to indicate Low and high beam).

The model of Raspberry Pi 2 provides six times processing capacity of previous versions. This 2-generation model of Raspberry Pi has an upgraded version of Broadcom BCM2836 processor, which is a powerful ARM Cortex-A7 based quad-core processor operate at 900MHz frequency also increase in storage capacity to 1GB. It runs [138] Raspbian, a Debian-based operating system having environment is similar to any popular Linux-based distribution. The only downside that prohibits some software from running on the Raspberry Pi development board is that the Raspberry Pi has an ARM processor, whereas most of software is developed for architecture-based processors intel x86 or intel x64. It prevents optimal use of CPU for other software's, and often leads to

poor performance [139]. Besides that, it is an outstanding pint size computer that can adapt to different purposes, be it for small projects or success at the production level.

Prototype Model

The prototype model shown in Fig.5.18 and schematic diagram of the model is presented in Fig. 5.19 which includes Raspberry Pi, a standard USB webcam and two LEDs on a bread board, a power bank. The Raspberry Pi board has been connected with two LEDs on a breadboard through GPIO pins. Two LEDs different coloured were used. $1K\Omega$ resistors use with each LED to limit the current value. The LEDs resembles to two types head lights one is low beam, and another high beam. Initially, assume that high beam LED is turned ON. It dips as soon as it encounters an oncoming high beam, and the low beam LED is turned ON. The video is taken by USB webcam. Raspberry Pi powered by a power bank (5V, 1.5A), which powers suitably main board as well as peripheral devices. As soon as it encounters an oncoming high beam, it dips, and the LED corresponding to the low beam is switched ON.

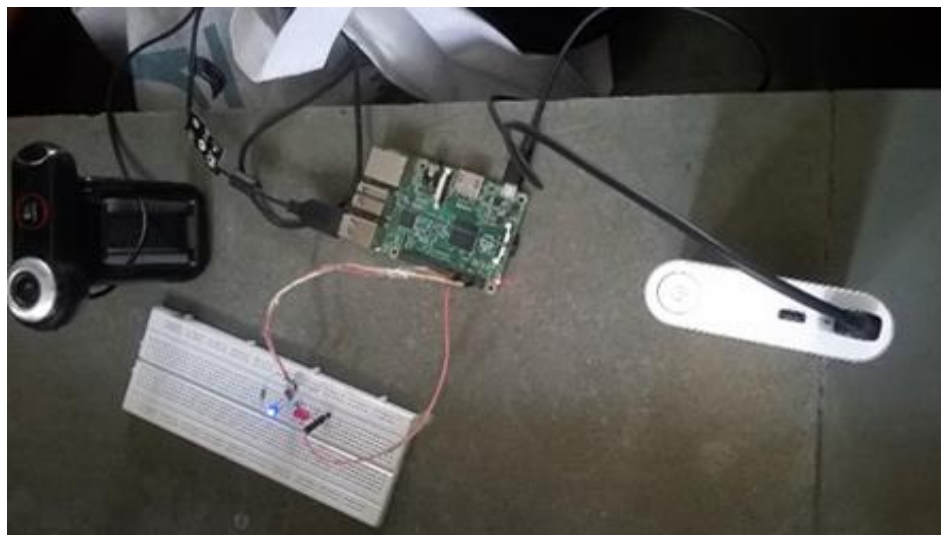


Fig. 5.18: Prototype Model Hardware

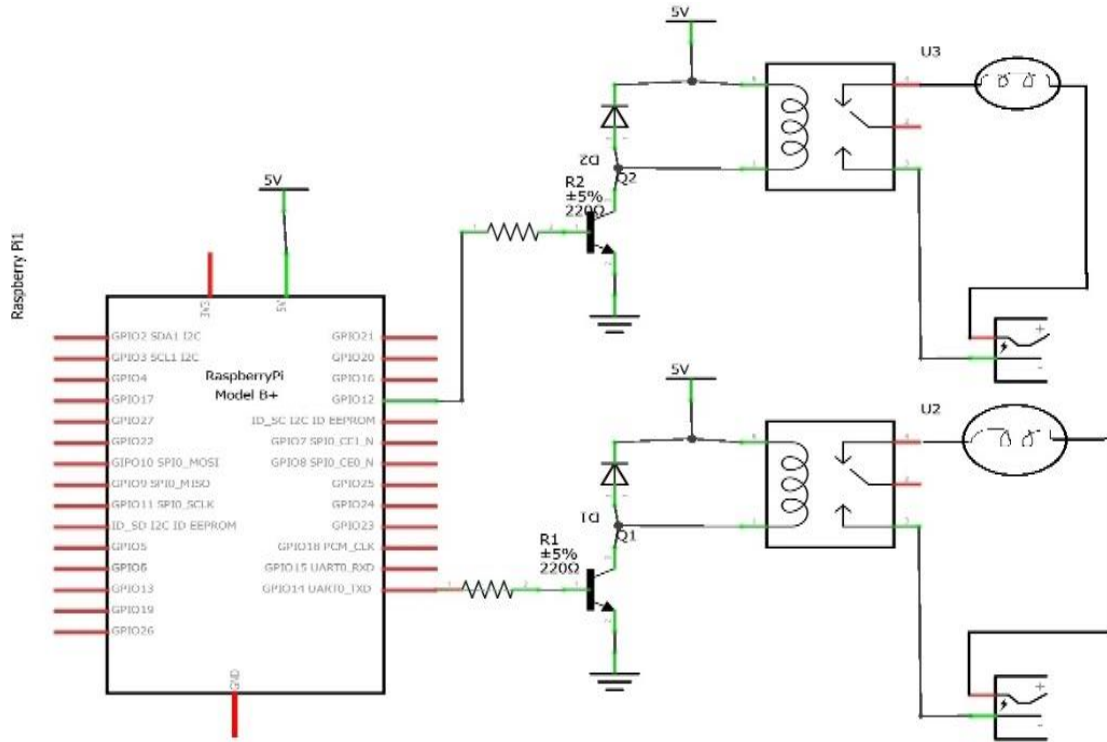


Fig. 5.19: Connection diagram of the dipper system

Testing of Prototype Module

The Logitech Webcam Pro 9000 [140] was used to capture the video in real-time. It is one of the best available USB Webcams. It has auto focus functionality which helped us to capture quality video. The Raspberry Pi is operated via a micro USB connector and required a relatively fixed 5 volts and at least 700mAh. The power is supplied via the micro USB that goes to CPU, GPU and all USB components particularly in network chip. The Raspberry Pi approximately 1100mAh power. This was maintained constant as well as, low power would reduce the speed of clock cycle and higher power would make it difficult to drop off the excess power, making it non-operation [141]. Connection diagram of the setup shown in Fig. 5.20. The testing was carried out using Raspberry Pi as the standalone hardware on a pre-recorded video to identify the frames that caused headlight dip feature. MATLAB is used for processing of Pre-recorded video. The video

would be processed in real time. So, the basic functions and associated libraries are loaded in the memory as soon as the system start. Then, as the video starts shooting, each frame would be taken and processed in real time, i.e. processing will be simultaneous. Note that we will not, in actual practice, store permanently any part of the video, as that is totally unnecessary and would hamper the system performance.



