Wireless Sensor Networks for Nuclear Reactor Applications

By

S.A.V. Satya Murty

Reg. No: ENGG 02200704009

Board of Studies: Engineering Sciences

Indira Gandhi Centre for Atomic Research, Kalpakkam

A thesis submitted to the

Board of Studies in Engineering Sciences

in Partial fulfillment of requirements

for the Degree of

Doctor of Philosophy

of

HOMI BHABHA NATIONAL INSTITUTE, MUMBAI

July 2014

HOMI BHABHA NATIONAL INSTITUTE

Recommendations of the Viva Voce Board

As members of the Viva Voce Board, we certify that we have read the dissertation prepared by **S.A.V. Satya Murty** entitled "***Wireless Sensor Networks for Nuclear Reactor Applications***" and recommend that it may be accepted as fulfilling the dissertation requirement for the Degree of Doctor of Philosophy.

Date:

Chairman – Dr. M. Sai Baba

Date:

Guide/ Convener – Dr. T. Jayakumar, Dean, Engineering Sciences of HBNI at IGCAR

Date:

Member 1– Dr. B.K. Panigrahi

Date:

Member 2 – Prof. Krishna. M.Sivalingam

Date:

External Examiner – Dr. Swades De, Associate Professor, IIT Delhi.

Final approval and acceptance of this dissertation is contingent upon the candidate's submission of the final copies of the dissertation to HBNI.

I hereby certify that I have read this dissertation prepared under my direction and recommend that it may be accepted as fulfilling the dissertation requirement.

Date:

____

Guide/ Convener – Dr. T. Jayakumar, Dean, Engineering Sciences of HBNI at IGCAR

Date:

Place: Kalpakkam

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

(S.A.V.Satya Murty)

Kalpakkam

July, 2014

DECLARATION

I, hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree/diploma at this or any other Institution/University.

(S.A.V.Satya Murty)

Kalpakkam

July, 2014

Dedicated to

My Father

Late Shri S.V.S. Acharyulu

Acknowledgements

I express my deep sense of gratitude to Dr. Baldev Raj, Former Director, IGCAR for his invaluable guidance, encouragement and mentorship. Inspite of his very busy schedule, he always gave me time and constantly shown the direction. He is singularly responsible for me registering for the Ph.D by repeatedly advising me the value of it. I am always indebted to him for the care he has taken in nurturing me and the guidance given to me.

I am extremely grateful to Dr.P.R.Vasudeva Rao, Director, IGCAR for his constant encouragement, support and his keen interest in this topic and my work.

I am highly grateful to Prof. Krishna.M.Sivalingam, Professor, Computer Science Department, IITM, Chennai, for his constant guidance and very stimulating technical discussions. I am indebted to him for his encouragement and constant help.

I express wholeheartedly my gratefulness to Dr.T.Jayakumar, Convenor of the Doctoral Committee, Dean, Engineering Sciences of HBNI at IGCAR and to Dr.M.Sai Baba, Chairman of the Doctoral Committee for their invaluable support, guidance and constant encouragement. But for their constant interest, follow up and encouragement, this thesis would not have become a reality. I express my sincere gratitude to Dr.B.K.Panigrahi, Member, Doctoral Committee for his constant encouragement.

I am highly indebted and no words are sufficient for expressing my sincere thanks to my colleague Smt. Jemimah Ebenezer for her invaluable and constant support and very useful technical discussions.

I am highly thankful to my other colleagues Shri Sukant Kothari, Smt. D.Baghyalakshmi, Smt. G.Sandhya Rani, Kum. Vinita Daiya, Smt. R.Vijayalaxmi, Shri T.S.Shri Krishnan and other colleagues from Computer Division and colleagues from other Divisions for their help and useful technical discussions.

I express my sincere love and gratitude to my wife Smt.S.Rajeswari and my son Mr.S.Venkata Deepak for their understanding and support, throughout the period of this Ph.D work. Even when I deprived them of my time which rightfully belongs to them, they understood my pressures and stood by me giving enough strength. Because of my official work pressures, whenever I wanted to give up, my wife constantly goaded me and encouraged me saying that I can do it. I am highly grateful to her for her support. My son has shown a great understanding of me, always cooperated with me and never demanded my time or anything which allowed me to brood over in the house also, about the work I have to do and plan for it. I am highly grateful to my loving son for his understanding beyond his age.

I am grateful to my mother, brothers and sisters and other family members who understood my difficulties, whenever I skipped many important family functions and encouraging me by constantly enquiring the progress of my Ph.D work.

Table of Contents

CHAPTER 1

Introduction

CHAPTER 2

Experiments & Research Studies

CHAPTER 3

Development of WSN nodes, Software, WNMS

CHAPTER 4

Deployment in Nuclear Applications

CHAPTER 5

Analysis & Discussion

CHAPTER 6

CHAPTER 7

Abstract

Wireless Sensor Networks (WSN) is an emerging technology with a potential to revolutionize the way we sense and transmit the information. The applications are many and look to be limited by our imagination and ingenuity. Some of the important applications are process monitoring, military surveillance, structural health monitoring, environment monitoring, health monitoring, Nuclear, Biological and Chemical attack detection, Water and Pollution monitoring, flood detection etc.

The advantages of Wireless Sensor Networks over wired networks are many. Some of the advantages are, there are no wires for transmission of data. Hence there is no cable and cabling cost which constitute a considerable amount in any major application. Also there are no associated fire risks. Wireless Sensor Networks can be established very fast when compared wired networks. Thus large amount of time is saved in emergency situations like disaster and relief operations. Wireless Sensor Networks permit automatic reconfiguration of routing nodes. So, even if an intermediate routing node fails, the network automatically reconfigures and the data is transmitted to the base station. In wired networks in similar situations if a cable gets cut in between, the sensed signal information is lost which could be a safety signal thus effecting the safety of the plant. Thus wireless sensor networks have the potential of reducing the capital cost and increasing the safety of the plant.

Nuclear Power is a clean source of energy with no green house gas emissions and is required for energy security for countries like India. Having attained the required maturity in the design of the nuclear reactors, the designer is now concentrating on increased safety and reduced unit energy cost. Wireless Sensor Networks offer a potential solution for this. Hence "Wireless Sensor Networks in Nuclear Applications" was chosen as the topic of the research.

However Wireless Sensor Networks pose many challenges viz. low processing power, low memory, smaller range, lower battery life, security etc. However the advantages outweigh the challenges that they have to be met with focused R&D. This thesis is a narration of the efforts made in research to find the suitability of the wireless nodes in various radiological laboratories which are made of thick concrete walls. As the ranges in specially constructed nuclear facilities are different and cannot be taken as the data sheet value, or they can be mathematically modeled it was decided to conduct various experiments in the actual environment to find achievable ranges and the feasibility of establishing WSNs in the nuclear facilities. Accordingly experimental studies were carried out in WSN Laboratory, Computer Centre, Radio Chemistry Laboratory and Fast Breeder Test Reactor by using the commercially available nodes to measure the ranges in different environments such as radiological laboratories, lead mini cells, hot cells etc. to measure the temperature, humidity, radiation level etc. Also experiments were conducted to know the life of batteries when the sensed signal is monitored for every second, every two seconds, every five seconds etc. Through these experimental studies it was observed that the commercially available nodes are not suited for establishing wireless sensor networks in nuclear facilities.

Hence after extensive research efforts, different types of wireless sensor nodes were designed inhouse and developed. The Sensor Node is based on ARM 7 architecture based LPC 2138 microcontroller with XBee transceiver and 230 V AC mains power supply. This node is extensively used in various deployments. As this node has limited processing power, the cluster node based on CORTEX M3 based LPC 1768 microcontroller and RF 230 transceiver and 230 V AC mains power supply was developed. The complete software stack that supports Zigbee standard was developed and incorporated in the nodes. The router nodes do not require much processing power and they are required in larger numbers. Hence to reduce the cost they are designed based on XBee controller with 230 V AC mains. Base Station node is developed on XBee controller along with USB port to connect it to a PC. The actuator node which raises the alarm when required by the base station is also designed and developed based on XBee controller, hooter and 230 V AC Mains supply. All the nodes have been thoroughly tested and deployed for longer duration to test its smooth working.

The Wireless Sensor Networks being established in various Nuclear Reactor applications have to be very robust under varying harsh environments. It was realized that the nodes have to be industrial grade to work in harsh non A/C, field environment. Accordingly all these nodes have been designed and developed with IP 54 compliant enclosures, industrial grade electronics components to withstand higher temperatures. Also the Printed Circuit Boards were designed with the tools to meet EMI/EMC standards.

Till date no literature is published or available to find the viability of WSNs in Nuclear Reactors for measuring various reactor parameters, anywhere in the world. Hence after the nodes were designed and tested, the research was continued to get first hand knowledge by establishing multiple Wireless Sensor Networks at Indira Gandhi Centre for Atomic Research for establishing their suitability to use in Nuclear Facilities. To start with a WSN was deployed in the computer centre for monitoring temperature and humidity of high performance cluster computer systems. Later it was expanded to all the facilities in computer centre This network is working smooth for the last two years.

A WSN was established at IN SOdium Test facility (INSOT), a facility made for testing the creep and fatigue properties of various nuclear materials in sodium environment, for detecting the sodium leaks (Sodium is the coolant in Fast Breeder Reactors). Initially a WSN was established for detecting nine signals. After the network was successfully tested for six months, the network had been expanded to cover fifty sodium leak detection signals. This is a fifteen noded WSN consisting of thirteen sensor nodes, a base station and an actuator node. Incase of a leak the base station sends the signal in wireless mode to the actuator node which switches on the hooter to draw the attention of the operator in control room. The network is working very well for the last one year.

Another WSN was established in SADHANA, a scaled down model of Safety Grade Decay Heat Removal System used in Prototype Fast Breeder Reactor to test the decay heat removal capacity in station blackout conditions. This network measures the temperature and humidity of air at outlet chimney in 11th floor, air at inlet chimney in the 5th floor and base station in the control

room in second floor. The parameters are displayed in graphical user interface developed using Lab VIEW. The network is working satisfactorily for the past sixteen months.

After getting enough experience with the nodes and designing and establishing the wireless sensor networks, a seven noded wireless sensor network was established to measure various temperature parameters of Non Nuclear Safety Signals in reactor containment building in Fast Breeder Test Reactor. After successful operation for few months a twenty five noded network was established covering various buildings of Fast Breeder Test Reactor corresponding to twelve temperature signals, seven vibration signals, two flow rate signals and with base station in the control room. The network is working very satisfactorily for the last few months.

For the deployed networks, the performance analysis has been done for throughput, packet drop ratio, packet delivery ratio, effect of interference and battery backup duration. Throughput experiments were conducted for 15 byte and 66 byte payload for varying transmission rates, with and without security enabled. Packet delivery ratio was measured for twenty five noded network and found to be 100% for transmission rates of 680 milli sec. and above. The through put was also measured and found to be 26.64 Kbps for a tolerance of 2.5% packet loss.

As part of the future work it is planned to design the wireless sensor nodes with radiation hardened components to measure parameters even in an incident conditions, establish multiple large networks in different channels of the ISM band concurrently and see the performance, develop light weight real time routing protocols etc. Also it planned to monitor various safety related parameters of the reactor over a long period and prove the network's robustness after getting the approval from regulatory authorities.

With the experience gained in successful experimentation, design and development of nodes and very successful deployment of multiple wireless sensor networks in various nuclear facilities including Fast Breeder Test Reactor and various performance measurements, the thesis concludes that wireless sensor networks are a viable solution in nuclear facilities.

Acronyms

ADC	Analog to Digital Converter
APTEEN	Adaptive Periodic Threshold sensitive Energy Efficient sensor Network
AES	Advanced Encryption Standard
AHX	Air Heat Exchanger
ASICs	Application Specific Integrated Circuits
AMCA	Asynchronous Multi-Channel Adaptation,
APS	Application Support
API	Application Programming Interface
BPSK	Binary Phase-Shift Keying
CWPAN	Chinese Wireless Personal Area Network
CBC-MAC	Chaining Message Authentication Code
CMOS	Complementary metal–oxide–semiconductor
CADR	Constrained Anisotropic Diffusion Routing
DAC	Digital to Analog Converter
DLL	Data Link Layer
DSME	Deterministic and Synchronous Multi-channel Extension
DHX	Decay Heat Exchanger
DSSS	Direct Sequence Spread Spectrum
ECG	Electro Cardiogram Sensor
EEG	Electro Encephalogram Sensor
EPRI	Electric Power Research Institute
FBTR	Fast Breeder Test Reactor

GPS	Global Positioning System
GUI	Graphical User Interface
IDSQ	Information-Driven Sensor Querying
HART	Highway Addressable Remote Transducer Protocol
HPC	High Performance Computing
ISM	Industrial, Scientific and Medical band
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
IEEE	Institute of Electrical and Electronics Engineers
ISP	In-System Programming
IAP	In-Application Programming
INSOT	IN Sodium Test facility
IETF	Internet area of Internet Engineering Task Force
I^2C	Inter-Integrated Circuit
KbPS	Kilo bits Per Second
KSPS	Kilo Samples Per Second
LQI	Link Quality Indication
LR-WPAN	Low Rate Wireless Personal Area Network
LLDN	Low Latency Deterministic Networks
LEACH	Low Energy Adaptive Clustering Hierarchy
Lab VIEW	Laboratory Virtual Instrumentation Engineering Workbench
MEMS	Micro Electro Mechanical Systems
MAC	Media Access Control
µTESLA	Micro version of Timed, Efficient, Streaming, Loss tolerant Authentication protocol
NBC	Nuclear, Biological and Chemical
O-QPSK	Offset- Quadrature Phase Shift Keying
PEGASIS	Power-Efficient GAthering in Sensor Information Systems
PFBR	Prototype Fast Breeder Reactor
PSSS	Parallel Sequence Spread Spectrum
RAM	Random-Access Memory

RF	Radio Frequency
RFID	Radio Frequency Identification Blink
RCL	Radio Chemistry Laboratory
RCB	Reactor Containment Building
RSSI	Received Signal Strength Indicator
RTD	Resistance Temperature Detector
RTQ	Routing Table Query
SADHANA	SAfety Grade Decay Heat removAl loop in Natrium
SNEP	Sensor Network for Encryption Protocol
SPIN	Sensor Protocol for Information via Navigation
SPI	Serial Peripheral Interface
SSP	Simple Security Protocol
TSCH	Time Slotted Channel Hopping
TEEN	Threshold sensitive Energy Efficient sensor Network
TSMP	Time Synchronized Mesh Protocol
UART	Universal asynchronous receiver/ transmitter
USB	Universal Serial Bus
VLSI	Very-Large-Scale Integration
WSN	Wireless Sensor Networks
WPAN	Wireless Personal Area Network
WIA-PA	Wireless network for Industrial Automation—Process Automation
WNMS	Wireless Network Management Station
X-CTU	X-Configuration and Test Utility
ZDO	Zigbee Device Objects

List of Figures

List of Tables

CHAPTER 1

1. Introduction

This chapter gives a brief introduction about the Wireless Sensor Networks (WSN) from the literature survey. It covers introduction about WSNs, their advantages, the applications, the challenges, architecture of WSN node, the commercial nodes available, various routing and security protocols and the international WSN standards.

1.1. Wireless Sensor Networks

Recent advances in Micro Electro Mechanical Systems (MEMS), tiny micro controllers, wireless technology have enabled the development of low cost, low power, multifunctional miniature sensor devices that can operate together in the form of a wireless sensor network and transmit the information of the sensed parameters about the physical environment being monitored in a wireless mode to the base station [1]. These nodes can sense, compute and communicate untethered for short distances. When deployed in large numbers in a sensor field, these sensors can automatically organize themselves in to an ad hoc multihop network to communicate with each other and with the sink node.

A US National Research Council report titled *Embedded Everywhere* mentions that the use of such networks “could well dwarf previous milestones in the information revolution” [2]. Wireless sensor networks provide an interface between the virtual world of information technology and the real physical world. They represent a fundamental paradigm shift between traditional wireless data communications to process communication.

These wireless sensor networks have many advantages viz. they do not require cables to transmit the sensed information. Hence there is no cable cost and cabling cost [3]. Also it removes the cable associated fire hazards [4][5]. WSNs can be very easily deployed in a short time. Because of their ability to reconfigure automatically, the sensed data is still transmitted to the base station even when in an intermediate routing node fails. The total cost will be much less when Wireless Sensors Nodes are employed in large numbers to sense about the physical environment being monitored. Hence the use of this technology appears to be limited only by our imagination and ingenuity. It is foreseen that the technology will be used for various applications sooner than later.

1.1.1. Applications

The wireless, small size and low cost nature of WSN nodes can provide significant advantages over other networks. In these, measurements can be taken from very close to the phenomenon and this finds potential applications of WSN in various hazardous areas where human presence is not recommended viz. radiation monitoring, explosive detection, military surveillance etc. In addition, domains like industrial process monitoring, environmental monitoring, structural monitoring, and health monitoring, forest fire detection, flood detection etc. are some of the other potential applications of WSN [6].

Process Monitoring

Process monitoring is the process of monitoring the condition, state or value of the output of a sensor and process the parameter by comparing it with a threshold value and take appropriate control action. Wireless sensor networks are capable of monitoring or controlling the systems to which they are coupled and have seen increased requirement in industrial applications over recent years [6][7].

For example, in reactor environment, for a given power, the speed of the primary pump which enables coolant to flow in the core to remove the heat out of the subassemblies is maintained constant to maintain the outlet temperature of the coolant. This is a process. Incase the outlet temperature crosses the threshold by 5 degrees the process has to give an alarm and if the temperature crosses by 10 degrees it has to shutdown the reactor. Similarly, for a given power, the outlet temperature of the steam out of the steam generator has to be maintained constant. To enable this, based on the outlet temperature of the secondary system, the feed water flow has to be controlled. This is another process where the outlet temperature of the steam out of the steam generator, secondary outlet temperature are measured and compared against respective thresholds and the control action of feed water flow control is done. Also, all information connected with the complete process is archived for future reference when a review of process trends could provide additional information. By utilizing WSN technology, sensing nodes will communicate sensed parameters wirelessly with the base station and the base station processes the sensed parameters and gives the commands to the controlling node wirelessly.

WSNs bring several advantages over traditional wired industrial monitoring and control systems. Without the wiring constraints, devices can be utilized in applications that are previously either physically unreachable or wiring is cost prohibitive. Furthermore, the industrial process system becomes highly scalable and flexible due to the device autonomy. For example, devices can be easily relocated and reorganized without tedious work of removing old cables and laying out new ones. In addition, newly added devices can be installed at any location without running data communication wires through concrete walls during factory expansion.

Military Surveillance and Target Tracking

The emergence of WSN originally started with military related research and it culminated in numerous applications in military. It can be used for detecting the enemy’s objects and their tracking, monitoring the friendly forces and their movement, battle field surveillance and battle damage assessment, reconnaissance of opposing forces and terrains, detecting the Nuclear, Biological and Chemical (NBC) attacks [8].

WSN can be used for detecting the enemy's objects like tank, truck, jeep etc. and its direction of travel, speed with which it is moving. This requires target detection, classification and tracking. The military commanders would also be interested in knowing the status of their own troops, the condition and the availability of the equipment and ammunition in the battle field. This is easily achieved through WSN. Every troop, vehicle, equipment and critical ammunition can be attached with a small sensor node that reports the status. These reports are gathered from the sensor nodes by the base station and sent to the commanders. The data can also be forwarded to the higher levels of the command hierarchy while being aggregated with the data from other units at each level.

WSN can be deployed in critical terrains where the opposing forces are moving and some valuable, detailed and timely intelligence can be gathered about the opposing forces and the terrain within minutes before opposing forces occupy the area and intercept them. WSN can also be used for battlefield surveillance by deploying the sensor nodes in the critical terrains, approach routes, paths etc. and it helps in monitoring the movements of the opposing forces. By deploying the Wireless nodes with proper sensors, the information regarding the NBC attacks can be found at the earliest and through proper action the casualties can be drastically reduced.

Environmental Monitoring

WSN can be used for habitat monitoring, precision farming, disaster management, home applications and many more. The habitat of the small birds, insects and animals can be studied by deploying the wireless sensor networks at their habitation. This study helps the researchers to findout their living conditions, tracking their movements and understanding the most favorable condition for breeding. The small sized wireless sensor nodes can be deployed very close to their place and their habitat can be studied without human intervention [9].

Precision farming is used to monitor the soil condition that helps in increasing the yield of the crop. The sensor nodes are embedded in the field at required places to give the complete analysis of the soil type, soil condition, water level etc. to decide the amount of fertilizers to be used and required pesticides level, etc. to maximize the yield.

Every year torrential rains are resulting in floods and subsequent damage to life and property. The unfortunate thing is that the people in the upstream are aware of the raising levels of the river, but the people in downstream do not come to know till the floods hit them. A flood warning system with wireless sensor network using steam gauges, rain gauge sensors help in alerting the people in time and thus reducing loss of life and damage to property.

Every year many square kilometers of forests are destroyed in fire. If the fire can be detected at an early stage and communicated to the people concerned, these natural resources can be saved. Sensor nodes that measure heat or smoke can be used to detect the fire and can be wirelessly connected to the authorities concerned for remedial action.

Water and air pollution are of great concern to all the people. The wireless sensor networks are used for measuring the quality of water in the reservoirs, from where the water is supplied to the people for drinking and transmit the information to the authorities. Also, it can be used for measuring the air pollution levels at different locations.

Structural Health Monitoring

Extreme events like earthquakes, fire accidents may cause enormous damage to the health of the civil structures without producing any apparently visible damage. Such damage can result in life threatening conditions evolving in the structure either in the immediate aftermath or long after the actual event has happened. The structural monitoring of civil structure and appropriate corrective action reduces the loss of human lives by warning about hazardous structures and impending collapses and provide the required information to the disaster management teams to evacuate the people from and near the structures. In addition to extreme events, the civil structures will undergo normal wear and tear due to corrosion, fatigue etc. thus reducing the operational life. This happens for the buildings, road bridges, rail bridges etc., and an early warning system will help in reducing the effects of the damage to the civil structure. Wireless Sensor Networks with sensor nodes equipped with vibration monitoring, acceleration, linear displacement, strain and angular displacement sensors can help in finding the soundness of the structure and alert the concerned, if required [8][9]. Wired networks are not suitable for these applications as any collapse would snap the wires and make the system inoperational.

Health Monitoring

Wearable Health Monitoring Systems allow an individual to closely monitor changes in his or her vital signs and provide feedback to help maintain an optimal health status. If integrated into a networked system, these systems can even alert medical personnel when life threatening changes occur. In addition, patients can benefit from continuous long term monitoring as part of a diagnostic procedure, can achieve optimal treatment to chronic conditions or can be supervised during recovery from an acute event or surgical procedure. If wired sensors are used, the wires may limit the patient’s activity and level of comfort. Wearable wireless sensor nodes provide the benefit of monitoring without causing much discomfort contributed through the hanging wires. Each sensor node can sense, sample and process one or more physiological signals. For example, an electro cardiogram sensor (ECG) can be used for monitoring heart activity, an electro encephalogram sensor (EEG) for monitoring brain activity, a blood pressure sensor for monitoring blood pressure, a breathing sensor for monitoring respiration etc. The data from all these sensor nodes is transmitted wirelessly to the doctor for continuous monitoring and health care [10].

Home Automation

The home appliances like refrigerator, washing machines, microwave oven etc. can be embedded with smart sensors and these sensors can communicate with each other and also with the external networks through Internet. Hence it is possible to operate these devices wirelessly from anywhere in the world through networks [9-11].

1.1.2. Challenges

In spite of the diverse applications, sensor networks pose a number of unique technical challenges due to the following reasons [12][13]:

Limited Processing Power: As the wireless sensor nodes are designed around low end microcontrollers, have a limited processing power. Hence they cannot do much processing on the sensed data and they transmit the data to the cluster head or to the base station for further processing. Again they cannot execute complex security algorithms.

Limited Memory: Again for the same reason that the wireless sensor nodes are designed around low end micro controllers to keep the power consumption low and cost less, they have a very limited memory. Hence the nodes can only support a low foot print operating system and store limited sensed data. Also they cannot store complex security algorithms.

Limited Range: The wireless sensor nodes are designed with low power transceivers. So, their range is limited. The nodes placed indoors have a still limited range.

Low power: The wireless sensor nodes are designed normally with two AA batteries. So they have to conserve their power to have a longer life.

Ad hoc deployment: Most sensor nodes could be deployed in regions which have no infrastructure at all. A typical way of deployment in a forest for forest fire detection would be tossing the sensor nodes from an aero plane. In such a situation, it is up to the nodes to identify and establish its connectivity and distribution.

Network Discovery and Organization: Due to the large scale of WSNs, each sensor node behaves based on its local view of the entire network, including topology and resource distribution. Here, resources include battery energy and sensing, computation, and communication capabilities. To establish such a local view, techniques such as localization and time synchronization are often involved. A local view depends on the initial deployment of sensor nodes, which is itself a challenging topic. The network is usually organized using either a flat or hierarchical architecture, above which topology control, MAC, and routing protocols can be applied accordingly.

Unattended Operation: In most cases, once deployed, sensor networks have no human intervention. Hence the nodes themselves are responsible for reconfiguration in case of any changes. It is required that a sensor network system be adaptable to changing connectivity (for e.g., due to addition of more nodes, failure of nodes etc.) as well as changing environmental stimuli.

Energy-Efficient Design: Once deployed, it is often not feasible to re-charge or replace the batteries of the sensor nodes. Thus, energy conservation becomes crucial for sustaining a sufficiently long network lifetime. Among the various techniques proposed for improving energy-efficiency, cross-layer optimization has been realized as an effective approach. Due to the nature of wireless communication, one performance metric of the network can be affected by various factors across layers. Hence, a holistic approach that simultaneously considers the optimization at multiple layers enables a larger design space within which cross-layer tradeoffs can be effectively explored.

Data-centric Paradigm: The operating paradigm of WSNs is centered on information retrieval from the underlying network, usually referred to as a data-centric paradigm. Compared to the address-centric paradigm exhibited by traditional networks, the data-centric paradigm is unique in several ways. New communication patterns resemble a reversed multicast tree. In-network processing extracts information from raw data and removes redundancy among multiple source data. The development of appropriate routing strategies that take the above factors into consideration is challenging.

Robustness: The vision of wireless sensor networks is to provide large scale, yet fine-grained coverage. This motivates the use of large numbers of inexpensive devices. However, inexpensive devices can often be unreliable and prone to failures. Rate of device failures will also be high whenever the sensor devices are deployed in harsh or hostile environments. Protocol designs must therefore have built-in mechanisms to provide robustness. It is important to ensure that the global performance of the system is not sensitive to individual device failures. Further, it is often desirable that the performance of the system degrade as gracefully as possible with respect to component failures.

Security: Since WSNs may operate in a hostile environment, security is crucial to ensure the integrity and confidentiality of sensitive information. To do so, the network needs to be well protected from intrusion and spoofing. The constrained computation and communication capabilities of sensor node make it unsuitable to use conventional encryption techniques. Lightweight and application-specific architectures are preferred instead.

Thus, unlike traditional networks, where the focus is on maximizing channel throughput or minimizing node deployment, the major consideration in a sensor network is to extend the system lifetime as well as the system robustness.

1.1.3. Architecture of WSN Node

The typical hardware of wireless sensor node consists of a sensing unit, processing unit, memory unit, radio unit and a power supply unit. The optional units that are present in some nodes specific to the application are location finding unit, power scavenging unit and actuator [13][14]. Fig.1 explains the connectivity of the key components of a sensor node.

Sensing Unit

The main purpose of wireless sensor network is to sense the environmental parameters. Due to bandwidth and power constraints, only low-data-rate sensors are mostly used by WSN nodes. Multi-modal sensing is an advanced feature which includes several sensors on the board of a single node. For example, the common sensors like temperature sensor, humidity sensor, light sensor and acoustic sensors may be present in the same sensor board. The sensing area of a sensor node depends on the type of physical sensors used on that node.

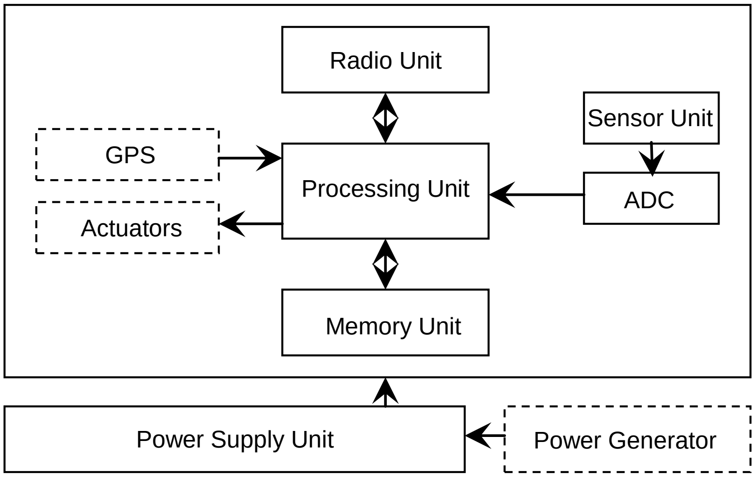


Fig. 1 Typical Sensor Node

Processing Unit

Usually it is a low power embedded processor which is aimed to do limited processing on the sensed data. The most suitable processing unit for sensor node is microcontroller. They perform tasks, process data and control the functionality of other components in the node. Alternatives that can be used as a processing unit are: microprocessor of ordinary PC, Digital Signal processors, or ASICs (Application Specific Integrated Circuits). The embedded processors are often used significantly for the processing unit. However, it should be noted that a sensor network may be heterogeneous and includes at least some nodes with comparatively greater computational power.

Memory Unit

Since the physical dimensions of the sensor node is an important factor for many applications, it is necessary to keep the node size as small as possible. Another factor is the cost constraints. To reduce the node cost, the memory is being limited. Most of the sensor nodes are designed with very little memory for processing; usually a few Kilo bytes of RAM as program memory for executing instructions and few more Kilo bytes of flash memory as data memory for storing the collected and processed data. Due to the technology improvements, the memory capacity is likely to improve over time.

Radio Unit

The Industrial, Scientific and Medical band (ISM) which gives free radio, huge spectrum allocation and global availability is being utilized by wireless sensor networks. The various choices of wireless transmission media are Radio frequency, Optical communication (Laser) and Infrared. Among these, RF based communication in the range of 2.4 GHz is the most suitable communication for many WSN applications worldwide. Generally the radio unit is being operated in three different modes ie. Transmit, Receive, and Sleep. The power consumed in transmit mode is much higher. In receive mode, the power consumption is also high when compared to that of sleep mode and hence usually the radios will go to sleep mode if there is no data to transmit.

Power Supply Unit

The usual form of power source for sensor node is battery. The lifetime of sensor node typically exhibits a strong dependency on battery life. Batteries provide energy for Sensing, Communication and Data Processing. More energy is required for data communication in sensor node and hence the communication must be made as less as possible. In many applications, the wireless sensor node has been deployed in such an unreachable terrain that replenishment of battery may be limited or impossible altogether. Most commercial nodes use two AA alkaline cells or one Li AA cell.

Location finding Unit

For the sensor networks, which are being placed, for outdoor measurements or monitoring, it is necessary to identify the location of the sensor. Otherwise the data will become useless. For example, if a sensor is identifying an adverse activity in its monitoring area, it should alert the sink or controlling station. The information should be the location where the adverse activity is happening and the type of activity according to its classification. Hence, based on the application requirement, some nodes may have location-finding unit. Usually it'll have the ability to communicate to the satellite to get the GPS information. However, even in such applications, only a fraction of the nodes may be equipped with GPS capability, due to cost constraints.

Actuators

Instead of simply sensing the various parameters, it is always good if provision is made for the operators to activate control signals based on the monitored information depending on the process being monitored. For such scenarios, the actuators are deployed along with the sensor nodes. They are the units which will perform the control actions based on the commands from the sink or the control station. This is a new requirement from the perspective of sensor network. The energy requirement is high for the actuators and the protocol for sending command from the sink is different from receiving data from the sensors to the sink. Such modifications shall be incorporated in hardware and software before implementing actuators in sensor network.

1.1.4. Commercial Nodes

Systems for remote sensing have existed for decades, but recent development in microelectronics and VLSI technology led to development of small sensor nodes. Earlier prototypes sensor nodes can be attributed to Smartdust project and NASA's sensor web project. The main characteristic of these developments were integrated radio and processing units with commercial off the shelf sensors. These developments led to different research programs in universities. Earlier prototypes use 8 bit microcontroller with monolithic radio transceiver. Advent of IEEE 802.15.4 standard and availability of compliant radios led to standardization of radio transceiver. Some of the commercially nodes are described below:

Mica Family of Motes

Mica family of nodes was one of the earliest prototypes of modern WSN nodes. It is initially developed at University of Berkeley and then taken up by Crossbow inc. and later by Memsic inc. This family contains 4 types of nodes namely- Mica [15], Mica2 [16], Mica2dot [18] and MicaZ [19]. IRIS [20] mote is the upgraded version of MicaZ mote with three times the radio range and twice the program memory. All these nodes are based on Atmel 8 bit microcontrollers with different type of transceivers. These nodes contain the logger flash for storing the measured data and provide 18/51 pin expansion connector, which supports analog inputs, digital I/O, SPI and UART interfaces. Other than to connect the variety of external peripherals, this connector is also useful in programming the sensor boards with the help of programming board. These motes are generally powered by two 1.5V AA industrial batteries. The general architecture of this family of nodes is shown in Fig. 2(a) and the images are shown in Fig. 3.

Cricket [21] is another variation of Mica2 node, which is developed at MIT as an indoor location system. It uses ultrasonic transmitter and receiver for sending and receiving pulses and then compares with the RF pulse transmission. This comparison establishes the difference of time of arrival and computes the distance between two coordinating nodes. Architecture for cricket mote is shown in Fig. 2(b).

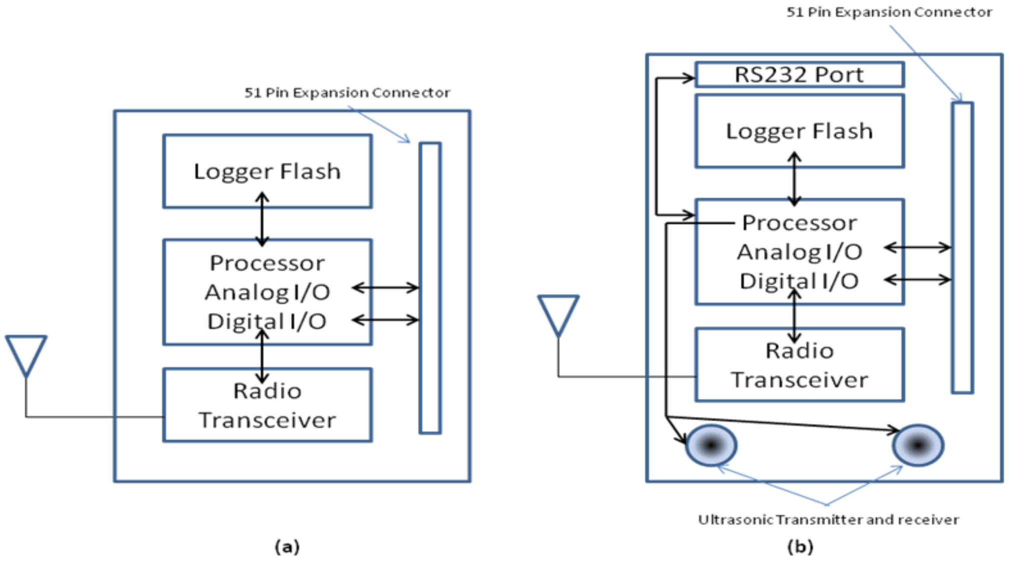


Fig. 2 (a) General Architecture and (b) Modified architecture of Cricket Motes

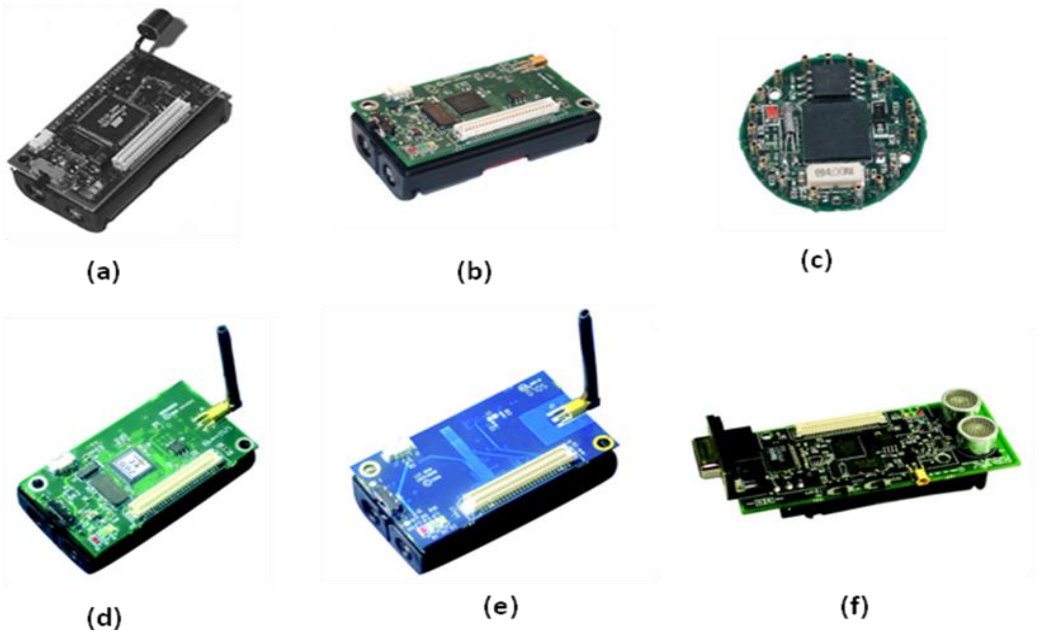


Fig. 3 Mica Family of motes:

(a)Mica, (b)Mica2, (c)Mica2dot, (d)MicaZ, (e)IRIS and (f)Cricket mode

Specifications of these nodes are compared in the table 1.

Table 1. Comparison of Mica Family of Nodes

	Mica [15]	Mica2 [16] [17] and Cricket [21]	Mica2dot [17] [18]	MicaZ [19]	IRIS[20]
Microcontroller	Atmega103L 4 MHz 8-bit CPU	Atmega128L, 7.3827 MHz 8 bit CPU	Atmega128L, 4 MHz 8 bit CPU	Atmega 128 8 - 16 MHz, 8 bit CPU	Atmel Atmega1281, 8 - 16 MHz, 8 bit CPU
Transceiver	RFM TR1000[22]-115 Kilobits per second and 916.5 MHz ASK	TI CC1100 [23]-38.4 K baud 315 / 433 / 868 and 915 MHz FSK	TICC1100- [23] 38.4 K baud 315 / 433 / 868 and 915 MHz FSK	TICC2420 [24], 250 Kbps, 2.4 GHz, IEEE 802.15.4 compliant	AT86RF230 [25]250 Kbps, 2.4 GHz, IEEE 802.15.4 compliant
Memory	128 KB flash program memory, 4 KB static RAM and 512 KB external memory	128KB Flash program memory, 4KB SRAM And 512K EEPROM	128KB Flash program memory, 4KB SRAM And 512K EEPROM	128 KB flash program memory, 4 KB static RAM and 512 KB external memory	128 KB flash program memory, 8 KB static RAM and 512 KB external memory

Different types of sensor and data acquisition boards have been developed for these nodes. Details of these sensor nodes are given in Table 2.

Table 2. Details of Sensor Boards

Name	Nodes Supported [26]	Sensor and Data acquisition details
MTS101	Mica, Mica2, MicaZ, IRIS	Light and temperature sensor with prototyping area
MTS300CA / MTS310CA	Mica, Mica2, MicaZ, IRIS	Light, temperature, microphone and buzzer MTS310 contains additional accelerometer and magnetometer
MTS400CA / MTS420CA	Mica2,MicaZ,IRIS	Relative Humidity, ambient light, temperature, pressure, accelerometer MTS420 has additional GPS module
MTS500CA/ MTS510CA	Mica2dot	Light, microphone and accelerometer
MDA300A	Mica, Mica2, MicaZ, IRIS	Light, humidity and provision for external sensors
MDA500A	Mica2dot	Prototyping area
MDA420A	Mica, Mica2	Tachometer input and RPM measurement

Telos Mote

Telos series of motes are developed by Moteiv. These nodes use MSP430 microcontroller because of its low power consumption in both sleep and active modes, faster wake-up time and relatively low operation voltage. The radio transceiver used in Telos motes is TI CC2420, which uses 2.4 GHz ISM band and compliant with IEEE 802.15.4. There are four versions of these motes, with same specifications (microcontroller and RF transceiver wise) but different form factors, namely Tmote, Tmote Sky (telosb), Tmote mini and Tmote mini Plus. These nodes are shown in fig.4.

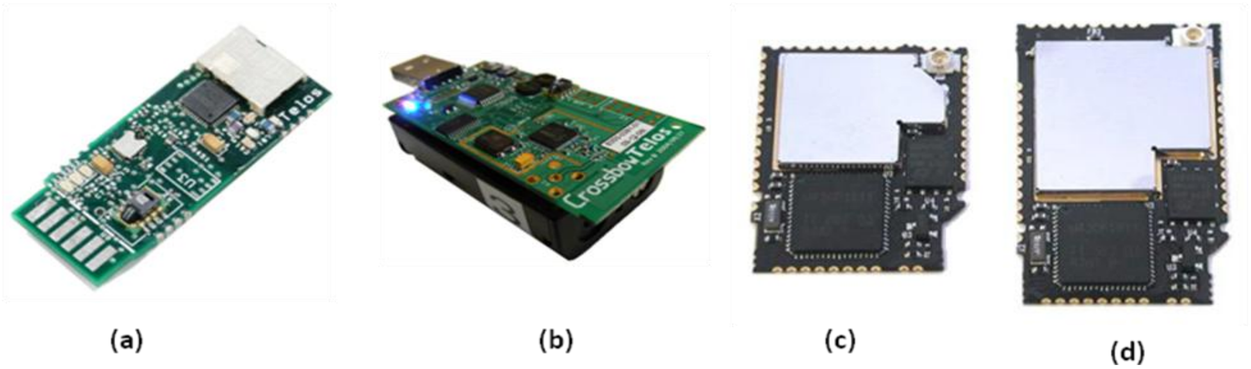


Fig. 4 (a) Tmote, (b) Tmote Sky, (c) Tmote mini, and (d) Tmote mini plus

Intel Motes

These nodes are designed by Intel Corporation. These nodes are designed as high performance mote to be used for advance applications. These modules follow modular approach, enabling it to be attached with different type of power supplies and sensor and data acquisition boards. There are two versions of nodes, namely- Intel Mote [27] and Intel Mote2 [28]. The images of these nodes are shown in Fig. 5(a) & 5(b).

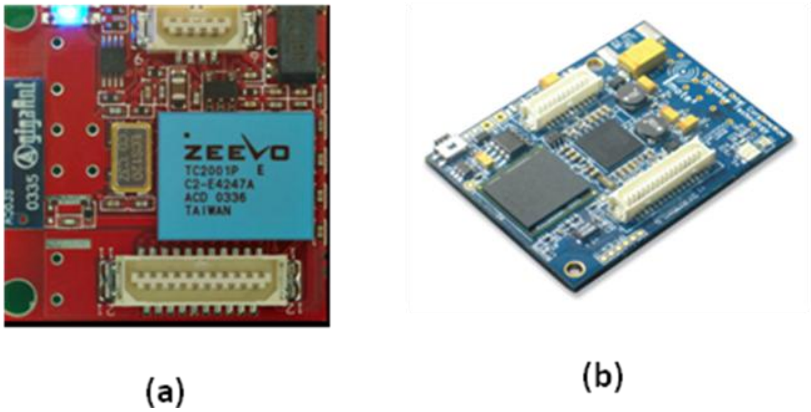


Fig. 5 (a) Intel Mote, (b) Intel Mote2

Intel Mote uses the integrated wireless microcontroller module with ARM7 TDMI core with CMOS Bluetooth Radio, whereas Intelmote2 was built around low power XScale CPU with separate IEEE 802.15.4 compliant radio. Specifications of these nodes are compared in Table 3.

Table 3. Comparison of Intel Nodes

	Intel Mote [27]	**Intel Mote2 [28]**
Microcontroller	ARM7 TDMI 12-48 MHZ	PXA271 XScale CPU 13 – 416MHz + Wireless XScale MMX coprocessor
Transceiver	CMOS Bluetooth radio integrated with microcontroller	TI CC2420[10], 250 Kbps, 2.4 GHz, IEEE 802.15.4 compliant
Memory	512 KB flash program memory, 64 KB static RAM	256kB SRAM, 32MB SDRAM and 32MB of FLASH memory.
Power Management	-	Dialogue Power Management IC

Apart from the explained nodes, there are multiple commercial nodes available in the market. Few of them are: BTnode, EPIC mote, Egs, EyesIFX, Sun SPOT, Waspmote, XYZ node, WSN430 mote, LOTUS, eKo Pro, GINA, Eldorado, OpenMote, OpenMoteSTM, KMote, Mulle mote, PowWow, Redbee, Rene, Shimmer, Tinynode, FireFly etc. The comparison of few of these nodes is given in Table 4.

Table 4. Comparison of other Commercial Nodes

Sensor Node Name	Microcontroller	Transceiver	Program +Data Memory	External Memory	Programming
BTnode	Atmel ATmega 128L 8 MHz	Chipcon CC1000 (433-915 MHz) and Bluetooth (2.4 GHz)	64+180 K RAM	128 KB FLASH ROM, 4 KB EEPROM	C and nesC Programming, TinyOS
EPIC mote	TI MSP430	CC2420	10 KB RAM, 48 KB flash		C and nesC Programming, TinyOS
SunSPOT	ARM 920T	2.4 GHz IEEE 802.15.4 radio with integrated antenna	512 KB RAM, 4 MB flash		Java
Waspmote	Atmel ATmega 1281	XBee, XBee-Pro	128 KB FLASH ,8 KB SRAM	ROM, 4 KB EEPROM, 2 GB SD card	C/Processing
XYZ	ML67 series ARM/THUMB microcontroller	CC2420	32 KB RAM	256 KB flash	C Programming, SOS
WSN430	TI MSP430-1611	CC1100	48 KB Flash , 10K RAM		

1.1.5. Routing Protocols

There are various ways to classify routing protocols that are used in wireless sensor networks. In flat routing, each node typically plays the same role and sensor nodes collaborate together to perform the sensing task. It is not feasible to assign a global identifier to each node in a wireless sensor network. This has led to data centric routing, where the base station sends queries to certain regions and waits for data from the sensor nodes located in the selected regions. Since data is being requested through queries, attribute-based naming is necessary to specify the properties of data. Examples of flat routing protocols include Directed Diffusion, Sensor Protocol for Information via Navigation (SPIN), Rumor Routing, Minimum Cost Forwarding Algorithm, Gradient-based Routing, Information-driven Sensor Querying (IDSQ) and Constrained Anisotropic Diffusion Routing (CADR), Active Query forwarding In sensor network (ACQUIRE) and Energy Aware Routing [29][30].

In hierarchical routing, also called cluster-based routing which was originally proposed in wired networks, there are well-known techniques with special advantages related to scalability and efficient communication. As such, the concept of hierarchical routing is also utilized to perform energy-efficient routing in wireless sensor networks. In a hierarchical architecture, higher energy nodes can be used to process and send the information while low energy nodes can be used to perform the sensing in the proximity of the target. This means that creation of clusters and assigning special tasks to cluster heads can greatly contribute to overall system scalability, lifetime, and energy efficiency. Hierarchical routing is an efficient way to lower energy consumption within a cluster and performing data aggregation and fusion in order to decrease the number of transmitted messages to the base station. Hierarchical routing is mainly two-layer routing where one layer is used to select cluster heads and the other layer is used for routing.

However, most techniques in this category are not about routing, rather on “who and when to send or process/aggregate” the information, channel allocation etc., which can be orthogonal to the multi hop routing function. Examples of routing protocols include Low Energy Adaptive Clustering Hierarchy (LEACH), Power-Efficient GAthering in Sensor Information

Systems (PEGASIS), Threshold sensitive Energy Efficient sensor Network (TEEN), Adaptive Periodic Threshold sensitive Energy Efficient sensor Network (APTEEN), Self Organization Protocol, Sensor Aggregates Routing, Virtual Grid Architecture Routing, Hierarchical Power-aware Routing and Two-Tier Data Dissemination [31][32].

1.1.6. Security Protocols

Since Wireless Sensor Network uses wireless as the transmission media, it is prone to eaves dropping, injection of packets etc. Hence security of data is very important in WSNs[33-36]. So, various security protocols have been developed. Some of them are explained below.

SPINS: Security Protocols for Sensor Networks

SPINS is a suite of security building blocks proposed by Perig et al. It is optimized for resource constrained environments and wireless communication. Due to the limited computation resources and program memory available in sensor nodes asymmetric cryptography cannot be used and instead symmetric cryptographic primitives are used to construct the SPINS protocols. SPINS has two secure building blocks: Sensor Network for Encryption Protocol (SNEP) and micro version of Timed, Efficient, Streaming, Loss tolerant Authentication protocol (μTESLA). SNEP provides data confidentiality, two-party data authentication, and data freshness. μTESLA provides authenticated broadcast for severely resource-constrained environments.

All cryptographic primitives (i.e. encryption, Message Authentication Code (MAC), hash, random number generator) are constructed out of a single block cipher for code reuse. This, along with the symmetric cryptographic primitives used, reduces the overhead on the resource constrained sensor network. In a broadcast medium such as a sensor network, data authentication through a symmetric mechanism cannot be applied as all the receivers know the key. μTESLA constructs authenticated broadcast from symmetric primitives, but introduces asymmetry with delayed key disclosure and one-way function key chains.

SNEP

SNEP uses encryption to achieve data confidentiality and MAC to achieve two-party authentication and data integrity. Apart from confidentiality, SNEP also addresses the important security property called semantic security. It ensures that an eavesdropper has no information about the plaintext, even if it sees multiple encryptions of the same plaintext. SNEP also takes care of data freshness ie. it ensures that data is recent and no adversary replayed the old messages.

μTESLA

Most of the proposals for authenticated broadcast are impractical for sensor networks, as they rely on asymmetric digital signatures for the authentication. The TESLA protocol provides efficient authenticated broadcast but it is not designed for limited computing environments. μTESLA solves these inadequacies of TESLA in sensor networks. It uses symmetric authentication but introduces asymmetry through a delayed disclosure of the symmetric keys, which results in an efficient broadcast authentication scheme.

TinySec [37]

TinySec is a Link Layer Security Architecture for Wireless Sensor Networks. It is a lightweight, generic security package that can be integrated into sensor network applications. It is incorporated into the official TinyOS release. Sensor networks use in-network-processing such as aggregation and duplicate elimination to reduce traffic and save energy. Since in-network-processing requires the intermediate nodes to access, modify, and suppress the contents of messages, end-to-end security mechanisms cannot be used to guarantee the authenticity, integrity, and confidentiality of messages.

Link-layer security architecture can detect unauthorized packets when they are first injected into the network. TinySec provides the basic security properties of message authentication and integrity using message authentication code (MAC) layer, message confidentiality through encryption, semantic security through an Initialization Vector (IV) and replay protection. TinySec supports two different security options: authenticated encryption (TinySec- AE) and authentication only (TinySec-Auth). With authenticated encryption, TinySec encrypts the data payload and authenticates the packet with a MAC. The MAC is computed over the encrypted data and the packet header. In authentication only mode, TinySec authenticates the entire packet with a MAC, but the data payload is not encrypted.

MiniSec [38]

MiniSec is a security protocol developed to provide end-to-end protection from network layer. Both TinySec and SNEP have developed solutions for providing secure communication in link layer. Although both protocols attempt to minimize energy consumption, under certain circumstances, they both demonstrate inefficient energy usage. The greatest advantage of this protocol over other security protocols for WSN is, it provides high security with low energy consumption. It not only provides data secrecy but also the replay protection, freshness, low energy overhead and resilience to lost messages. It has two operating modes namely: MiniSec–U for Unicast communication and MiniSec–B for Broadcast communication. The latter does not require per-sender state for replay protection and thus scales to large networks. Both schemes employ the Offset Code Block (OCB) encryption scheme to provide for data secrecy and authentication, while using a counter as a nonce.

The two modes differ in the way they manage the counters. MiniSec-U, employ synchronized counters, which require the receiver to keep a local counter for each sender while MiniSec-B has no such requirement. Instead, meta-data to prevent replay attacks is stored in a bloom filter. Similar to SNEP, MiniSec-U maintains a synchronized monotonically increasing counter between a sender and receiver as Initializing Vector (IV). However, MiniSec-U includes the last *x* bits of the counter along with each packet. It is called *Last Bits Optimization*, and the last *x* bits of the counter is called the *LB value*. By keeping *x* low, the radio's energy consumption is almost as low as not sending the counter at all.

1.1.7. WSN Standards

A Wireless Personal Area Network (WPAN) is a network for interconnecting devices deployed over small workspace, where the interconnections are wireless. Wireless Sensor Network is a special type of WPAN, where interconnecting devices in the network are capable of sensing and sensor data will be transmitted to a central device (Base Station/Sink). IEEE 802.15 group of standards define different WPAN standards for different applications. WSN is defined by IEEE 802.15.4 standard.

IEEE 802.15.4 [39][40]

It is a physical and media access layer standard for low rate WPANs (LR-WPAN). The main objective of the LR-WPAN is ease of installation, reliable data transfer, short range operation, extremely low cost and reasonable battery life. An LR-WPAN device comprises a PHY layer, which contains the radio frequency (RF) transceiver along with its low-level control mechanism, and a MAC sub layer that provides access to the physical channel for all types of transfer. The definition of the upper layers consisting of a network layer, which provides network configuration, manipulation & message routing, and an application layer, which provides the intended function of the device are outside the scope of this standard. Application specific standards such as Zigbee, Wireless HART, 6LoWPAN, ISA 100.11a are built on top of the IEEE 802.15.4 standard.

The standard specifies the following four PHY layers:

- An 868/915 MHz direct sequence spread spectrum (DSSS) PHY layer employing binary phase-shift keying (BPSK) modulation
- An 868/915 MHz DSSS PHY layer employing offset quadrature phase-shift keying (O-QPSK) modulation

- An 868/915 MHz parallel sequence spread spectrum (PSSS) PHY layer employing BPSK and amplitude shift keying (ASK) modulation
- A 2450 MHz DSSS PHY layer employing O-QPSK modulation

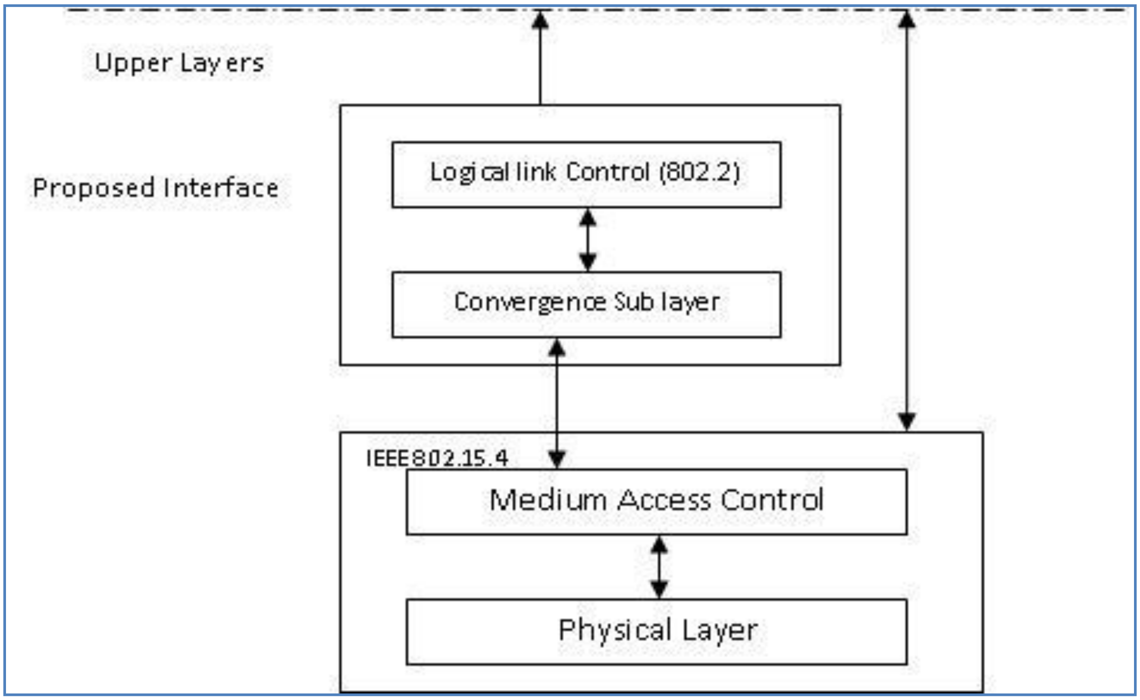


Fig. 6 Low Rate WPAN architecture

The frequency channels are defined through a combination of channel numbers and channel pages. Table 5 shows the supported frequency bands and respective data rates in the IEEE 802.15.4 standard. According to the standard, 868/915 MHz BPSK PHY layer is mandatory for any IEEE 802.15.4 compliant 868/915 MHz radio.

Table 5. Frequency bands and Data rates

PHY layer (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (K symbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS
	902–928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary Orthogonal
	902–928	1000	O-QPSK	250	62.5	16-ary Orthogonal
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

Mandatory PHY layer is using CSMA-CA for channel access and fully acknowledged protocol for transfer reliability. It supports low power consumption, Energy Detection (ED) and Link Quality Indication (LQI). The addressing of nodes is executed in two ways as 16-bit short address and 64-bit extended address. Depending on the application, IEEE 802.15.4 LR-WPAN defines star or peer-to-peer topology for its network.

In the star topology the communication is established between devices and a single central controller, called the PAN coordinator. A device typically has some associated application and is either the initiation point or the termination point for network communications. The peer-to-peer topology also has a PAN coordinator; however, any device may communicate with any other device as long as they are in range of one another. Peer-to-peer topology allows more complex network formations to be implemented, such as mesh networking topology.

IEEE 802.15.4e

IEEE 802.15.4e [41][42] is the amendment of MAC sub layer of IEEE 802.15.4 for industrial and process automation applications. The main design goal of the IEEE 802.15.4 was energy efficient operation, whereas the real time aspects were not considered. Industrial applications have critical requirements such as low latency, deterministic behavior and agility against harsh RF environment. Different applications may have conflicting requirements. IEEE 802.15.4e has been developed to incorporate different MAC behaviors associated with different applications. These MAC behaviors cover the enhancements proposed by WirelessHART, ISA100.11a, Wireless network for Industrial Automation—Process Automation (WIA-PA) and Chinese Wireless Personal Area Network (CWPAN). The main key element of IEEE 802.15.4e is the support of channel hoping, which significantly increases the robustness against harsh RF environment and multipath fading.

As per IEEE 802.15.4e, these MAC behavior and enhancements are defined as follows-

- Time Slotted Channel Hopping (TSCH), for application domains such as process automation
- Low Latency Deterministic Networks (LLDN), for application domains such as factory automation
- Deterministic and Synchronous Multi-channel Extension (DSME), for general industrial and commercial application domains includes Channel diversity to increase network robustness
- Radio Frequency Identification Blink (RFID), for application domains such as item and people identification, location, and tracking
- Asynchronous Multi-Channel Adaptation (AMCA), for large infrastructure application domains

The additional MAC enhancements not specifically tied to a particular application domain mode are as follows:

- Low-energy (LE) protocol, to allow very low duty cycle devices to send ad hoc data using minimal amounts of energy,
- Information elements (IE) to provide extensible MAC data transfers
- Enhanced beacons (EB) and enhanced beacon requests (EBR), to allow coordinator devices to send beacons with specifically requested data
- The MAC multipurpose frame, which provides the scalability and extensibility to allow this standard to address new application needs with minimal MAC changes
- MAC performance metrics to provide upper layers with critical information on the quality of the communication links
- Fast Association (FastA) to reduce the time required to associate

IEEE 802.15.4g

IEEE 802.15.4g [43] is the amendment of IEEE 802.15.4 specifically targeted for very large scale process control applications such as utility smart grid network. The application has been defined as a network of large scale, geographically distributed network with multiple sinks and sources. Other design goals include outdoor operation, high density deployment and data rate up to 1Mbps and large data frames. Different frequencies have been included in this specification to cover most regional markets.

Zigbee

Zigbee standard [44-46] is the widely used application standard for IEEE 802.15.4. Its application varies from process monitoring, home and building automation, smart energy applications to health care, retail and telecom services.

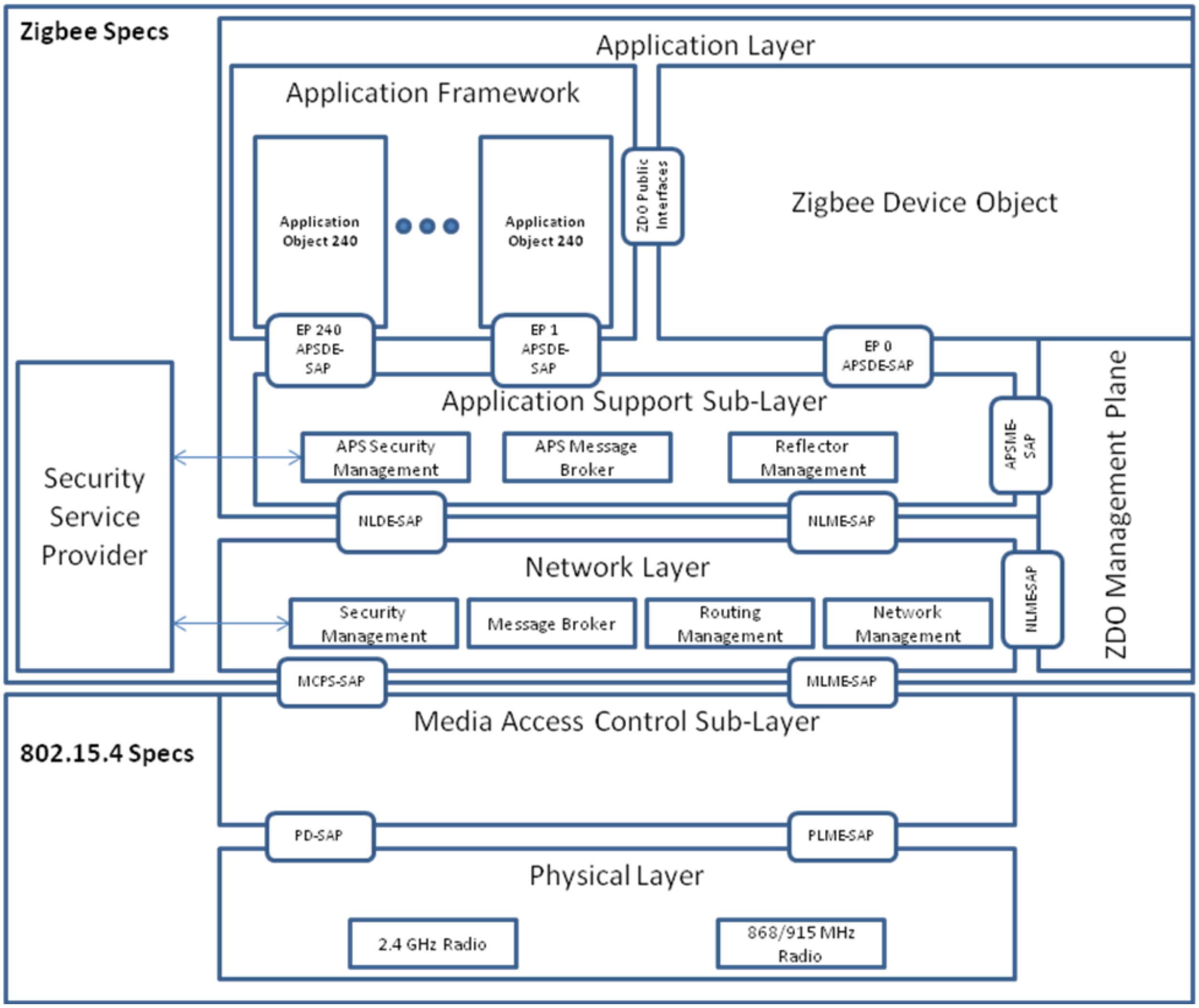


Fig. 7 ZigBee Architecture

Zigbee is a low cost, low power, wireless mesh standard, which defines higher layer protocols for low power digital radios based on IEEE 802.15.4. It is suitable for applications which require short range wireless transmission of data at relatively low rate. The Zigbee stack architecture made up of a set of blocks called layers. Each layer provides a specific set of services to the layer above. Every layer consists of two entities – data entity and management entity. Data entity provides services related to data transmission and a management entity provides management services. Every service entity provides their services through an interface, which is called Service Access Point (SAP).

Lower layers in Zigbee defined by IEEE 802.15.4 are physical layer (PHY) and media access control (MAC) sub-layer [Fig. 7]. Zigbee layers include network layer and framework for the application layer. Application framework consists of Application Support (APS) sub-layer and Zigbee Device Objects (ZDO). Application objects defined by manufacturer use the application framework and share the services of APS and ZDO.

Wireless HART and ISA100.11a

Wireless HART [47] is the wireless equivalent of the Highway Addressable Remote Transducer Protocol (HART). The physical layer of HART protocol has been replaced by IEEE 802.15.4 PHY layer. Since the IEEE 802.15.4 MAC sub layer was not found suitable for low latency and deterministic applications, Wireless HART has proposed new Data Link Layer (DLL) extension to IEEE 802.15.4 MAC sub layer for industrial applications. ISA100.11a [48] is independently developed standard for industrial network of sensor and actuators. Similar to Wireless HART, it also uses the IEEE802.15.4 PHY layer but its modified MAC sub layer is not compliant to IEEE 802.15.4 MAC sub layer [49].

Both standards use the time synchronized channel hopping technology for their data link functions, which is based on Time Synchronized Mesh Protocol (TSMP) [50] developed by Dust Networks. Other similarities are source and graph routing, security, centralized management functions and similar terminology for different devices in the network. ISA100.11a uses 6LoWPAN [51] at the network layer, hence supports the IPv6 address space and UDP at the transport layer. Whereas, Wireless HART has independently developed address space and transport layer. At the application layer, Wireless HART only supports the HART protocol, whereas because of its use of 6LoWPAN, ISA100.11a supports different network protocols such as tunneling and IPv6.

6LoWPAN

IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) [51-54] is the working group in the internet area of Internet Engineering Task Force (IETF). This standard defines the method to send IPv6 packets over IEEE 802.15.4 networks. It enables the IPv6 capabilities to the individual sensor nodes. It defines the IPv6 header compression mechanism, fragmentation and reassembly mechanism for IPv6 packets, address resolution mechanism (128 bit IPv6 address to 64bit/16 bit IEEE 802.15.4 address and vice versa), routing mechanisms (mesh routing in IEEE802.15.4 network, routing between IPv6 and IEEE802.15.4 networks, mesh under and route over routing) and different security and management functions.

EnOcean

EnOcean [55] is a new ISO/IEC standard (ISO/IEC 14543-3-10) [56] for wireless application with ultra low power consumption. It is also optimized for energy harvesting solutions. It is developed as independent of IEEE 802.15 family of standard and hence supports different physical and MAC sub layer schemes. Its physical layer is designed for extreme low power operation with smaller data packets so that energy harvested by efficient exploitation of slightly mechanical motion and fluctuation in environmental parameters such as light, vibration and temperature can be fully utilized for node operation.

IEEE 1902.1 (RuBee)

RuBee [57][58] is a two way, active wireless protocol designed for harsh environment, high security asset visibility applications. It utilizes long wave magnetic signals to send and receive short data packets. It uses low frequency at 131 kHz and modulation of magnetic field created via magnetic dipole antenna, in the near field. Because of this it is very immune to interference and can operate with negligent attenuation in metal and/or water based obstacles. It is very limited in range and data rate and hence could be useful only for local deployment. It is being used for asset tracking for high security goods. RuBee is the only wireless technology to be ever approved for use in secure facilities by the U.S. Department of Energy (DoE)

.

DASH7

DASH7 [59][60] is an open source wireless sensor networking standard for wireless sensor networking, which operates in the 433 MHz unlicensed ISM band. DASH7 provides multi-year battery life, range of up to 2 km, indoor location with 1 meter accuracy, low latency for connecting with moving things, a very small open source protocol stack, AES 128-bit shared key encryption support, and data transfer of up to 200 Kbit/s.

1.2. Motivation for Research

As mentioned in this chapter, Wireless Sensor Networks is a promising technology with a potential to emerge in a big way and its usage looks to be limited only by our ingenuity and imagination.

Nuclear Power is a clean technology free from carbon emissions and is essential for energy security for countries like India. However, the safety of nuclear plants is very important for the designers, operators and general public. Having attained the required maturity in nuclear technology, the designer is now concentrating on reduced unit energy cost and increased safety. Wireless sensor networks play an important role in achieving both the objectives.

Wired networks usually impose a very high cabling cost and installation costs in nuclear power plants. A recent study funded in part by Electric Power Research Institute (EPRI) concluded that adding cabling in existing nuclear plants costs[61] twice as much as the initial cabling cost. In addition to cost, over time, the heat, water etc. degrade the wires and cause maintenance issues or even may effect the safety. The extension of older plants' licenses necessitates more instrumentation to monitor ageing components. However installing wired sensing systems will be prohibitively expensive. Fortunately the cost of wireless systems will be a fraction of that of the wired systems. This reduces the capital cost of the plant. When a large number of sensor nodes have to be deployed in space constrained area and/or in hazardous areas, the most feasible solution is wireless sensor network. In particular, with the ability of nodes to sense, process data, and communicate, they are well suited to perform event detection, which is one of the prominent applications of wireless sensor networks. Hence it can be deployed for nuclear reactor applications, where presently thousands of signals are wired to the control room.

All the wires corresponding to these signals are routed through the cable trays and could be a fire hazard leading to safety issues. Also incase any wire in the cable tray gets cut or open the information regarding that signal is completely lost in a wired network which could effect the safety. In a wireless sensor network even an in between routing node fails the network automatically reconfigures itself and the sensed data is passed on to the control room. These advantages of reduced capital cost and improved safety and the vision that future nuclear plants use this technology extensively necessitates that the challenges the technology poses have to be addressed and confidence has to be created in the nuclear regulators by deploying a number of wireless sensor networks and proving it's reliability and robustness. This has given the motivation for doing research in the development of wireless sensor networks for nuclear reactor applications and deploying them in various nuclear facilities and analyzing their performance.

The thrust of the research in this work is to design, develop suitable, robust & industrial grade Wireless Sensor Nodes that can be deployed in Nuclear Plants and facilities, a harsh environment where temperatures are high and environment is dusty. Also it was aimed to establish the usage of this emerging technology successfully by deploying multiple and typical Wireless Sensor Networks in the Nuclear Reactor Environment and other Nuclear Facilities and assess their performance by conducting various experiments in the established networks. The main aim of this research was to prove through practical research and development that wireless Sensor Networks are a dependable and viable technology which improves safety and reduces the cost. Thus the development of routing and security protocols is visualized as future scope and work will be pursued as indicated in the Future Scope in Chapter 7 of the thesis.

1.3. Objectives & Scope of Research

Considering the importance of wireless sensor network in nuclear reactors, intensive research and development activities are carried out. As the commercially available nodes are not found to be suitable for use in nuclear environment, different types of wireless sensor nodes have been designed and developed. Various wireless sensor networks have been deployed in the laboratories, nuclear facilities and the fast breeder test reactor. The performance of the networks has been analyzed and found to be satisfactory working over a long period which has given enough confidence that these networks can be successfully used in nuclear reactors.

The thesis is organized as follows:

Chapter 2 covers the various experiments conducted out by establishing test WSNs, the signal penetration studies carried out and range and RSSI measurements made.

Chapter 3 narrates the various development works carried with respect to development various WSN nodes, Software Stack, WSN management Station etc.

Chapter 4 covers the actual deployment of WSNs in Computer Division and other nuclear facilities including Fast Breeder Test Reactor.

Chapter 5 explains the analysis and performance studies of the various deployments of WSNs, throughput analysis, packet drop ratio, overhead effects of implementing security protocols.

Chapter 6 gives the conclusion of the thesis that the WSNs are a promising solution for implementation in nuclear reactors.

Chapter 7 gives the future scope.

CHAPTER 2

2. Experiments & Research Studies

2.1. Introduction

By design and construction the nuclear facilities especially the radiological facilities including the nuclear reactor buildings are constructed with thick walls of high density concrete to ensure the radiation levels are contained. Establishing wireless sensor networks in these facilities is a challenging task because the signal ranges cannot be estimated or mathematically modeled. Hence signal penetration studies have been actually conducted for various typical environments for knowing the ranges and the inter node distance. Indira Gandhi Centre for Atomic Research is a big nuclear R&D centre with different radiological facilities and it has given scope to carry out enough research studies. The chapter explains the various signal penetration studies carried out in the centre by deploying various WSNs to collect sufficient information which is required for designing the WSNs.

2.2. Test Deployments at RCL

Initially the commercially available WSN nodes (IRIS) were thoroughly tested at WSN lab for functionality. As part of extended experiment and pre-research studies, the field deployments have been taken up. It is decided to conduct experimental deployments at Radio chemistry Laboratory for radiation monitoring [62 - 70].

The experimental set up of WSN has been established at Radio Chemistry Laboratory (RCL) to evaluate the feasibility to monitor the radiation dose levels at different locations of the laboratory continuously and transmit to a centralized monitoring station. Initially the site survey has been done using Wi-spy spectrum analyzer [71] to identify the interference at 2.4GHz spectrum range within the building and it is found that the spectrum is clear and is fully available. Experiments have been conducted to find the number of nodes needed to cover the maximum linear distance of around 200 m, almost the entire laboratory area in RCL building. The nodes are configured to work at 2410MHz frequency which is channel 11 in the frequency spectrum defined by IEEE 802.15.4 standard. Experiment was conducted with simulated radiation source instead of real ones and it is found that 18 numbers of nodes are needed to cover the entire RCL building. The layout of RCL laboratory and deployment of WSN nodes are shown in Figure.8. After that, simulated source has been replaced by Cesium-137 (Cs137) with source strength of 9.9 µCi as radiation source. The sources are kept at three different locations namely L-10, L-4 and C-7 (Fig. 8).

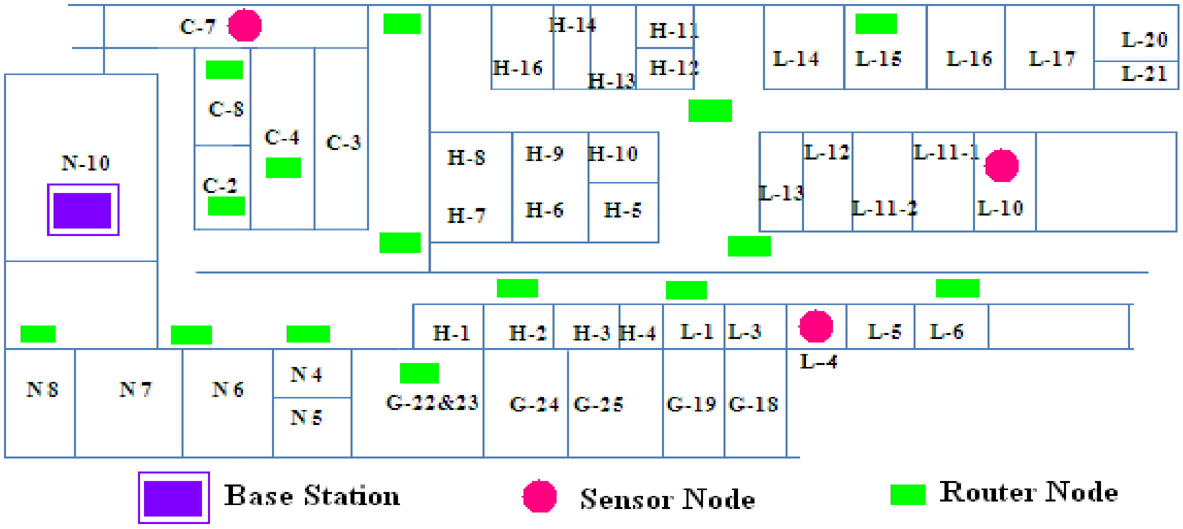


Fig. 8 Layout of RCL with sensor nodes

Area Gamma Monitors based on Geiger Muller counter have been connected to sensor nodes which are used to monitor the radiation emitted from the Cs-137. Remaining 15 nodes in the WSN acted as routing nodes to transfer the radiation data to base station in multiple hops. The base station is kept at N-10, which is connected to a laptop PC for displaying and data logging. (Fig. 9) The whole network was running for few hours and collected the data. The position of nodes was set in such a way that they provide multiple routing paths and hence the fault tolerance has been achieved even in the presence of single node/ link failure. Fault tolerance has been tested by powering off one router node and ensuring that the data transmission is taking place. It has also been verified using the topology view in the wireless network management station, where the powered off node is shown in red colour and the path of transmission is rerouted through nearby node.

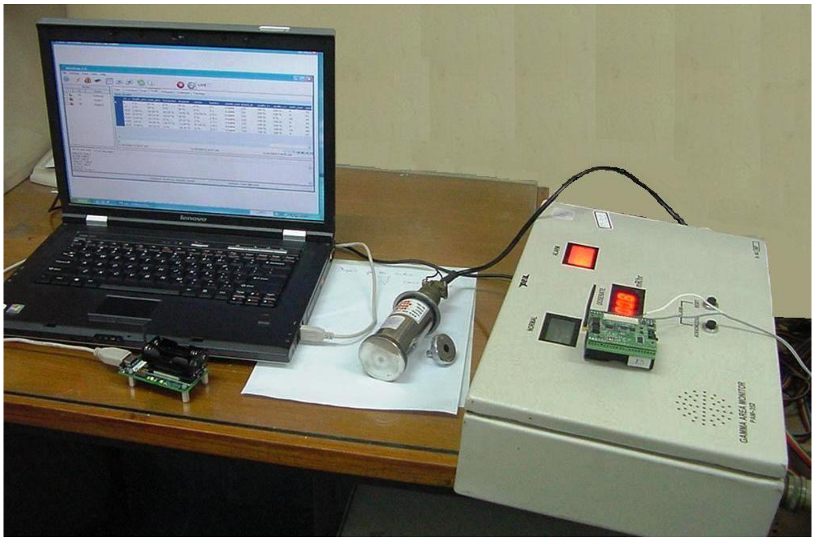


Fig. 9 Experimental setup with AGM and Base station

From the experimental studies, it has been found that, WSN looks to be one of the suitable technologies to establish a centralised radiation monitoring at RCL. In our experiments, the analog voltage measured by the sensor has been converted to digital data. It has been routed through multi hop WSN to be received by the base station and logged at the PC. The received mV signal has been converted to mR/hr. The comparison of the data displayed by local indicators (Area Gamma monitor) and data logged by the network for the three sources were compared. Good agreement is seen between the source signal and logged data. This ensures the accuracy and reliability of the network. But, the experiment gave the idea that the commercially available nodes are not very much suitable for the permanent deployment. Hence it was decided to design and develop our own nodes in house for reactor deployments.

2.3. Penetration Studies

For identifying the signal strength of the transceivers used at 2.4GHz, the signal penetration experiments were carried out at various locations. Initially, the commercially available IRIS nodes were tested at computer division. It is identified that the penetration power of the transceiver used by IRIS (Atmel AT86RF230) is significantly good since it was able to cross 4 walls of normal size and reach the distance of 30 meters**.** The same effect was observed with the in-house developed nodes with XBee transceiver and much higher distance was covered by XBee pro transceivers.

Penetration Studies at Hot Cell, RCL

The experiment was later extended to RCL to check the penetration power of the radio signal through the concrete wall/ glass shielding of lead mini cell and hot cell [70]. In lead mini cell, the thickness of the glass shield is 400 mm and the lead brick thickness is around 200 mm. In hot cell, the thickness of the glass shield is 1.5 m and the average density is 2.5 gm/cc. The thickness of the concrete door is 1.5 m with the average density of 2.5 gm/cc. The radioactive source Cesium-137 (Cs^{137}) with source strength of 9.9 μCi along with Area Gamma Monitor has been kept inside the lead mini cell and hot cell and the signal strength has been measured (Fig. 10). The radio signal is able to cross those barriers even in the presence of obstructions and reach the base station. For experimentation, the base station connected to laptop PC is placed around the hot cell in locations like operating area, service area and the linking corridor. These experiments were repeated several times to verify the repeatability and stability for the network.