Fig. 5.20: Original frame

We expand this by interfacing it with laptop. we simulated another prototype. The processor of laptop's is more powerful than Raspberry Pi's. We used laptop with Intel-i5, 4th gen processor running at 2.5 GHz clock frequency. The prototype used Arduino development board for interfacing with hardware. The entire system has been simulated. The testing was carried out on a pre-recorded video, and image processing was performed using MATLAB. Proteus simulation software was used for the purpose. Here, we linked MATLAB to a virtual serial port, which was in turn linked to Arduino, and Arduino was simulated on Proteus. Everything was being done on the same laptop. Figure 5.25 shows the simulated prototype.

5.2.4 Results

The algorithm can be shown stepwise on a sample/Original frame. Fig. 5.20 shows the sample frame. Figure 5.21 to 5.22 shows the status of the frame after each level of processing. The first thing to be done with the frame is cropping it by 30 per cent from top as shown in Fig. 5.21. Next, the resultant frame is converted to grey scale. Grey scale images are faster to process, and ideal for real time processing applications. Fig. 5.22 show the Gray scale frame of captured image.



Fig. 5.21: Cropped frame



Fig. 5.22: Greyscale frame

Since, the highlights need to be separated from other stray lights, thresholding is an important part of the algorithm. It allows to focus primarily on the headlights. After careful study on the frames, thresholding at 78% was considered apt. the results are dissipated in Fig. 5.23(a) and (b).



Fig. 5.23 (a): Frame after Thresholding

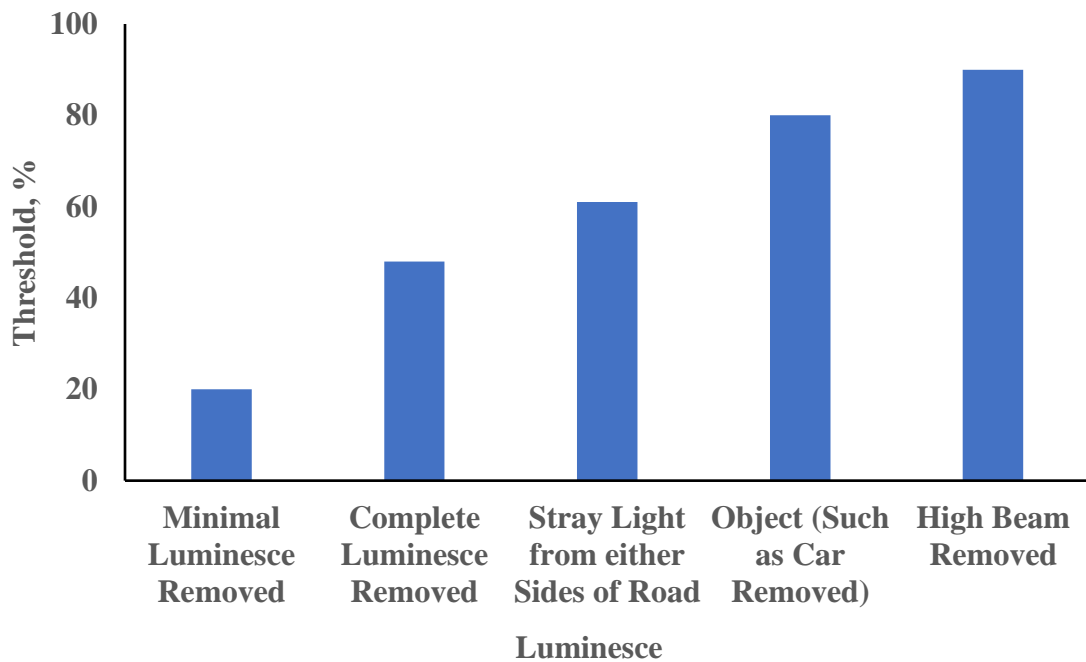


Fig. 5.23(b): Thresholding at various percentages

The MSER region obtained after processing the thresholding of head lights are presented in Fig. 5.24.

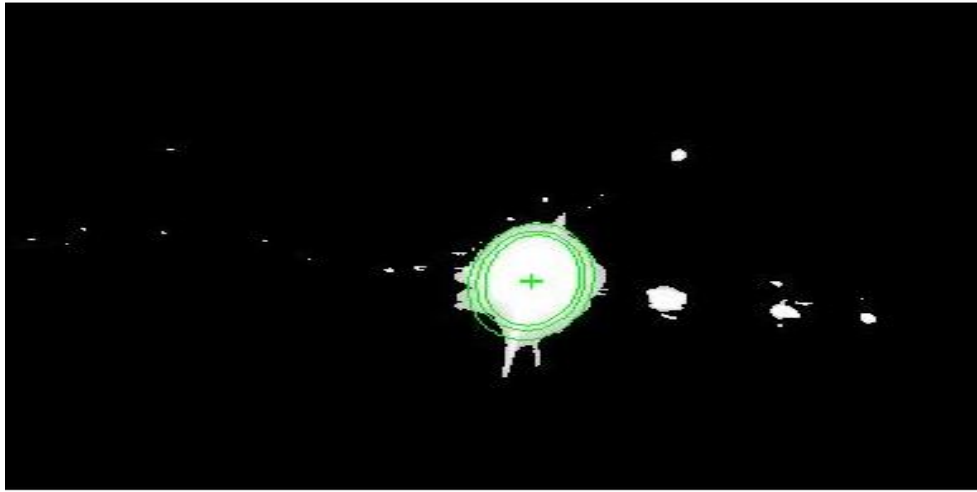


Fig. 5.24: MSER regions after processing

Open CV implementation of MSER is more stable than MATLAB's, because there is right amount of contiguous detection in Open CV, unlike MATLAB. The simulation confirmed that the hardware prototype was not getting affected by lower processing capability and memory capacity of Raspberry Pi as compared to laptop's simulated environment and Proteus simulation for testing purpose are presented in Fig. 5.25.