Fig. 10 Photo of a typical Geiger Muller tube

Penetration Studies across RCB, FBTR

The penetration studies were further extended to Fast Breeder Test Reactor (FBTR) where the wireless sensor network deployment is planned. In FBTR, the reactor assembly, primary sodium system and associated circuits are housed in Reactor Containment Building (RCB) [72 – 74]. The RCB wall is built with one meter thickness using high density of RCC to contain the radiation. Sensors that are necessary for safe operation of the reactor have been wired from RCB to control room. The Atmel AT86RF230 wireless transceiver, configured to transmit continuous signals at 2410MHz at 0dbm power level, had been placed inside RCB. The similar transceiver was configured as receiver and connected to base station, (a laptop computer) and placed outside RCB, to measure the Received Signal Strength Indication (RSSI). The 2dbi omni-directional antenna has been used. RSSI was checked at various locations outside RCB namely near RCB entrance, near cable penetration and around RCB wall. The experimental setup was as shown in Fig. 11.

The same experiment was repeated with various combinations of transceivers namely XBee, XBee-Pro [75] and Wi-Fi and with 7dbi omni-directional antenna. The observations are shown in Table 6. It is found that RF230 transceivers are receiving signals in 2 hops when one more router is placed between the double doors of the person air lock entrance. The results are same for 2dbi antenna and 7dbi antenna. Based on the results of the above experiments, it is decided to use the cable penetration location for wireless signal transmissions between sensors inside RCB to the control room.

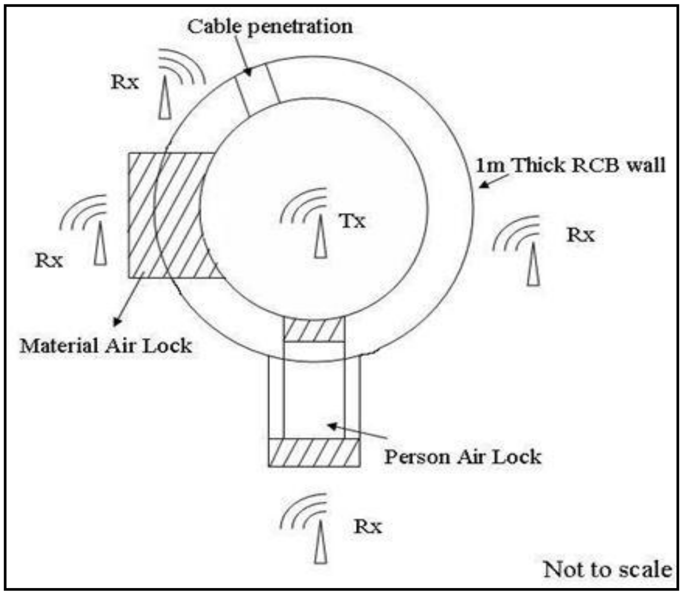


Fig. 11 Penetration Studies at RCB, FBTR

Table 6. Observations of Signal Penetration Experiment

Transmitter	Receiver	Person Air Lock	Cable penetration	Material Air Lock	Around RCB wall
AT86RF230	AT86RF230	X	X	X	X
XBee	XBee	X	√	X	X
XBee	XBee-Pro	√	√	X	X
XBee-Pro	XBee-Pro	√	√	X	X
AR2112A (Wi-Fi)	AR2112A (Wi-Fi)	√	√	X	X
X - Signal does not pass **√ - Signal pass through**					

2.4. Range and RSSI Measurements

Before deploying any wireless sensor network, it is mandatory to identify the probable location for placing the adjacent nodes. The transmission range of each node should have a common area with the reception range of its neighboring nodes. Moreover, the signal strength of the transmitted signal should be well above the minimum threshold to get identified by the receiver without any data loss [76]. For ascertaining this formation, it is obligatory to have a quantitative measure of the signal strength. The hardware of each transceiver is providing support for finding out the Link Quality and Received Signal Strength of the wireless link between two neighboring nodes. For our deployments, we have identified Received Signal Strength Indicator (RSSI) as useful parameter and have conducted experiments with that.

The aim of this experiment is to do distance estimation and further position estimation in both indoor and outdoor environments with a minimal error by incorporating a radio stack device (AT86RF230 inbuilt in IRIS motes) which uses IEEE802.15.4 standard. The device possesses an inbuilt Received Signal Strength Indicator (RSSI) [77] which measures incoming signal strength and updates the value of RSSI registers automatically. So here, distance is computed based on received signal strength between mobile node and reference node or base station. As there is a variation in measured RSSI value of the order of +_ 7 db due to multipath fading and shadowing, experiment has been repeated 40 times. Finally, using statistical technique a database is prepared. It consists of set of equations for a range of RSSI values, by using them approximate distance is calculated. A separate database for indoor and outdoor environment is created.

Further using this distance estimation, position estimation of mobile node in a plane with four reference nodes at corners of square/ rectangle plane is done. Mobile node, will collect signals from all reference nodes, reads out the RSSI value and sends the information to a monitoring application on PC connected through base station. This approach is no doubt a cost effective and simple but it is less accurate. Results can be improved by using a refining algorithm. For much better position estimation or tracking Link Quality Indication (LQI) can be used along with RSSI.

Selection of Hardware and OS for Experimentation

For doing experiments with wireless sensor networks, initially commercially available nodes were procured and used. The major concerns in a wireless sensor network are energy efficiency, size and cost. Hence IRIS nodes from Crossbow have been identified as a low-power, low cost, small, power-efficient, flexible and commercially available hardware platform [78]. IRIS nodes are based on Atmel's Atmega 1281 microcontroller, developed by Berkeley University of California with AT86RF230 as radio. IRIS runs TinyOS, a Tiny Operating System for sensor networks, from its internal flash memory. TinyOS can be suited for such applications because it is a small, open-source, energy efficient software operating system designed specifically for large scale, self-configuring sensor networks. It supports an energy efficient wireless communication stack. Also TinyOS has control on various power down modes of the micro controller and RF transceiver. For initial experiments with wireless sensor nodes, the IRIS motes and TinyOS platform have been chosen.

Experimentation: Position Estimation using RSSI

Initially Distance Estimation Experiment [79] has been conducted to form a database with RSSI and distance. The position estimation experiment is for locating the position of a Blind node moving in a symmetric plane either square or rectangle. Experiment was actually performed over 200 X 200 cm. plane in Lab [80]. Following are the requirements for the experiment:

1. A Blind mote – programmed with *RssiCollection,* which collects the data from all reference nodes, reframe the incoming packets by the received signal RSSI value and transmit to Base Station.

2. Four Reference nodes - programmed for sending empty packets continuously their coordinates
3. A Base station node - it is also programmed with *RssiCollection* but will not do any modification in incoming packets. It directly forwards them to PC.

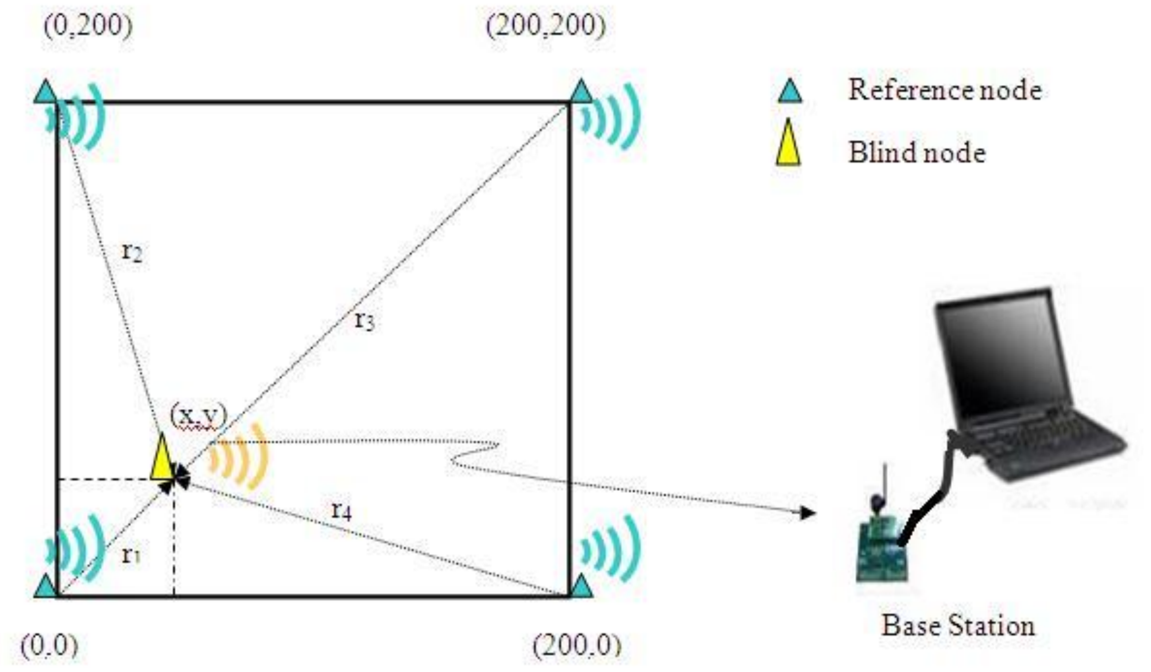


Fig. 12 Setup for Position Estimation

The reference nodes send their coordinates as soon as the system is switched on. It is collected by base station node and displayed on PC. Then, they send empty packets continuously with 1 second time interval, which is collected by blind node. At blind node, the packet is modified by adding RSSI value and the ID of source from which the packet was received, and then the packet is sent to base station. Base station receives the packet, update *finalRSSI* field and sends it to PC. The java code in PC collects all data, calculates average of ten RSSI values of each reference node, refers Distance Estimation database and calculates the distance between reference node and blind node which is denoted by r_i. The x, y coordinates are calculated using the following equations:

$$x = (r_1 * r_1 + r_2 * r_2 - r_3 * r_3 - r_4 * r_4 + L*L + B*B) / (2*(L+B))$$

$$y = (-r_1 * r_1 + r_2 * r_2 - r_3 * r_3 + r_4 * r_4 + L*L + B*B) / (2*(L+B))$$

where L and B are Length and Breadth respectively.

Estimated position coordinates of the blind node are displayed on PC.

2.5. Summary

For designing any wireless sensor network in any nuclear facility we should know where to locate the sensor nodes, router nodes, node connected to the base station and actuator nodes if required. The type of architecture to be chosen depends on the number of sensor nodes, the distance between the nodes, amount of processing to be done by sensor nodes etc. and it is decided whether any cluster head nodes are required. For deciding the location of each node, the approximate range each node can transmit & receive, the environment in which the nodes are located etc. should be known. However in nuclear facilities the buildings and the walls are by design constructed with high density concrete to contain the radiation levels within the permissible limits. Hence the range of each node cannot be decided based on the data sheet details nor can be mathematically modeled. So, the range each node covers for various environments was identified by establishing the wireless sensor networks in different nuclear facilities and got the base data. As part of this, wireless sensor networks were established in radio chemistry laboratory and fast breeder test reactor with various radio transceivers. The RSSI values are also measured and penetration studies were carried out for arriving at the optimal ranges This experimentation and pre research studies helped in getting the required information for designing the wireless sensor networks.

CHAPTER 3

3. Development of WSN Nodes, Software, WNMS

3.1. Introduction

After conducting various experimental deployments in Radiation related Laboratories, penetration studies at Reactor Containment Building and range tests, it has become apparent that the commercially available nodes are not suitable for the permanent deployment in reactor environment. These nodes are not robust enough to work in field environment. They are not convenient to use with the signal conditioning modules developed for the various process signals of the nuclear facilities. Most of the commercially available nodes are using two AA batteries as energy source. In a nuclear plant where the process signals have to be monitored on 24x7x365 basis, the batteries require frequent replacement disturbing the process monitoring. Hence the in-house nodes are designed to address all these issues. The specific issues solved through the in-house design are the in-house nodes are based on Mains Power supply. Also the nodes have been designed with industrial grade components and with IP 54 casings to withstand harsh environment of the field. The nodes designed enable mounting of the various types of signal conditioning modules required for various process signals of nuclear facilities. Also the commercial nodes are denied to Indian Nuclear Facilities like IGCAR. So there is a need for in-house design. Zig Bee communication protocol is chosen for the communication as it is one the most popular protocols. When this development work was started in 2009, Zig Bee products are very popular and most used and easily available in the market and were developed on IEEE 802.15.14 standard. Wireless HART and ISA 100.11a based components have come to the market subsequently.

Also the specific issues/boundary conditions solved through the in-house design are the industrial grade nodes designed using industrial grade components and IP 54 casings enabled us to use them in harsh field environments. Also in the first sensor node developed, provision has been made to use X-Bee or X-Bee Pro transceivers which provide transmit power of 3 dbm and 18 dbm respectively. This enabled us to use them based on the range requirements as the nodes with X-Bee Pro transceiver provide higher range. Also a separate routing nodes have been developed to reduce overall cost for use in areas where no sensing, computation is involved and routing is only required.

There is no published literature on the experience of using wireless sensor networks in nuclear facilities. To that extent there is no theoretical backing. However the design of nodes, the selection of appropriate transceivers, design of various wireless sensor networks was done with the theoretical backing only. For example the decision to use the different transceivers was based on theoretical figures of their transmit power and receiver sensitivity, range available, the battery rating in terms of mAH and the power consumption of the nodes, processing power of the microcontrollers chosen etc.

The nuclear reactor containment building is of high thickness, made up of high density concrete wall. Because of this, the RF signal of 2.4 GHz used in X Bee and X Bee Pro transceivers and RF 230 transceiver could not penetrate through these walls. The possibility of using Ultra Wide Band (UWB) communication was thought of. It was not chosen because for the RF signal to penetrate, the UWB communication had to be operated in KHz range. However in India the communication and measurement systems range in UWB has to be operated as per the FCC guidelines from 3.1 GHz to 10.6 GHz and 6.0 to 7.25 GHz as per the India's National Frequency Plan-2011. If we operate in this range the penetration range will be still be lower as the penetration power is inversely proportional to frequency of operation. Also the range in UWB communication is less (about 10m), needing more number of routing nodes.

Hence it was decided to develop the ***total*** solution to Wireless Sensor Network for Nuclear Reactor Applications. The research and development work includes the development of wireless senor nodes, the complete protocol /software stack, the wireless sensor network management station for monitoring the measured parameters and managing the deployed nodes, security protocols for providing secure communication and other small tools like wireless sniffer, which are to be used during deployment phase. The development activities undertaken for the purpose of research and deployment are explained below.

3.2. Development of WSN nodes

For various deployments, five types of wireless sensor nodes are designed in-house and developed. They are namely: sensor / edge node, cluster head node, router node, base station and actuator node.

3.2.1. Sensor node

In-house designed and developed sensor nodes are operating at 2.4 GHz ISM band. The sensor node consists of mainly ARM 7 processor, External ADC, Power supply unit to take input from AC mains and ZIGBEE module. Fig. 13 shows the block diagram of wireless sensor node.

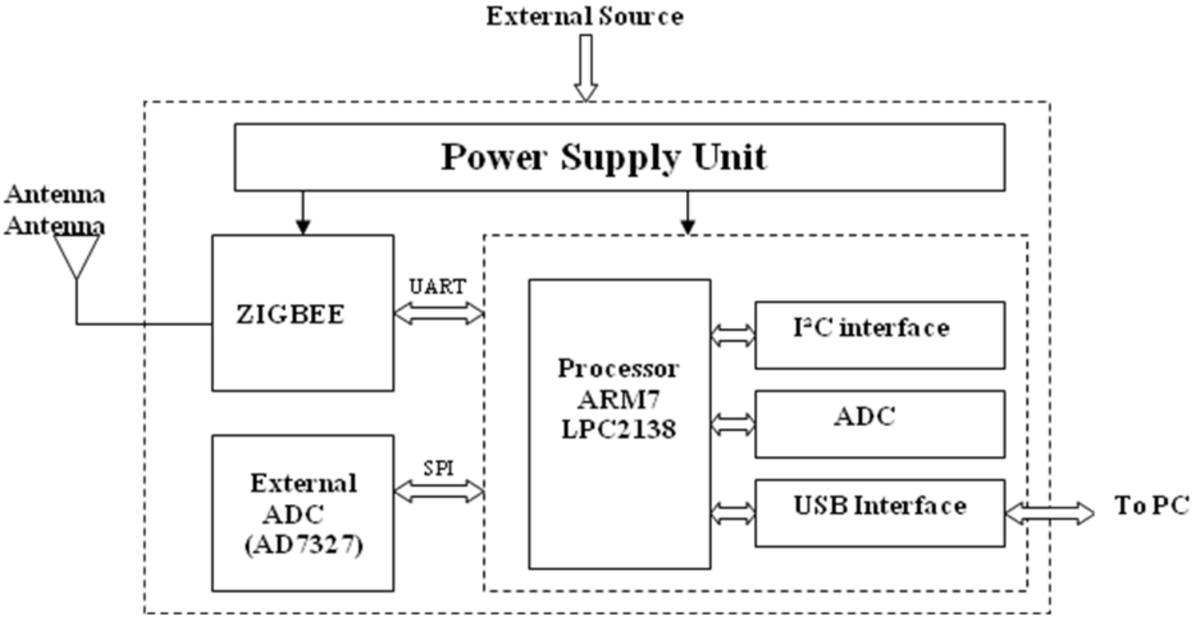


Fig. 13 Block Diagram of in-house developed sensor node

The different parts of the block diagram are described below:

Processor

The microcontroller used in this board is LPC2138 [81], which is based on ARM7 architecture. It is a general purpose 32 bit processor of tiny size, which offers high performance with very low power consumption. It uses a 128-bit wide memory interface and a unique accelerator architecture to enable 32-bit code execution at a maximum clock rate of 60 MHz. It is optimized for low-power operation, has 512 KB of Flash and 32KB of SRAM. There are two numbers of 8-channel 10-bit A/D converters (for a total of 16 analog inputs) with conversion times of as low as 2.44µs per channel. It has a 10-bit D/A converter for generating variable analog outputs and offers up to forty-seven numbers of 5V tolerant GPIOs. It has a CPU operating voltage range of 3.0V to 3.6V (3.3V ±10%)

It has support for In-System Programming (ISP) and In-Application Programming (IAP), which minimize the programming time. Each 256-byte line takes 1 ms to program, while single flash selector or full chip erases take only 400ms. It has two numbers of 32-bit timers (with four capture and four compare channels each), a PWM unit (with 6 outputs), a real time clock, and a watch dog timer. Multiple serial interfaces, including two UARTs, two Fast IIC and two SPI serial interfaces, increase the design flexibility. It also has test or debug interface using JTAG.

Different interfaces are used to connect the external peripherals to microcontroller. SPI interface is used to connect the external 12 bit ADC (AD7327) to LPC 2138. UART 1 has been used for programming the XBee-Pro chip. UART0 has been used for in system programming, which is used for programming and reprogramming the on chip flash memory, using the boot loader. 8 LEDS are connected to GPIO pins to display the status. The external interface consists of a 40 pin expansion connector, designed to interface with a variety of sensing boards. The expansion connector is divided into sections to handle 14 analog signals, 4 power control lines, SPI lines and I2C bus signals. This expansion connector can be used to connect the Wireless sensor node with the signal conditioning board of different sensing devices.

Power Supply Unit

Sensor node gets power from Universal Serial Bus (USB) for programming. It also has the flexibility to operate with different power supplies depending on the availability of supply in the field during deployment. The node requires mainly 3.3V DC supply for its internal ADC operation and external ADC requires 12V DC for its operation. The power supply board takes 230V AC as input and generates 12V DC using AC to DC converter RAC10-12SB.This 12V DC is converted to 5V using LM 7805 voltage regulator and then it is further converted to 3.3V using voltage regulator LD1117. Battery has been provided to act as a backup power source to main board even when complete board power goes off. The block diagram of the power supply board is shown in Fig. 14.

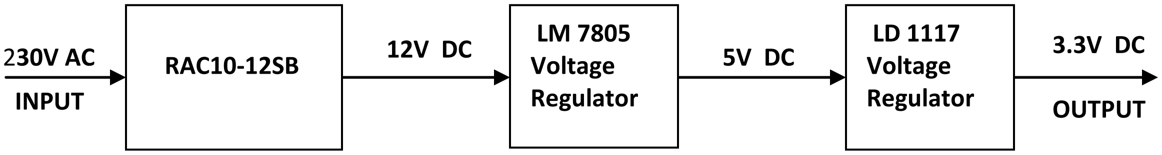


Fig. 14 Power Supply unit block diagram

AD7327 (external ADC)

The AD7327 [82] is an 8-channel, 12-bit successive approximation ADC available in 20 lead TSSOP package. It operates with low a power of 17 mW and at a maximum throughput rate of 500ksps. It contains a 2.5V internal reference for selectable analog input range of 0 to 10V, however external reference operation is also provided by connecting 3.3V to REFIN/OUT pin to accept analog input range of 0 to 12V. For 0 to 12V input range selection, minimum of 12 V_{DD} and grounding of V_{SS} is required. It requires a low voltage 2.7V to 5.25V V_{CC} supply to power the ADC core.

Hardware interfacing of AD7327 with LPC 2138

AD7327 is interfaced with the microcontroller through Serial Peripheral Interface (SPI). V_{DRIVE} pin is connected to the supply voltage of the microcontroller. The voltage applied to the V_{DRIVE} input controls the voltage of the serial interface. It comprises CS, DOUT, SCLK and DIN pins forming the serial peripheral interface. The AD7327 behaves as a slave SPI device. The serial clock applied to the SCLK pin via SCK pin of microcontroller provides the conversion clock and controls the transfer of information to and from the AD7327 during a conversion. To initialize the conversion, microcontroller pulls the chip select (CS) pin to low and data is sent to AD7327 through the DIN pin and the converted data is received fromAD7327 through DOUT pin. The hardware interfacing of LPC 2138 and AD7327 is shown in the Fig. 15.

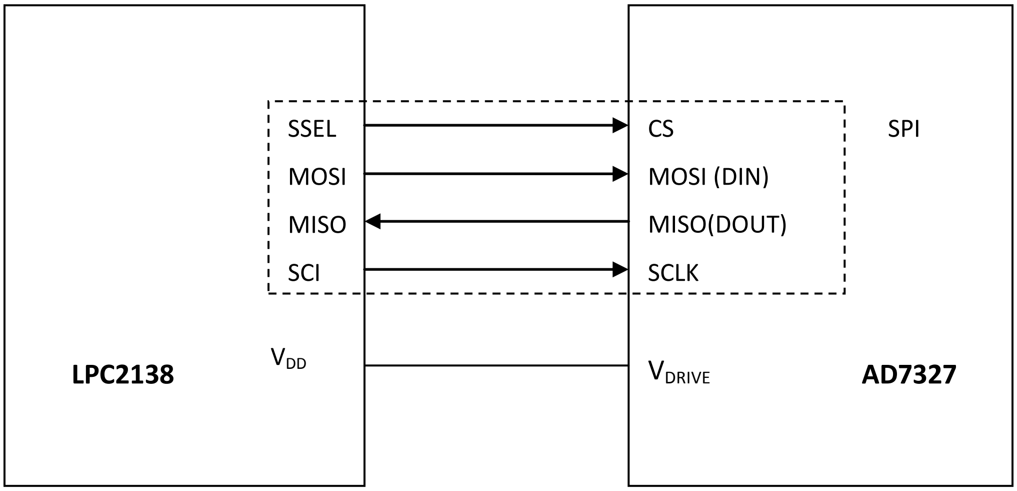


Fig. 15 LPC 2138 and AD7327 Interface

USB Interface

The Universal Serial Bus (USB), is an external bus which provides fast and functional means of connecting board to PC. The WSN main board gets power required for its operation from USB when board is connected to PC.

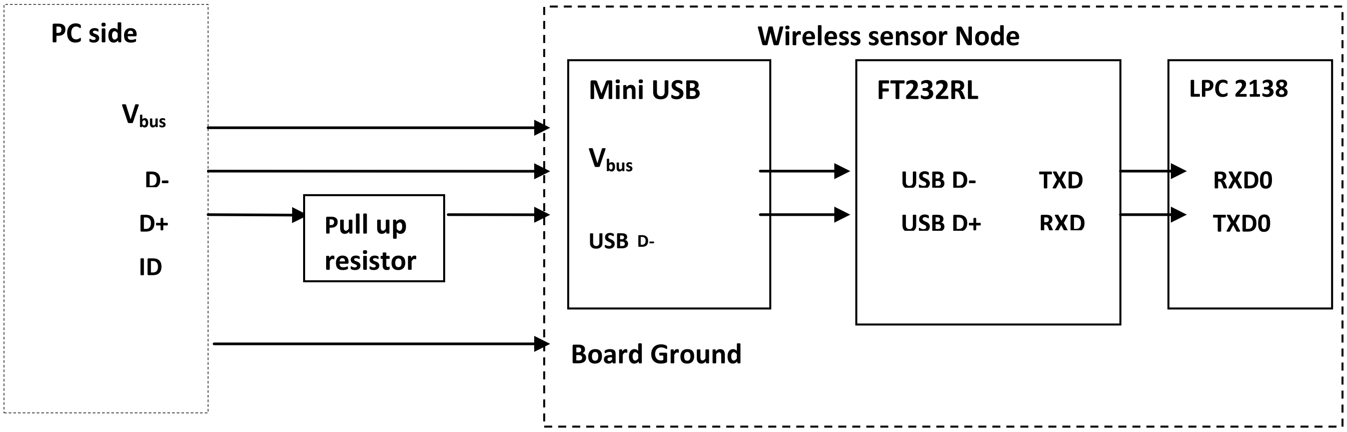


Fig. 16 USB Interface

FT232RL IC [83] provides a quick way of USB connection with LPC 2138 microcontroller UART0. TXD and RXD pins of FT232RL are connected to RXD0 and TXD0 pins (respectively) of microcontroller for transferring data between Microcontroller and PC.

Wireless Section

It consists of XBee or XBee-Pro [75] transceiver chips. These chips provide transceiver interface between the antenna and the microcontroller. It operates in 2.4 GHz ISM band. The transmit modulation scheme is offset-QPSK (O-QPSK) and spreading method is DSSS.

The XBee and XBee-Pro chips contains the firmware which implements the Zig bee and Znet protocols. These chips interface with LPC 2138 through UART1. XBee Module UART comprises DIN, CTS, RTS and DOUT pins. The XBee Module UART performs tasks, such as timing and parity checking, that are needed for data communications. Serial communication consists of two UARTs (LPC 2138's and XBee's) configured with compatible settings (baud rate, parity, start bits, stop bits, data bits).

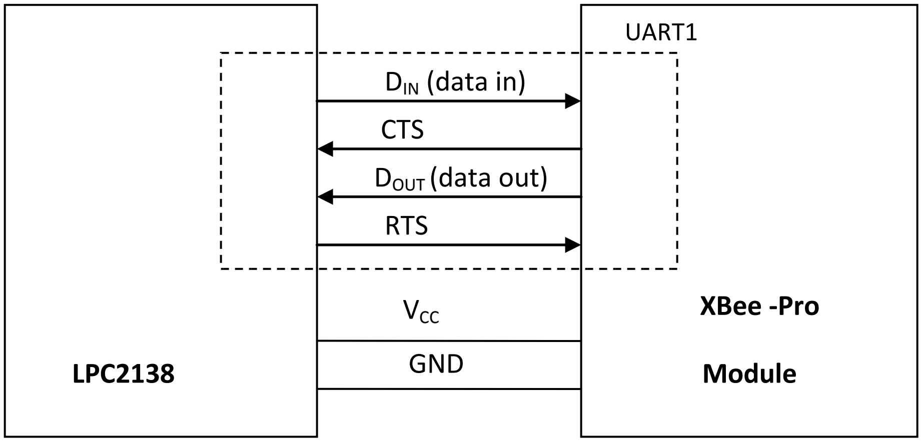


Fig. 17 LPC2138 to XBee-Pro Interface

Data enters the XBee Module UART through the DI pin as an asynchronous serial signal. It is stored in the DI buffer until it is transmitted. When the packetization timeout parameter threshold is satisfied, the module attempts to initialize an RF connection. If the module cannot immediately transmit (for instance, if it is already receiving RF data), the serial data continues to be stored in the DI Buffer. If large amount of serial data is sent to the module, CTS flow control is enabled by de-asserting CTS to signal the LPC 2138 to stop sending serial data and when the DI buffer has enough free space data is sent again. By sending messages smaller than the DI buffer size and by setting baud rate lower than the fixed RF data rate, loss of data between LPC 2138 and XBee module is prevented.

When RF data is received, the data enters the DO buffer and is then sent out through DOUT pin to LPC 2138. Once the DO Buffer reaches capacity, any additional incoming RF data will be lost. To prevent loss of RF data, RTS flow control is enabled so that LPC 2138 signals the module to send data out from the DO buffer using DO pin by re-asserting RTS.

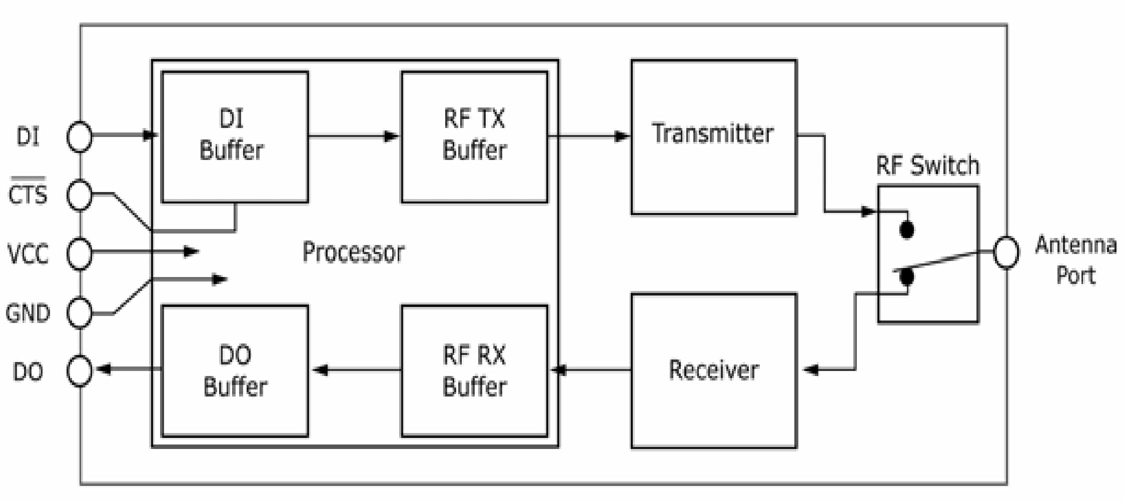


Fig. 18 Internal data flow diagram

The XBee module supports both transparent and API (Application programming Interface) serial interfaces. When operating in transparent mode, the module acts as a serial line replacement and the module parameters are configured using AT command interface. For simple applications, AT firmware is suitable. When operating in API mode, all data entering and leaving the module is contained in frames that define operations or events within the module. The API provides alternative means of configuring modules and routing data at the host application layer. A host application can send data frames to the module that contains address and payload information instead of using command mode to modify addresses. The module will send data frames to the application containing status packets; as well as source, and payload information from received data packets. The API firmware is recommended for applications where

- RF data has to be sent to multiple destinations without entering command mode.
- Remote configuration commands have to be sent to manage nodes in the network.
- Success/failure status of each transmitted RF packet has to be received.
- Source address of each received packet has to be identified.

Antenna

The Antenna used is an omni-directional antenna. It is a 2dB gain, vertically polarized antenna which provides uniform, donut shaped, 360° radiation pattern .This radiation pattern is suitable for point-to-multipoint broadcasting in all directions. It is used for 2.4GHz applications and is interfaced with the transceiver chips through RP-SMA connector. The specifications of the node developed in-house are given in Table 7.

Table 7. Specifications of the In-house Developed Sensor Node

1	Microcontroller	LPC2138 [81]
2	Interfaces	2 UART, I^{2}C support, SPI, GPIO
3	Internal ADC	10 bit successive approximation ADC- 6 channels
4	LED Indication	Power indication LEDs and channel LEDs
5	Real- time Clock	Real-time clock with independent power and dedicated clock input
6	Transceiver	XBee /XBee-Pro radio chips [75]
7	Antenna	2.4GHz. Omni directional antenna
8	Modulation scheme	Offset Quadrature Phase Shift Keying (O-QPSK)
9	Spreading method	Direct Sequence Spread Spectrum (DSSS)
	Power Source Options	
10	Input Power	Single phase 230VAC supply
	Battery Power	11.1 ~ 11.5 V DC @ 1150mAh
11	Output Power	12V, 5V, 3V DC @ 833mA

The external interface of in-house developed node consists of a 40 pin expansion connector, designed to interface with a variety of sensing boards. The expansion connector is divided into sections to handle analog signals, power control lines, SPI lines and I^{2}C bus signals. This expansion connector is used for connecting the node with the signal conditioning

PCBs of temperature, vibration, radiation, sodium leak detector etc. The photograph of the developed node is given in Fig. 19.

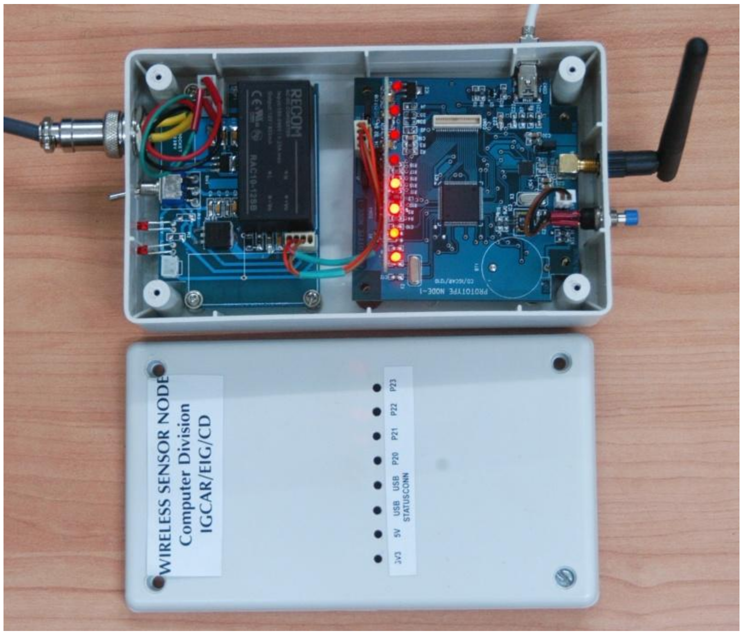


Fig. 19 In-house developed sensor node

3.2.2. Cluster Head Node

The block diagram of the in-house developed cluster head node is shown in Fig. 20.

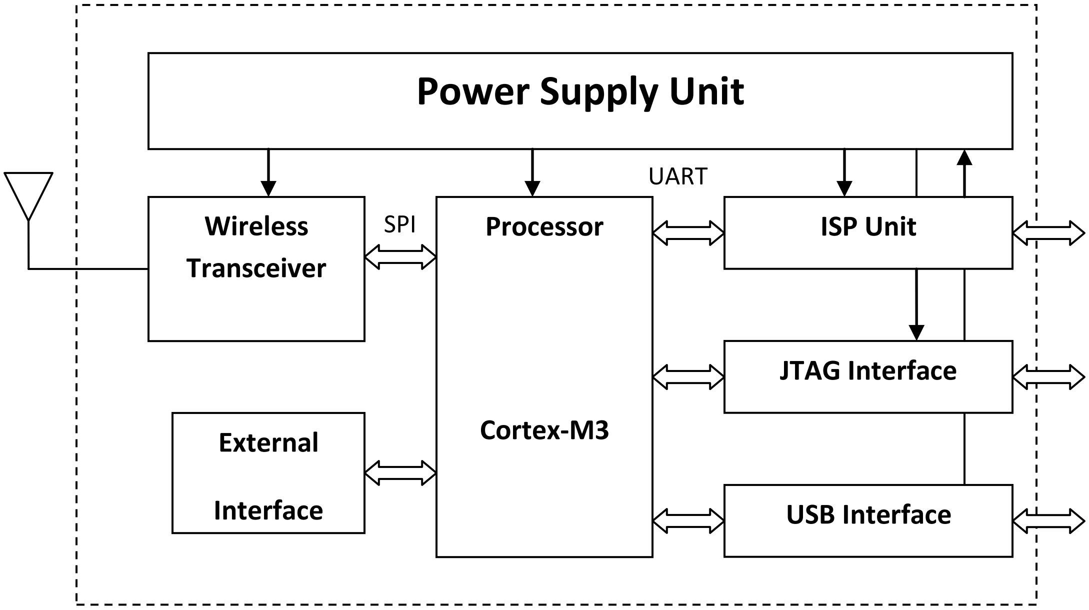


Fig. 20 Block Diagram of Cluster Head Node

Power Supply Unit

The cluster head node mainly requires digital 3.3V for its operation. Three types of provisions have been given to generate the required 3.3V. Main power source is the adaptor. When the node is connected to PC through USB port, it is deriving its power from USB port. Battery has been provided to act as a backup power source for Real time clock in LPC1768 even when the node is turned off. Digital 5V has been provided extra for external interface which wish to derive power from the board. Analog 3.3V is required for ADC operation and for operation of RF part of AT86RF230 [84] transceiver chip.

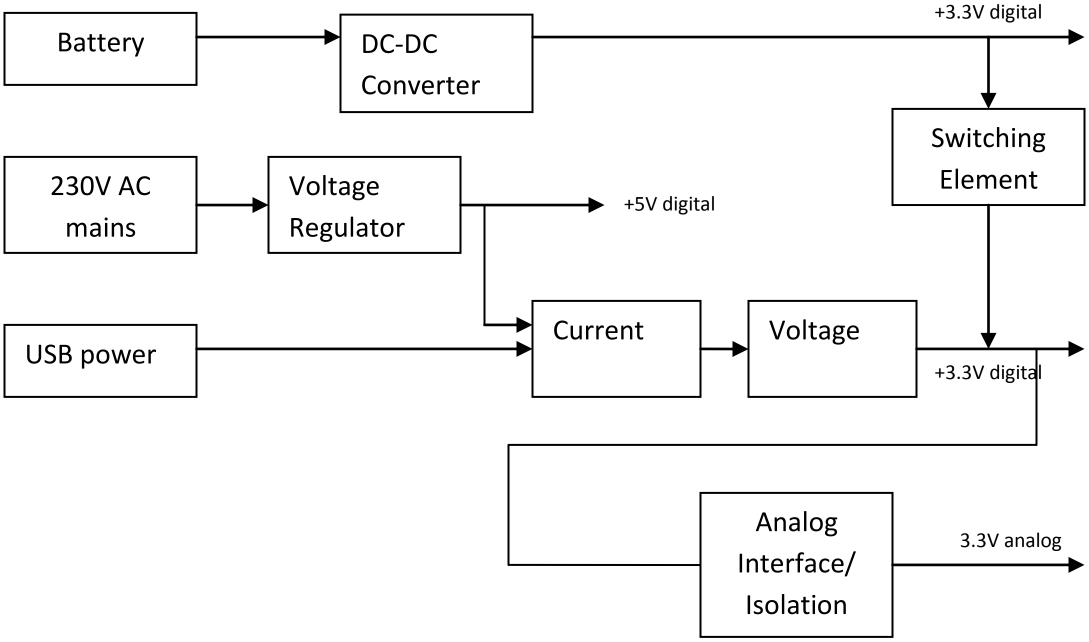


Fig. 21 Power Supply Unit

The power supply board takes 230V AC as input and generates 12V DC using AC to DC converter RAC10-12SB. This 12V DC is converted to 5V using LM 7805 voltage regulator and then it is further converted to 3.3V using voltage regulator LD1117. Battery has been provided to act as a backup power source to main board even when complete board power goes off. The block diagram of the power supply board is shown in Fig. 21. As maximum current requirement is nearly of 300mA, current limiter chip FPF2123 is used. USB power is also regulated through same path. In this analog and digital grounds are isolated to avoid noise propagation. Provision is provided for manual shorting of both grounds if required.

Processor- LPC1768

The microcontroller used in cluster head node is LPC1768, which is based on Cortex-M3 [85] architecture. Cortex-M3 is the ARM based architecture which has been specifically developed for highly deterministic real time and power constrained embedded systems. Cortex M3 architecture is chosen because, the main requirements for the design of cluster head node are high performance: which enables more tasks to be executed in parallel, low interrupt latency, which enables fast reaction to external events and power saving mode which allows node to operate on battery for long duration.

Different interfaces are used to connect the external peripherals to microcontroller. SPI interface is used to connect the wireless module to LPC1768. Other than SPI lines some GPIO lines are connected to the wireless module which controls the operation and state transition in RF module. UART has been used for in system programming (ISP), which is used for programming and reprogramming the on chip flash memory, using the boot loader software. JTAG pins have been connected to the JTAG connector and with the external debugger hardware; they can be used to debug and trace. 6 LEDs also have been connected to GPIO pins.

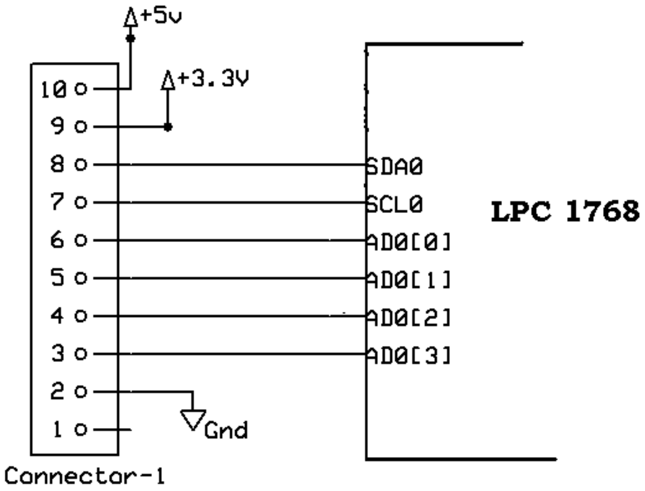


Fig. 22 External Sensing Interface

The external interface consists of a 10 pin expansion connector as shown in Fig. 22, which is designed to interface with a variety of sensing boards. The expansion connector is divided into sections of 4 analog lines, 4 power control lines and an I^{2}C bus (2 lines). This external connector can be used to connect the cluster head node with different sensing devices if needed.

Wireless Section

It consists of AT86RF230 [84] transceiver chip. This chip provides a complete radio transceiver interface between the antenna and the microcontroller. It comprises the analog radio transceiver and the digital demodulation including time and frequency synchronization and data buffering. It operates in 2.4 GHz ISM band. The transmit modulation scheme is offset-QPSK (O-QPSK) with half-sine pulse shaping and 32-length block coding. An internal 128 byte RAM for RX and TX (Frame Buffer) buffers the data to be transmitted or the received data.

RF230-LPC1768 interface

Radio chip and the microcontroller have been interfaced through SPI and additional control signals. Serial Peripheral Interface (SPI) comprises pins SEL, SCLK, MOSI (Master Out Slave In) and MISO (Master In Slave Out). The radio chip behaves as a slave SPI device. This SPI is used for frame buffer and register access. Microcontroller supplies the clock signal via SCI pin to SCLK. To initialize the communication, microcontroller pulls the SEL pin to low and data sent to transceiver through the MOSI pin and data received from the transceiver through MISO pin. CLKM, IRQ, SLP_TR and RST are the additional control lines which are connected to the GPIO/IRQ interface of the microcontroller LPC1768. A low signal on RST pin resets the transceiver. The SLP_TR pin is used to start the wireless transmission of the data stored in the internal buffer. CLKM is used to clock the microcontroller in the absence of the external crystal of microcontroller. In our design, this pin has not been connected. The interface between AT86RF230 and LPC1768 has been shown in Fig. 23.

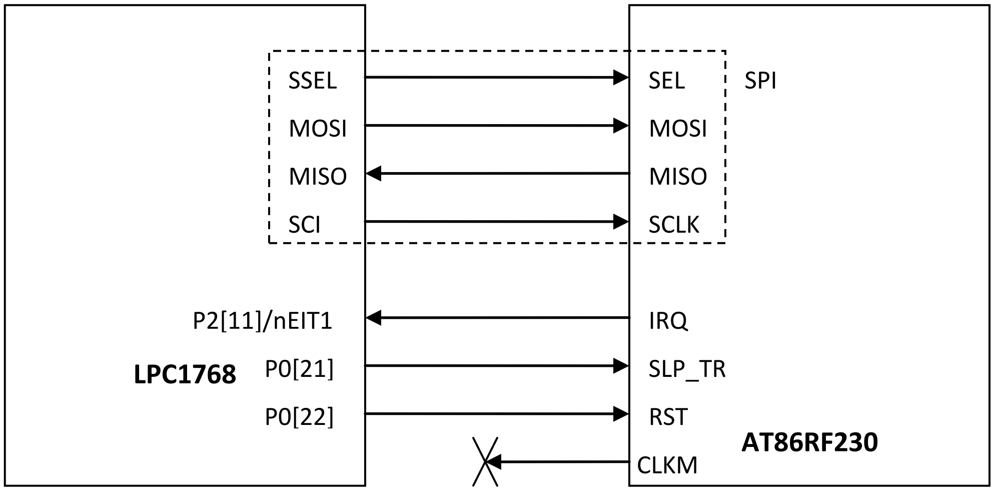


Fig. 23 LPC1768 to AT86RF230 interface

AT86RF230-Antenna interface

The other interface from radio chip is the interface between the chip and antenna. RF230 provides a differential RF port (RFP/RFN) which is designed for a 100Ω differential load. 50 Ω antenna has been used with the single feeder line for prototype board. Hence to convert the 100 Ω balanced differential RF port to 50 Ω single ended RF port balun is used. The differential port should connect via a series capacitor to the balun to provide AC coupling of the RF signal to RF pins. The balun output is connected to SMA connector. This connection alone doesn't guarantee the maximum power transfer between the radio and antenna. Hence the trace lines between the RF chip and antenna should be impedance control lines for maximum power efficiency. The routing of RF output pins RFP and RFN to balun input must have differential impedance of 100 Ω and likewise the routing between balun output to antenna connector must have impedance of 50 Ω. While designing PCB layout of this part care need to be taken so that trace lines don't result in significant impedance mismatch. The block diagram of AT86RF230 to antenna interface is shown in fig. 24.

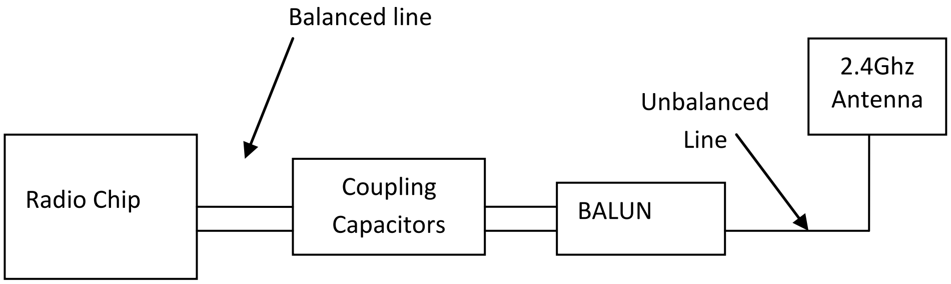


Fig. 24 AT86RF230 to antenna interface

USB Interface

The Universal Serial Bus (USB) is an external bus being used here to provide a fast and functional means for connecting board to PC. Three characteristics that define the USB technology are speed, power, and convenience [86][87]. The block diagram of USB interface is given in Fig. 25.

- When board is connected to PC the cluster head node extracts power required for all operation through USB port only.
- The cluster head node forwards all the data collected through radio communication to PC at high data rate. It also can be configured to take data from PC and transmit it through radio interface.
- USB gives convenience as it is plug and play, automatic detect and it is easily available in all PCs.

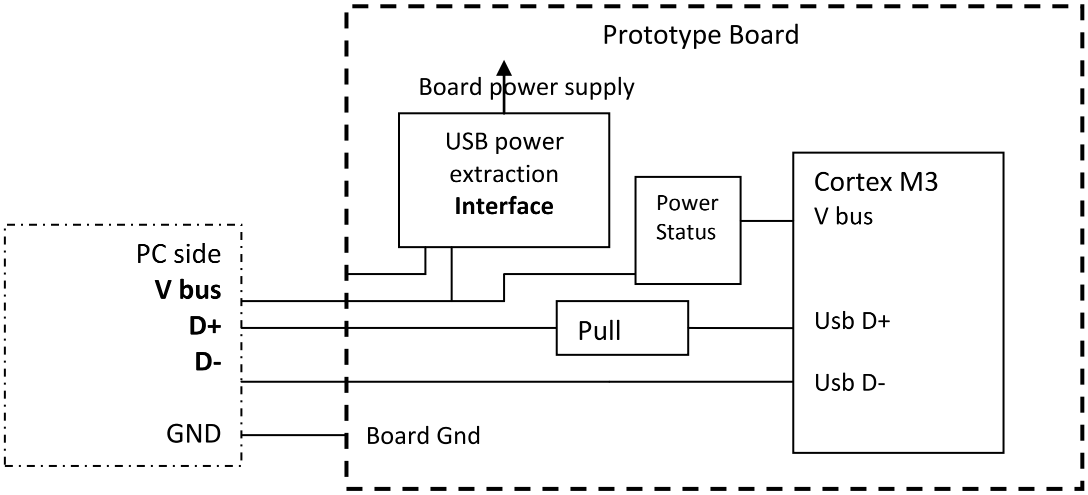


Fig. 25 USB Interface

The specifications of the cluster head node developed in-house are given in Table 8.

Table 8. Specifications of the Cluster Head node

1	Microcontroller	LPC1768
2	Interfaces	2 UART, I^{2}C support, SPI, GPIO
3	External ADC Interface	12 bit successive approximation A/D converter (AD7327) - 8 channels
4	Internal ADC	12 bit successive approximation A/D converter- 6 channels
5	Special Feature	Integrated humidity and temperature sensor.
6	Industrial enclosures	Protection against hostile industrial environment.
7	Transceiver	AT86RF230 / AT86RF231
8	Antenna	2.4GHz. Omni directional antenna
9	Modulation scheme	Offset Quadrature Phase Shift Keying (O-QPSK)
10	Spreading method	Direct Sequence Spread Spectrum (DSSS)

	Power Source Options	
11	Input Power	Single phase 230VAC supply
	Battery Power	11.1 ~ 11.5 V DC @ 1150mAh
12	Output Power	12V, 5V, 3V DC @ 833mA

3.2.3. Router node

Each sensor node comprises of a sensing unit, microcontroller, ADC, memory, transceiver and a power unit. In a network based on the location of deployment of coordinator and end devices, many router nodes may be required to be used for forwarding the data to the base station. Hence routing node has been designed and developed in house which is compatible to both Xbee and Xbee pro transceivers [75]. Block diagram of the routing node is shown in Fig. 26

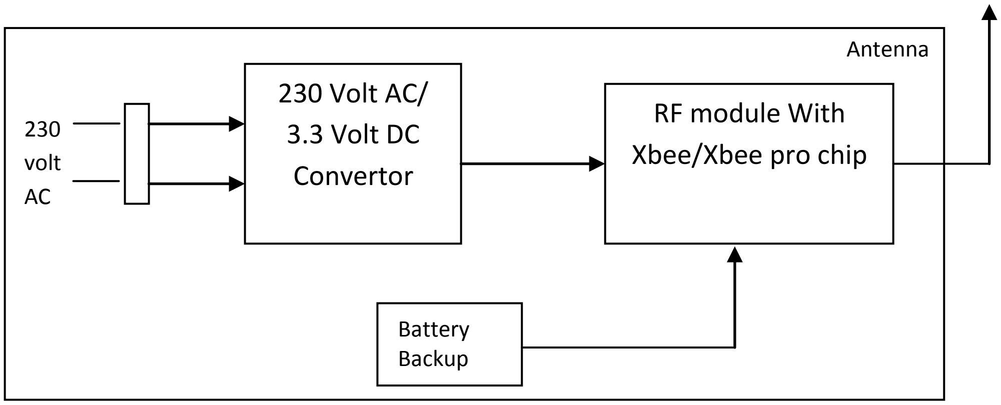


Fig. 26 Block diagram of WSN Routing Node

The designed routing node requires only 3.3 volt DC to work, hence an SMD regulator which provides 3.3volt DC with 1200mA current rating from 230 volts AC is used. The node has been provided with a Reset button which is easily accessible from outside. LED indicators are also provided for A*ssociate* and *RSSI* Pins to indicate the association with the network and the signal strength. As the nodes will be placed in remote areas, it has been developed with rechargeable battery backup. The image of the routing node is given in Fig. 27.

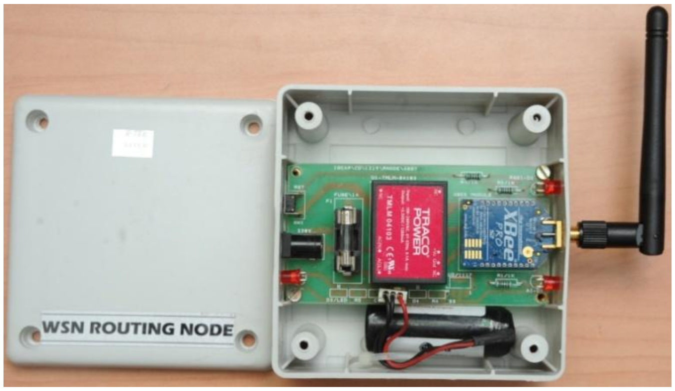


Fig. 27 In-house Developed Router Node

3.2.4. Base station Node

Base station or Gateway node is a collection unit in any wireless sensor network to gather data from distributed sensor nodes. It is interfaced with a PC via USB to display the received data in GUI and log it in database. As it will not do any processing with the received data, microcontroller is not needed. It simply needs a transceiver and power supply unit. The simple diagrammatic explanation of the functioning of base station is given in Fig. 28.

To collect data from the deployed network which consists of in-house developed sensor nodes and router nodes, it is necessary to have the base station developed in-house. It is designed compatible to both Xbee and Xbee pro chips. The designed base station has a transceiver unit powered from USB. As the transceiver unit needs only 3.3V DC, the 5V DC from the USB has been regulated to 3.3V. The photograph of the in-house developed basestation node is shown in Fig. 29.

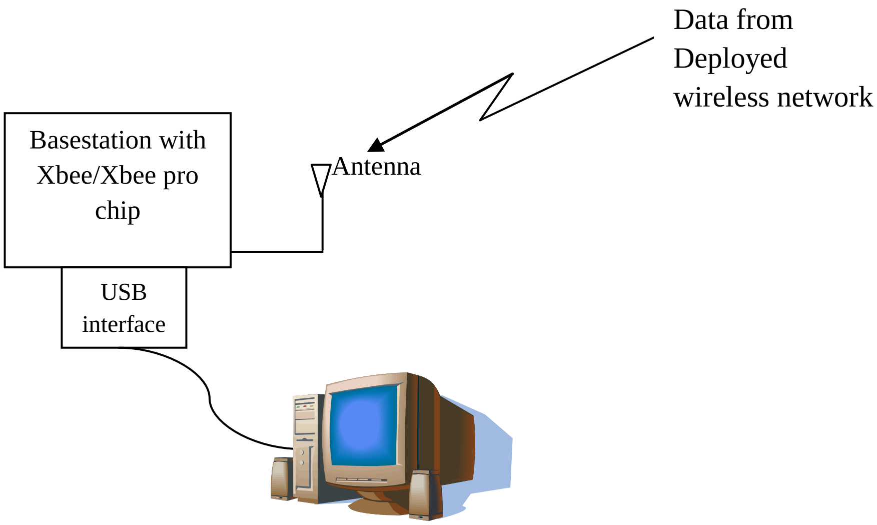


Fig. 28 Functioning of Basestation Node

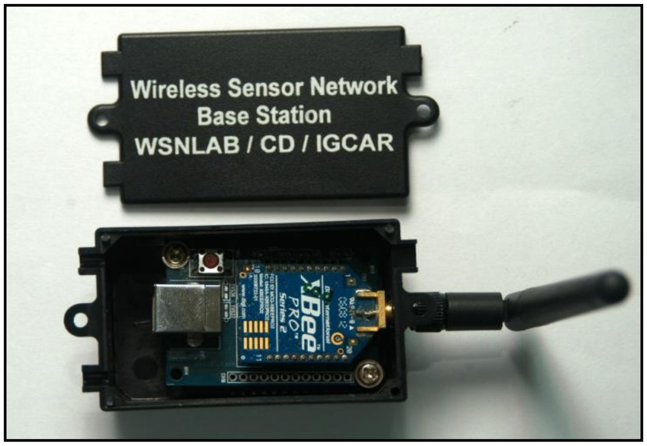


Fig. 29 Basestation Node

3.2.5. Actuator Node

Sensor nodes gather information about the physical world and transmit the collected data to basestation. But data collection alone may not be sufficient in some applications. Some control actions, specific to application is essential to prevent mishaps or incidents. For this purpose actuator nodes are required [88]. Basestation is used to bridge sensor nodes to the actuator nodes. Actuator node performs actions to change the behavior of the environment / physical system. Effective use of actuator node enhance the reliability in event control and reporting.

Actuator node has been developed at IGCAR for INSOT WSN deployments and the details are given below. The hardware annunciation of sodium leak signal is achieved by using actuator node. Actuator PCB shown in Fig.1 consists of a relay contact which is energized when sodium leak signal appears. This triggers the buzzer connected to it and gives alarm to alert the operators. Manual reset for annunciation is provided by the acknowledge push button of the actuator PCB. Actuator circuit schematic is shown in Fig. 30.

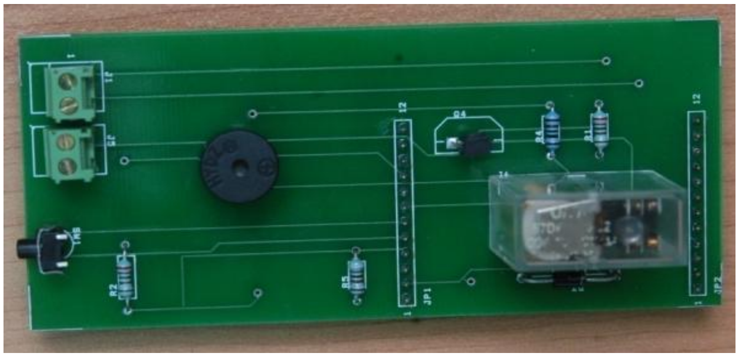


Fig. 30 Actuator PCB

In Fig. 31, NPN transistor Q4 is being used to control relay with a 12V coil, operating from a +12V supply. Series base resistor R1 is used to set the base current for Q4, so that the transistor is driven into saturation (fully turned on) when the relay is to be energized. That way, the transistor will have minimal voltage drop, and hence dissipate very little power as well as delivering most of the 12V to the relay coil. Power diode D3 is connected across the relay coil, to protect the transistor from damage due to the back-EMF pulse generated in the relay coils Inductance when Q4 turns off.

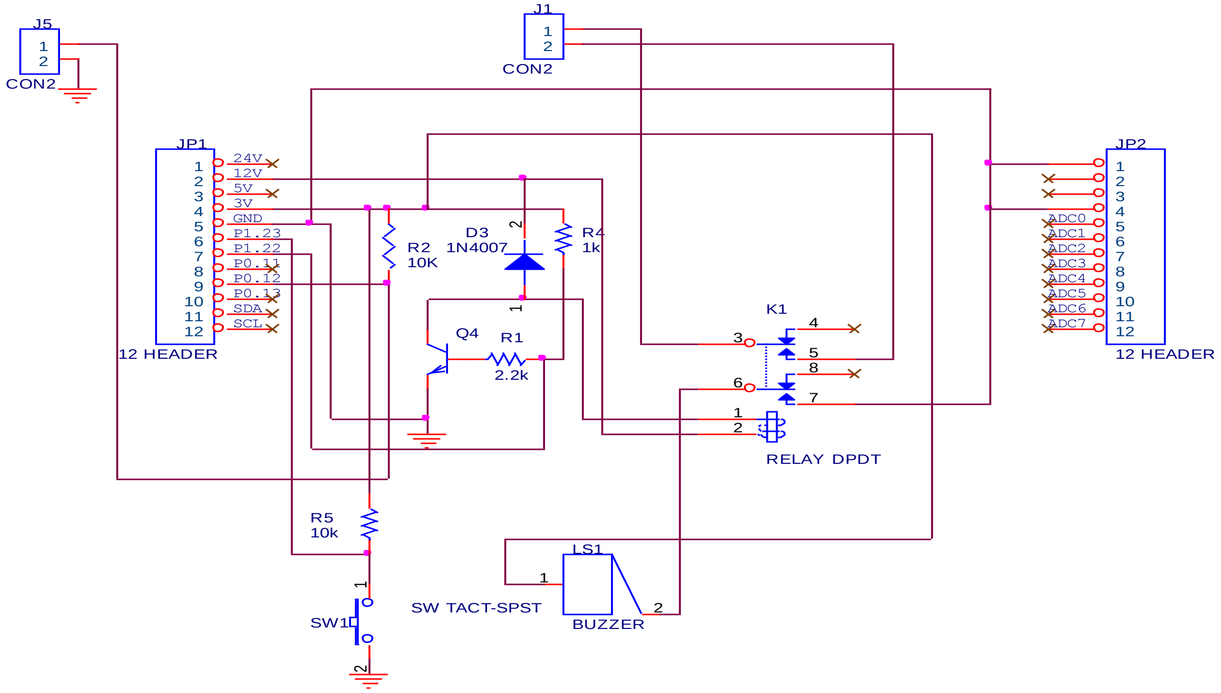


Fig. 31 Schematic of Actuator PCB

The Actuator PCB has been designed, developed and connected with the main board of the sensor node. It has been placed in the INSOT WSN and tested for its functionality.

3.3. Development of Software Stack

Wireless sensor network applications are often characterized by energy restriction, less processing power and small memory footprint. The limitation of hardware resources generally makes development of system software challenging. So, the software optimization is essential and is done. Code optimization and memory optimization has also been incorporated with the stack. Hence the application developer needs to consider different alternatives for the system software [89]. Generally operating system based design is preferred because it provides a framework for the convenient and easy application software development. The advantages of OS based design are concurrency, efficient memory and I/O management, separation of OS kernel and application code. Some of the examples are Tiny OS, Contiki, Free RTOS, µOS, Pico OS and Sens OS. Contiki OS is designed for energy and memory constrained embedded networked systems and hence it is useful for wireless sensor network applications [90-92]. It also supports multithreading, event driven programming and inter process communication using message passing. Hence Contiki OS has been chosen for the development of software stack for in-house developed nodes.

Software stack has been written in accordance with the 802.15.4 for prototype sensor boards. The architecture of communication stack is shown in Fig. 32.

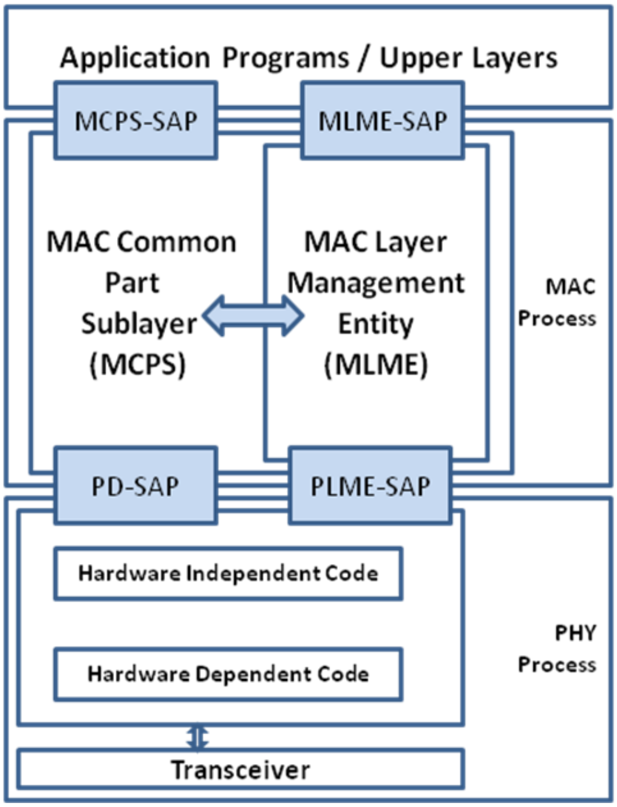

Application Programs / Upper Layers
MCPS-SAP
MLME-SAP
MAC Common Part Sublayer (MCPS)
MAC Layer Management Entity (MLME)
MAC Process
PD-SAP
PLME-SAP
Hardware Independent Code
Hardware Dependent Code
PHY Process
Transceiver

Fig. 32 IEEE 802.15.4 Communication Stack Architecture

In this implementation, PHY and MAC layers are implemented as Contiki processes *phy_proc* and *mac_process*. Physical layer process controls the driver code for radio chip. Transceiver used in our WSN node is AT86RF230. It is compliant with IEEE 802.15.4 2.4 GHz physical layer and also automates the some of the MAC layer functions such as such as FCS computation, energy detection / RSSI computation, CSMA-CA, frame retransmission, frame acknowledgement and address filtering. This lower layer has been divided into two parts to facilitate reuse of upper layer code for future platforms. Hardware dependent part defines the low-level hardware and interrupt functions to control the operations of the radio chip and hence control the behavior of the radio chip. Hardware independent part configures different network parameters and also implements data transmission and reception functions. Radio and hardware dependent and independent code of *phy_process* together constitutes the Physical layer of the IEEE 802.15.4.

Media Access Control sub-layer provides the addressing and channel access mechanisms for several nodes to communicate within multiple access network that incorporates a shared wireless medium. *mac_process* implements the non beacon mode of MAC sub layer of the IEEE 802.15.4. The MAC layer provides the interface between physical layer and next higher layer above the MAC layer. The MAC layer provides the services to next higher layer through two entities- MAC management service MLME (MAC Layer Management Entity) and MAC data service MCPS (MAC Common Part Layer). These two entities can be accessed through their respective SAPs (Service Access Points) - MCPS-SAP and MLME-SAP, by the next higher layer.

MAC layer implements request/confirm or indication/response primitive to provide the service to higher layer. This primitive handling scheme should be implemented as an asynchronous operation, so that it should not block the control flow. These services have been implemented as separate blocks, which are invoked by their respective primitives. In our implementation, these primitives are implemented as callback functions, the format of which has been derived from IEEE 802.15.4.

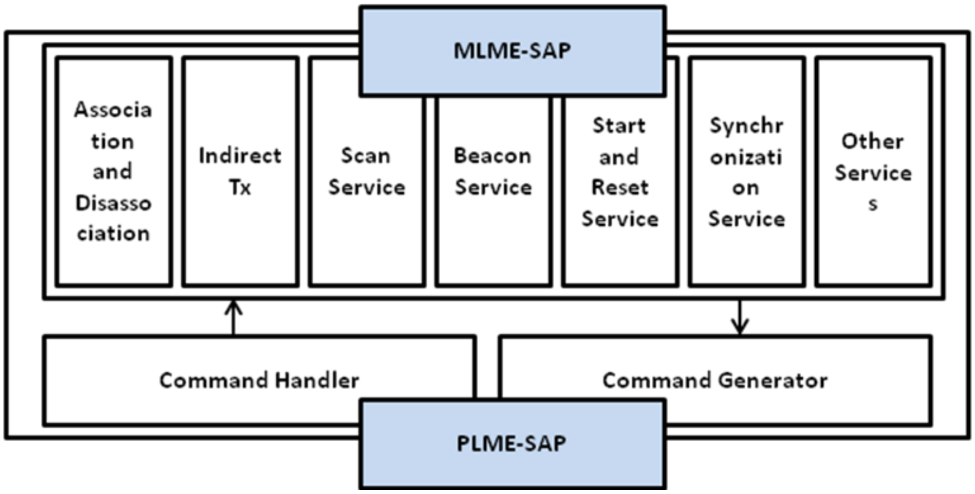


Fig. 33 MAC Service Handler

The reception of transmission frame at radio chip is reported to the *phy_process*, which then retrieves the frame from the chip using hardware dependent code. This event will then be reported to MAC sub layer after putting the received frame in the MAC receive queue. MAC process then calls the event handler which then retrieves the frame from the MAC receive queue and passes to the frame parser. Frame parser then segregates the frames based on the frame control type. There are four types of frames: data frames, acknowledge frames, command frames and beacon frames. Command frames sent to the command handler, based on the type of command will be handed to their respective service handlers. Arrival of other frames, along with the content will be notified to the higher layer. Transmission of the frame is enabled by implemented driver code at PHY layer.

The developed 802.15.4 MAC can be used to develop different application programs to implement different network topologies. Different application programs which are based on the MAC layer have been developed and tested with the WSN nodes. Following application development works have been carried out using developed software stack-

1. Zigbee is a low cost, low power, wireless mesh standard, which defines higher layer protocols for low power digital radios based on IEEE 802.15.4. Open source Zigbee stack has been ported to the prototype WSN board using MAC stack.

2. IEEE 802.15.4 also supports 128 bit AES standard for security. Security layer has been enabled in developed MAC layer. Radio chip used in this case is AT86RF231.
3. This stack has been used for 802.15.4/ Zigbee sniffer development in conjunction with Wireshark network protocol analyzer

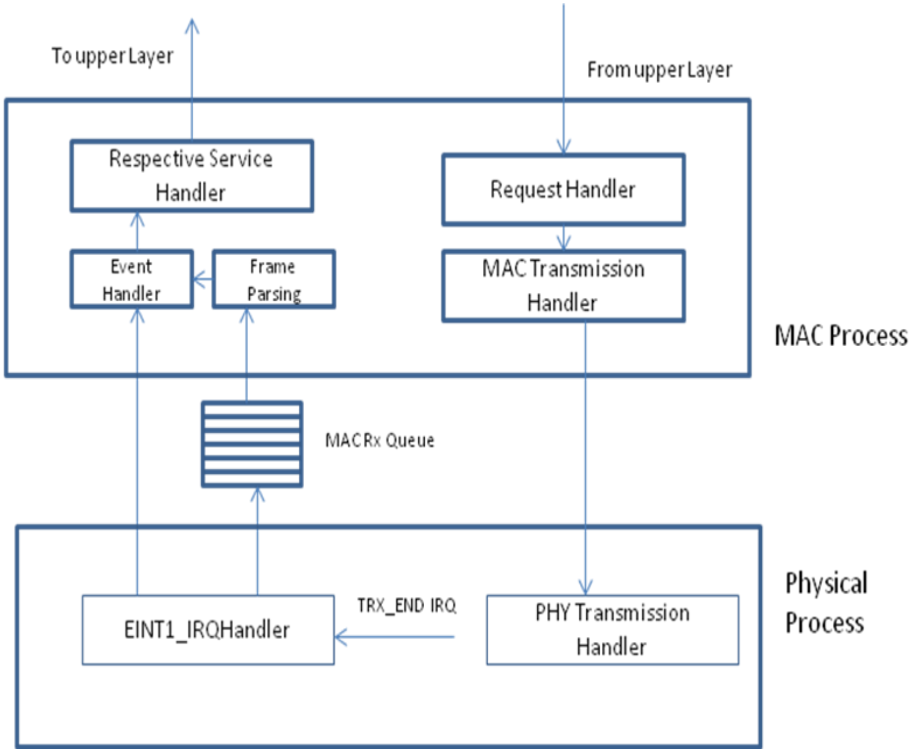


Fig. 34 Communication Process Model

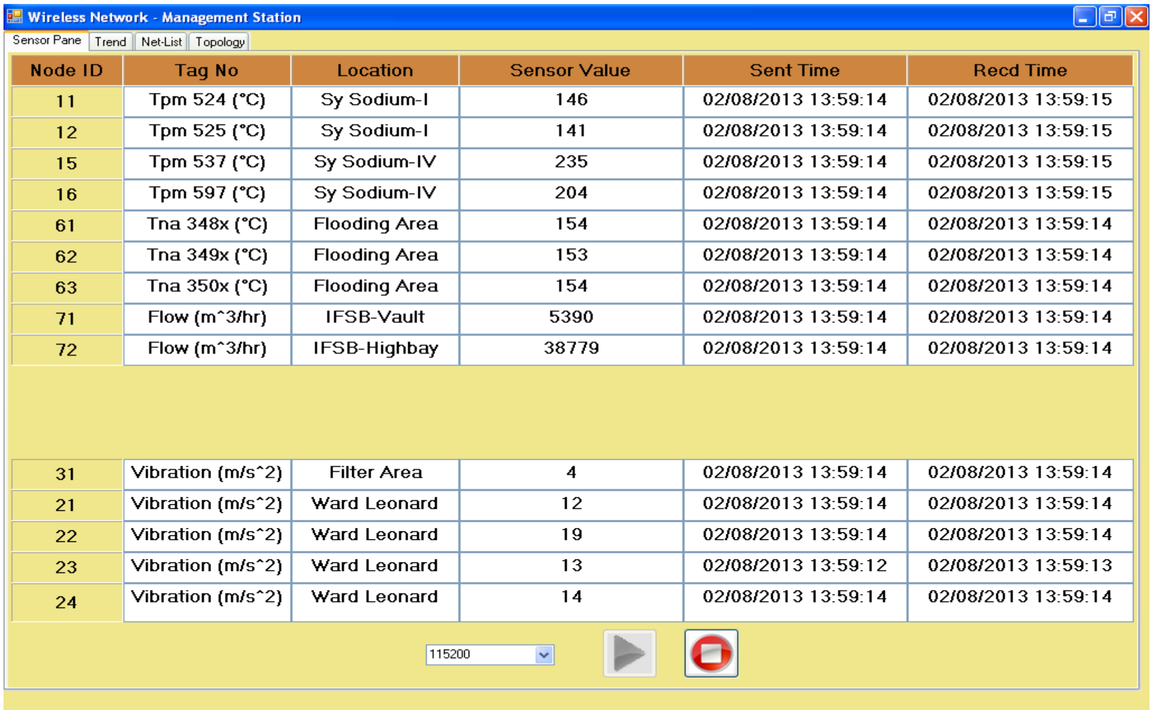
3.4. Development of WSN Management Systems

For any deployed network, either wired or wireless, the Network Management System (NMS) is mandatory for the proper administration and maintenance. NMS is a combination of hardware and software used to monitor and administer a computer network or networks. In wired network an NMS manages the network elements, also called managed devices. Device management includes faults, configuration, accounting, performance and security (FCAPS) management. Management tasks include discovering network inventory, monitoring device health and status, providing alerts to conditions that impact system performance, and identification of problems, their source(s) and possible solutions.

Similar to wired network, to manage and configure wireless sensor network nodes from a remotely located base station, a Wireless Network Management Station (WNMS) has been designed and developed. Since the requirements of the WSN are extremely different form that of wired network, the specifications and requirements of WNMS vary widely from a standard wired NMS. WNMS is implemented to receive sensor readings, packet sent time and packet received time and displays them at PC connected to base station node. WNMS has various tabs like ‘sensor pane’, ‘trend view’, ‘network topology’ and ‘network list’ for providing convenience to the network administrator. It is having database connectivity for logging various events and the data collected from the sensors. Following are the different views of WNMS developed in-house:

Sensor Pane

In this tab, the wirelessly transmitted sensor reading is being displayed alongside its node ID, tag number, location and unit of the sensor reading. Time at which each packet has been created (Sent Time) and time at which the packet was received at the base station (Recd. Time) were also displayed in the tab. To manually synchronise the nodes at desired time, command can be sent from WNMS by clicking on the synchronize button. This will sent the current time to all nodes and synchronise them. Baud rate at which PC has to communicate with the coordinator can also be set from this tab. By default it has been set to 115200 bauds per second. Command buttons to open or close the COM port being used has been provided. Auto-detection of coordinator node has been made, so while the WNMS starts it will open port of coordinator using preset default settings.



Node ID	Tag No	Location	Sensor Value	Sent Time	Recd Time
11	Tpm 524 (°C)	Sy Sodium-I	146	02/08/2013 13:59:14	02/08/2013 13:59:15
12	Tpm 525 (°C)	Sy Sodium-I	141	02/08/2013 13:59:14	02/08/2013 13:59:15
15	Tpm 537 (°C)	Sy Sodium-IV	235	02/08/2013 13:59:14	02/08/2013 13:59:15
16	Tpm 597 (°C)	Sy Sodium-IV	204	02/08/2013 13:59:14	02/08/2013 13:59:15
61	Tna 348x (°C)	Flooding Area	154	02/08/2013 13:59:14	02/08/2013 13:59:14
62	Tna 349x (°C)	Flooding Area	153	02/08/2013 13:59:14	02/08/2013 13:59:14
63	Tna 350x (°C)	Flooding Area	154	02/08/2013 13:59:14	02/08/2013 13:59:14
71	Flow (m^3/hr)	IFSB-Vault	5390	02/08/2013 13:59:14	02/08/2013 13:59:14
72	Flow (m^3/hr)	IFSB-Highbay	38779	02/08/2013 13:59:14	02/08/2013 13:59:14
31	Vibration (m/s^2)	Filter Area	4	02/08/2013 13:59:14	02/08/2013 13:59:14
21	Vibration (m/s^2)	Ward Leonard	12	02/08/2013 13:59:14	02/08/2013 13:59:14
22	Vibration (m/s^2)	Ward Leonard	19	02/08/2013 13:59:14	02/08/2013 13:59:14
23	Vibration (m/s^2)	Ward Leonard	13	02/08/2013 13:59:12	02/08/2013 13:59:13
24	Vibration (m/s^2)	Ward Leonard	14	02/08/2013 13:59:14	02/08/2013 13:59:14

115200

Fig. 35 Sensor Data View of WNMS

Trend View

In this tab, the graph of sensor readings data of individual nodes for the past half an hour will be shown. Graph will have time as X-axis and also contains legend of individual node Ids. WNMS scans the sensor readings every 10 seconds once and updates it in this trend tab. Any data older than half an hour will be deleted to accommodate new values. Manually refreshing the chart can be done by clicking anywhere on the chart.

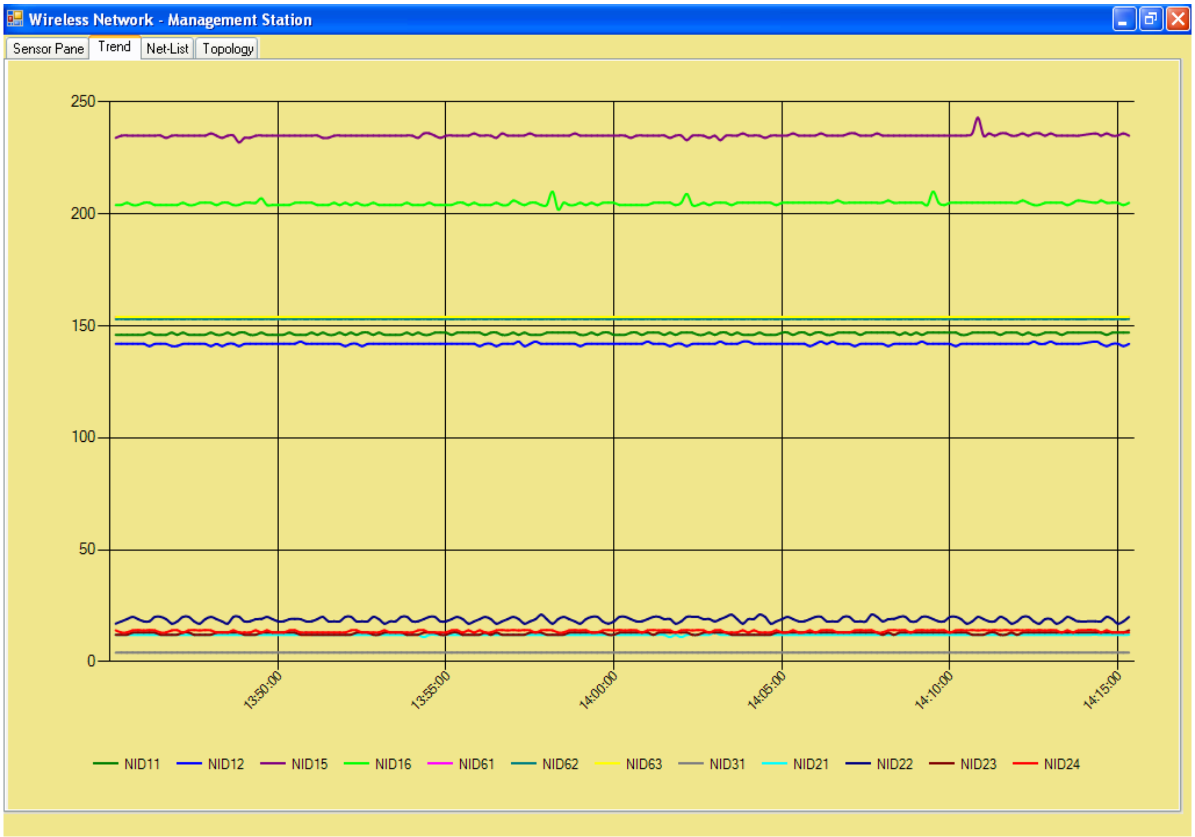
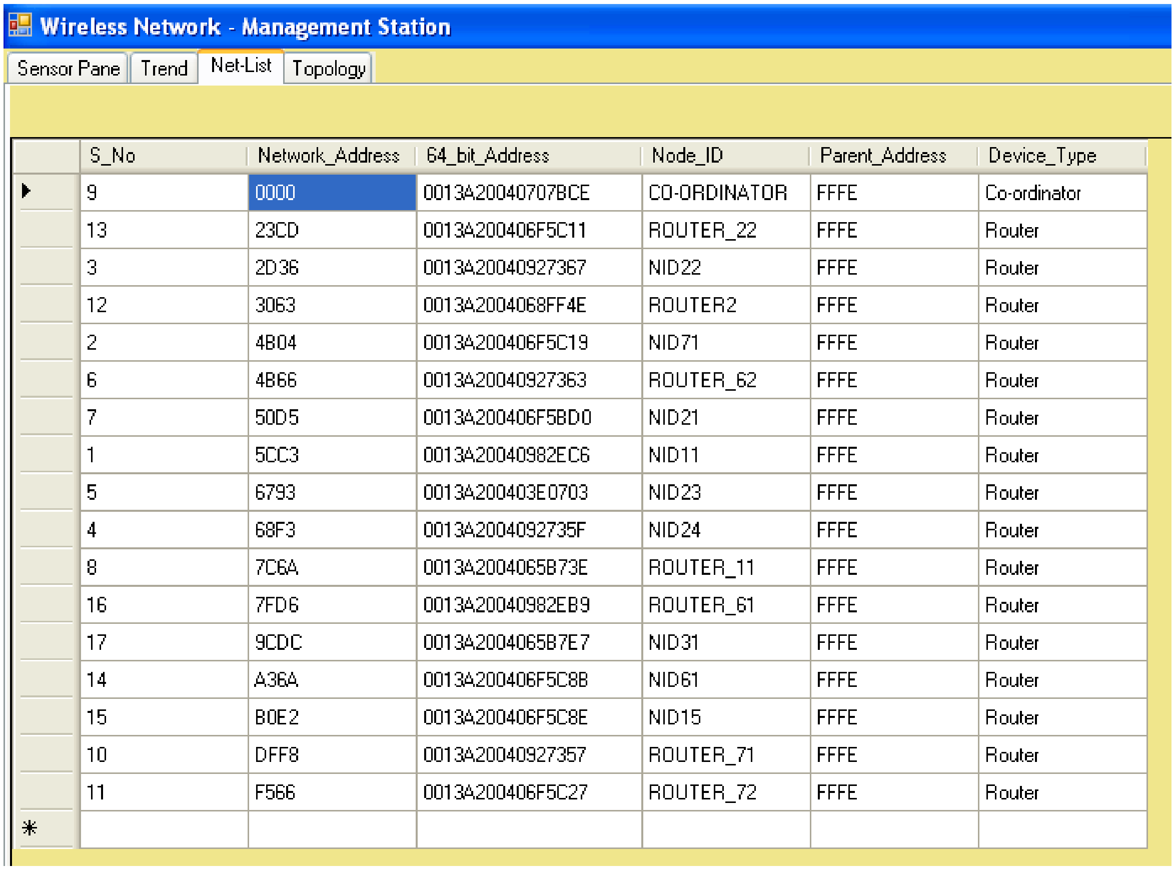


Fig. 36 Trend View of WNMS

Network List view

Individual nodes in the network will be enquired for its information by sending a network discovery command from base station. Each node will furnish data like 16-bit network address, 64-bit XBee address, its node ID, its parent 16-bit network address (if any) and device type (whether it is a Router or End device or Co-ordinator). This command can be manually sent at any time by the network administrator and the list of nodes in the network will be updated in this network list tab. Any new node if joined will be appended in the table without deleting the older nodes or the order.