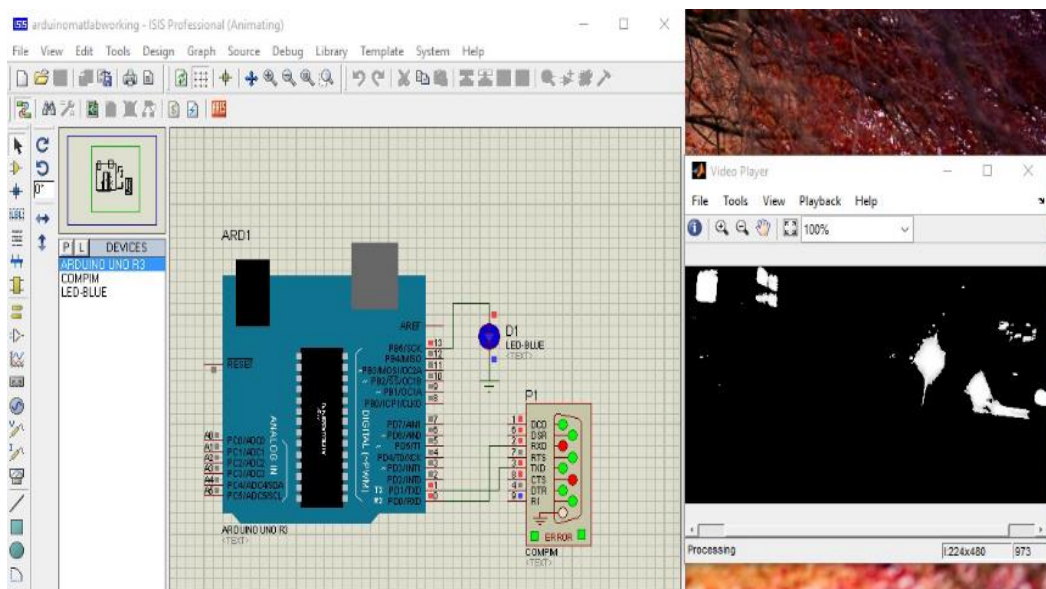


Fig. 5.25: Proteus simulation for testing purpose

5.3 Conclusion

An intelligent system that loyally monitors and controls electrical appliance, at home, for intelligent buildings has been developed. An incessant watch on electrical appliances can be kept through a website. Our aim here is to come up with an optimized solution that minimizes electricity consumption during peak hours. The sensor systems are computerized with user friendly UIs, keeping heterogeneity in users in mind.

Detection of headlights by a hardware prototype in real time has been achieved using MSER blob detection algorithm implemented in OpenCV running on Raspberry Pi. As soon as headlights are detected, the code sends a trigger. This trigger will be used to drive the relay for automatic dipping the high beam headlights. That works in real time with a certain time delay.

CHAPTER 6

CONCLUSION AND FUTURE WORK

In this chapter, the whole work is concluded and summarised. The present investigation was conducted on efficient and secure wireless sensor network and its' applications on smart home automation and automatic dipper system to reduce road accidents during night. During the course of present study, it was found that few important areas need further in-depth research in the area of WSN.

6.1 Conclusions

In this thesis, we present a methodology for optimal selection of combination of modulation schemes and error correcting codes for improving energy efficiency of sensor nodes. We also proposed methods for malicious node detection and prediction. The thesis also discusses implementation smart home automation system and auto dipper for vehicles. Energy efficiency is an important aspect of WSN. We proposed a method for optimal selection of modulation schemes and error correcting codes for improving energy efficiency of sensor node. This system examined different combinations of Hamming codes, RS codes, and CCs. Application-defined parameters such as distance (d) and path loss exponent (n) also play a major role in selecting the energy optimal ECC. Furthermore, varying the error-correcting capability (t), code word length (N), and modulation parameters affect the selection of the optimal ECC. It is observed that the node energy reaches a minimum at a certain error-correcting capability (t), as well as a code word length (N). Three different energy components; the signal, the circuit, and the computation energy have been assessed. The term crossover distance (d_{xo}) beyond which use an ECC is profitable from the energy perspective is formulated.

The formulation shows the nature of shift in the crossover distance with the change in the ECC, the modulation scheme as well as the system configuration. This analysis is done for the nodes functioning in the additive white Gaussian noise (AWGN) channel. This study decreases the search space by eliminating many of the existing ECCs and modulation variants, and the optimum energy consuming ECC-Modulation configuration for the sensor node is obtained. Simulation results show that the sensor node with Reed-Solomon codes and BPSK modulation consumes optimal energy under certain operating conditions. At distance (d) = 60m an optimal ECC-modulation pair RS ($N=63$) code with correcting capability (t) = 4 & BPSK modulations schemes gives 48% energy savings.

As the overall behaviour of sensor network depends as all participating node, Malicious node detection is as important part of proper function of sensor network. We propose a novel Clustered Based WTE scheme for detection and SVM based method for time series prediction of malicious node in this thesis. Clustered Based WTE scheme less propagation time in comparison of without clustering WTE scheme. The propagation time is least for SVM with highest detection rate and accuracy in comparison of Clustered Based WTE, Autoregressive (AR) prediction model. Though, the introduction of Prediction and Decision block in algorithm makes it slightly costly but the edge over other parameters makes it ideal for industrial monitoring, defence monitoring, medical monitoring, where the accuracy is most important with almost no lag, for example in industrial monitoring any toxic gas is leaked then the detection and response should be made as soon as possible thus Accuracy and Propagation time is the key requirement here. Also, unlike AR prediction, in SVM there is no trade-off between propagation time and accuracy, both the parameters are achievable at same time. So, SVM is better where accuracy and prediction time both are must. Proposed EKF technique with weighted

moving average to update estimation and estimation error, thereafter uses seasonality factor to improve the prediction. The scheme thus takes non-linearity in the account and improves upon the novel- Kalman Filter prediction. From the graphs and simulation, it was found out that the malicious nodes were marked successfully with high detection ratio and low misdetection ratio. The scheme gives an accuracy of 83.33% and misdetection percentage 16.67% over 168 data points. It suitably tracks the data given to it, with consideration of seasonality factor; data tracking is further enhanced.

Home automation is one of the applications of WSN. We present low cost, compact and flexible ZigBee based home automation for remote control of house hold devices. This system assures optimal usage of electricity, thereby reducing carbon footprint. In this thesis we developed a smart system that monitor and control the Home/Domestic electrical appliances. Continuous tracking of home electrical devices may be managed via website. The proposed systems are computerized with user friendly User Interface, keeping heterogeneity in users in mind. Our proposed system regularly monitors and control the home appliance remotely. It's really user-friendly and simple to navigate for new consumers. One another real time implementation is in field of automation i.e., Auto Dipper system in vehicles. A MATLAB code for simulating real time processing has been developed and tested successfully on a sample pre-recorded video shot under suitable circumstances. Detection of headlights by a hardware prototype in real time has been realized using MSER blob detection algorithm implemented in OpenCV running on Raspberry Pi. As soon as headlights are detected, the code sends a trigger. This trigger will be used to drive the relay for automatic dipping the high beam headlights. Developed system works in real time with a certain time delay. Such systems have enormous potential in self-driven automated vehicles, as under such scenarios they would drive on the road reliable and responsibly

6.2 Future works

- i) The framework presented in this thesis can be extended to advanced ECC techniques like LDPC codes with static, as well as dynamic WSNs. In future, the reduction in computation energy will allow us to incorporate more computation on the sensor node and will hence widen the application domain of WSNs. With the same amount of computation, the savings in energy will contribute to an enhanced node life. Intuitively, the circuit energy will also affect the crossover distance in the same manner as the computation energy does. The researchers can extend this approach in different remote areas like battlefield scenario, glacier environment, coal mines, oil refineries where measurement of physical quantities is very complex difficult and optimal results can be achieved. The sensor node energy model can be modified with advanced Digital Signal Processors, microcontrollers for small power consumption.
- ii) Also find the various attacks, whole network can be secure and free for any threats.
- iii) In future, a whole building appliance monitor and control. People will be aware of possible power wastage. In Auto Dipper system delay can be reduced to improve the hardware. Instead of using USB webcam, we can use Pi Cam for it has a dedicated GPU in Raspberry Pi. However, reflection from trailing vehicles is still an issue. In future improve it.