S_No	Network_Address	64_bit_Address	Node_ID	Parent_Address	Device_Type
9	0000	0013A20040707BCE	CO-ORDINATOR	FFFE	Co-ordinator
13	23CD	0013A200406F5C11	ROUTER_22	FFFE	Router
3	2D36	0013A20040927367	NID22	FFFE	Router
12	3063	0013A2004068FF4E	ROUTER2	FFFE	Router
2	4B04	0013A200406F5C19	NID71	FFFE	Router
6	4B66	0013A20040927363	ROUTER_62	FFFE	Router
7	50D5	0013A200406F5BD0	NID21	FFFE	Router
1	5CC3	0013A20040982EC6	NID11	FFFE	Router
5	6793	0013A200403E0703	NID23	FFFE	Router
4	68F3	0013A2004092735F	NID24	FFFE	Router
8	7C6A	0013A2004065B73E	ROUTER_11	FFFE	Router
16	7FD6	0013A20040982EB9	ROUTER_61	FFFE	Router
17	9CDC	0013A2004065B7E7	NID31	FFFE	Router
14	A36A	0013A200406F5C8B	NID61	FFFE	Router
15	B0E2	0013A200406F5C8E	NID15	FFFE	Router
10	DFF8	0013A20040927357	ROUTER_71	FFFE	Router
11	F566	0013A200406F5C27	ROUTER_72	FFFE	Router

Fig. 37 NetList View of WNMS

Network Topology

In the field, a node will route a packet to its destination using its routing table. In this way a definite path between the nodes is followed for each packet to reach base station. This topology can dynamically change due to various reasons, to adapt to the changes in the field. In this tab, all the nodes in the network are displayed as an icon with its node ID, 16-bit network address and its device type. Even WNMS can differentiate sensor connected node and other nodes. The topology view of how individual nodes are connected towards base station alone is drawn using an arrowed line depicting real-time topology of nodes in the field.

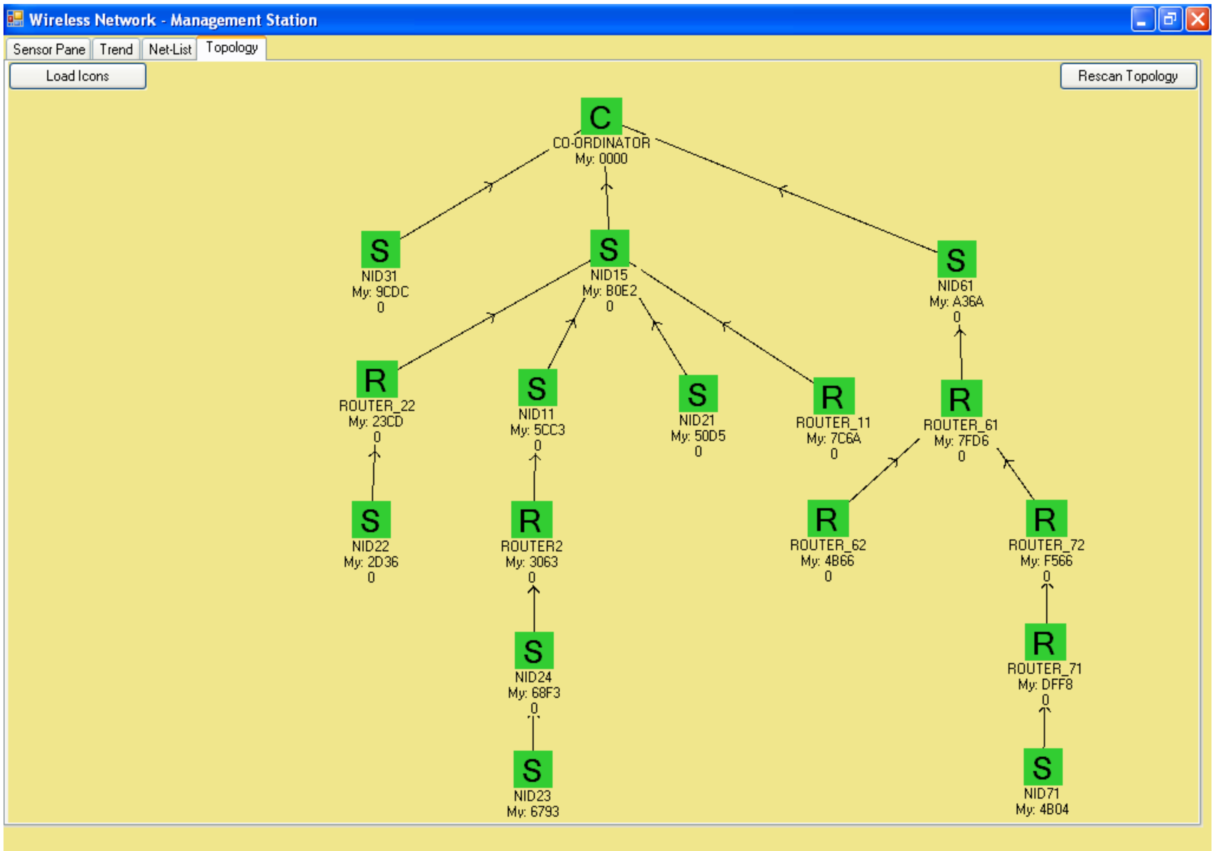


Fig. 38 Topology View of WNMS

In background, every node will be enquired for its routing table in the order of network list table. WNMS will wait for duration of one second for the response of nodes. Based on the response, indications to show that the nodes are active or busy or not communicating through 3 levels of colour change (viz. green, orange and red) is provided. If a particular node is not responding in the first query, green colour icon changes to orange colour; if not responding for next query, icon changes to red colour and stays red till it gets a valid response from the node.

As initial development, Visual Basic 6 was used for building WNMS. Due to lack of multithreading in VB6, it exhausted a single CPU core. To overcome this problem and to increase the efficiency of WNMS, it has been upgraded using VB2010 with multithreading.

WNMS has been incorporated with additional features like auto-detection of nodes, setting up of PC baud rate to interface with the coordinator, synchronizing time across all the nodes and some more code optimisations for better performance of the GUI.

3.5. Development of Security Protocol

In general, communication channel is insecure and an adversary may try to extract the critical data by eaves dropping the messages exchanged between the legitimate sensor nodes in a network. Hence security is an essential requirement for nuclear applications. For the wireless sensor networks inside reactor complex, a Simple Security Protocol (SSP) has been designed and developed.

For any WSN, before deploying, each node is assigned a unique ID from a set of legitimate IDs by an authority. Also the keys are already established while deployment. The protocol is designed in such a way that it can successfully route the packets to the intended destination with non zero probability. The goal of our developed protocol is to address the basic security requirements like data secrecy and authentication along with a simple re-keying mechanism to improve the level of security. Although it is anticipated that the life time of the key shared between the nodes exceeds the life time of the nodes, it is possible in some cases that the life time of the key expires and re-keying should take place. New keys need to be generated in an efficient way. Re-keying increases the security by extending the life time of the key.

SSP is developed in the second generation mote operating system (TinyOS-2.x) and designed to run on all the platforms. The issue of life time of key is addressed by providing 3 methods of re-keying namely parallel generator, serial generator and rotates.

Data Confidentiality, Authentication and Integrity

SSP provides two modes of operation namely: authentication only and authentication with encryption. In Authentication only mode the MAC is computed over the data and it is sent along with the payload by the sender. The receiver recomputes the MAC in the same way as the sender does it. A packet will be accepted in case if the two values are equal otherwise it will be rejected. In SSP, the MAC is computed using the Cipher Block Chaining Message Authentication Code (CBC-MAC) [97]. The MAC computed is of 4 bytes length. The following shows the data exchanged between the nodes A and B using Authentication only mode: $A \rightarrow B : D_A \| MAC(K_{AB},D_A)$.

Where: A and B are communicating nodes; D_A denotes the plain text (sensor readings) sent by the node A; K_{AB} denotes the master (symmetric) key shared between the nodes A and B; M_A denotes the encrypted message sent by the node A; C_A denotes the 16-bit counter value maintained by the node A and MAC (K_{AB},M) denotes the computation of message authentication code over (MAC) of a message M with MAC key as (K_{AB},M).

In Authentication and encryption mode, the data is encrypted and MAC is computed over the encrypted data and is sent along with the payload. For encryption it is ideal to choose an energy and memory efficient cryptographic algorithm. Even though SkipJack [98] has a poor memory efficiency, it is the most energy efficient cryptographic algorithm. Energy consumption affects the network life time and hence it is an important requirement in the sensor networks. Hence the block cipher used in our protocol is SkipJack.

Typically for an 'x' byte block cipher, a mode of operation is typically required to break the 'x' bytes and to use the block cipher in a special way to encrypt the message block by block. We use the Cipher Block Chaining (CBC) mode [99] of operation with Cipher Text Stealing (CTS) [11] as the data encryption scheme. The CBC mode of encryption is given by $C_i = E_k(P_i \oplus C_{i-1})$, C_o= IV where as the decryption operation is given by $P_i = D(C_i) \oplus C_{i-1}$, C_o= IV where C is the cipher text block, P is the plain text block, E is the encryption function and IV is the initialization vector. The CTS allows processing of messages that are not evenly divisible into blocks.

The data exchanged between the nodes A and B using Authentication and encryption mode is : $A \rightarrow B : M_A \| C_A \| MAC(K_{AB},M)$. Here a counter is maintained which will be used in Initialization vector(IV) . The IV is unique in order to provide semantic security. The length of IV is 8 bytes. The format is Dest || Src || len || handler || C_{source} where dest and src denotes the destination address and source address, len denotes the length of the message sent, handler denotes the AM message handler and C_{source} denotes the 16 bit counter maintained by the source node. We transmit the C_{source} along with the payload so that the receiver can learn about the counter used in IV at sender.

Re-keying Mechanism

In SSP, semantic security is achieved by using re-keying mechanisms. Since a 2 byte counter is being used, after 65536 packets are sent (using same key for the same data between a pair of nodes), the key needs to be modified. Hence re-keying mechanism should be adopted after every 2^16 packets are transmitted.

We employ a simple yet effective key update scheme. The key update mechanisms include: parallel method, serial method and rotation. The parallel method consists of setting $K_i= F_{K_{i-1}}(K_0)$ and serial method sets $K_i=F_{K_{i-1}} (K_{i-1})$ where the re-keying function F can be same as the block cipher used in encryption. In the rotate method the key is rotated one bit circularly left. All the methods do not require extensive computation.

The key packet contains only the method adopted for re-keying. No key is sent in the message. In this way the overhead of transmitting the new key is avoided. It also guarantees that an adversary can have no idea about the new key being generated as a result of re-keying mechanism.

Re-keying in Unicast communication

In case of unicast communication, the re-keying process is

A → B : Key_Mode

B → A : Ack

After sending the key packet (Key_Pkt), the node 'A' blocks the sending and receiving of normal data packet until it receives an acknowledgment from node 'B'. Upon receiving the key packet, node 'B' performs the same re-keying operation and sends back an acknowledgment (Ack) to the ‘A’. The node ‘A’ resumes the data sending and receiving after the acknowledgment has arrived.

There is a possibility of key packet or acknowledgment being lost during the transit. In case if a key packet/acknowledgment is lost, the node 'A' re-transmits the same key packet (without performing the re-keying operation) after waiting for a random back-off period. Re-transmission can be done up to a maximum of three times. The node 'B' is assumed to be dead or compromised if it does not send the acknowledgment even after three re-transmissions. In such a case, the node 'A' can stop further communication with 'B'.

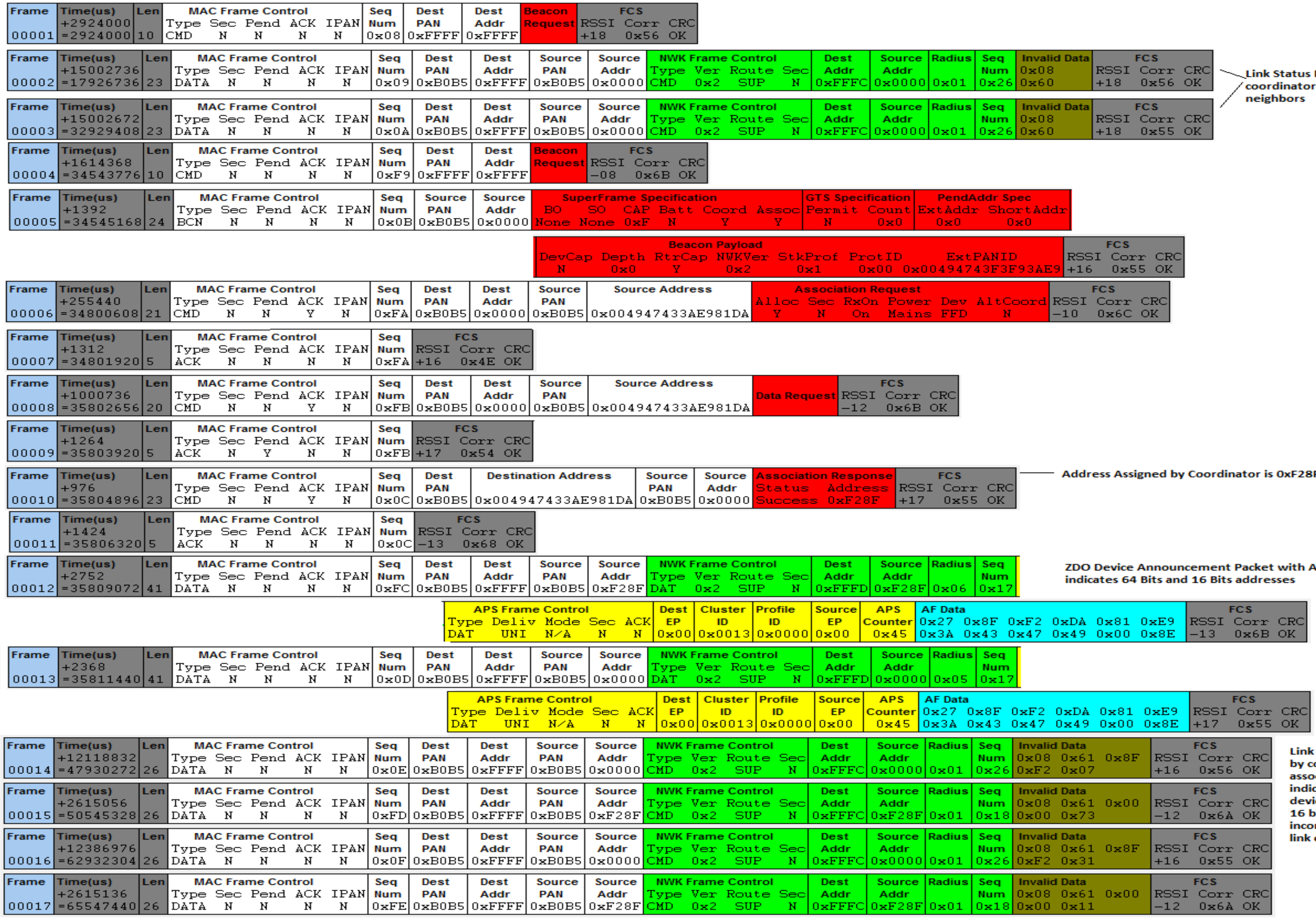
3.6. Development of Wireless Sniffer

A packet analyzer is a combination of software and hardware that can intercept the traffic passing over a digital network or a part of network. Captured packets then can be decoded to show the content of various fields in the packet and can be analyzed. It is useful in troubleshooting the problem which can arise during the development and deployment. Packet analyzer solutions are very important component in network traffic analysis. Network traffic analysis is the process of capturing network traffic and then analyze it to determine anomaly and security vulnerability in the network. Information gathered during traffic analysis then can be useful to improve the network deployment and network security strategies. In the wired network, there are different tools available for packet captures and analysis, such as Wireshark [100][104], tcpdump, snoop, ngrep.

In case of wireless communication, the role of packet analyzer becomes more important because in some of the cases it is the only way to analyze the different types of packet. In case of wired network, it is easy to capture network traffic without knowing anything upfront about network parameters. But in the case of wireless this process becomes complicated.

Wireless networks use shared medium for transmission, hence they can operates on multiple channels to avoid the interference from other wireless networks. Hence it is required to select the operating channel before any capture. Channel hopping can be used to detect the operating channel for target network. Other problem could be distance between transmitting nodes and sniffer hardware, variation in range can cause incomplete data traffic capture. Installed WiFi cards can be used to capture the packet in monitoring mode.

In WSN, Packet analyzer is useful during deployment phase, to analyze different network scenarios and traffic monitoring. It can also be used in development phase for protocol debugging. Some of the commercially available Zigbee sniffers are Zena [101], Smart RF Protocol Packet Sniffer [102], Peryton Series of sniffers for IEEE 802.15.4/ ZigBee/ RF4CE/ 6LoWPAN [103] etc. During initial development Zena has been used for packet capture and analysis. Fig. 39 shows the captured packets using Zena Network Analyzer.



```
Frame|Time(us)  |Len|   MAC Frame Control        |Seq |Dest  |Dest  |Beacon |     FCS
     |+2924000  |   |Type Sec Pend ACK IPAN      |Num |PAN   |Addr  |Request|RSSI Corr CRC
00001|=2924000  |10 |CMD   N   N    N    N       |0x08|0xFFFF|0xFFFF|       |+18  0x56 OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Dest  |Dest  |Source|Source|NWK Frame Control  |Dest  |Source|Radius|Seq |Invalid Data|     FCS
     |+15002736 |   |Type Sec Pend ACK IPAN |Num |PAN   |Addr  |PAN   |Addr  |Type Ver Route Sec |Addr  |Addr  |      |Num |0x08        |RSSI Corr CRC
00002|=17926736 |23 |DATA  N   N    N    N  |0x09|0xB0B5|0xFFFF|0xB0B5|0x0000|CMD  0x2  SUP   N |0xFFFC|0x0000|0x01  |0x26|0x60        |+18  0x56 OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Dest  |Dest  |Source|Source|NWK Frame Control  |Dest  |Source|Radius|Seq |Invalid Data|     FCS
     |+15002672 |   |Type Sec Pend ACK IPAN |Num |PAN   |Addr  |PAN   |Addr  |Type Ver Route Sec |Addr  |Addr  |      |Num |0x08        |RSSI Corr CRC
00003|=32929408 |23 |DATA  N   N    N    N  |0x0A|0xB0B5|0xFFFF|0xB0B5|0x0000|CMD  0x2  SUP   N |0xFFFC|0x0000|0x01  |0x26|0x60        |+18  0x55 OK
```

Link Status Messages by coordinator 0x60 indicates No neighbors

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Dest  |Dest  |Beacon |     FCS
     |+1614368  |   |Type Sec Pend ACK IPAN |Num |PAN   |Addr  |Request|RSSI Corr CRC
00004|=34543776 |10 |CMD   N   N    N    N  |0xF9|0xFFFF|0xFFFF|       |-08  0x6B OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Source|Source|   SuperFrame Specification        |GTS Specification|   PendAddr Spec
     |+1392     |   |Type Sec Pend ACK IPAN |Num |PAN   |Addr  | BO   SO  CAP Batt Coord Assoc      |Permit  Count    |ExtAddr ShortAddr
00005|=34545168 |24 |BCN   N   N    N    N  |0x0B|0xB0B5|0x0000|None None 0xF  N    Y     Y        | N       0x0     | 0x0      0x0

                                                   |                    Beacon Payload                                  |     FCS
                                                   |DevCap Depth RtrCap NWKVer StkProf ProtID      ExtPANID            |RSSI Corr CRC
                                                   |  N     0x0    Y     0x2     0x1    0x00  0x00494743F3F93AE9       |+16  0x55 OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Dest  |Dest  |Source|  Source Address  |          Association Request            |     FCS
     |+255440   |   |Type Sec Pend ACK IPAN |Num |PAN   |Addr  |PAN   |                  |Alloc Sec RxOn Power Dev AltCoord       |RSSI Corr CRC
00006|=34800608 |21 |CMD   N   N    Y    N  |0xFA|0xB0B5|0x0000|0xB0B5|0x004947433AE981DA|  Y    N   On  Mains FFD    N          |-10  0x6C OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |     FCS
     |+1312     |   |Type Sec Pend ACK IPAN |Num |RSSI Corr CRC
00007|=34801920 |5  |ACK   N   N    N    N  |0xFA|+16  0x4E OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Dest  |Dest  |Source|  Source Address  |            |     FCS
     |+1000736  |   |Type Sec Pend ACK IPAN |Num |PAN   |Addr  |PAN   |                  |Data Request|RSSI Corr CRC
00008|=35802656 |20 |CMD   N   N    Y    N  |0xFB|0xB0B5|0x0000|0xB0B5|0x004947433AE981DA|            |-12  0x6B OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |     FCS
     |+1264     |   |Type Sec Pend ACK IPAN |Num |RSSI Corr CRC
00009|=35803920 |5  |ACK   N   Y    N    N  |0xFB|+17  0x54 OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Dest  |Destination Address|Source|Source|Association Response|     FCS
     |+976      |   |Type Sec Pend ACK IPAN |Num |PAN   |                   |PAN   |Addr  |Status   Address    |RSSI Corr CRC
00010|=35804896 |23 |CMD   N   N    Y    N  |0x0C|0xB0B5|0x004947433AE981DA |0xB0B5|0x0000|Success  0xF28F     |+17  0x55 OK
```

Address Assigned by Coordinator is 0xF28F

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |     FCS
     |+1424     |   |Type Sec Pend ACK IPAN |Num |RSSI Corr CRC
00011|=35806320 |5  |ACK   N   N    N    N  |0x0C|-13  0x68 OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Dest  |Dest  |Source|Source|NWK Frame Control  |Dest  |Source|Radius|Seq
     |+2752     |   |Type Sec Pend ACK IPAN |Num |PAN   |Addr  |PAN   |Addr  |Type Ver Route Sec |Addr  |Addr  |      |Num
00012|=35809072 |41 |DATA  N   N    N    N  |0xFC|0xB0B5|0xFFFF|0xB0B5|0xF28F|DAT  0x2  SUP   N |0xFFFD|0xF28F|0x06  |0x17

                         |   APS Frame Control      |Dest|Cluster|Profile|Source|APS    |AF Data                        |     FCS
                         |Type Deliv Mode Sec ACK   |EP  |ID     |ID     |EP    |Counter|0x27 0x8F 0xF2 0xDA 0x81 0xE9 |RSSI Corr CRC
                         |DAT   UNI  N/A   N   N    |0x00|0x0013 |0x0000 |0x00  | 0x45  |0x3A 0x43 0x47 0x49 0x00 0x8E |-13  0x6B OK
```

ZDO Device Announcement Packet with AF Data indicates 64 Bits and 16 Bits addresses

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Dest  |Dest  |Source|Source|NWK Frame Control  |Dest  |Source|Radius|Seq
     |+2368     |   |Type Sec Pend ACK IPAN |Num |PAN   |Addr  |PAN   |Addr  |Type Ver Route Sec |Addr  |Addr  |      |Num
00013|=35811440 |41 |DATA  N   N    N    N  |0x0D|0xB0B5|0xFFFF|0xB0B5|0x0000|DAT  0x2  SUP   N |0xFFFD|0x0000|0x05  |0x17

                         |   APS Frame Control      |Dest|Cluster|Profile|Source|APS    |AF Data                        |     FCS
                         |Type Deliv Mode Sec ACK   |EP  |ID     |ID     |EP    |Counter|0x27 0x8F 0xF2 0xDA 0x81 0xE9 |RSSI Corr CRC
                         |DAT   UNI  N/A   N   N    |0x00|0x0013 |0x0000 |0x00  | 0x45  |0x3A 0x43 0x47 0x49 0x00 0x8E |+17  0x55 OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Dest  |Dest  |Source|Source|NWK Frame Control  |Dest  |Source|Radius|Seq |Invalid Data  |     FCS
     |+12118832 |   |Type Sec Pend ACK IPAN |Num |PAN   |Addr  |PAN   |Addr  |Type Ver Route Sec |Addr  |Addr  |      |Num |0x08 0x61 0x8F|RSSI Corr CRC
00014|=47930272 |26 |DATA  N   N    N    N  |0x0E|0xB0B5|0xFFFF|0xB0B5|0x0000|CMD  0x2  SUP   N |0xFFFC|0x0000|0x01  |0x26|0xF2 0x07     |+16  0x56 OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Dest  |Dest  |Source|Source|NWK Frame Control  |Dest  |Source|Radius|Seq |Invalid Data  |     FCS
     |+2615056  |   |Type Sec Pend ACK IPAN |Num |PAN   |Addr  |PAN   |Addr  |Type Ver Route Sec |Addr  |Addr  |      |Num |0x08 0x61 0x00|RSSI Corr CRC
00015|=50545328 |26 |DATA  N   N    N    N  |0xFD|0xB0B5|0xFFFF|0xB0B5|0xF28F|CMD  0x2  SUP   N |0xFFFC|0xF28F|0x01  |0x18|0x00 0x73     |-12  0x6A OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Dest  |Dest  |Source|Source|NWK Frame Control  |Dest  |Source|Radius|Seq |Invalid Data  |     FCS
     |+12386976 |   |Type Sec Pend ACK IPAN |Num |PAN   |Addr  |PAN   |Addr  |Type Ver Route Sec |Addr  |Addr  |      |Num |0x08 0x61 0x8F|RSSI Corr CRC
00016|=62932304 |26 |DATA  N   N    N    N  |0x0F|0xB0B5|0xFFFF|0xB0B5|0x0000|CMD  0x2  SUP   N |0xFFFC|0x0000|0x01  |0x26|0xF2 0x31     |+16  0x55 OK
```

```
Frame|Time(us)  |Len|   MAC Frame Control   |Seq |Dest  |Dest  |Source|Source|NWK Frame Control  |Dest  |Source|Radius|Seq |Invalid Data  |     FCS
     |+2615136  |   |Type Sec Pend ACK IPAN |Num |PAN   |Addr  |PAN   |Addr  |Type Ver Route Sec |Addr  |Addr  |      |Num |0x08 0x61 0x00|RSSI Corr CRC
00017|=65547440 |26 |DATA  N   N    N    N  |0xFE|0xB0B5|0xFFFF|0xB0B5|0xF28F|CMD  0x2  SUP   N |0xFFFC|0xF28F|0x01  |0x18|0x00 0x11     |-12  0x6A OK
```

Link status messages by coordinator and associated device 0x61 indicates one neighbor device followed with 16 bit address and incoming and outgoing link cost

Fig. 39 Wireless Sniffed Packets: One Coordinator and One Router

Sensor node can also be used as sniffer hardware to capture packets and then captured data can be shown with appropriate GUI and packet dissector program. We have designed dedicated hardware for sniffer and Wireshark has been chosen as packet analyzer application. Following section describes the different components of the IEEE 802.15.4/ Zigbee sniffer

IEEE 802.15.4/ Zigbee Sniffer

IEEE 802.15.4/ Zigbee Sniffer has LPC1768 microcontroller and AT86RF230 wireless transceiver. It is USB powered and uses USB interface to provide fast and functional means of connecting board to PC. Fig. 40 shows the general block diagram for sniffer hardware.

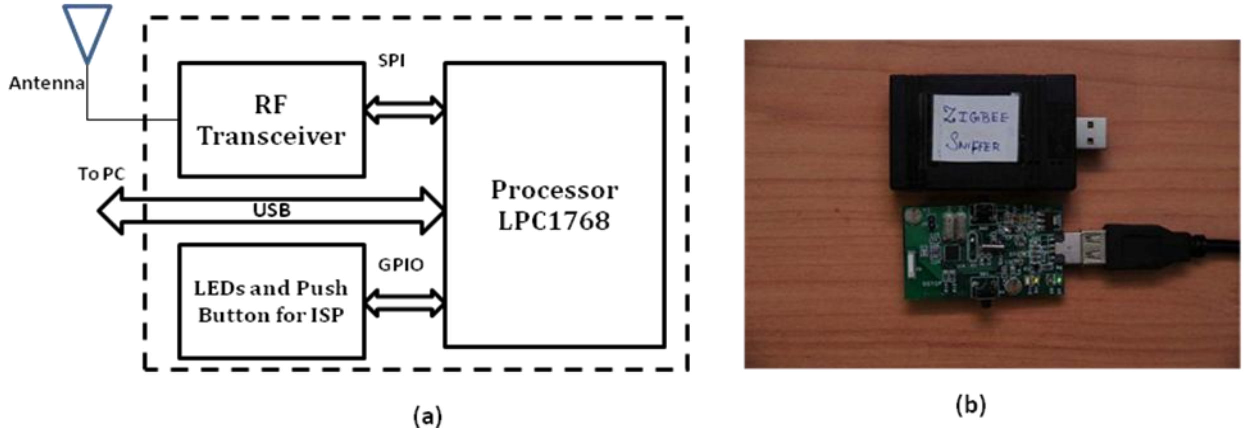


Fig. 40 Zigbee Sniffer hardware (a) Block Diagram and (b) With USB powered

It uses chip antenna and provides LED indication for 3.3V DC voltage and for one general purpose I/O line and during USB connect and USB data transfer. This hardware is pre loaded with USB boot loader, which can be activated by push button. This feature is useful for firmware upgradation.

Driver for AT86RF230 has been already written for the WSN sensor node. AT86RF230 has two operating modes namely basic operating mode and extended operating mode. Basic operating mode provides the basic radio functionalities and Extended operating mode has been designed to support IEEE 802.15.4-2003 compliant frame. To use the

AT86RF230 for sniffer the receiver should accept all the packets in the operating channel. This is only possible in the Basic operating mode of transceiver. In this mode, the address filtering (which discards all the packet not intended for this node) and auto acknowledgement feature is disabled. The radio should be in Rx listen state to accept all the packets which in this case is RX_ON. In this way, sniffer operation can be enabled using driver layer by setting the current state to the RX_ON.

Embedded code has been written to enable basic operating mode for AT86RF230. Since it is connected to the PC via USB interface, the source code also contains the USB device stack for LPC1768 USB device controller, which implements standard-compliant serial link (RS-232) emulation. All the received packets will be dumped to this virtual serial port.

Connection to Wireshark Network Protocol Analyzer

Wireshark is a network protocol analyzer, which is used for network troubleshooting, security problem examination, debugging protocol implementation and reverse engineering [104]. It is cross-platform software, which uses GTK+ widget toolkit to implement its user interface, and *lib_pcap* for packet dissection. It also supports 802.15.4 based protocols such as Zigbee and 6LoWPAN.

There are three main ways to feed the data to Wireshark-

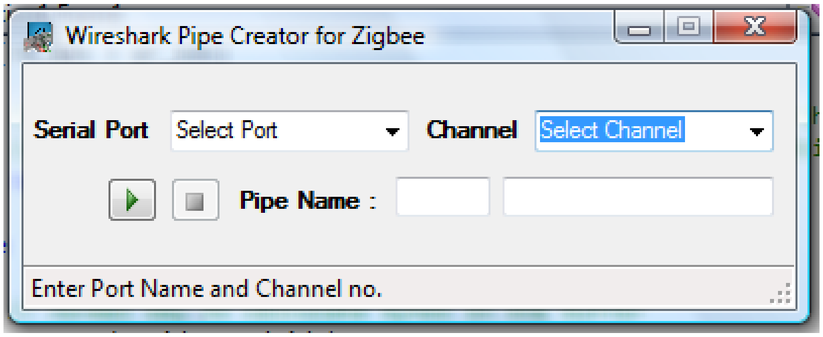
1. Data capture via network interfaces like Ethernet and/or WiFi adapter. Since we are using our own developed hardware, feeding the Wireshark is not straightforward through this method. Ethernet interface has to be emulated in the hardware and 802.15.4 frames have to be encapsulated inside Ethernet packets. Example- RZRAVEN USB Stick [105]
2. Second method is to save the captured packets into a file, which then can be read by Wireshark. Therefore it is only useful in offline analysis.
3. Third method is to use named pipe to feed the Wireshark. Example- Wireshark Zigbee Utility [106] and WSBridge [107]

In the case of second and third methods the appropriate *lib_pcap* file format header has to be added to captured packets, to make the packets recognizable in Wireshark.

We used third method to feed the Wireshark using named pipe. Named pipe is an extension for pipe concept and is one of the methods for Inter-Process Communication (IPC).

Pipes allow separate processes to communicate without designing explicitly to work together. Named pipe is also called FIFO, which refers the property of the IO stream. The “name” of a named pipe is actually a file name within the file system. As previously mentioned, all the captured packets will be sent to Virtual Serial Port. Since Wireshark uses *lib_pcap* for packet capture, appropriate headers have to be added to the received serial data packets. After creating the named pipe this serial data can be sent to the named pipe, which is then received by Wireshark.

The application for the sniffer has been written using C#. A small GUI also has been created to select the proper serial port and the channel for sniffing. Associated program to enable channel selection and start/stop the capture has been added in embedded C program which has been loaded in the sniffer hardware. Screenshots of GUI [Fig. 41, 42], which has been written in C#, and Wireshark has been shown in Fig. 43.



Wireshark Pipe Creator for Zigbee

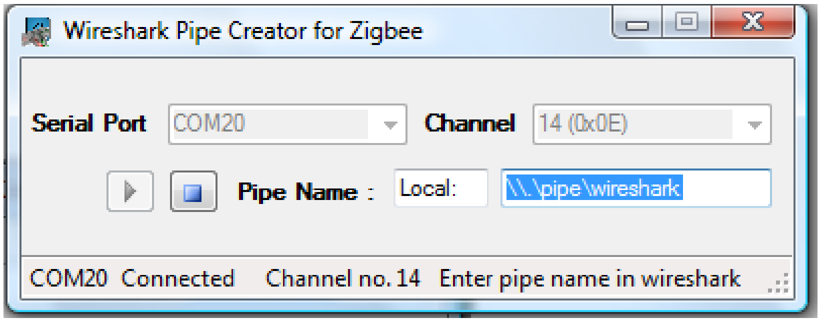
Serial Port: Select Port

Channel: Select Channel

Pipe Name :

Enter Port Name and Channel no.

Fig. 41 Screenshot of Wireshark Pipe Creator GUI



Wireshark Pipe Creator for Zigbee

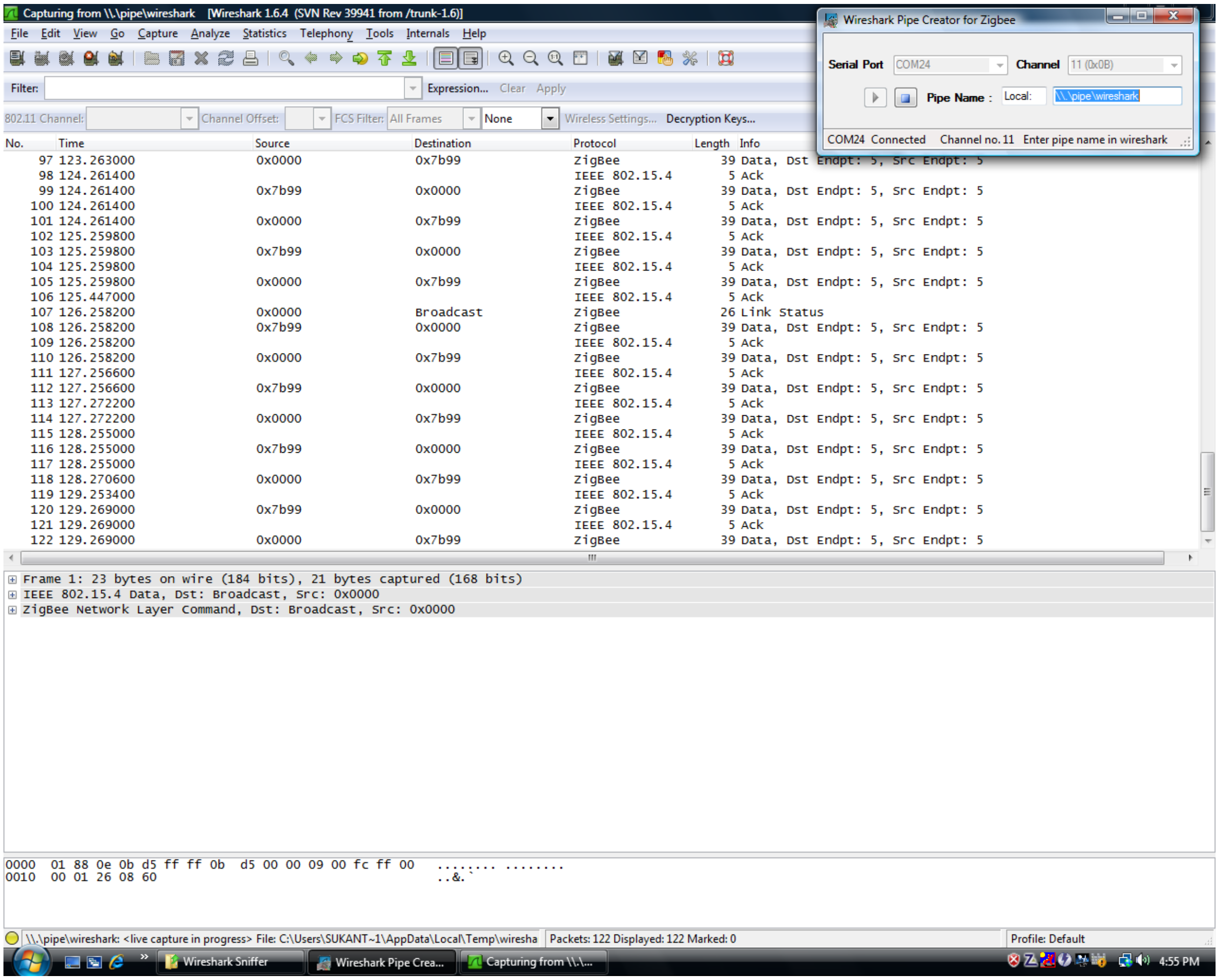
Serial Port: COM20

Channel: 14 (0x0E)

Pipe Name : Local: \\.\pipe\wireshark

COM20 Connected   Channel no. 14   Enter pipe name in wireshark

Fig. 42 Port and Channel Selection


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply
Wireless Settings... Decryption Keys...
Wireshark Sniffer
Wireshark Pipe Crea...
Capturing from \\.\...
4:55 PM

Capturing from \\.\pipe\wireshark [Wireshark 1.6.4 (SVN Rev 39941 from /trunk-1.6)]

Filter:

802.11 Channel: Channel Offset: FCS Filter: All Frames None

Wireshark Pipe Creator for Zigbee

Serial Port COM24 Channel 11 (0x0B)

Pipe Name : Local: \\.\pipe\wireshark

COM24 Connected Channel no. 11 Enter pipe name in wireshark

```
No.  Time        Source   Destination  Protocol       Length Info
  97 123.263000  0x0000   0x7b99       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
  98 124.261400                        IEEE 802.15.4   5 Ack
  99 124.261400  0x7b99   0x0000       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
 100 124.261400                        IEEE 802.15.4   5 Ack
 101 124.261400  0x0000   0x7b99       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
 102 125.259800                        IEEE 802.15.4   5 Ack
 103 125.259800  0x7b99   0x0000       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
 104 125.259800                        IEEE 802.15.4   5 Ack
 105 125.259800  0x0000   0x7b99       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
 106 125.447000                        IEEE 802.15.4   5 Ack
 107 126.258200  0x0000   Broadcast    ZigBee         26 Link Status
 108 126.258200  0x7b99   0x0000       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
 109 126.258200                        IEEE 802.15.4   5 Ack
 110 126.258200  0x0000   0x7b99       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
 111 127.256600                        IEEE 802.15.4   5 Ack
 112 127.256600  0x7b99   0x0000       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
 113 127.272200                        IEEE 802.15.4   5 Ack
 114 127.272200  0x0000   0x7b99       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
 115 128.255000                        IEEE 802.15.4   5 Ack
 116 128.255000  0x7b99   0x0000       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
 117 128.255000                        IEEE 802.15.4   5 Ack
 118 128.270600  0x0000   0x7b99       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
 119 129.253400                        IEEE 802.15.4   5 Ack
 120 129.269000  0x7b99   0x0000       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
 121 129.269000                        IEEE 802.15.4   5 Ack
 122 129.269000  0x0000   0x7b99       ZigBee         39 Data, Dst Endpt: 5, Src Endpt: 5
```

```
⊞ Frame 1: 23 bytes on wire (184 bits), 21 bytes captured (168 bits)
⊞ IEEE 802.15.4 Data, Dst: Broadcast, Src: 0x0000
⊞ ZigBee Network Layer Command, Dst: Broadcast, Src: 0x0000
```