REFERENCES

- [1]. B. Jan, H. Farman, H. Javed, B. Montrucchio, M. Khan, and S. Ali, “Energy efficient hierarchical clustering approaches in wireless sensor networks: A survey”, *Wireless Communications and Mobile Computing*, vol. 2017, pp 1-14, 2017.
- [2]. A. P. Abidoye, N. A. Azeez, A. O. Adesina, and K. K. Agbele, “ANCAEE: A novel clustering algorithm for energy efficiency in wireless sensor networks”, *Wireless Sensor Network*, vol. 3, pp.307-312, 2011. (<http://dx.doi.org/10.4236/wsn.2011.39032>).
- [3]. L. Kong, Q. Xiang, X. Liu, X.-Y. Liu, X. Gao, G. Chen, and M.-Y. Wu, “ICP: Instantaneous clustering protocol for wireless sensor networks”, *Computer Networks*, vol. 101, pp. 144-157, 2016. (<http://dx.doi.org/10.1016/j.comnet.2015.12.021>).
- [4]. S. K. Singh, M. P. Singh, and D. K. Singh, “Energy efficient homogenous clustering algorithm for wireless sensor networks”, *International Journal of Wireless and Mobile Networks (IJWMN)*, vol. 2, no. 3, pp. 65-82, 2010. (<http://dx.doi.org/10.5121/ijwmn.2010.2304>).
- [5]. F. Engmann, F. A. Katsriku, J. D. Abdulai, K. S. Adu-Manu, and F. K. Banaseka, “Prolonging the lifetime of wireless sensor networks: A review of current techniques”, *Wireless Communications and Mobile Computing*, pp.1-23, 2018. (<https://doi.org/10.1155/2018/8035065>).
- [6]. Y. Sankarasubramaniam, I. F. Akyildiz, S. W. McLaughlin, "Energy efficiency-based packet size optimization in wireless sensor networks", in *International IEEE Workshop on Sensor Network Protocols and Applications*, pp. 1-8 February, 2003.
- [7]. G. Balakrishnan, M. Yang, Y. Jiang, and Y. Kim, “Performance analysis of error control codes for wireless sensor networks", in *Proceeding of International Conference Information Technology*, USA, April 2007, pp. 876-879.
- [8]. M. P. Singh, P. Kumar, “An efficient forward error correction scheme for wireless sensor network” *Procedia Technology*, vol. 4, pp. 737–742, 2012.

- [9]. S. Chouhan, R. Bose, and M. Balakrishnan, "Integrated energy analysis of error correcting codes and modulation for energy efficient wireless sensor nodes", *IEEE transactions on Wireless Communication*, vol. 8, no. 10, pp. 5348–5355, 2009.
- [10]. S. Srivastava, C. Spagnol, and E. Popovici, "Analysis of a set of error correcting schemes in multi-hop wireless sensor networks", in *Proceedings Ph.D. Research in Microelectronics and Electronics*, Cork, Ireland. July 2009, pp.12-17.
- [11]. D. G. Padmavathi and M. D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks", *International Journal of Computer Science and Information Security*, vol. 4, no.1, pp. 117-125, 2009.
- [12]. E. Ayday, F. Delgosha, and F. Fekri, "Location-aware security services for wireless sensor networks using network coding", in *26th IEEE International Conference on Computer Communication (Infocom)*, Barcelona, Spain, 6 to 12 May, 2007. [DOI: 10.1109/INFCOM.2007.146](https://doi.org/10.1109/INFCOM.2007.146)
- [13]. S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks", in *CCS'03: Proceeding of the 10th ACM conference on Computer and Communication Security*, October 2003, pp.62-72.
- [14]. S. Chouhan, R. Bose and M. Balakrishnan, "A framework for energy consumption-based design space exploration for wireless sensor nodes", *IEEE Transaction of Computer-Aided Design Integrated Circuits Systems*, vol. 28, no. 7, pp. 1017-1024, 2009.
- [15]. S. Chouhan, R. Bose, and M. Balakrishnan, "System-level design space exploration methodology for energy-efficient sensor node configurations: An experimental validation", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 31, no. 4, pp. 586-596, 2012.
- [16]. S. Cui, A. J. Goldsmith and A. Bahai, "Energy constrained modulation optimization", *IEEE Transaction Wireless Communication*, vol. 4, no.7, pp.2349-2360, 2005.
- [17]. A. Y. Wang, S. H. Cho, C. Sodini, and A. Chandrakasan, "Energy efficient modulation and MAC for asymmetric RF microsensor systems", in *Proceeding of International Symposium Low Power Electronics Design*, August 2001, pp. 106-111.

- [18]. A. Ghaida, AL-Suhail, Khalid W. Louis, and T. Y. Abdallah, "Energy efficiency analysis of adaptive error correction in wireless sensor networks", *International Journal of Computer Science*, vol. 9, no 4 (2), 2012.
- [19]. N. A. Alrajeh, U. Marwat, B. Shams and S. S. H. Shah, "Error-correcting codes in wireless sensor networks: an energy perspective", *Journal of Applied Mathematics & Information Sciences*, vol. 9, no. 2, pp 809-818, 2015.
- [20]. C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks", *ACM Sensys*, pp. 162-175, 2004.
- [21]. H. Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, Lixia Zhang, "Self-securing Ad Hoc wireless networks", in *IEEE ISCC (IEEE Symposium on Computers and Communications)*, Italy, 2002.
- [22]. S. Alam and Debashis De, "Analysis of security threats in a wireless sensor network", *International Journal of Wireless & Mobile Networks*, vol. 6, no. 2, pp. 35-46, 2014.
- [23]. S. Y. Chen and S.F. Chang, "A review of smart living space development in a cloud computing network environment", *Computer Aided Design Applications*, vol. 6, pp. 513–527, 2009.
- [24]. B. Yuksekkaya, A. Kayalar, M. B. Tosun, M. K. Ozcan and Z. Alkar, "A GSM, Internet and Speech Controlled Wireless Interactive Home Automation System", *IEEE Transactions on Consumer Electronics*, vol. 52, no. 3, pp. 837–843, 2006.
- [25]. K. Yeol Lee and Jae Weon Choi, "Remote-Controlled Home Automation System via Bluetooth Home Network", *SICE Annual Conference. Fukui*, 2003, vol. 3, pp. 2824 –2829.
- [26]. F. Baig, Saira Beg and Muhammad Fahad Khan, "ZigBee based home appliances controlling through spoken commands using handheld devices", *International Journal of Smart Home*, vol. 7, no. 1, pp 19-26, 2013.
- [27]. R. Teymourzadeh, S. A. Ahmed, K. W. Chan, and M. V. Hoong, "Smart GSM based home automation system", in *IEEE Conference on Systems, Process & Control*, Kuala Lumpur, Malaysia, 13-15 December, 2013. (DOI: 10.1109/SPC.2013.6735152)
- [28]. A. Alheraish, "Design and implementation of home automation system", *IEEE Transactions on Consumer Electronics*, vol. 50, no. 4, pp. 1087-1092, 2004.