```
0000  01 88 0e 0b d5 ff ff 0b  d5 00 00 09 00 fc ff 00   ........ ........
0010  00 01 26 08 60                                      ..&.`
```

\\.\pipe\wireshark: <live capture in progress> File: C:\Users\SUKANT~1\AppData\Local\Temp\wiresha Packets: 122 Displayed: 122 Marked: 0 Profile: Default

Fig. 43 Screenshot of Live capture using Pipe creator GUI and Wireshark

3.7. Summary

After deciding to develop the different types of wireless sensor nodes required for deployment in nuclear reactor environment, a literature survey is carried out to find suitable architecture and the microcontrollers. It was decided and the sensor nodes were developed based on ARM 7 based LPC 2138 controller. Also as there is no requirement of mobility and to avoid changing the battery power source often, the nodes were designed to be 230 V AC mains powered with required power module. To implement data aggregation and encryption, the node required more power. Hence another Cluster node based on Cortex LPC 1768 controller, RF 230 Transciever and mains powered was developed. The router nodes does not require much processing power. Hence they were developed based on X-Bee controller was developed. The base station which collects the sensed information from various nodes was developed with USB connectivity. In some applications, when the desired parameter crosses it’s threshold, it is required to alert the operator through an alarm. To meet this requirement an actuator node with hooter was developed. When the base station finds a condition that requires immediate operator attention, it sends a packet in wireless mode to the actuator node to raise the alarm through hooter. All the nodes were thoroughly tested in the laboratory before deployment. As part of the development, for easy deployment and for debugging a Wireless Network Management Station was developed for getting the topology and trend views. Also a wireless packet sniffer is developed. As the nodes are developed from abinitio complete software stack was developed. To ensure security an improved security protocol was developed.

CHAPTER 4

4. Deployment in Nuclear Applications

4.1. Introduction

After developing the required sensor node, cluster head node, router node and actuator node, base station nodes they were tested in the laboratory thoroughly. Then they were deployed in various nuclear facilities. The chapter briefly explains the deployment details in various nuclear facilities of IGCAR. It explains how the deployment is carried out first in computer division, then in IN SOdium Test facility [INSOT], Safety grade decay heat removal facility and finally in Fast Breeder Test Reactor. The deployment is carried out in all these facilities in such an order to increase the complexity with each deployment. The performance and successful operation are ensured through constant monitoring in all these facilities. The chapter explains all the details of deployment.

4.2. Deployment of WSN at Computer Division

High Performance Computing (HPC) cluster is a parallel processing system, which consists of collection of interconnected stand-alone computers cooperatively working together as a single, integrated computing resource.

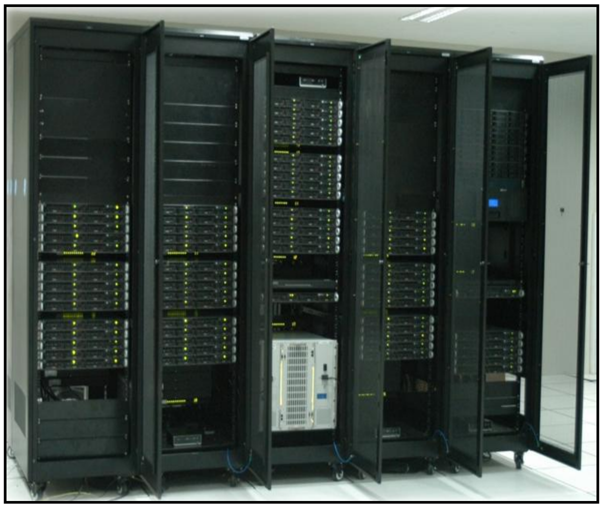


Fig. 44 128 node High Performance Computing Cluster

Need for Temperature and Humidity Monitoring

The temperature and humidity at the 2X128 node HPC clusters have to be maintained in 16˚C and 50 % RH respectively for its smooth functioning. If the air conditioning fails even for 10 minutes temperature raises beyond set limit and the HPC cluster will automatically shut down due to over temperature. As the continuous monitoring of temperature and humidity is essential in the 128 node HPC Clusters, Wireless Sensor Network has been established. The sensor node senses and transmits the current value of temperature and humidity to the base station. Network has been deployed with redundancy and fault tolerance. The data collected at base station is made available to the administrators of HPC for necessary action. Once the WSN has been established to monitor HPC cluster, it has become very simple to expand the same network to monitor the humidity and temperature of the whole computer centre.

WSN based Monitoring System at Computer Centre

The flat architecture has been chosen for WSN. This network consists of two sensor nodes with temperature sensors, two routing nodes and a base station. The computer centre layout and deployment of nodes were shown in the Fig. 45. Initially the site survey has been done using a handheld spectrum analyzer to identify the interference at 2.4GHz spectrum range. Commercially available IRIS nodes were used for initial deployment. All nodes were configured to work at 2410MHz frequency in channel 12 with 3dbm power level. The group ID was also configured. The ¼ wave dipole antenna is used.

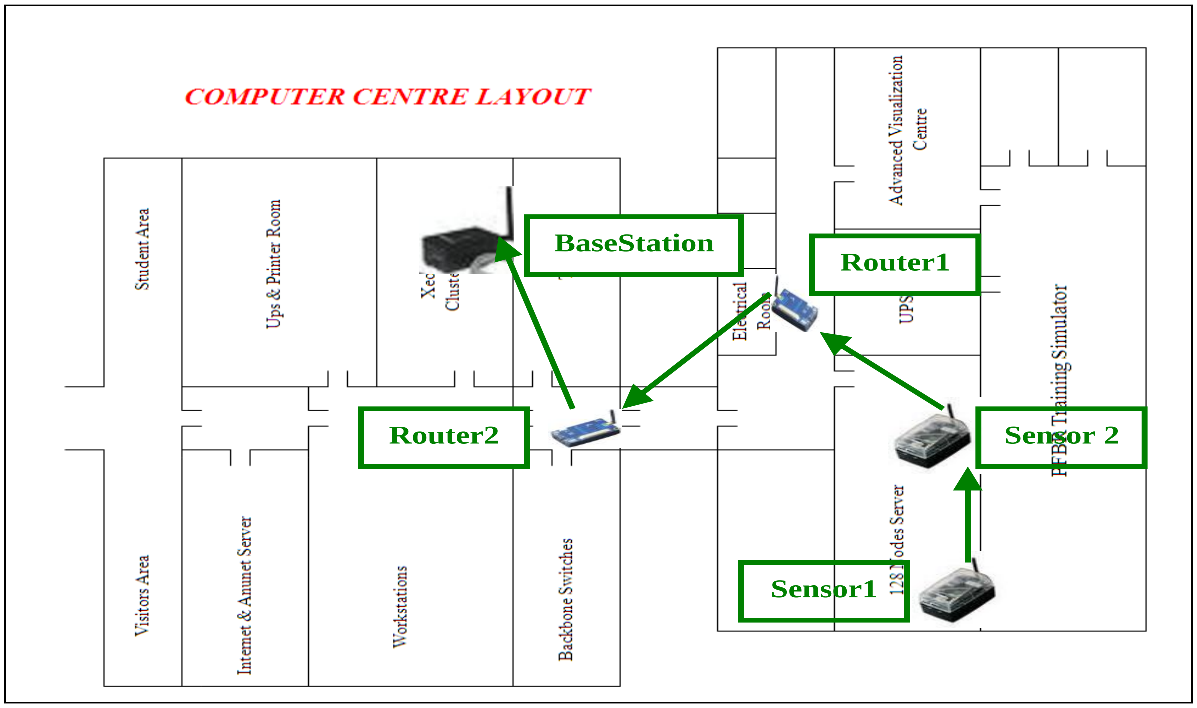


Fig. 45 Topology view of HPC Cluster Monitoring WSN

Two sensor nodes are placed inside and outside HPC rack to monitor the outlet and inlet air temperature of HPC cluster respectively as shown in Fig. 46. The signal strength has been measured for identifying the proper position of router nodes till the signal reaches the base station that is connected to the HPC administrator’s PC where the data is logged.

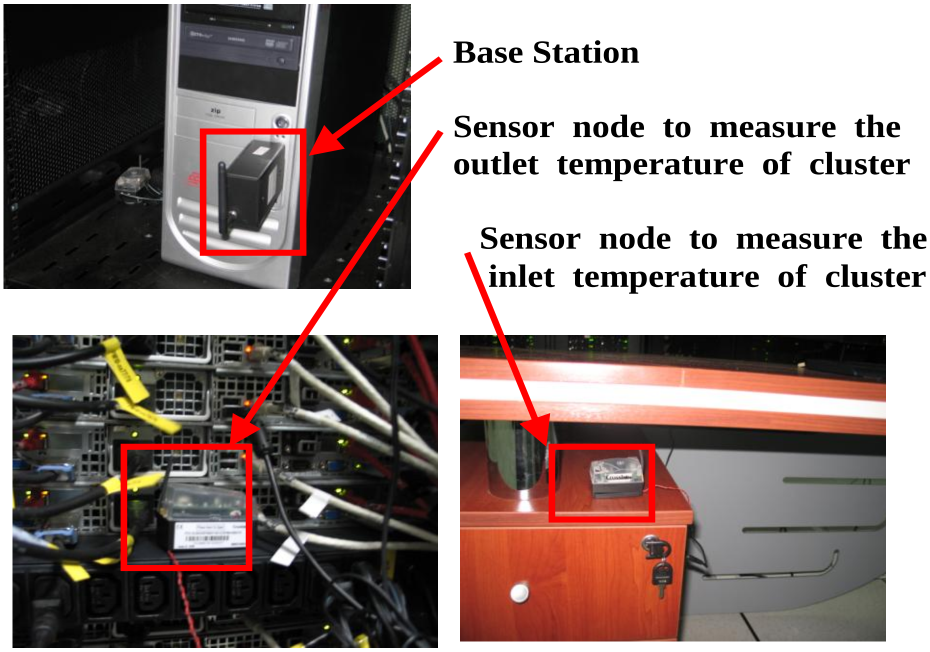

Base Station
Sensor node to measure the outlet temperature of cluster
Sensor node to measure the inlet temperature of cluster

Fig. 46 Initial WSN Deployment at CD

Enhancement of WSN at Computer Center

The performance of the initial deployment using IRIS nodes is not satisfactory. The main issue is related to battery power; for one second data rate, the batteries last for about a day only. In order to improve the network performance it is planned to replace the IRIS nodes with the in-house developed WSN sensor node. The RTD is used as temperature sensor & SHT15 is used as humidity sensor. A signal conditioning board as shown in Fig. 47 has been designed and developed.

The WSN has been expanded for monitoring the room temperature and humidity of the whole computer centre with the sensor nodes placed at Simulator room, Server room, Campus Backbone area and HPC cluster Air inlet, rack. The expanded WSN setup consists of 4 sensor nodes and 3 router nodes with Xbee chip as transceiver and a base sation. The expanded network for monitoring the whole computer centre has been named as CCNET. [Fig. 48].

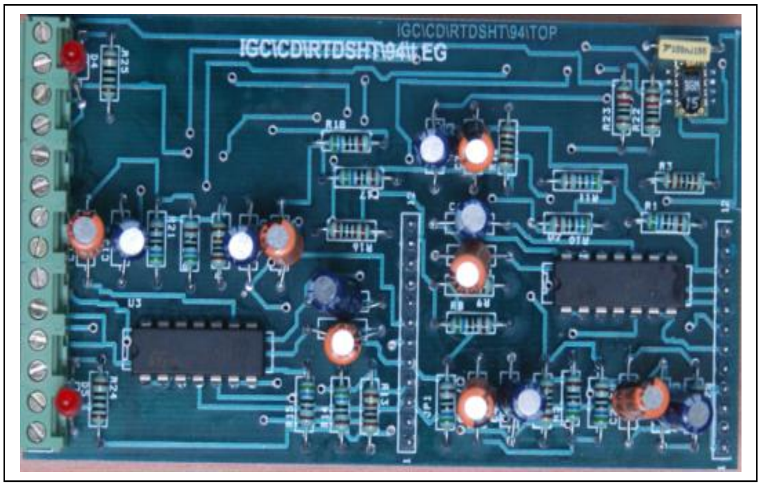


Fig. 47 Signal Conditioning board for Temperature and Humidity measurement

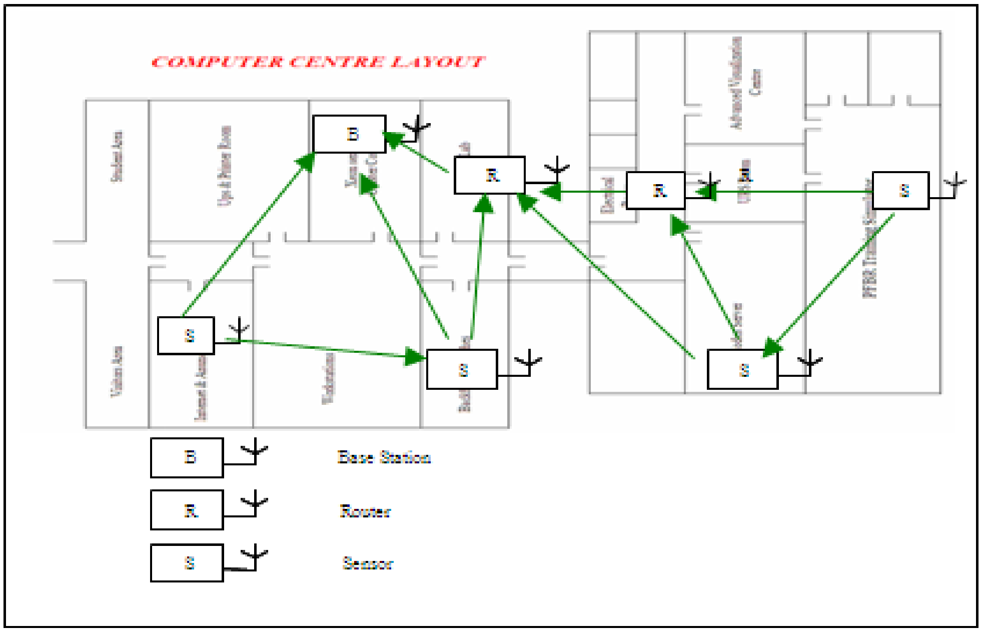


Fig. 48 Topology view of CCNET

Further the CCNET has been enhanced by replacing the USB connectivity base station with the Ethernet based gateway, designed using Wiznet module as in the Fig. 49. The collected data will be fed to Ethernet network (data highway) which can be viewed from any PC connected to network. This established setup has been effectively maintained and working well for more than 2 years.

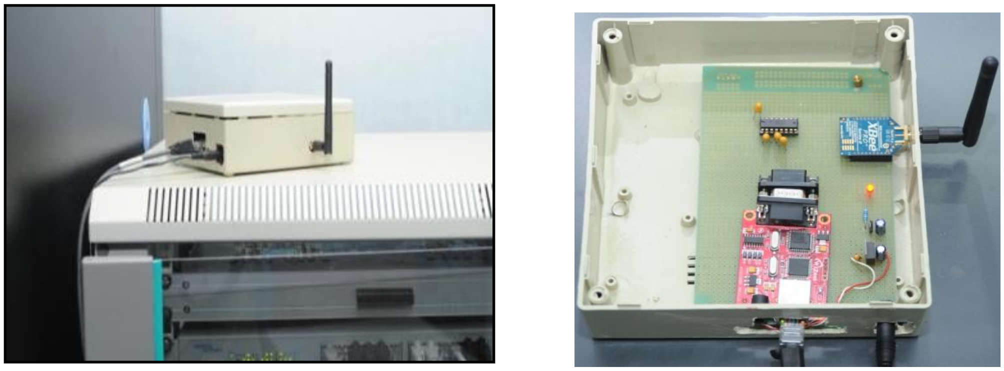
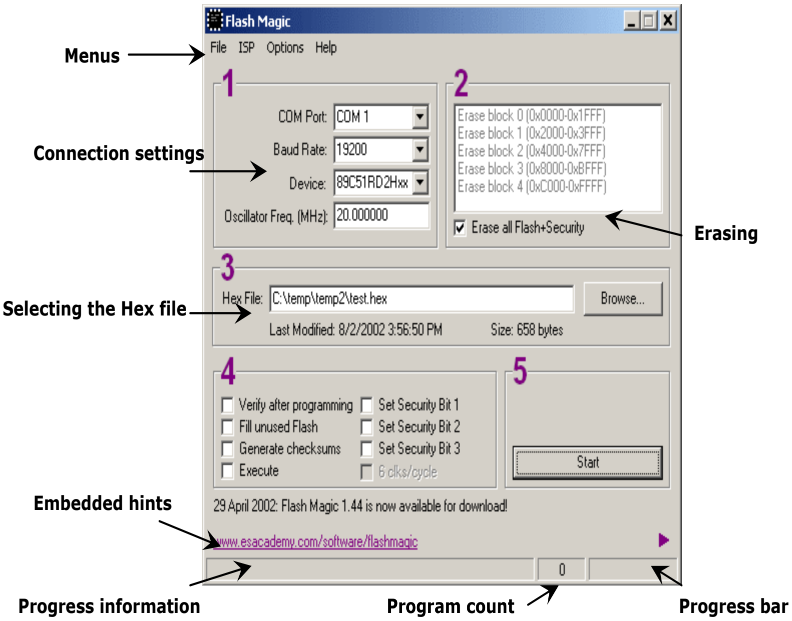


Fig. 49 Deployed Ethernet based Gateway

Software Details of Deployment

WSN based deployment the code has been developed using KEIL Embedded Development tool for ARM processor[108]. The program dynamically reads the ADC values and averages them for accuracy. The averaged values were in turn converted to engineering units using the conversion formula. The nodes were programmed with compiled hex code using the Flash Magic utility software for continuous monitoring. The screenshot of the main Flash Magic window is shown in Fig. 50. The transceiver XBee-Pro radio chips are configured to work in 2450MHz in channel 14 with 3dbm power level. Link is established for continuous data monitoring at an interval of 5 minutes. The transceiver chips were configured either as coordinator or router & end devices using X-Configuration and Test Utility (X-CTU) [109]software as shown in Fig. 51.



COM Port: COM 1
Baud Rate: 19200
Device: 89C51RD2Hxx
Oscillator Freq. (MHz): 20.000000

Erase block 0 (0x0000-0x1FFF)
Erase block 1 (0x2000-0x3FFF)
Erase block 2 (0x4000-0x7FFF)
Erase block 3 (0x8000-0xBFFF)
Erase block 4 (0xC000-0xFFFF)
☑ Erase all Flash+Security

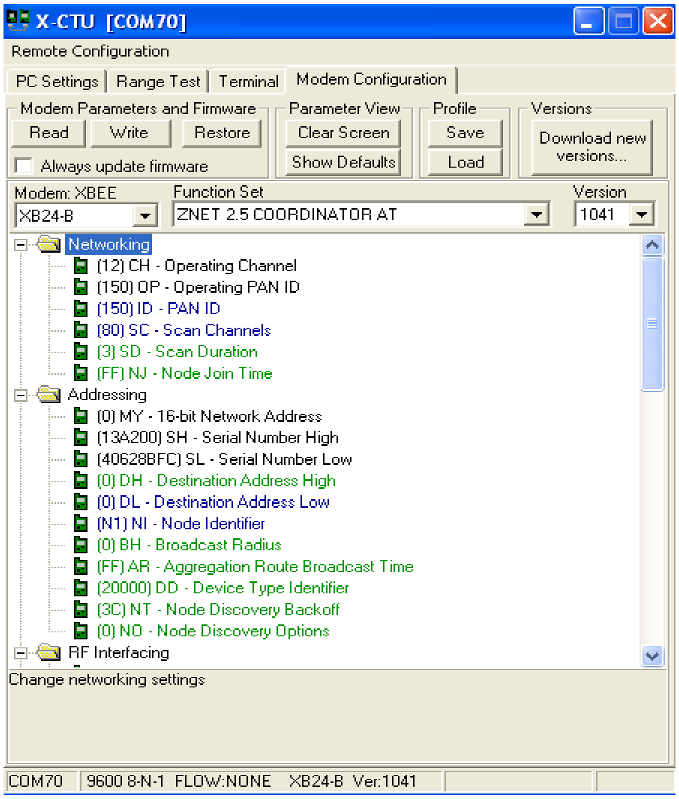
Hex File: C:\temp\temp2\test.hex
Last Modified: 8/2/2002 3:56:50 PM Size: 658 bytes

□ Verify after programming □ Set Security Bit 1
□ Fill unused Flash □ Set Security Bit 2
□ Generate checksums □ Set Security Bit 3
□ Execute □ 6 clks/cycle

29 April 2002: Flash Magic 1.44 is now available for download!
www.esacademy.com/software/flashmagic

0

Fig. 50 FlashMagic



□ Always update firmware

Modem: XBEE XB24-B
Function Set ZNET 2.5 COORDINATOR AT
Version 1041

- Networking
  - (12) CH - Operating Channel
  - (150) OP - Operating PAN ID
  - (150) ID - PAN ID
  - (80) SC - Scan Channels
  - (3) SD - Scan Duration
  - (FF) NJ - Node Join Time
- Addressing
  - (0) MY - 16-bit Network Address
  - (13A200) SH - Serial Number High
  - (40628BFC) SL - Serial Number Low
  - (0) DH - Destination Address High
  - (0) DL - Destination Address Low
  - (N1) NI - Node Identifier
  - (0) BH - Broadcast Radius
  - (FF) AR - Aggregation Route Broadcast Time
  - (20000) DD - Device Type Identifier
  - (3C) NT - Node Discovery Backoff
  - (0) NO - Node Discovery Options
- RF Interfacing

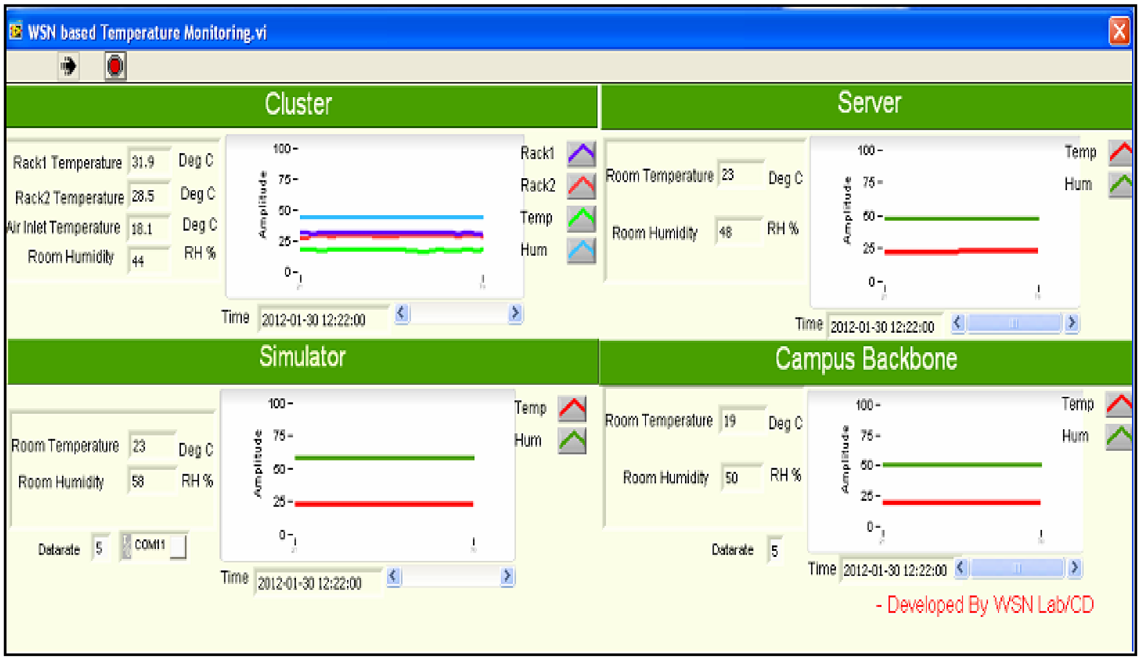
Change networking settings

COM70 9600 8-N-1 FLOW:NONE XB24-B Ver:1041

Fig. 51 Configuring using X-CTU

Monitoring GUI

The temperature measured by the sensors need to be displayed at the PC connected to base station. For that, GUI has been developed using Lab VIEW. Laboratory Virtual Instrumentation Engineering Workbench (Lab VIEW) [110] is a programming language with Graphical Language developed by National Instruments. It is built for the design, simulation, modification, and compilation of digital instrumentation systems. The basic unit of the resulting program is the virtual instrument (VI) that consists of executable code controlled via a graphical front panel on the screen similar to a real instrument. In contrast to conventional programming languages, it is programmed on the basis of block diagrams and front panel elements. These elements are connected by means of a wiring tool. After having tested a virtual instrument, the graphical language built from an application, compiles standalone executable code.



Cluster

Rack1 Temperature 31.9 Deg C
Rack2 Temperature 28.5 Deg C
Air Inlet Temperature 18.1 Deg C
Room Humidity 44 RH %
Time 2012-01-30 12:22:00

Server

Room Temperature 23 Deg C
Room Humidity 48 RH %
Time 2012-01-30 12:22:00

Simulator

Room Temperature 23 Deg C
Room Humidity 58 RH %
Datarate 5 COM11
Time 2012-01-30 12:22:00

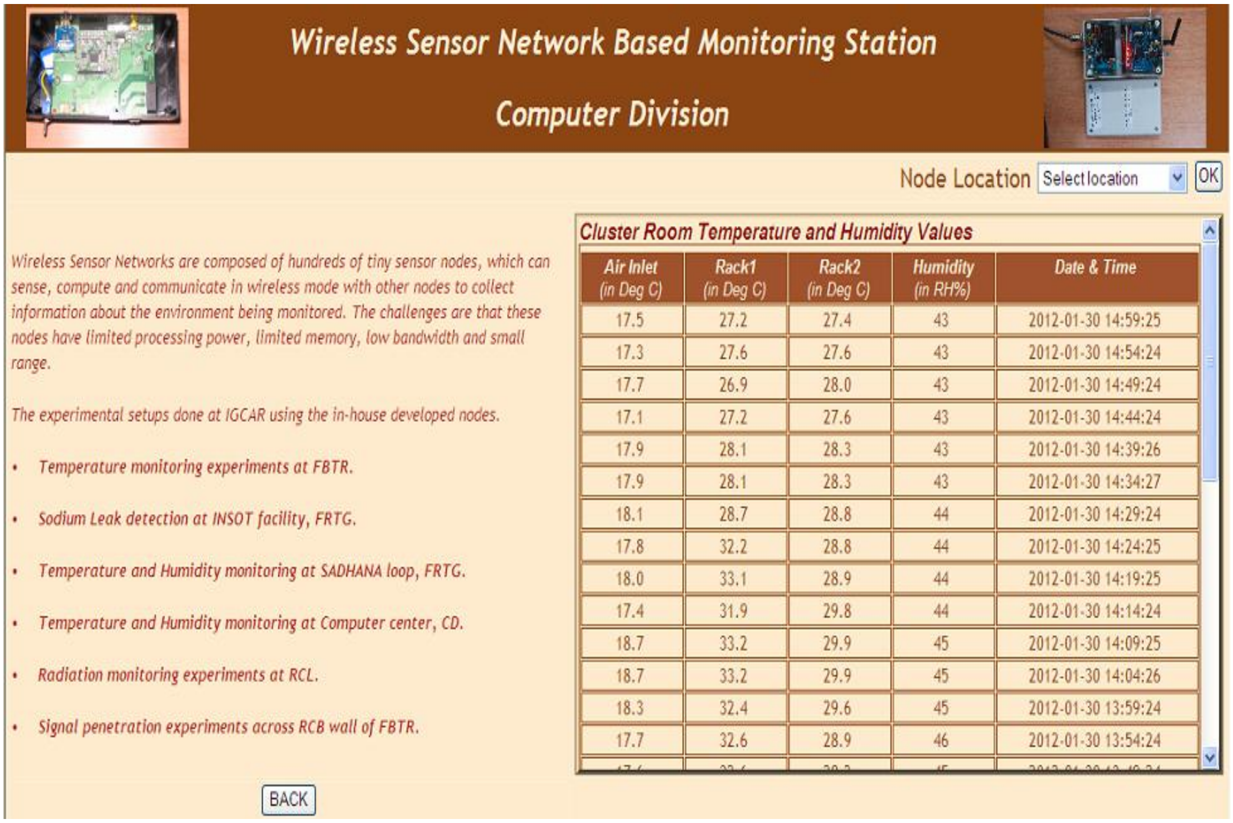
Campus Backbone

Room Temperature 19 Deg C
Room Humidity 50 RH %
Datarate 5
Time 2012-01-30 12:22:00

- Developed By WSN Lab/CD

Fig. 52 LabVIEW based Monitoring GUI

Fig. 52 shows the Lab VIEW based Monitoring GUI to display the temperature and humidity value in the server PC along with the graphical display. MS access is used as the database to log the values with time stamp. The logged database is web enabled by executing the Active Server Page (ASP) script on IIS server. When executed, it gets connected to MS Access database in which the data received by base station is logged. When a browser requests, it returns the real time data namely HPC cluster rack temperature, Air inlet temperature, Humidity value and Time stamp in the browser by referring the cluster.mdb file. The snapshot of web enabled database is shown in the Fig. 53.



Wireless Sensor Network Based Monitoring Station

Computer Division

Node Location Select location OK

Wireless Sensor Networks are composed of hundreds of tiny sensor nodes, which can sense, compute and communicate in wireless mode with other nodes to collect information about the environment being monitored. The challenges are that these nodes have limited processing power, limited memory, low bandwidth and small range.

The experimental setups done at IGCAR using the in-house developed nodes.

- Temperature monitoring experiments at FBTR.
- Sodium Leak detection at INSOT facility, FRTG.
- Temperature and Humidity monitoring at SADHANA loop, FRTG.
- Temperature and Humidity monitoring at Computer center, CD.
- Radiation monitoring experiments at RCL.
- Signal penetration experiments across RCB wall of FBTR.

Cluster Room Temperature and Humidity Values

Air Inlet (in Deg C)	Rack1 (in Deg C)	Rack2 (in Deg C)	Humidity (in RH%)	Date & Time
17.5	27.2	27.4	43	2012-01-30 14:59:25
17.3	27.6	27.6	43	2012-01-30 14:54:24
17.7	26.9	28.0	43	2012-01-30 14:49:24
17.1	27.2	27.6	43	2012-01-30 14:44:24
17.9	28.1	28.3	43	2012-01-30 14:39:26
17.9	28.1	28.3	43	2012-01-30 14:34:27
18.1	28.7	28.8	44	2012-01-30 14:29:24
17.8	32.2	28.8	44	2012-01-30 14:24:25
18.0	33.1	28.9	44	2012-01-30 14:19:25
17.4	31.9	29.8	44	2012-01-30 14:14:24
18.7	33.2	29.9	45	2012-01-30 14:09:25
18.7	33.2	29.9	45	2012-01-30 14:04:26
18.3	32.4	29.6	45	2012-01-30 13:59:24
17.7	32.6	28.9	46	2012-01-30 13:54:24

Fig. 53 Web based GUI for CCNET monitoring

4.3. Deployment of WSN at IN Sodium Test (INSOT) facility

A 500MWe, Prototype Fast Breeder Reactor (PFBR) is being constructed at Kalpakkam. Sodium is used as the coolant in PFBR. The IN Sodium Test (INSOT) facility [111], [112] was constructed in Indira Gandhi Centre for Atomic Research (IGCAR) to test the mechanical properties of Fast Reactor components under the influence of sodium. Sodium in the liquid form is circulated in heat transport circuits of FBRs and experimental sodium loops in FRTG. The material used for these sodium circuits is austenitic stainless steel with all weld construction. Even though all possible measures are taken to prevent sodium leak by adequate design, fabrication, quality assurance, operation and maintenance, the possibility of a sodium leak cannot be completely ruled out. Potential regions of leakage in sodium circuits are near welds, high stress areas and regions subjected to thermal striping. Leaks in sodium systems have the potential of being exceptionally hazardous due to the reaction of liquid sodium with oxygen and water vapor in the air. It also reacts with concrete releasing hydrogen and leading to damage and loss of strength of concrete structures. Sodium catches fire when it comes in contact with air or moisture. Wire type leak detectors and spark plug type leak detectors are used as the primary leak detectors in single wall pipe lines of secondary sodium circuits and experimental loops. The wire type and spark plug type leak detectors are connected to the electronic chassis or the analog card of PLCs to process the signal from the detector. The PVC insulated copper cables are used for this purpose.

To reduce the cables, cable routing and cable space required between the leak detectors and their electronics it was attempted to connect the leak detectors and their electronics by wireless link. This extends the detector capability even when the cable is damaged due to external means. To experience the performance of the wireless based connectivity of leak detectors, nine numbers of leak detectors of INSOT fatigue loop are disconnected from the existing electronic system and connected to the in house developed Wireless Sensor Nodes during the loop shutdown period. The data was communicated to base station located in control room with PC for displaying the status of leak detectors.

Sodium Leak Detection

When liquid sodium leak occurs, it reacts violently with air/moisture, generates heat and thick smoke and leads to fire [113]. Many detection methods are used to detect sodium leak but the wire type and spark plug type leak detectors are the most common type. Sodium is a good conductor of electricity. Sensors used for sodium leak detection operate based on the good electrical conductivity of sodium. The general arrangement of wire type leak detectors over the pipeline is shown in Fig. 54.Wire type leak detector system [114] consists of a Nickel wire insulated with ceramic beads which is laid over the surface of the pipe all along its length. The exposed portion of the wire is in close proximity to the pipe surface. If any sodium leaks from the pipeline and contacts the wire, it bridges the small gap between the wire and the pipe surface, grounding the sensor. In spark plug type leak detector the centre electrode is extended to region where the leaked sodium is expected to get collected. The sensor wire / electrode is excited by a DC supply and the presence of this excitation voltage is the indication of no sodium leak. The electronic circuitry of the leak detection system identifies the grounding if any and gives sodium leak alarm.

Hardware Details of Deployment

The hardware circuit for sodium leak detection is shown in Fig. 54. Leak detector is connected to terminal 2&3 and two resistors 470Ω and 100 Ω are connected on both the legs of sensor. A current limiting resistor of 1kΩ is also introduced with 12V DC excitation to the terminal 2. The resistance that offered by the sensor circuit across 1&4 determines the status of the detector. The potential present at the terminal 1 with respect to ground (terminal 4) is the output and it depends on the sensor status. The various conditions of leak sensor along with their ranges are shown in table 9.

Table 9. Conditions Table for Leak Detection System

S.No	Conditions	Colour Identification in CRT	Resistance in Ω		Voltage in Volts	
			Typical	Allowed Range	Typical	Allowed Range
1	Cable short	Yellow	0	0 to 52.6	0	< 0.132
2	Leak	Red	100	57.2 to 188	0.249	0.1442 to 0.461
3	Healthy	Green	570	428.5 to 1105	1.315	1.0 to 2.28
4	Open	Blue	Infinity	10K to M	12	> 8.16

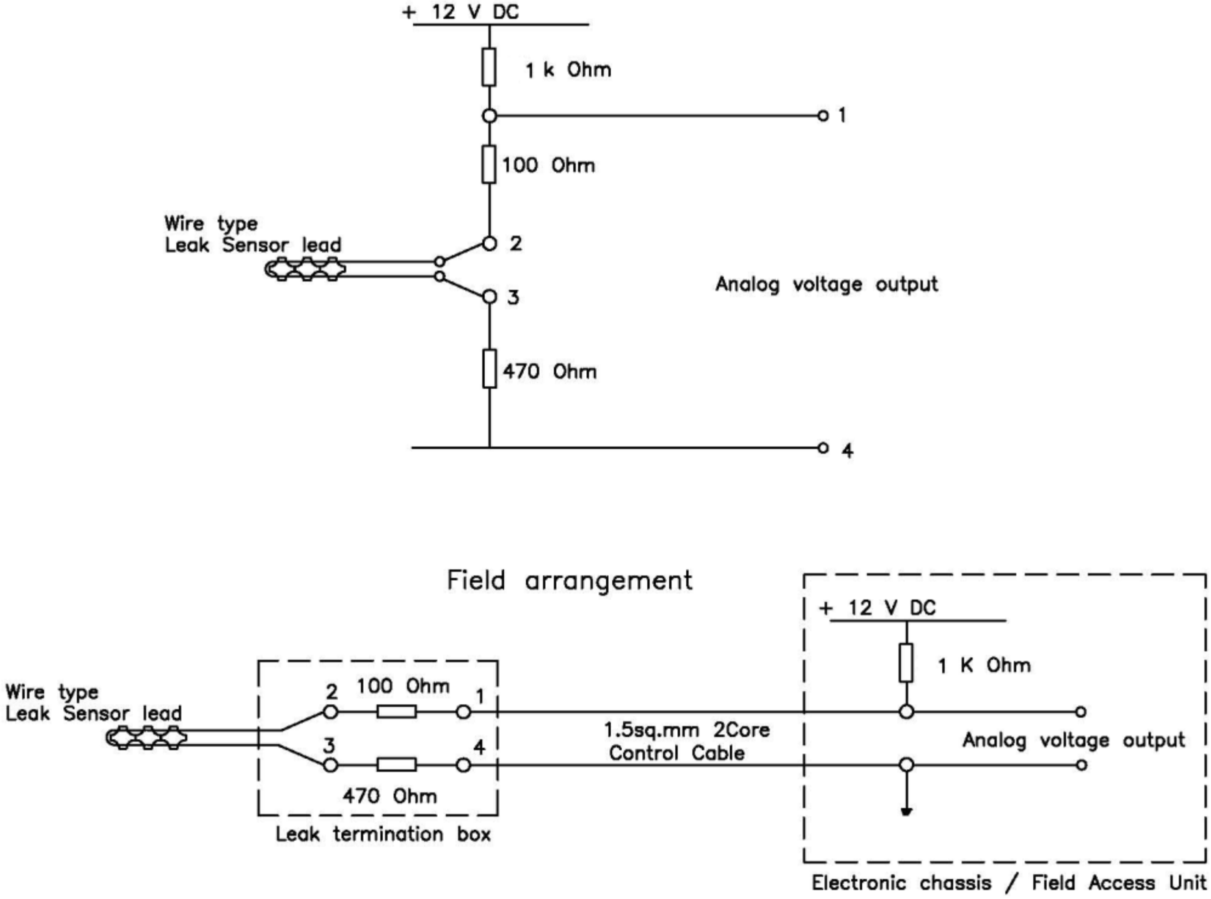


Fig. 54 Sodium Leak Detection Circuit Details

Software Details of Deployment

The code to implement WSN based leak detection has been developed using Keil Embedded Development tool for ARM. The program dynamically reads the voltage from sensor node and displays various conditions like *Leak, Cable open, Cable short* and *Healthy*. For the field operator to understand the healthiness, various LED signaling with different flashing rates has been included in coding. For continuous monitoring, all the signals have been sampled in periodic interval of 1 second. The sodium leak event is treated with utmost priority and the program includes the code to energize the relay in case leak signal is detected. Compilation of the programming code in Keil crosscompiler results in the hex file which is downloaded to the microcontroller with the help of *FlashMagic* utility.

Graphical User Interface for Sodium Leak Detection

For displaying the status of sodium leak detection system to the control room, a GUI has been developed in Visual Basic language. The GUI displays the node id, sensor tag number, location of the sensor and status of the sensor. Database connectivity has been given to GUI in order to store the data collected by the base station for future analysis. Options are provided in the GUI to change the data storage intervals in database.

Initial Deployment of WSN for Sodium Leak Detection at INSOT

Prior to deployment, interference effect studies were done. Wi-Spy, a USB based spectrum analyzer has been employed to identify the interference present in the operating frequency of 2410MHz. Interference was identified as small spikes below the range of -100dbm (0.1pW), which is absolutely negligible [115].

During the first phase deployment, three number of WSN nodes have been placed across three floors at INSOT. Three nearby leak detectors were connected to each node. The location of the nodes was decided in such a way that the wireless signals from the nodes are from different directions. It also had to pass through number of structures, doors and walls etc., depicting the actual plant conditions. All the nodes were transmitting the data to the base station located in control room. The basestation is configured to receive the signals from the sensor nodes and is connected to PC for displaying the leak detector status. An actuator node was also programmed to trigger a relay when sodium leak happens. All the sensor nodes are powered by 230 volts, 50 Hz, AC supply while the base station is powered from the USB connectivity of PC. Performance was monitored and it worked satisfactorily for a period of 15 months.

Feasibility testing for establishing WSN at INSOT during loop operation

If sodium leak detection has to be done without disturbing the existing wired setup and when the loop is in operation, the WSN node has to be connected in parallel to the existing system. Hence the feasibility test of taking parallel connection from the wired sodium leak detection system has been done.

Second phase deployment and performance analysis of WSN at INSOT

A 15 noded WSN with 13 sensor nodes connected to 50 leak signals and one base station, one actuator node has been established in INSOT facility. The network is distributed across three floors of the building covering nearly 80 m² area. One router node is placed in each of the three floors to provide redundant path. The base station was connected to a PC through USB port and receives the field data from the sensor nodes. The status of the leak detectors were displayed in the PC. Actuator node for actuating buzzer in case of sodium leak was installed in the control room. The implemented scheme of existing and deployed WSN based leak signal processing system is shown in Fig. 55. The screenshot of the GUI displaying 50 leak signal status and routing node status is shown in Fig. 56.

This deployment was carried out during the loop shut down condition and subsequently during normal operation of the loop when sodium is flowing through the loops. WSN based leak detection system was functioning as redundant system in parallel mode for selected 50 leak channels in fatigue loop. The leak detectors were simulated in the loop area for *leak*, *cable short* and *cable open* conditions and the corresponding indications and buzzer alarm for *leak* condition were observed in the control room WSN PC and existing SCADA system. The performance of the system was tested and analyzed. The system was found functioning as expected in a stable manner.

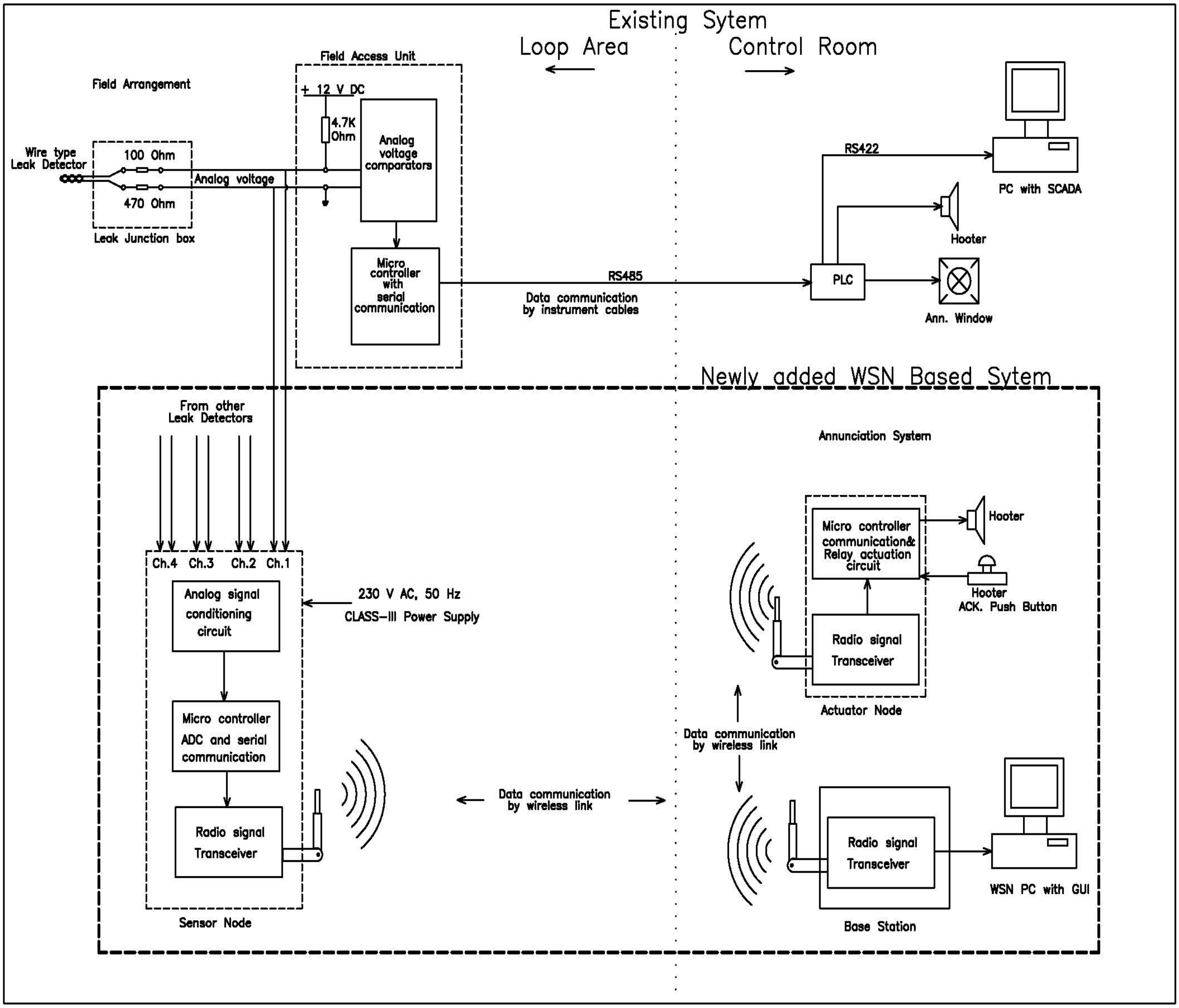
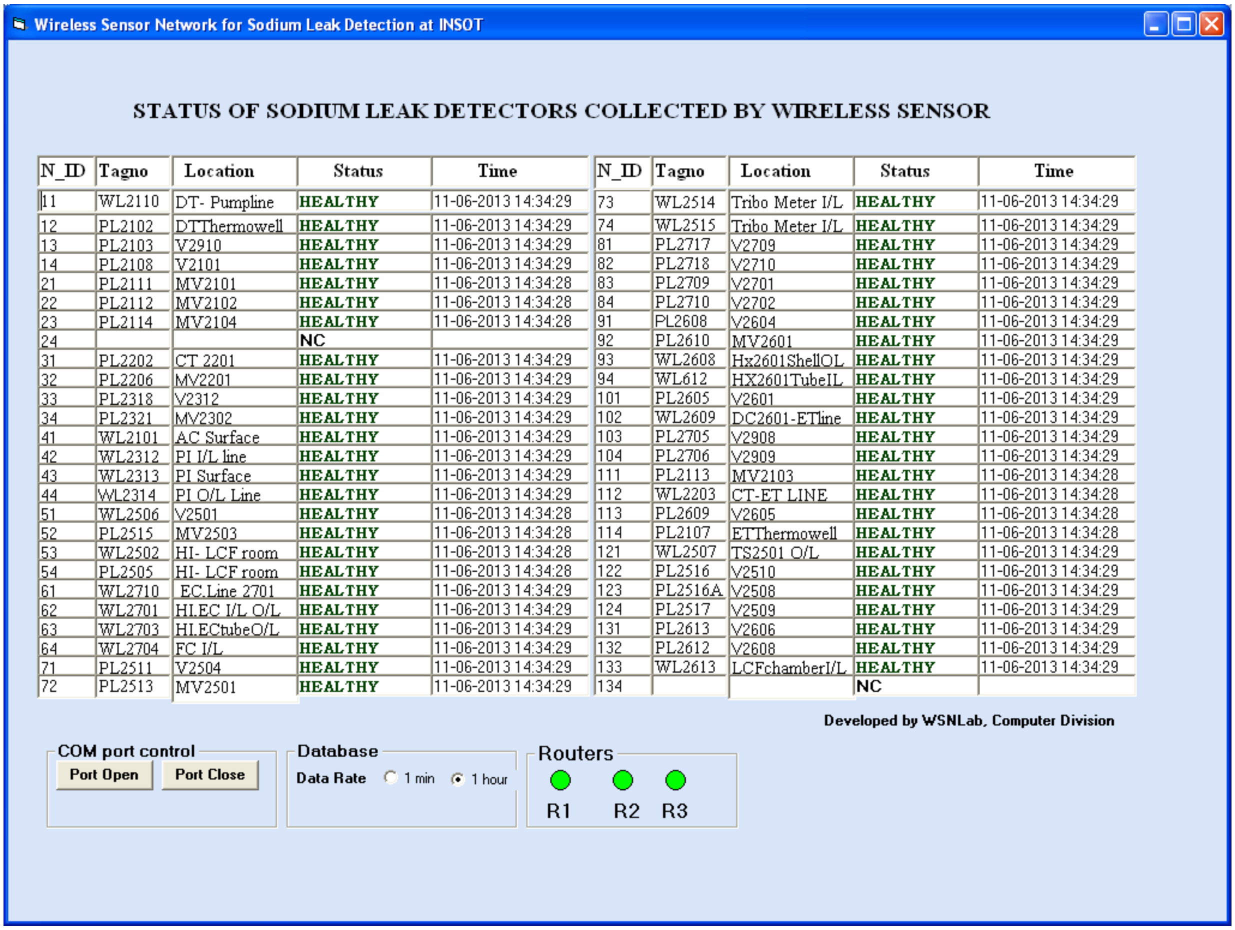


Fig. 55 Implemented scheme for Sodium Leak Detection by WSN in parallel mode



STATUS OF SODIUM LEAK DETECTORS COLLECTED BY WIRELESS SENSOR

N_ID	Tagno	Location	Status	Time
11	WL2110	DT- Pumpline	HEALTHY	11-06-2013 14:34:29
12	PL2102	DTThermowell	HEALTHY	11-06-2013 14:34:29
13	PL2103	V2910	HEALTHY	11-06-2013 14:34:29
14	PL2108	V2101	HEALTHY	11-06-2013 14:34:29
21	PL2111	MV2101	HEALTHY	11-06-2013 14:34:28
22	PL2112	MV2102	HEALTHY	11-06-2013 14:34:28
23	PL2114	MV2104	HEALTHY	11-06-2013 14:34:28
24			NC	
31	PL2202	CT 2201	HEALTHY	11-06-2013 14:34:29
32	PL2206	MV2201	HEALTHY	11-06-2013 14:34:29
33	PL2318	V2312	HEALTHY	11-06-2013 14:34:29
34	PL2321	MV2302	HEALTHY	11-06-2013 14:34:29
41	WL2101	AC Surface	HEALTHY	11-06-2013 14:34:29
42	WL2312	PI I/L line	HEALTHY	11-06-2013 14:34:29
43	WL2313	PI Surface	HEALTHY	11-06-2013 14:34:29
44	WL2314	PI O/L Line	HEALTHY	11-06-2013 14:34:29
51	WL2506	V2501	HEALTHY	11-06-2013 14:34:28
52	PL2515	MV2503	HEALTHY	11-06-2013 14:34:28
53	WL2502	HI- LCF room	HEALTHY	11-06-2013 14:34:28
54	PL2505	HI- LCF room	HEALTHY	11-06-2013 14:34:28
61	WL2710	EC.Line 2701	HEALTHY	11-06-2013 14:34:29
62	WL2701	HI.EC I/L O/L	HEALTHY	11-06-2013 14:34:29
63	WL2703	HI.ECtubeO/L	HEALTHY	11-06-2013 14:34:29
64	WL2704	FC I/L	HEALTHY	11-06-2013 14:34:29
71	PL2511	V2504	HEALTHY	11-06-2013 14:34:29
72	PL2513	MV2501	HEALTHY	11-06-2013 14:34:29

N_ID	Tagno	Location	Status	Time
73	WL2514	Tribo Meter I/L	HEALTHY	11-06-2013 14:34:29
74	WL2515	Tribo Meter I/L	HEALTHY	11-06-2013 14:34:29
81	PL2717	V2709	HEALTHY	11-06-2013 14:34:29
82	PL2718	V2710	HEALTHY	11-06-2013 14:34:29
83	PL2709	V2701	HEALTHY	11-06-2013 14:34:29
84	PL2710	V2702	HEALTHY	11-06-2013 14:34:29
91	PL2608	V2604	HEALTHY	11-06-2013 14:34:29
92	PL2610	MV2601	HEALTHY	11-06-2013 14:34:29
93	WL2608	Hx2601ShellOL	HEALTHY	11-06-2013 14:34:29
94	WL612	HX2601TubeIL	HEALTHY	11-06-2013 14:34:29
101	PL2605	V2601	HEALTHY	11-06-2013 14:34:29
102	WL2609	DC2601-ETline	HEALTHY	11-06-2013 14:34:29
103	PL2705	V2908	HEALTHY	11-06-2013 14:34:29
104	PL2706	V2909	HEALTHY	11-06-2013 14:34:29
111	PL2113	MV2103	HEALTHY	11-06-2013 14:34:28
112	WL2203	CT-ET LINE	HEALTHY	11-06-2013 14:34:28
113	PL2609	V2605	HEALTHY	11-06-2013 14:34:28
114	PL2107	ETThermowell	HEALTHY	11-06-2013 14:34:28
121	WL2507	TS2501 O/L	HEALTHY	11-06-2013 14:34:29
122	PL2516	V2510	HEALTHY	11-06-2013 14:34:29
123	PL2516A	V2508	HEALTHY	11-06-2013 14:34:29
124	PL2517	V2509	HEALTHY	11-06-2013 14:34:29
131	PL2613	V2606	HEALTHY	11-06-2013 14:34:29
132	PL2612	V2608	HEALTHY	11-06-2013 14:34:29
133	WL2613	LCFchamberI/L	HEALTHY	11-06-2013 14:34:29
134			NC	

Developed by WSNLab, Computer Division

Database

Data Rate ○ 1 min ● 1 hour

Fig. 56 Screenshot of the GUI during loop operating condition

In order to test the feasibility of expanding the network to connect 100 leak detectors, a 30 node network has been setup and data has been collected for 2 hours. Performance of the expanded network has been tested and analyzed. Fig. 57 shows few images of the deployed network.

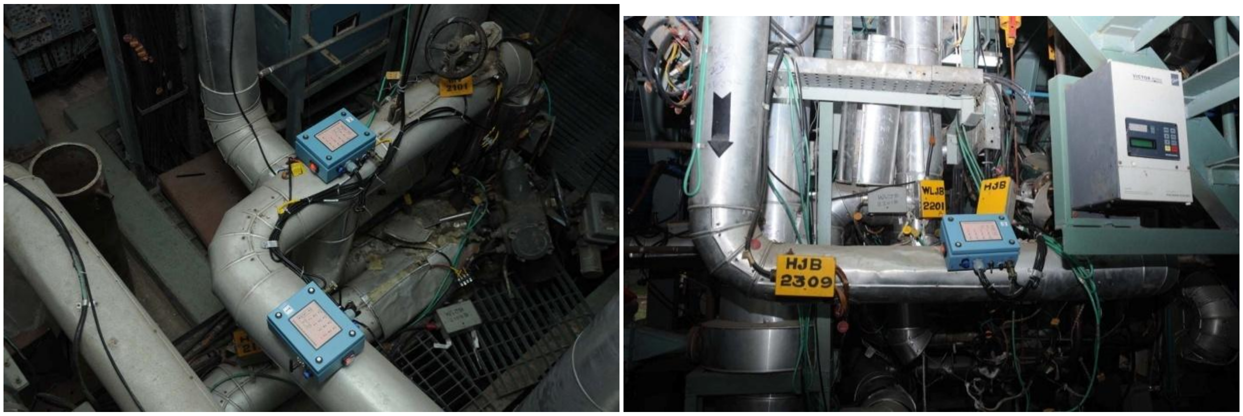


Fig. 57 Images of the deployed network at INSOT

4.4. Deployment of WSN at SADHANA

A 355 kW capacity sodium test facility named SADHANA (SAfety Grade Decay Heat removAl loop in Natrium) is constructed at IGCAR to study the thermal hydraulics behavior of Safety Grade Decay Heat Removal of PFBR [116]. This facility is located in Engineering Hall-III. In SADHANA the sodium in Test Vessel 4 (TV 4) which simulates hot pool of PFBR is heated by immersion electrical heaters. This heat is transferred to the secondary sodium through DHX. The secondary sodium gets circulated in the secondary loop by the buoyancy head developed in the loop due to the temperature difference in hot and cold legs of the loop. The heat from secondary sodium circuit is rejected to the atmosphere through the AHX. A 20 m high chimney develops the air flow required to transfer the heat from secondary sodium to the atmosphere through AHX. The capacity of SADHANA loop is 355kW and the height difference between the thermal centers of DHX and AHX is 19.5m. This 1:22 scaled model loop is designed on Richardson number similitude. Sodium hold up in this facility is 3m^3. The experimental facility contains a sodium to sodium decay heat exchanger, sodium to air heat exchanger, a test vessel containing sodium pool, Chimney and associated piping. Annular linear induction pump (ALIP) is used for sodium circulation in the primary side. Immersion heaters are used for heating the sodium pool in test vessel.

SADHANA loop is highest in the Hall-III structure and spreads from storage tank to 9th floor (upto~27mtrs). The air chimney extends up to 46 meter elevation, ends at open terrace of Hall-III building. The experimental study requires the air temperature and humidity at inlet (5th floor) and out let (open terrace) data to be acquired along with other plant data. To accomplish this, sensors have to be installed at both the locations and terminated with data acquisition system by suitable cables. The cabling from the terrace to control room and the cable entry penetrations on the building walls may be avoided by introducing wireless connectivity. Hence it is decided to deploy WSN for covering the area vertically at SADHANA to measure and acquire two humidity and two temperature signals from Chimney. Table 10 gives the details of sensors on sensor network deployed.

Chimney Outlet Temperature Measurement

Range	: From ambient temp. to 300 °C
Sensor	: Type K thermocouple, SS sheathed, ungrounded Sensor output
	: ~41.6 µV / °C (1 – 12.5 mV approximately)
Accuracy	: ±1% of the range
Location	: air chimney outlet at open terrace of Hall-III
Read out required at	: PC of SADHANA in control room of Hall-III (First floor)
Display	: continuous
Data logging	: Every minute or every hour selection option to be made available to operator.

Humidity measurement

Range	: ambient (0-100% Rh)
Sensor	: Humidity transmitter
Sensor output	: 4-20mA DC
Accuracy	: ±1% of the range
Location	: One at open terrace of Hall-III and other at 5th floor of Hall-III loop structure

Read out required at	: PC of SADHANA in control room of Hall-III (First floor)
Display	: continuous
Data logging	: Every minute or every hour selection option to be made available to operator.

Table 10. Details of sensors on WSN

Sl.No	Sensor Tag No.	Location	Sensor Node	Sensor Node Location	Terminal No.
1	HT 1	Humidity transmitter at air inlet (5th floor)	1	5th floor Loop area	1&2
2	HT 2	Humidity transmitter at air outlet (Hall-III terrace)	2	11th floor staircase	1&2
3	T1283	Thermocouple at chimney outlet (Hall-III terrace)	2	11th floor staircase	3&4
4	T1284	Thermocouple at chimney outlet (Hall-III terrace)	2	11th floor staircase	5&6

Deployment Details of WSN

The SADHANA WSN was established using in-house developed WSN nodes operating at 2.4 GHz ISM band. The microcontroller used in the WSN node is LPC2138, which is based on ARM architecture which offers high performance for very low power consumption and price. The radios used in the developed WSN nodes were either XBee or XBee-PRO RF Modules. The signal conditioning circuit has been designed for three numbers of K type thermocouple and humidity sensors. It takes care of noise suppression, amplification of the thermocouple mV output and the conversion of humidity current signal to voltage signal. The cold junction compensation has also been taken care. The designed signal conditioning board is shown in Fig. 58.

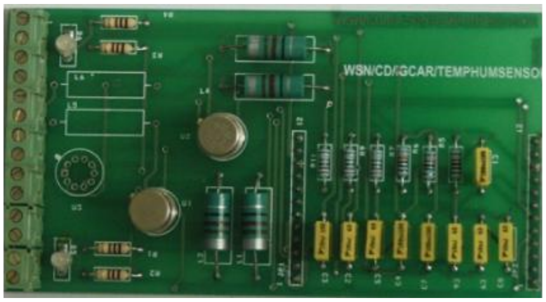


Fig. 58 Signal conditioning board

Design and Implementation of WSN at SADHANA

Flat architecture has been chosen for this network and it consists of two sensor nodes and a base station. One sensor node is located in 11th floor (chimney outlet at terrace of Hall-III building) with two K-type thermocouples and one humidity sensor connected to it. Another sensor node has been placed in 5th floor (chimney inlet) with one humidity sensor connected to it. The two sensor nodes data was collected by the base station in the control room and displayed on the PC monitor. Initially the site survey has been done using Wi-Spy, a spectrum analyzer to identify the interference at 2.4GHz spectrum range with in Hall-III building. No interference was found. All nodes were configured to work at 2425MHz frequency in channel ‘F’ with 3dbm power level. Omni directional 2dBi dipole high gain antenna is used and oriented vertically in all nodes. The signal strength has been measured for identifying the proper position of router node till the signal reaches base station. The schematic diagram of the deployed wireless sensor network for SADHANA is shown in Fig. 59.

Software Details of Deployment

For this WSN based deployment the code has been developed using KEIL Embedded Development tool for ARM. The program dynamically reads the ADC values and averages them for accuracy. The averaged values were in turn converted to engineering units using the conversion formula. The nodes were programmed with compiled hex code using the Flash Magic utility software for continuous monitoring. The transceiver XBee-Pro radio chips are configured to work in 2425MHz in channel ‘F’ with 3dbm power level. Link is established for continuous data monitoring in the interval of 1 minute. The transceiver chips were configured either as coordinator or router & end devices using X – Configuration and Test Utility (X-CTU) software.

Monitoring GUI

The temperature and humidity measured by the sensors need to be displayed at the PC connected to base station. For that, GUI has been developed using Laboratory Virtual Instrumentation Engineering Workbench (LabVIEW) [108]. It is a programming language with Graphical Language developed by National Instruments. It is built for the design, simulation, modification, and compilation of digital instrumentation systems. The GUI displays the sensor tag number with location of the sensor, temperature and humidity values measured in ºC and RH% respectively. The graphical view is also provided in the GUI. The snap shot of the GUI is shown in Fig. 60. The sensed data collected by the base station has been stored in the Ms Access database for future reference. The option of logging the data at different intervals namely 2sec, 1 min, and 5 min is provided in the GUI using option buttons. Since it is monitored continuously, the file size may grow rapidly. Hence to manage the file size, a script has been included to automatically move the data logged in database to a separate file at regular interval.

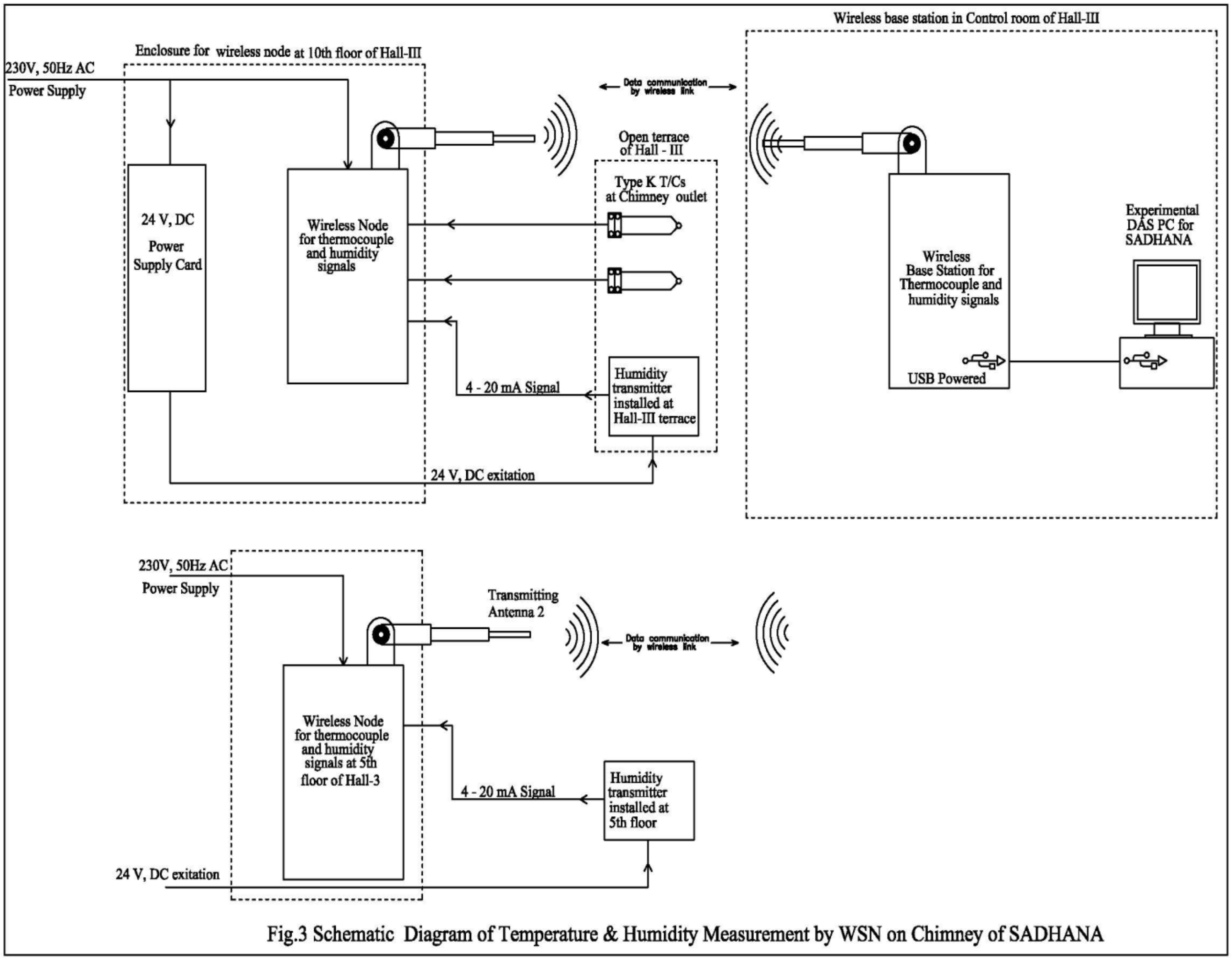
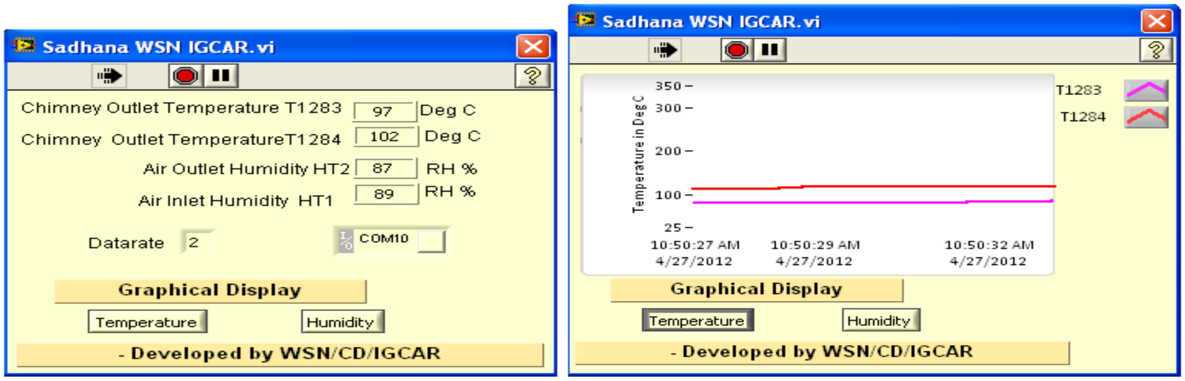

Wireless base station in Control room of Hall-III
Enclosure for wireless node at 10th floor of Hall-III
230V, 50Hz AC
Power Supply
Data communication by wireless link
Open terrace of Hall - III
Type K T/Cs at Chimney outlet
24 V, DC
Power Supply Card
Wireless Node for thermocouple and humidity signals
Wireless Base Station for Thermocouple and humidity signals
Experimental DAS PC for SADHANA
USB Powered
4 - 20 mA Signal
Humidity transmitter installed at Hall-III terrace
24 V, DC exitation
230V, 50Hz AC
Power Supply
Transmitting Antenna 2
Data communication by wireless link
Wireless Node for thermocouple and humidity signals at 5th floor of Hall-3
4 - 20 mA Signal
Humidity transmitter installed at 5th floor
24 V, DC exitation
Fig.3 Schematic Diagram of Temperature & Humidity Measurement by WSN on Chimney of SADHANA

Fig. 59 Deployed Wireless Sensor Network at SADHANA



Sadhana WSN IGCAR.vi

Chimney Outlet Temperature T1283 97 Deg C

Chimney Outlet TemperatureT1284 102 Deg C

Air Outlet Humidity HT2 87 RH %

Air Inlet Humidity HT1 89 RH %

Datarate 2

COM10

Fig. 60 Snap shot of GUI for SADHANA Monitoring

4.5. Deployment of WSN at FBTR

FBTR is a loop type, sodium cooled fast reactor, based on the design of the Rapsodie reactor [117] with several major design modifications. It uses Pu-U mono-carbide developed indigenously as the driver fuel, and went critical in 1985. Though it is a research reactor, it is equipped to generate power (around 3 MWe) and operates at 20.3 MWt power now [118]. The major components in FBTR are: reactor core, reactor assembly, primary sodium loop, secondary sodium loop, steam water circuit, turbo generator, fuel handling, core monitoring, instrumentation and control, and many other auxiliary systems. The reactor core consists of 745 closely packed locations, with fuel at the centre, surrounded by nickel reflectors, thorium blankets and steel reflectors [119]. The core is vertical and freestanding, with the subassemblies supported at the bottom by the Grid Plate. The Reactor Vessel houses the core and serves as a conduit for the primary sodium coolant flow through the core. Heat generated in the reactor is removed by two primary sodium loops, and transferred to the corresponding secondary sodium loops. Each secondary sodium loop is provided with two once-through steam generator modules. Steam from the four modules is fed to a common steam water circuit comprising a turbo-generator and a 100% dump condenser. Stainless steel (SS 316) is the principal material of construction for the reactor and coolant circuits.

Safety of the reactor is ensured by multiple interlocking and diverse mechanisms in all stages. From design level itself, FBTR is protected against transient over-power accident by feedback through negative temperature and power coefficients, double envelope of the primary sodium loops safeguards against loss-of-coolant accident and operation of two pumps in parallel to safeguard against loss of flow accidents [120]. The instrumentation and control system of FBTR uses two-out-of-three logic to protect against failure. For ensuring safety, hundreds of sensors are employed through out the plant and are being continuously monitored at the centralized control room. To enhance the safety, it is always better to introduce diverse path for these sensor signals to reach control room, which will ensure the availability of signals for processing, even if one path fails. However in the reactor all the signal cables are routed together and pass through cable trays. A diverse mechanism to reliably transmit the state of signals to the processing electronics will surely enhance the reactor safety. Hence, there is a strong need to use wireless signal transmission in such critical field as the nuclear reactors.

Signal Conditioning Board for Temperature Measurement

In FBTR, ANSI type K thermocouples have been used for measuring temperatures at various locations because of their wide temperature range, high sensitivity (of approximately 41 µV/°C) and ruggedness. The cold junction compensation has been done using PT100 Resistance Temperature Detector (RTD). A signal conditioning board has been designed for K type thermocouple, as shown in Fig. 61, which takes care of noise suppression and amplification of the mV output. It also converts the RTD output voltage to an acceptable range by the external 12 bit ADC of the WSN node. The designed boards have been thoroughly tested and validated for their performance at the process instrumentation lab of FBTR and ensured that they do not load the existing wired system. They have undergone parallel connection testing using calibrator CA71, High accuracy calibrator and thermo-bath setup outputs, static and transient load testing by connecting thermocouple in parallel with the isolation module DSCA30.

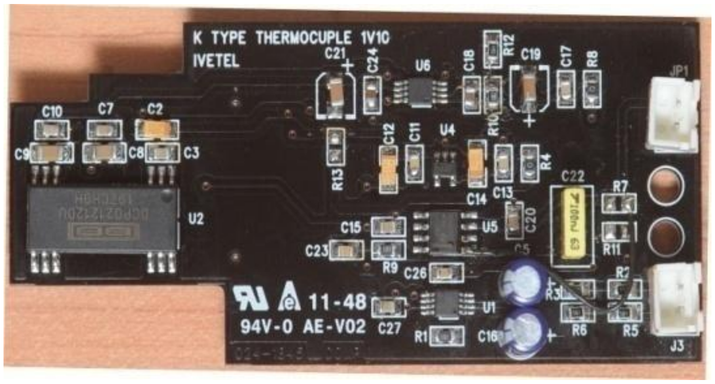


Fig. 61 Signal Conditioning Board for Thermocouple

Signal Conditioning Board for Vibration

Vibration is an important parameter to be monitored continuously for rotating machinery to ensure the condition monitoring. In FBTR, the vibration monitoring is done periodically for the Ward Leonard Systems which continuously pump sodium to remove the generated heat. The signal conditioning circuit for the vibration sensor AC102 has been developed, as shown in Fig. 62 to measure the root mean square (RMS) value of acceleration. The analog output of sensor is fed to a low power, wide band, and high precision, true rms-to-dc converter. The resulting DC average level is scaled and fed to an external 12 bit ADC of the WSN node.

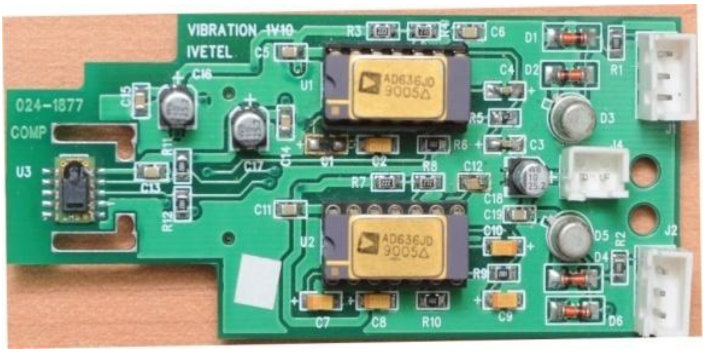


Fig. 62 Signal Conditioning Board for Vibration Sensor

Deployment Details of FBTR Network

The actual deployment of wireless sensor network in FBTR has to connect multitude of sensors from a small area as dense network. The deployment necessitates fault tolerance and redundancy which is assured by the chosen flat architecture with mesh topology. Before placing the network, a site survey has been done at FBTR using Wi-Spy, a USB based spectrum analyzer [71]. It helps in identifying the interference present at 2.4 GHz. The data collected during site survey is shown in Fig. 63. Interference was identified as small spicks below the range of -70dbm (100pW), which is absolutely negligible.

Hence, it is assured that the whole spectrum is available for WSN deployment at FBTR. As an initial step a wireless sensor network has been deployed with 4 numbers of NNS temperature signals at 0th level, inside RCB. They are tube side of heat exchanger temperature, purification circuit bypass valve temperature, and 2 signals from primary thermo fluid temperature. 2 numbers of router nodes were used to link the signals to the PC connected to the base station at control room. Based on the results from the signal penetration experiment explained in Chapter 2, better RSSI value is observed near cable penetration. Hence a router is positioned outside the cable penetration at −2.8m level of the reactor. The signals were monitored continuously for every 2 seconds in the PC at control room for 45days.

The network has been enhanced by introducing nodes to connect NNS signals from outside RCB. 8 numbers of temperature signals and 3 numbers of vibration signals were connected to WSN nodes. 3 router nodes were used to route the signals to control room. The signals are distributed outside the RCB namely turbine building, secondary sodium loop area, sodium flooding area, Ward Leonard system and blower cabin in filter room as shown in Fig. 64.

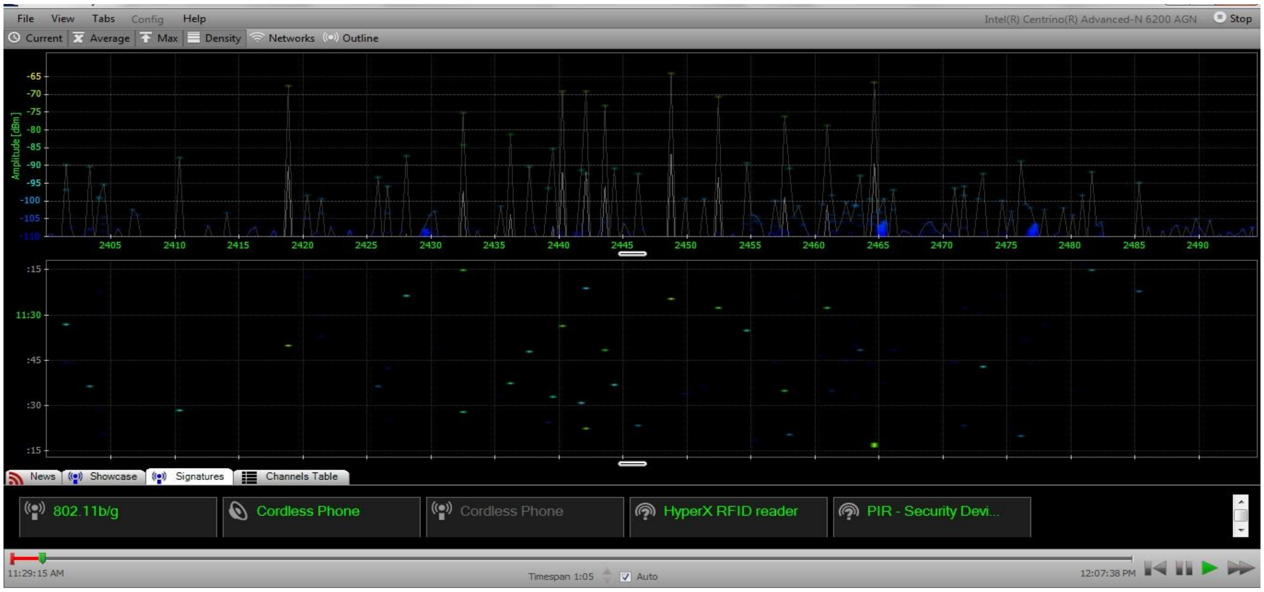


Fig. 63 Output of Spectrum Analyzer

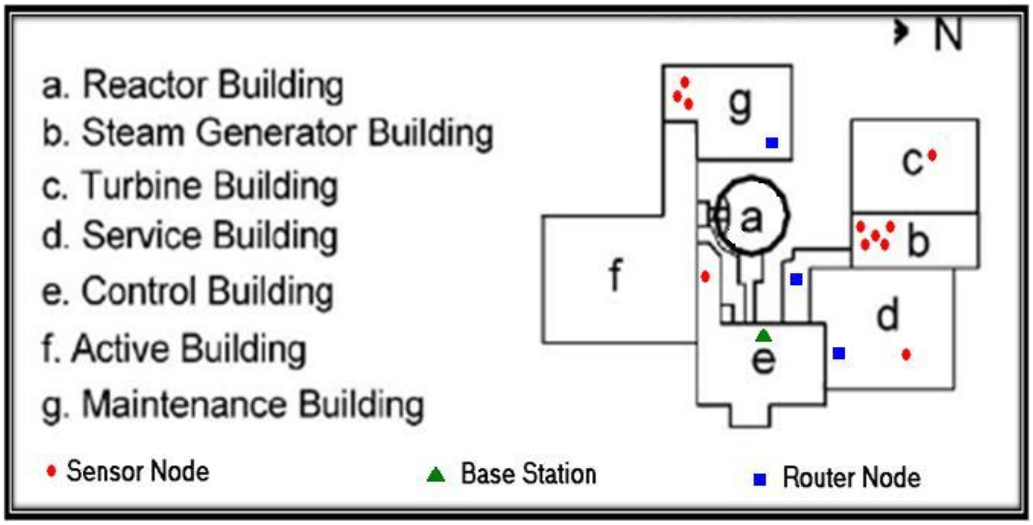


Fig. 64 Network Deployment Layout at FBTR

The temperature signals are hydrogen injection line temperature, 2 numbers of secondary sodium temperatures, 2 numbers of argon circuit line temperatures and 3 numbers of sodium flooding area temperatures. The vibration signals are from Ward Leonard system, blower cabin in filter room and turbine building. Signals are monitored and stored in data base continuously in the PC at control room for analysis.

Software Details of deployment

WSN nodes were programmed with the code developed using KEIL Embedded Development tool for ARM based microcontroller[108]. The program dynamically reads the ADC values and is being averaged for accuracy. For temperature sensors, the averaged values were in turn converted to engineering units using the conversion formula as given below.