- [29]. M. Van Der Werff, X. Gui and W.L. Xu, "A mobile based home automation system, applications and systems", in *2nd International Conference on Mobile Technology*, Guangzhou. 15-17 November, 2005,
- [30]. F. Baig, S. Baig, and M. F. Khan, "Controlling home appliance remotely through voice command", *International Journal of Computer Applications*, vol. 48, no. 17, pp.1-5, 2012.
- [31]. Eddie M C Wong, "A phone based remote controller for home and office automation", *IEEE Transactions on Consumer Electronics*, vol. 40, no. 1, pp. 28-34, 1994.
- [32]. A. Napoleon, K. Karthik, M. Kamalakannan, M. Amarnath and A. Nidhin, "Implementation of Zigbee Based Home Automation System Using Voice Recognition", *International Journal of Engineering Research & Technology (IJERT)*, 2013, vol. 2, no. 5, pp. 723- 733.
- [33]. E. Irmak, A. Kose and G. Gocmen, "Simulation and ZigBee based wireless monitoring of the amount of consumed energy at smart homes", in *5th International Conference on Renewable Energy Research and Applications, Birmingham, UK*, 20-23 November 2016.
- [34]. O. M. Bader, Al-thobaiti, I.I.M. Abosolaiman, H. M. Mahdi, S.H. A. Almalki and M.S. Soliman, "Design and implementation of a reliable wireless real-time home automation system based on arduino uno single-board microcontroller", *International Journal of Control, Automation and Systems*, vol. 3, no. 3, pp. 11–15, 2014.
- [35]. A. R. Delgado, Rich Picking, Vic Grout, "Remote-controlled home automation systems with different network technologies", in *Proceedings of 6th International Network Conference (INC 2006)*, University of Plymouth, 11-14 July, pp. 357-366. (Retrieved from <http://www.newi.ac.uk/groutv/p5.pdf>).
- [36]. S. Wang, Y. Wang and M. Dai, "Development of monitoring system for thermal Energy consumption in intelligent Home", in *IEEE Chinese Automation Congress (CAC)*, China. 30 November to 3 December, 2018.
- [37]. T. V. Narkar, "Automatic dipper light control for vehicles", *International Journal of Research in Engineering and Technology*, vol.5, no.3, pp. 97-101, 2016.

- [38]. N. Maheswaran, K. Thamilan, P. S. Vijayakumar, D. Vadivel, "Automatic light- dim and dip control for automobiles", *International Journal of Engineering Trends and Technology (IJETT)*, vol. 29, no. 1, pp. 41-45, 2015.
- [39]. H. Sharma and Vibhav Kumar Sachan, "Performance analysis of modulation techniques for energy efficient wireless sensor networks", in *International Conference on Communication and Electronics (ICCE-2012)*, India, October 2012, vol. 1, pp.79.
- [40]. J. Abouei, N. Konstantinos, Plataniotis, and S. Pasupathy, "Green modulation in proactive wireless sensor networks", Technical report, September 2009, (available at <http://www.dsp.utoronto.ca/~abouei/>).
- [41]. F. M. Costa and Hideki Ochiai, "A comparison of modulations for energy optimization in wireless sensor network links", Department of Electrical and Computer Engineering, Yokohama National University Yokohama, Kanagawa 240-8501, Japan, December 2010.
- [42]. V. Pushpa, H. Ranganathan and M. Palanivelan, "BER analysis of BPSK for blocks codes and convolution codes over AWGN channel", *International Journal of Pure and Applied Mathematics*, vol.114, no.11, pp. 221-230, 2017(special issue).
- [43]. M. R. Islam, "Error correction codes in wireless sensor network: an energy aware approach", *World Academy of Science, Engineering and Technology*, vol. 61, pp. 26-31, 2010.
- [44]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on sensor networks", *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-114, 2002.
- [45]. J. H. Kleinschmidt, W. C. Borelli, "Adaptive error control using ARQ and BCH codes in sensor networks using coverage area information", in *IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, Tokyo, Japan, 13-16 September, 2009, pp. 1796-1800.
- [46]. Z. H. Kashani and M. Shiva, "Power optimized channel coding in wireless sensor networks using low-density parity-check codes", *The Institution of Engineering and Technology*, vol. 1, no. 6, pp. 1256-1262, 2007.
- [47]. M. R. Islam, J. Kim, "On the use of low-density parity check code for capacity and bit error rate sensitive wireless sensor network at Nakagami-n channel", *IETE Technical Review*, vol. 25, no. 5, pp. 277-284, 2008.

- [48]. C. C. Wang, G. N. Sung, J. M. Huang, L. H. Lee and C.P. Li, "A low power 2.45GHz WPAN modulator/demodulator", Elsevier, Microelectronics Journal, vol. 41, no. 2-3 pp.150–154, 2010. (available at www.elsevier.com/locate/mejo).
- [49]. N. Sadeghi, K. I. and S. Howard, "Analysis of error control code use in ultra-low-power wireless sensor networks", in *IEEE International Symposium on Circuits and Systems (ISCAS)*, Kos, Greece, December 2006, pp 3558-3561.
- [50]. M. Sartipi, F. Fekri, "Source and channel coding in wireless sensor networks using LDPC codes", in *Proceedings of IEEE Communications Society Conference Sensor and Ad Hoc Communications and Networks*, Santa Clara, CA, USA, October 2004. pp. 309-316.
- [51]. K. Sumathi and D. M. Venkatesan, "A survey on detecting compromised nodes in wireless sensor networks", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5, pp. 7720-7722, 2014.
- [52]. A. B. Karuppiah and S. Rajaram, "False misbehaviour elimination of packet dropping attackers during military surveillance using WSN", *Advances in Military Technology*, vol. 9, no. 1, pp 19-30, 2014.
- [53]. T. Arampatzis, J. Lygeros, and S. Manesis, "A survey of applications of wireless sensors and wireless sensor networks," in *Proceeding of IEEE International Symposium of. Intelligent Control*, vol. 1. Limassol, Cyprus: IEEE, June 2005, pp. 719–724.
- [54]. H. Luo, P. Zerfos, J. Kong, S. Lu, L. Zhang, "Self-securing Ad-Hoc wireless networks", in *Proceedings of the Seventh International Symposium on Computers and Communications (ISCC'02)*, Italy, 2002, pp. 567-574.
- [55]. W. Du, L. Fang, and P. Ning, "LAD: Localization anomaly detection for wireless sensor networks", in *19th International Parallel and Distributed Processing Symposium (IPDPS'05)*, Denver, Colorado, USA, April 4-8, 2005.
- [56]. I. M. Atakli, H. Hu, Y. Chen, W. S. Ku and Z. Su, "Malicious node detection in wireless sensor networks using weight trust evaluation", in *Symposium on Simulation of Systems Security (SSSS'08)*, Ottawa, Canada, April 2008, pp. 838-843.
- [57]. H. Hu, Y. Chen, W.-S. Ku, Z. Su and C.-H. J. Chen, "Weighted trust evaluation-based malicious node detection for wireless sensor networks",

- International Journal of Information and Computer Security, vol. 3, no. 2, pp. 148, 2009.
- [58]. K. P. Tuyaa and W. Okelo-Odongo, "Enhanced weighted Trust Scheme for detection of malicious nodes in Wireless Sensor Networks", International Journal of Computer applications (0975-8777), vol 155, no.4, pp. 34-38, 2016.
 - [59]. Rajkumar, Vani B. A., G. Rajaraman and H. G. Chandrakanth, "Security attacks and its countermeasures in wireless sensor networks", International Journal of Engineering Research and Applications, vol. 4, no. 10 (Part-1), pp. 04-15, 2014.
 - [60]. M. L. Messai, "Classification of attacks in wireless sensor networks", in *International Congress on Telecommunication and Application 14*, University of A. MIRA Bejaia, Algeria, April 2014, pp. 23-24.
 - [61]. R. R. Panda, B.S. Gouda, and T. Panigrahi, "Efficient fault node detection algorithm for wireless sensor networks", in *Proceeding International Conference of High-Performance Computation Application*, Bhubaneswar, Odisha, India, 2014, pp.1-5.
 - [62]. M. Panda and P.M. Khilar, "Energy efficient distributed fault identification algorithm in wireless sensor networks", Journal of Computer Network and Communication, pp.1-16, 2014.
 - [63]. D. I. Curiac, M. Plastoi, O. Baniyas, C. Volosencu and A. Doboli, "Combined malicious node discovery and self -destruction technique for wireless sensor network", in *IEEE 3rd International Conference on Sensor Technologies and Applications*, Athens, Glyfada, Greece 18-23 June, 2009, (10.1109/SENSORCOMM.2009.72)
 - [64]. D. I. Curiac, O. Baniyas, F. Dragan, C. Volosencu and Octavian Dranga, "Malicious node detection in wireless sensor networks using an autoregression technique", in *3rd International Conference on Networking and Services (ICNS-07)*, Athens, Greece, June 2007 (10.1109/ICNS.2007.79)
 - [65]. T. Sathyamoorthi, D. Vijayachakaravarthy, R. Divya And M. Nandhini, "A simple and effective scheme to find malicious node in wireless sensor network", International Journal of Research in Engineering and Technology, vol. 3, no. 2, 2014.
 - [66]. D. I. Curiac C. Volosencu, A. Doboli, O. Dranga and T. Tomasz, "Discovery of malicious nodes in wireless sensor networks using neural

- predictors”, WSEAS Transactions on Computers Research, vol. 2, no. 1, pp. 38-43, 2007.
- [67]. R. Akbani, T. Korkmaz, G.V.S. Raju, "A machine learning based reputation system for defending against malicious node behavior", in *Proceeding of the Global Communications Conference (GLOBECOM 2008)*, New Orleans, LA, USA, pp. 2119-2123. 1-5 December, 2008.
 - [68]. A. Abusitta, M. Bellaiche and Michel Dagenais, “An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment”, *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 7, no. 9, pp. 1-18, 2018. (<https://doi.org/10.1186/s13677-018-0109-4>)
 - [69]. I. Nicholas Sapankevych and R. Sankar, “Time series prediction using support vector machine: A survey”, *IEEE Computational Intelligent Magazine*, vol.4, no. 2, pp. 24-28, 2009. (10.1109/MCI.2009.932254)
 - [70]. R. Samsudin, A. Shabri, and P. Saad, “A comparison of time series forecasting using support vector machine and artificial neural network model”, *Journal of Sciences*, vol.10, no. 11, pp. 950-958, 2010.
 - [71]. Zakaria El Mrabet, Youness Arjoune, Hassan El Ghazi, Badr Abou Al Majd and Naima Kaabouch, “Primary User Emulation Attacks: A Detection Technique Based on Kalman Filter”, *Journal of Sensors and Actuator Networks*, vol. 7, no. 26, pp. 1-14, 2018,
 - [72]. C-L Lin, Y-M Chang, C-C Hung, C-D, Tu, and C-Y Chuang, “Position estimation and smooth tracking with a fuzzy-logic based adaptive strong tracking Kalman Filter for capacitive touch panel”, *IEEE Transactions on Industrial Electronics*, vol. 62, no. 8, pp. 5097-5108, 2015.
 - [73]. M.A. Caceres, F. Sottile, and M.A. Spirito, “Adaptive location tracking by Kalman Filters in wireless sensor network”, in *5th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, Marrakech, Morocco, 12-14 October, 2009, pp. 123-128.
 - [74]. C. Bell, C. Fausset, S. Farmer, J. Nguyen, L. Harley and W.B. Fain, “Examining social media use among older adults”, in *International Proceedings of 24th ACM Conference on Hypertext and Social Media*, Paris, France, May 2013, 1–3, pp. 158–163.

- [75]. P.N. Dawadi, D. J. Cook, M. Schmitter-Edgecombe and C. Parsey, “Automated assessment of cognitive health using smart home technologies”, *Journal of Technology and Health Care*, vol.21, no. 1, pp. 323-343, 2013. (doi: 10.3233/THC-130734)
- [76]. M. J. Rantz, G. Alexander, C. Galambos, A. Vogelsmeier, L. Popejoy, M. Flesner, A. Lueckenotte, C. Crecelius, M. Zwygart-Stauffacher, R. J Koopman., “Initiative to test a multidisciplinary model with advanced practice nurses to reduce avoidable hospitalizations among nursing facility residents”, *Journal of Nursing Care Quality*, vol. 29, no. 1, pp. 1-8, 2013.
- [77]. Place Lab MIT, Available online: http://web.media.mit.edu/~kl/A_PlaceLab_Sept1-2004.pdf (accessed on 10 January 2015).
- [78]. M. Heinz, P. Martin, J.A. Margrett, M. Yearn, W. Franke, H.I. Yang, J. Wong and C. K. Chang, “Perceptions of technology among older adults”, *Journal of Gerontological Nursing*, vol. 39, pp. 42–51, 2013.
- [79]. H.I. Yang, R. Babbitt, J. Wong and C. K. Chang, “A framework for service morphing and heterogeneous service discovery in smart environments”, *Impact Analysis of Solutions for Chronic Disease Prevention and Management. ICOST. Lecture Notes in Computer Science*, vol. 7251. Springer, Berlin, Heidelberg, 2012.
- [80]. R. Piyare and M. Tazil, “Bluetooth based home automation system using cell phone”, in *IEEE 15th International Symposium on Consumer Electronics*, June 2011, Singapore, pp. 192–195. (<http://dx.doi.org/10.1109/ISCE.2011.5973811>)
- [81]. H. B. Stauffer, “Smart Enabling System for Home automation”, *IEEE Transactions on Consumer Electronics*, vol. 37, no. 2, pp. 29-35, 1991.
- [82]. Baki Koyuncu, “PC Remote Control of Appliances by Using Telephone Lines”, *IEEE Transactions on Consumer Electronics*, vol. 41, no. 1, pp. 201-209, 1995.
- [83]. W. H. Kim, S. Lee, J. Hwang, “Real-time energy monitoring and controlling system based on Zigbee sensor networks”, *Procedia Computer Science*, vol. 5 pp. 794-797, 2011.
- [84]. V. S. Narayanan and S. Gayathri, “Design of wireless home automation and security system using PIC microcontroller”, *International Journal of Computer*

- Applications in Engineering Sciences, vol. 3 (Special Issue), pp. 135-140, 2013.
- [85]. Ahmad, A.W., Jan, N., Iqbal, S., Lee, C. "Implementation of ZigBee-GSM based home security monitoring and remote-control system", in *IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS), Seoul, Korea (South)*, 07 Aug -10 Aug 2011, pp.1-4.
 - [86]. P. S. Chinchansure and C. V Kulkarni, "Home automation system based on FPGA and GSM", in *International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 3-5 January 2014, pp. 1–5.
 - [87]. Indian Road Network.
(https://en.wikipedia.org/wiki/Indian_road_network#National_Highways).
 - [88]. NHAH (<http://www.nhai.org/roadnetwork.htm>).
 - [89]. Quora (<https://www.quora.com/Why-do-most-Indians-drive-with-high-beam-in-the-night-even-in-well-lit-roads>).
 - [90]. Troxler Effect (https://en.wikipedia.org/wiki/Troxler%27s_fading).
 - [91]. P. F. Alcantarilla, L. M. Bergasa, P. Jiménez, I. Parra, D. F. Llorca, M. A. Sotelo and S. S. Mayoral, "Automatic Light Beam Controller for driver assistance", *Machine Vision and Applications*, March 2011, DOI 10.1007/s00138-011-0327-y.
 - [92]. Y. L. Chen, "Night-time vehicle light detection on a moving vehicle using image segmentation and analysis techniques", *WSEAS Trans. Computer*, vol. 8, no. 3, pp. 506–515, 2009.
 - [93]. O'Malley, R., Glavin, M., E. Jones, "Vehicle detection at night based on tail-light detection", 1st International Symposium on Vehicular Computing Systems, 2008. Dublin
 - [94]. Blob Detection
([https://en.wikipedia.org/wiki/Feature_detection_\(computer_vision\)#Types_of_image_feature](https://en.wikipedia.org/wiki/Feature_detection_(computer_vision)#Types_of_image_feature)).
 - [95]. Local features detection and extraction techniques in MATLAB.
(<http://in.mathworks.com/help/vision/ug/localfeature-detection-and-extraction.html>).
 - [96]. S.B. Wicker, "Error control systems for digital communication and storage", vol. 1, Prentice Hall: Upper Saddle River, NJ, USA, 1995.
 - [97]. Lin, S. and Costello, D.J., "Error control coding", Prentice Hall: Upper Saddle River, NJ, USA, 2001.

- [98]. Symon Haykin, "Communication systems", 4th edition, John Wiley & Sons, USA 2001.
- [99]. J. G. Proakis, "Digital communications", 4th edition, New York: McGraw-Hill, New York, 2001.
- [100]. B. Sklar, "Digital communications fundamentals and applications", 2nd edition, Pearson Education Inc., New Jersey, USA, 2012.
- [101]. Shu Lin and Danial J. Castello, "Error control coding–Fundamentals and applications", 2nd edition, Pearson Education Inc., New Jersey, USA, 2004.
- [102]. H. Sharma, V.K. Sachan, "Optimization of energy efficiency in wireless sensor networks using error control codes", in *Students Conference on Engineering and Systems (SCES-2012)*, MNNIT, Allahabad, proceeding, March 2012, pp. 79. (Published on IEEE Explore digital library ISBN no. 978-1-4673-0456-6).
- [103]. T. S. Rappaport, "Wireless communications: Principles and practice", 4th edition, Prentice Hall, Upper Saddle River, NJ, USA, 2001.
- [104]. A. Hac, "Wireless sensor network design", John Willey & Sons, Ltd, Padstow, Cornwall 2003.
- [105]. Holger Carl and Andreas Willing, "Protocols and Architecture for Wireless Sensor Networks" John Willey and Sons Publication, Germany, 2005.
- [106]. Moteview 2.0 User Manual & Mica2 Datasheets
- [107]. "Qualnet"5.0 Scalable Network Technologies, Inc., <http://www.scalable-networks.com/qualnet>.
- [108]. MATLAB www.mathworks.com/simulink, R 2013.
- [109]. S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", in *CCS'03: Proceedings of 10th ACM Conference on Computer and Communication*, pp.62-72, October 2003. <https://doi.org/10.1145/948109.948120>.
- [110]. X. Liu and J. Shi, "Clustering routing algorithms in wireless sensor networks: An overview", *KSII Transactions on Internet and Information Systems*, vol. 6, no. 7, pp. 1735-755, 2012.
- [111]. O. Ghorbel, M.W. Jmal, M. Abid and H. Snoussi, "Distributed and efficient one-class outliers detection classifier in wireless sensor network," in *Proceedings of International Conference Wired/Wireless Internet Communications*, 2015, pp. 259-273.

- [112]. Nicholas I. Sapankevych and Ravi Sankar, "Time series prediction using support vector machine: A survey", IEEE Computational Intelligent Magazine, vol.4 no. 2 pp. 24-38, 2009. DOI 10.1109/MCI.2009.932254.
- [113]. R. Samsudin, A. Shabri and P.Saad, "A comparison of time series forecasting using support vector machine and artificial neural network model", Journal of Sciences, vol. 10, no. 11, pp. 950-958, 2010.
- [114]. T. Joachims, "Making large-scale SVM learning practical", LS8-Report, University of Dortmund, LS VIII-Report, 1998
- [115]. A.J. Smola and B. Scholkopf, "A Tutorial on Support Vector Regression", NeuroCOLT, Technical Report NC-TR-98-030, Royal Holloway College, University of London, UK September, 2003.
- [116]. S. Gunn, "Support vector machine for classification and regression", ISIS Technical report, 1998.
- [117]. S. Sutharan, M.Alzahrani, S. Rajasegarar, C. Leckie and M. Palaniswami, "Labelled data collection for anomaly detection in wireless sensor network", in *Proceeding of 6th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, Australia, 7-10 December, 2010, pp 269-274.
- [118]. <https://www.uncg.edu/cmp/downloads/lwsndr.html>
- [119]. K. Chelli, "Security issues in wireless sensor networks: attacks and countermeasures", in *Proceedings of the world Congress on Engineering, (WCE)*, London U.K. July 1-3, 2015.
- [120]. B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, On the survivability of routing protocols in Ad Hoc wireless networks", in *Proceedings of Secure Communication-05, IEEE*, 2005.
- [121]. A. Geetha and N. Sreenath, "Byzantine attacks and its security measures in mobile Ad Hoc networks", International Journal of Computing, Communication and Instrumentation Engg. (IJCCIE), vol. 3, no. 1, pp. 42-47, 2016.
- [122]. A. Geetha and N. Sreenath, "Cohen kappa reliability coefficient-based mitigation mechanism for byzantine attack in MANETS", International Journal of Applied Engineering, vol. 10, no. 9, pp. 23989-24001, 2015.

- [123]. S. Chaudhary, and R. Mehra, "Adaptive filter design and analysis using least square and least path norm", International Journal of Advances in Engineering and Technology, vol.6, no. 2, pp. 836-841, 2013.
- [124]. V. Vij, and R. Mehra, "FPGA based Kalman Filter for wireless sensor network", International Journal Computer Technology and Applications, vol 2, no. 1, pp. 155-159, 2011.
- [125]. S. J. Julier and J. K. Uhlmann, "New extension of the Kalman Filter to nonlinear systems," International Society for Optics and Photonics, pp. 182-193, vol. 4, 1997. <http://doi: 10.1117/12.280797>
- [126]. C-L Lin, Y-M Chang, C-C Hung, C-D, Tu, and C-Y Chuang, "Position estimation and smooth tracking with a fuzzy-logic based adaptive strong tracking Kalman Filter for capacitive touch panel", IEEE Transactions on Industrial Electronics, vol. 62, no. 8, pp. 5097-5108, 2015.
- [127]. M. A. Caceres, F. Sottile, and M.A. Spirito, "Adaptive location tracking by Kalman filters in wireless sensor network," in *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2009, pp. 123-128.
- [128]. Grayscale conversion algorithm.
(<http://in.mathworks.com/help/matlab/ref/rgb2gray.html#bui8mj-9>).
- [129]. C. Poynton, "Digital video and HD: Algorithms and Interface", 2nd edition, Morgan Kaufmann Publishers, USA, 2012.
- [130]. Halogen lamps(<https://www.which.co.uk/reviews/cars/artical/car-headlight-bulbs-explained>).
- [131]. Colour spectrum (<https://www.physics.sfasu.edu/astro/color/spectra.html>).
- [132]. Halogen lamp Spectrum
(https://en.wikipedia.org/wiki/Halogen_lamp#Spectrum).
- [133]. Thresholding in image processing.
([https://en.wikipedia.org/wiki/Thresholding_\(image_processing\)#Definition](https://en.wikipedia.org/wiki/Thresholding_(image_processing)#Definition))
- [134]. P. Forssén, D. Lowe, S-H Wang, "MSER region detectors",
(http://www.micc.unifi.it/delbimbo/wpcontent/uploads/2011/03/slide_corso/A34%20MSER.pdf).
- [135]. T. Lindeberg, "Discrete Scale-Space Theory and the Scale-Space Primal Sketch," Ph.D. thesis, Department of Numerical Analysis and Computing

Science, Royal Institute of Technology, S-100 44 Stockholm, Sweden, May 1991. (ISSN 1101-250.ISRN KTH NA/P--91/8--SE) (The grey-level blob detection algorithm is described in section 7.1).

- [136]. J. Matas, O. Chum, M. Urban and T. Pajdla, “Robust wide baseline stereo from maximally stable extremal regions”, in *British Machine Vision Conference (BMVC 2002)*, vol. 22 (BMVC Press 2002), 2002, pp. 384-393.
- [137]. MSER parameter meaning in open CV (<http://stackoverflow.com/questions/17647500/exact-meaning-of-the-parameters-given-to-initialize-mser-in-opencv-2-4-x>).
- [138]. Raspberry Pi documentation. www.raspberrypi.org.
- [139]. 5 Things you can't Do with raspberry Pi 2, (<http://www.makeuseof.com/tag/5-things-cant-raspberry-pi-2/>),
- [140]. Logitech webcam pro 9000, (http://support.logitech.com/en_us/product/webcam-pro-9000)
- [141]. USB gives you wings, (<http://www.raspberry-pi-geek.com/Archive/2013/01/Timely-tips-for-speeding-up-your-Raspberry-Pi>).

LIST OF PUBLICATIONS

Following are the publications in Journals and Conference out of this research work:

- [1]. **Bhavnesht Jaint**, S. Indu, Neeta Pandey, “Detection Techniques of Malicious Node in WSN: A Review”, Communicated on International Journal of Advance Science and Technology on June, 2020.
- [2]. **Bhavnesht Jaint**, S. Indu, Neeta Pandey. “Energy Efficient Communication Techniques for wireless Sensor Network” International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, no. 7, pp.1368-1373, May 2019.
- [3]. **Bhavnesht Jaint**, S. Indu, Neeta Pandey “Wireless sensor Network Based Controlling and Monitoring for Smart Homes using ZigBee” International Journal of Recent Technology and Engineering (IJRTE), vol. 7, no. 6, pp.1635-1641, March 2019.
- [4]. **Bhavnesht Jaint**, S. Indu, Neeta Pandey, Khushbu Pahwa, “Malicious Node Detection in Wireless Sensor Networks Using Support Vector Machine” 3rd International Conference on Recent Developments in Control, Automation & Power Engineering, (RDCAPE 2019), 10-11 October, 2019 U.P., India. (Scopus Index Conference).
- [5]. **Bhavnesht Jaint**, Vishwamitra Singh, S.K. Singh, P. Mittal, S. Indu, Neeta Pandey, “A novel approach for Detection of Malicious Nodes in WSN using Linear AR Prediction and Clustered Weighted Trust Evaluation”, ICSPVCE, 28-30 March 2019, Delhi.
- [6]. **Bhavnesht Jaint**, Priyesh, Ayush Mishra, S. Indu, Neeta Pandey “Extended Kalman Filtering Technique to detect Malicious Nodes in a WSN”, ICSPVCE, 28-30 March 2019, Delhi.
- [7]. **Bhavnesht Jaint**, Vishwamitra Singh, L. K. Tanwar, S. Indu, Neeta Pandey, “An Efficient Weighted Trust Method for Malicious Node Detection in Clustered Wireless Sensor Networks”, ICPEICES, 22-24 October, 2018, Delhi, India.

- [8]. **Bhavnesb Jaint**, Samdish Arora, Saksham Saxena, Chanpreet Singh, S. Indu, “Automatic Dipper System Using Camera in Vehicles” IEEE Region 10 Symposium (TENSYP) 14-16 July 2017, Cochin, India. DOI 978-1-5090-6255-3.