```
If ( mV<= 4.095)
{  Temperature = (-0.1455 * mV2) + (24.96* mV) + (0.115); }
else { if (mV>=4.096  && mV<=8.938)
{ Temperature = (0.104 * mV2) + (23.47*mV)+ (2.073);  }
else if (mV>=8.939 && mV<=15.132)
{ Temperature = (-0.08 * mV2) + (26.22*mV) - (7.715);  }
else if (mV>= 15.133)
{ Temperature = (-0.018 *mV2) + (24.25*mV) + (7.25);   }
```

The nodes are programmed for continuous monitoring. All the signals have been sampled at periodic interval of 2 seconds. The compiled hex code was loaded to the nodes using the Flash Magic utility. The transceivers chips XBee or XBee-Pro are configured at channel C of IEEE 802.15.4 Standard at 2410MHz with a power of 1mW (0dbm) using X – Configuration and Test Utility (X-CTU) software [109]. It is a simple-to-use graphical interface to configure the radio chips. The routing protocol used is ZigBee. The nodes are configured as coordinator, router and end devices. End devices are connected to temperature or vibration sensors as needed. Nodes are programmed to transmit the packets in standard IEEE 802.15.4 packet format with node ID, temperature / vibration value and packet originated time.

Monitoring Wireless Network Management Station

For displaying the temperature and vibration parameters in the control room, a wireless network management station (WNMS) has been developed using Visual Basic as front end and access database as back end. The data received by the sensor nodes are stored continuously in the database for further analysis. Initially during network discovery process, WNMS transmits Network Discovery (ND) command through coordinator. ND command is from the ZigBee Data Objects command set. All nodes those who received ND in that network respond immediately with their node ID. To each responded node, Routing Table Query (RTQ) command will be sent and from the information collected, the *topology view* of WSN is created. ND will be repeated for every 5 minutes and the newly added nodes will be discovered. If the identified node is not responding for more than 15 seconds, WNMS will change the colour of the node to orange in the *topology view*. In the absence of any response till the next ND, it will be indicated in red. The *topology view* is to show the current links to the coordinator, but not the mesh view of the network. WNMS also provides a table view of all the nodes with the information of node ID, tag number, location, temperature / vibration value, packet sent time and packet received time. The *trend view* of WNMS is to provide a graphical display of the logged values of temperature / vibration that have been received for one hour duration. The detailed explanation about WNMS is given in Chapter 3.4

4.6. Summary

Wireless Sensor Network is successfully deployed in High Performance Computer Facility and other server rooms of Computer Centre to constantly monitor the temperature and humidity. The network is successfully working for more than two years without any problem.

Then a wireless sensor network was established in INSOT facility for monitoring any sodium leak in the incipient stage itself at fifty locations and raise an alarm incase of any leak, through the actuator node. The status of the fifty leak detectors is continuously displayed in the control room and stored in a database. The network is working satisfactorily without any problem for more than one year.

A wireless sensor network was established for temperature and humidity measurement of air intake and outlet in the Safety Grade Decay Heat Removal system of Prototype Fast Breeder Reactor scaled down model. The network is working satisfactorily for the last 18 months.

After gaining enough experience and proving its reliable operation, a twenty five noded network is established in Fast Breeder Test Reactor. The network monitors reactor systems' temperature signals, pressure signals and vibration signals. The measurements were compared with measurements by wired networks, they are fully matching for the last 6 months. It has given enough confidence that wireless sensors can be successfully deployed in Nuclear Reactor environments where the safety is a major concern.

In the nuclear plant no hazardous/contaminating agents propagation was expected as in a chemical plant. However, the radiation levels can go higher incase of unlikely incident, which will be continuously monitored and appropriate action taken. However even in nuclear facilities where there is possibility of flooding due to, say, a water pipe burst, the wireless sensor nodes can be positioned in higher elevations so that communication and process monitoring can still take place.

The experience gained can be parameterized. Infact, the aim of establishing multiple networks is to parameterize the experiences and use this expertise in establishing wireless sensor networks in other nuclear power plants and nuclear facilities.

Based on this experience, a general methodology can be suggested for deploying WSNs in similar/ new scenario in a nuclear facility. For example: i) The Reactor Containment Building in any nuclear plant which houses the reactor will be made up of high density concrete of about 1 meter thick and the transceivers that work at 2.4 GHz cannot penetrate this wall. However in the reactors, there will be cable penetrations to route the cables at few meters depth and signals can pass through these cable penetrations. ii) In nuclear power plants where there are many walls separating different buildings within the same reactor complex and a lot of piping and equipment is erected, the range of wireless signal can be taken as about 30 m and in corridors as about 50m for X Bee transceiver and about 60m across the walls and 100m in the corridor with X Bee Pro transceiver. iii) automatic reconfiguration is a very big advantage in WSNs, because if any of the routing nodes fail, the network automatically reconfigures and will reroute the traffic. iv) Wireless Sensor nodes can be located in areas not easily accessible for taking readings v) WSN nodes can be located in glove boxes and the data can be collected. vi)Ingress Protected (IP 54 or IP 68) nodes with industrial grade components are required to with stand the harsh field environment.

To test and ensure and to debug the smooth working of wireless sensor networks a Wire Network Management System was successfully developed and tested.

CHAPTER 5

5. ANALYSIS & DISCUSSION

5.1. Introduction

This chapter gives briefly the research & development work done for analyzing the performance of some typical wireless sensor networks established. This includes performance analysis, Packet drop ratio. The chapter also covers the overhead analysis because of implementing security encryption. It also analyses the delay occurred in transmission at different nodes. The interference analysis in a typical wireless sensor network established is explained.

5.2. Performance Analysis for WSN at WSN lab

Performance analysis is mandatory for any established system and hence wired / wireless is not an exception to that. Network performance study can be done by calculating network throughput and packet drop ratio. Throughput is the average rate of successful message delivery over a communication channel. The throughput is usually measured in bits per second (bps or Kbps) and sometimes in data packets per second or data packets per slot. In general throughput is given by

*Throughput = (Total number of bytes received / time duration) * (8/1024) Kbps*

In wireless network, environment definitely affects the throughput. Along with this the wired part for packet transmission / reception to / from radio chip on hardware side also affects the network throughput. So, various experiments were conducted taking in to consideration all the factors that affect wireless network throughput. Parameters affecting throughput are:

1. Technology for transfer of data from microcontroller to transmitter
2. Radio transmission (Delay calculations experiment in FBTR deployment section)
3. Technology for transfer of data from receiver to microcontroller

Parameters (1) and (3) fall in same category of serial interface of microcontroller and transceiver (in case transmitter and receiver is single unit). Serial interfaces along with its maximum data rate are given below:

• Universal asynchronous receiver/ transmitter (UART)	0.8 Mbps with 921600 baud rate
• Serial peripheral interface (SPI)	4 Mbps
• Inter-integrated circuit (I^2C)	0.1 Mbps

Throughput experiment for varying data rate conducted on Different baud rates of UART

With baud rate of 9600 bps, time taken by each bit = 0.104 ms

Time taken for each byte to transmit = 10 * 0.104 ms= 1.04 ms
(including start and stop bit time)

Time taken for 15 byte data payload to transmit = 15 * 1.04 ms= 15.6 ms

No. of packets arriving at coordinator = 7 (per sec data rate)

Total time required for processing all 7 packets = 109.2 ms

Table 11. Time required for receiving 15 byte /66 byte data payload at different baud rates and Time Interval

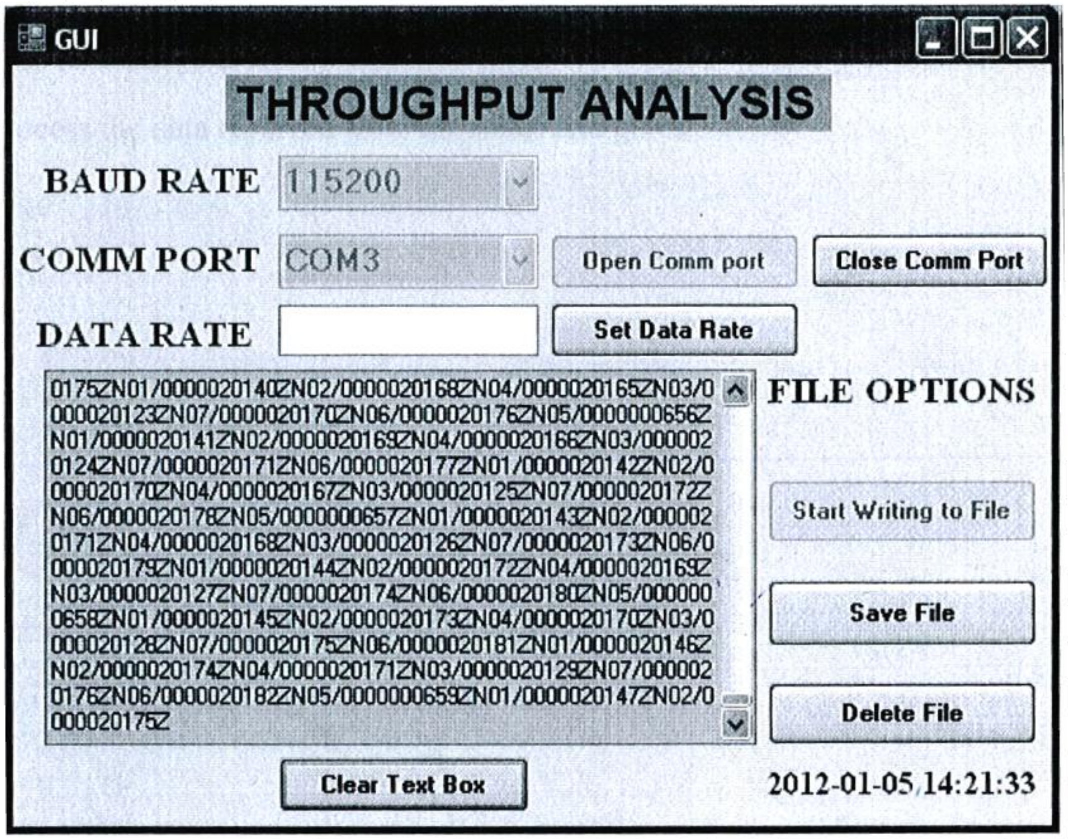
Transmission Rate (in sec)	Time required for 9600 baud rate (ms)		Time required for 115200 baud rate (ms)	
	15 byte payload	**66 byte payload**	**15 byte payload**	**66 byte payload**
1	109.20	480	9.114	40.101
0.5	218.40	960	18.228	80.202
0.25	436.80	1920	36.456	160.404
0.20	546.00	2400	45.570	200.505
0.15	720.72	3168	60.152	266.640
0.10	1092.00	4800	91.400	401.010

Result: Time required is less for transmission, if we increase UART processing speed by choosing higher baud rate for coordinator. So the highest baud rate supported by XBee chip which is 115200 is chosen for all future deployments.

Two payload sizes of 15 bytes and 66 bytes are chosen as they are typical size of the frame and maximum frame length excluding headers. These two sizes have been chosen to see the effect of size of the packet on throughput and packet delivery ratio.

Throughput experiment on seven nodes for varying data rate conducted on Security enabled and disabled conditions

The experimental test-bed consists of 7 in-house developed nodes and one base station. The nodes are configured in channel “0x10”, with 2x8C firmware, with packetization timeout default value of 3 sec. Each source transmits the 15 byte/ 66 byte data payload (66 byte payload results in full frame length utilization for security node) to the base station with the programmed data rate. The data rate is varied from 1 second to 0.15 second, in order to study the packet delivery ratio and throughput at the base station (with and without security). The baud rate of coordinator and other nodes was initially set to 9600 baud rate later changed to 115200 for better performance. GUI has been developed using C# to study the throughput and packet delivery ratio. Image of the GUI is shown below in Fig. 65.



BAUD RATE 115200

COMM PORT COM3

DATA RATE

```
0175ZN01/00000201402ZN02/0000020168ZN04/0000020165ZN03/0
000020123ZN07/0000020170ZN06/0000020176ZN05/0000000656Z
N01/0000020141ZN02/0000020169ZN04/0000020166ZN03/000002
0124ZN07/0000020171ZN06/0000020177ZN01/0000020142ZN02/0
000020170ZN04/0000020167ZN03/0000020125ZN07/0000020172Z
N06/0000020178ZN05/0000000657ZN01/0000020143ZN02/000002
0171ZN04/0000020168ZN03/0000020126ZN07/0000020173ZN06/0
000020179ZN01/0000020144ZN02/0000020172ZN04/0000020169Z
N03/0000020127ZN07/0000020174ZN06/0000020180ZN05/000000
0658ZN01/0000020145ZN02/0000020173ZN04/0000020170ZN03/0
000020128ZN07/0000020175ZN06/0000020181ZN01/0000020146Z
N02/0000020174ZN04/0000020171ZN03/0000020129ZN07/000002
0176ZN06/0000020182ZN05/0000000659ZN01/0000020147ZN02/0
000020175Z
```

2012-01-05 14:21:33

Fig. 65 Screen shot of GUI developed for Throughput Analysis

Table. 12. & Table. 13 are the Network Throughput and Packet Delivery ratio from the experiment. It is observed that up to 200msec, packet delivery was 100% for 15 bytes payload and up to 500 msec, packet delivery was 100% for 66 bytes of payload. Since data security is an important issue with reactor applications, the experiment was conducted with and without the security enabled. 128 bit AES encryption is the security protocol supported by XBee transceiver. For 15 byte payload for both security enabled and disabled network packet drop starts around 150ms, but drop is 0.02% higher for security enabled network. Though packets can drop at any time due to transmission errors or problem in the communication media, here the packet dropping is due to channel capacity, ie. if we send packets faster than once in every 150 ms, the channel will not be free and packets get dropped. Without security, overhead is less and so the resultant throughput is slightly better with 66 bytes of data and there is no difference with 15 bytes. The transmission interval necessary for any signal from FBTR is not less than 1sec, which is well within 100% packet delivery ratio.

Table 12. Network Throughput

Transmission Rate (in sec)	Network Throughput (in bits/sec) With Security Enabled		Network Throughput (in bits/sec) With Security Disabled	
	15 bytes Payload	**66 bytes Payload**	**15 bytes Payload**	**66 bytes Payload**
1	840	3696	840	3696.292
0.5	1680	7384.958	1680	7392.878
0.25	3360	14773.88	3360	14782.53
0.20	4199.565	18433.07	4200.132	18456.53
0.15	5599.097	24303.25	5599.164	24575.17

Table 13. Packet Delivery Ratio

Transmission rate (in sec)	**Packet Delivery Ratio (%) With Security Enabled**		**Packet Delivery Ratio (%) With Security Disabled**	
	15 bytes Payload	**66 bytes Payload**	**15 bytes Payload**	**66 bytes Payload**
1	100	100	100	100
0.5	100	100	100	100
0.25	100	99.940	100	100
0.20	100	99.741	100	99.871
0.15	99.979	98.62	99.991	99.746

Throughput experiment and packet delivery ratio on twenty five nodes for varying data rates

To determine maximum throughput of XBee based flat architecture WSN in a normal working environment, an experimental setup similar to the above network has been established with 25 numbers of sensor nodes and one base station. It can be done for other scenarios also. Individual nodes have been configured, tested and deployed across Computer Division building. Each node has been programmed to transmit its maximum allowable bytes (127 Bytes). Experiment has been performed for data rates varying from 1 second to 500 milliseconds. The topology map of 25 nodes according to its number of hops and physical location of the nodes is shown in Fig. 66. Though a much larger size network can be chosen, because of logistical reasons a 25 node network was chosen.

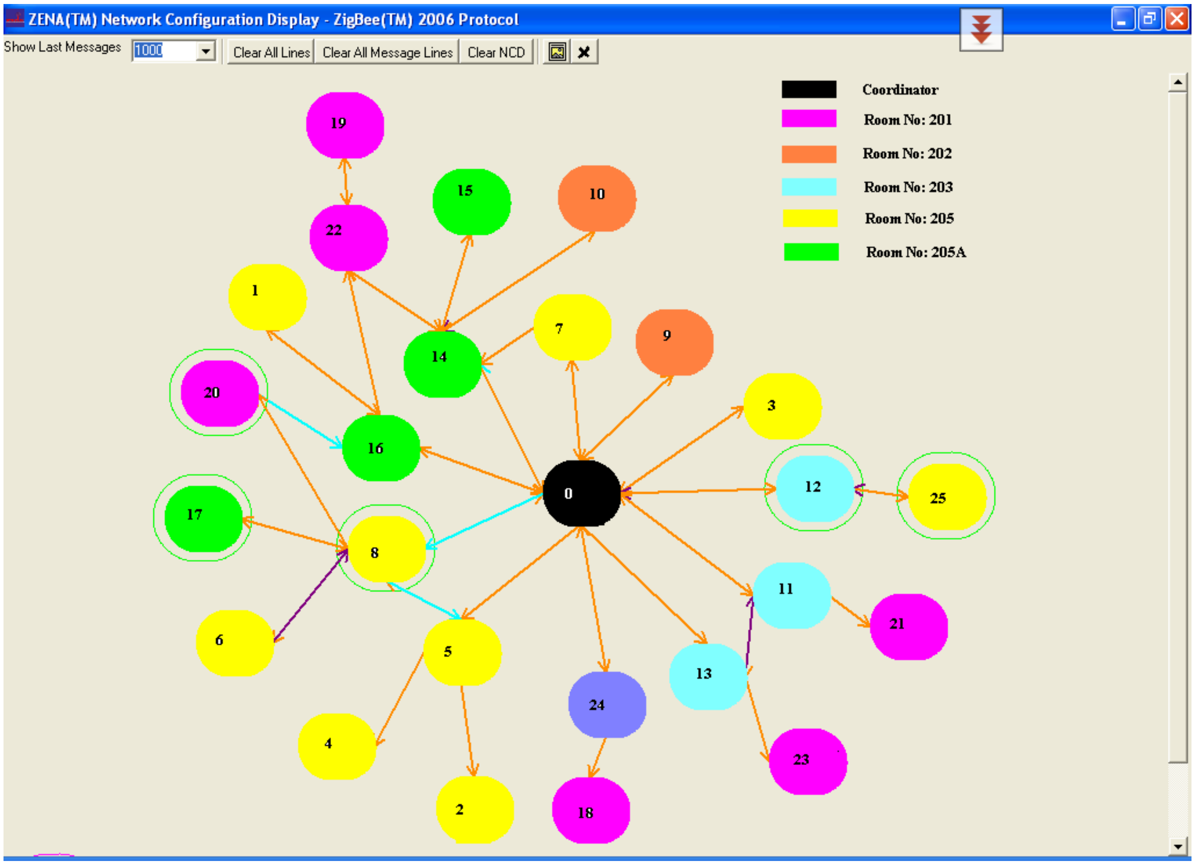


Fig. 66 Topology of 25 noded network

Table 14. Throughput and Packet Delivery Ratio Analysis

Data Rate (ms)	Theoretical count	Received counts	loss	Packet delivery Ratio (%)	Data Throughput (Kbps)
1000	52600	52600	0	100	16.40625
750	60125	60125	0	100	21.875
700	64425	64421	4	99.99379123	23.43604482
680	66325	66272	53	99.92009046	24.10755859
650	69375	69281	94	99.8645045	25.20618503
600	75125	73220	1905	97.46422629	***26.65037438***
580	77750	68377	9373	87.94469453	24.87659732
560	80525	65494	15031	81.33374728	23.82824627
540	83500	64441	19059	77.1748503	23.44722014
520	86700	63032	23668	72.70126874	22.93759981
500	90100	57887	32213	64.24750277	21.08121185

For a tolerance of 2.5% loss in packets maximum achievable throughput was 26.65 Kbps in a 25 noded flat architecture 2 hop XBee network. [Fig. 67.]

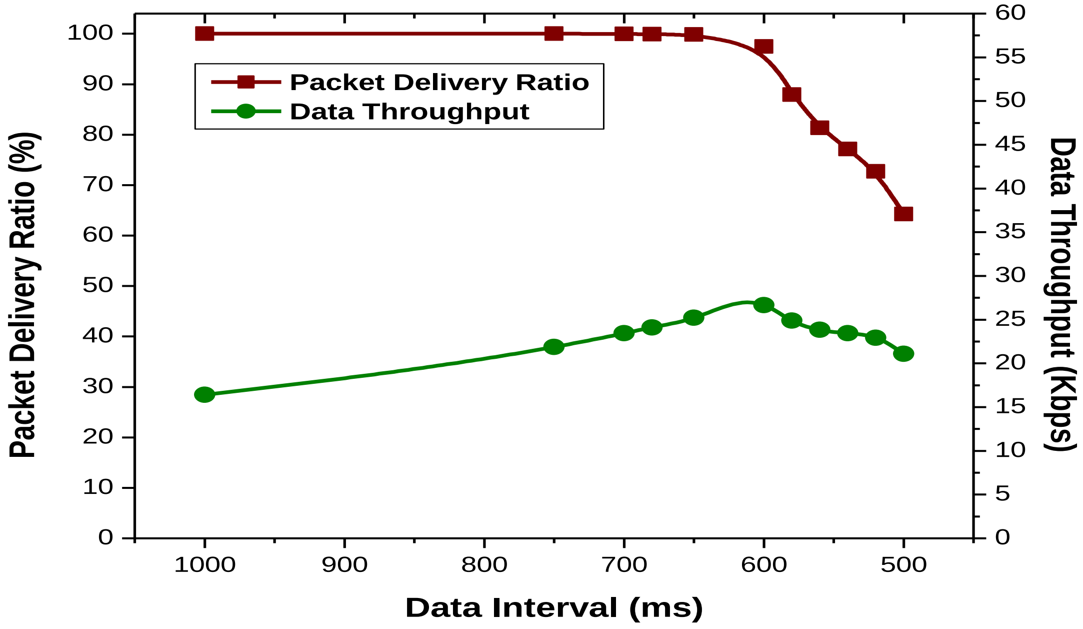
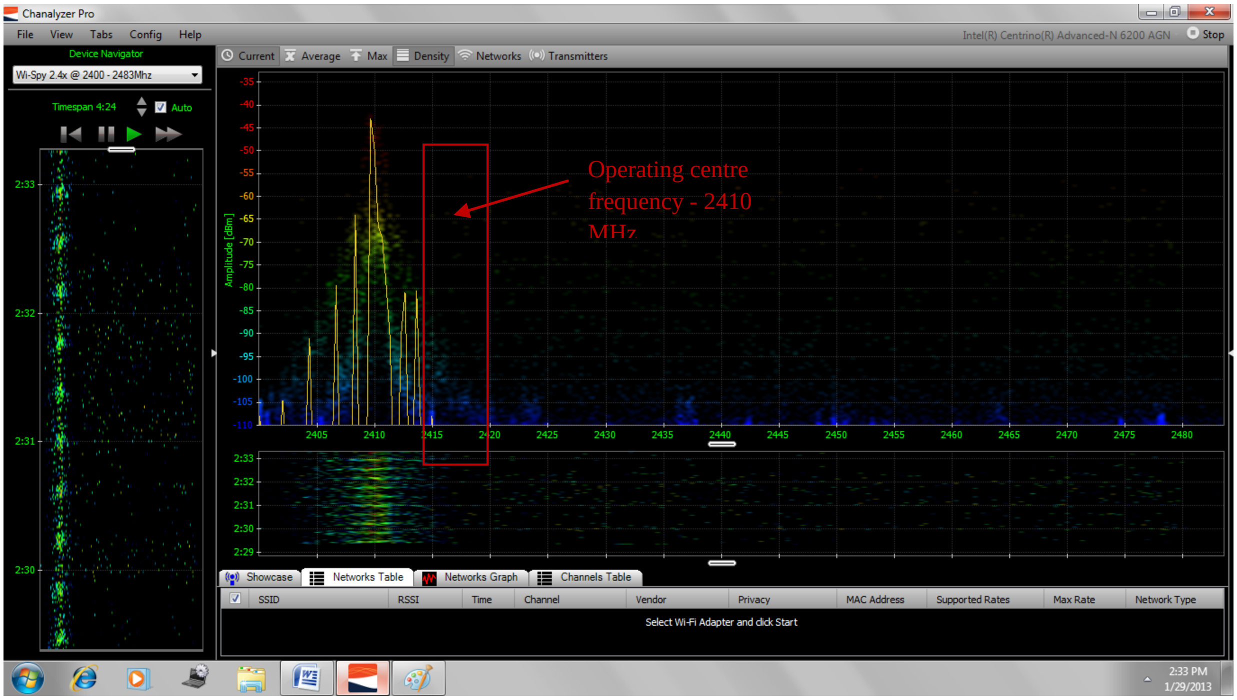


Fig. 67 Graphical view of Throughput and Packet Delivery Ratio Analysis

5.3. Performance Analysis for WSN at INSOT

The performance of wireless communication of deployed WSN with 13 sensor nodes and 1 base station has been analyzed by measuring Throughput, Packet Delivery Ratio, Interference effect, Network topology verification and battery backup duration testing.

- **Throughput Measurement:** For the deployed 13 node network, with the packet size of 98 bytes, each transmitted in 1 sec interval, the data in the air is: 10,192 bits per second. As per IEEE 802.15.4 standard, the data rate available for any wireless sensor network is 250Kbps. Hence, for this network 100% throughput was achieved.
- **Packet Delivery Ratio Measurement**: Sensor nodes are transmitting data at the rate of 1 sec. With each data packet, time tag is attached. In an hour, each sensor node transmits 3600 packets. Total number of data packets generated for 13 node network for an hour is 46,800. From the database it is found that, the number of packets received at the base station for an hour is 46,800. Zero packet drop ratio is observed which in turn represents 100% packet delivery ratio.
- **Interference effect**: WiSpy, a USB based Spectrum analyzer has been employed to identify the interference present in the operating frequency of 2410MHz at INSOT. The screenshot of the collected data is shown in Fig. 68. Interference was identified as small spikes below the range of -100dbm (0.1pW), which is absolutely negligible.
- **Network topology:** Wireless network analysis has been done using ZENA, an IEEE 802.15.4 packet analyzer supporting 2.4GHz frequency spectrum. Network topology has been drawn when it was formed, observed and recorded the packet transactions as they occur for further analysis. The topology of the formed network is verified using ZENA and is shown in Fig.69.
- **Battery backup duration testing:** Every sensor node and actuator node has battery backup with auto changeover. The battery backup time for all the nodes have been tested practically by turning off the 240V AC supply and made to run with battery. It was observed that all the nodes have run approximately 3 hours when nodes were transmitting at 1sec interval.



Wi-Spy 2.4x @ 2400 - 2483Mhz

Timespan 4:24 ☑ Auto

☑	SSID	RSSI	Time	Channel	Vendor	Privacy	MAC Address	Supported Rates	Max Rate	Network Type

Select Wi-Fi Adapter and click Start

Operating centre frequency - 2410 MHz

Fig. 68 Screenshot of the interference spectrum

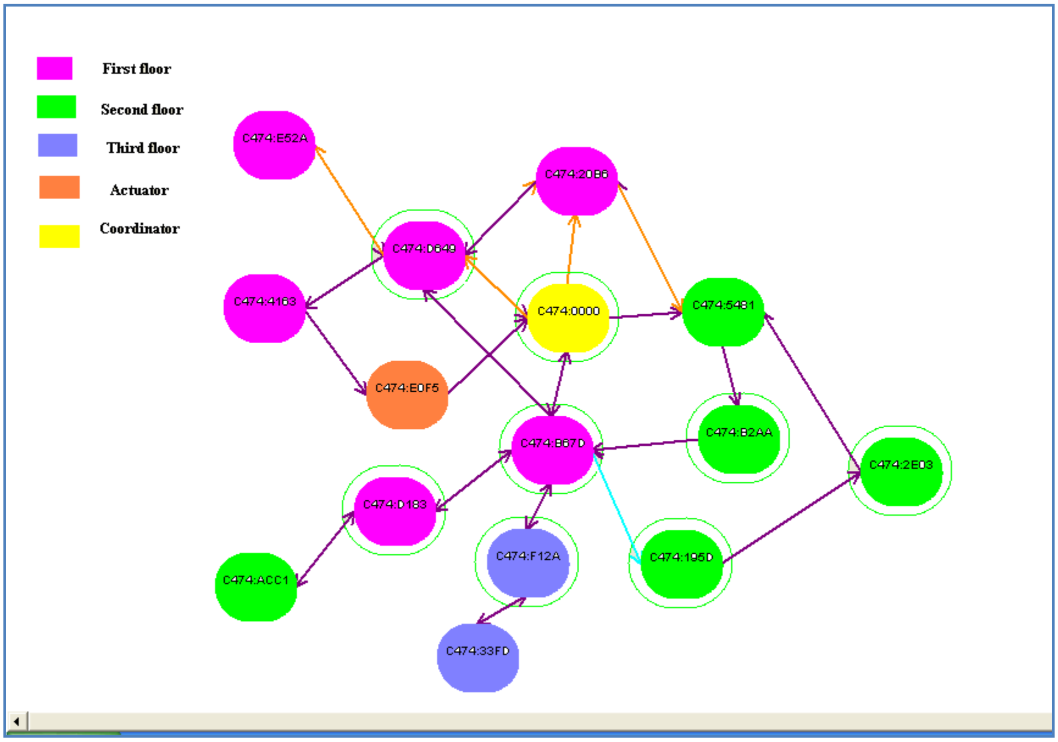


Fig. 69 Topology of the deployed network (Instantaneous)

Experiment with 30 nodes

In order to test the feasibility of expanding the network to connect 100 leak detectors, a 30 node network has been setup and data has been collected for 2 hours. 30 nodes have been chosen as it covers the complete area of three floors of INSOT area covering about 80 sq.m. and covering a good number of leak detectors of 100.

Deployment of additional sensor nodes

The existing deployed 13 node network has been expanded to 30 numbers by additionally deploying 17 sensor nodes. The additional sensor nodes were distributed in such a way that they cover all the three floors of the loop area and the control room. Four numbers of nodes were distributed in each floor and five numbers of nodes were placed in the control room. Since the aim of the experiment is to verify the possibility of having error free wireless communication, sensors were not connected to the additional nodes. The topology of the expanded network is shown in Fig. 70.

- **Performance Analysis:** Performance analysis has been done for the expanded network also by measuring Throughput and Packet delivery ratio.
- **Throughput Measurement:** For the expanded 30 node network, with the packet size of 98 bytes, each transmitted in 1 sec interval, the data in the air is: 23,520 bits per second. The topology of the extended network is shown in Fig. 68. As per IEEE802.15.4 standard, the data rate available for any wireless sensor network is 250Kbps. Hence, for this network 100% throughput is achieved.
- **Packet delivery ratio Measurement:** Sensor nodes are transmitting data at the rate of 1 sec. With each data packet, time tag is attached. In an hour, each sensor node transmits 3600 packets. Total number of data packets generated for 30 node network for two hours is 2,16,000. From the database it is found that, the number of packets received at the base station for two hours is 2,16,000. Zero packet drop ratio is observed which in turn represents 100% packet delivery ratio.

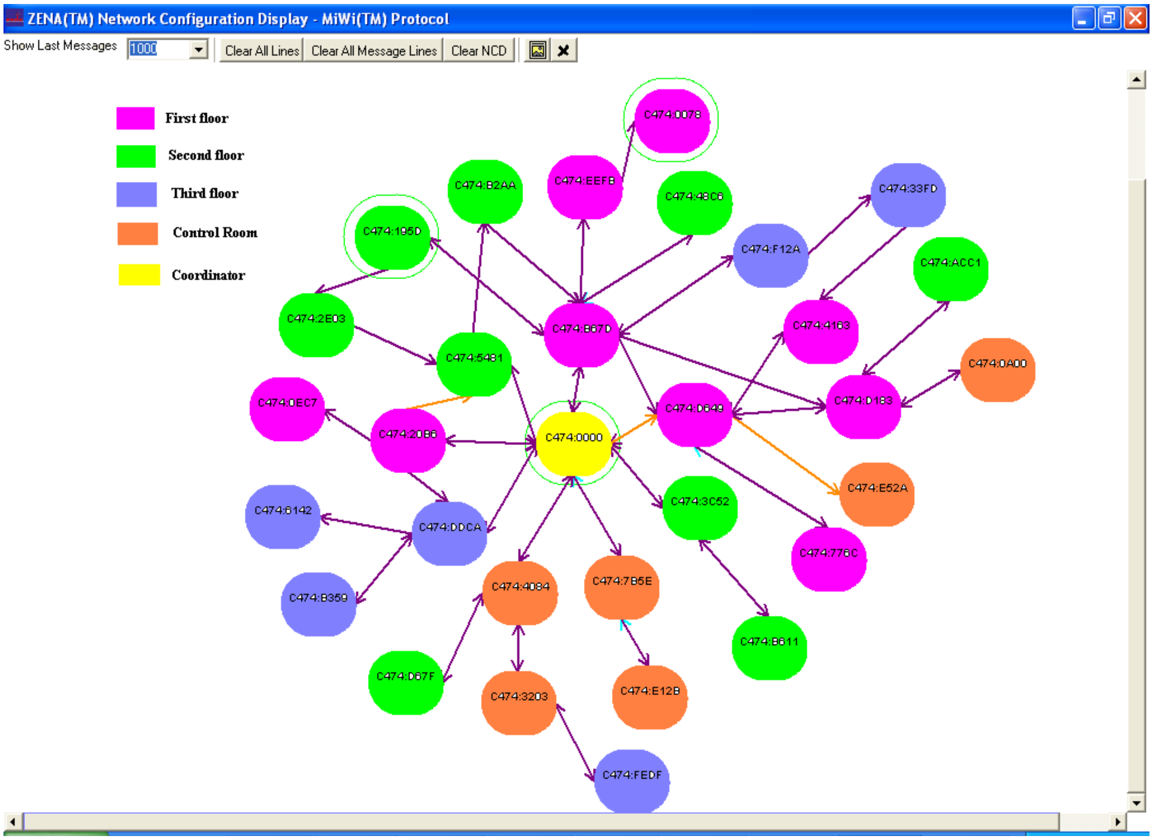


Fig. 70 Topology of the deployed network (Instantaneous)

The Performance of the expanded network has been tested, analyzed and it was found satisfactory.

5.4. Performance Analysis for WSN at FBTR

To manage and configure wireless sensor network from a remotely located Basestation, a Wireless Network Management Station (WNMS) has been designed and developed. Using that, the data analysis has been done for FBTR network. Transmitted packets are time stamped by WSN node using real time clock. To maintain correct time in WSN node, node synchronization packets are being transmitted periodically from the base station. This node time synchronization mechanism is application level synchronization with time in dd/mm/yyyy,hh:mm:ss format.

For the purpose of evaluation of the network parameters, data readings from 24-07-2012 to 09-08-2012 have been taken. This analysis is FBTR deployment specific and should be considered with transceiver and channel specific network parameters. These transceiver and channel specific performance evaluation experiments have been conducted in the WSN lab. Those results are also applicable to the FBTR WSN deployment.

Delay Calculations

In industrial networks, minimal transmission delay is expected, irrespective of the medium involved. Based on the packet sent time and packet receive time delay for all packets have been calculated. Since the minimum resolution for this deployment is 1 second, all the time delays more than 1 second has been segregated and a tabular representation of day wise percentage of zero second delay has been prepared. The Average of percentage of zero second delay for the analysis duration was found to be 99.96. Percentage of zero second delay has been shown in Table 15. This table signifies the latency of the network. It indicates whether the packets will be delivered in real time or not.

Table 15. Delay (Percentage of Zero second delay)

Day	NodeID 11	NodeID 13	NodeID 15	NodeID 18	NodeID 19	NodeID 22	NodeID 23	Average
24-07-12	99.97	99.90	99.99	99.98	99.99	99.99	99.99	99.97
25-07-12	99.96	99.94	100.00	99.99	99.99	99.99	99.92	99.97
26-07-12	99.95	99.90	100.00	99.97	99.99	99.99	99.85	99.95
27-07-12	99.94	99.91	100.00	99.99	99.99	99.99	99.92	99.96
28-07-12	99.95	99.92	100.00	99.99	99.99	99.99	99.85	99.96
29-07-12	99.96	99.91	100.00	99.98	99.98	99.99	99.84	99.95
30-07-12	99.96	99.90	99.99	100.00	99.98	99.99	99.75	99.94
31-07-12	99.96	99.89	99.99	99.99	99.98	99.99	99.91	99.96
01-08-12	99.95	99.88	100.00	99.99	99.99	100.00	99.98	99.97
02-08-12	99.94	99.90	99.99	99.99	99.99	100.00	99.98	99.97
03-08-12	99.93	99.91	99.99	99.99	99.99	99.99	99.98	99.97

04-08-12	99.93	99.91	99.99	99.97	99.98	99.97	99.97	99.96
05-08-12	99.94	99.92	99.98	99.97	99.96	99.96	99.96	99.95
06-08-12	99.93	99.91	99.99	99.98	99.99	99.98	99.98	99.97
07-08-12	99.97	99.92	99.99	99.98	99.99	99.98	99.93	99.97
08-08-12	99.93	99.89	100.00	99.93	99.99	99.98	99.85	99.94
09-08-12	99.95	99.92	100.00	99.98	99.98	99.95	99.93	99.96
Average	99.95	99.91	99.99	99.98	99.98	99.98	99.92	**99.96**

Packet Drop Ratio

Other important parameter to consider in industrial network is the ability to deliver the sensor data without any loss. This analysis has been conducted to calculate the packet drop ratio for FBTR deployment. Nodes setup in FBTR has been programmed to transmit the sensor readings every two second once. So for a node, 1800 packets would have been transmitted towards base station in one hour. For the analysis, seven nodes in the network were considered. Thus, in an hour, a total of 43,200 packets would have reached base station theoretically. The practical packet drop ratio has been calculated across all the nodes for the analysis duration from the database and is found to be $0.51*10^{-5.}$ Packet drop ratio calculation has been shown in Table 16. This table signifies packet drop ratio. It indicates packet loss in a given time.

In the various network deployments made, the number of hops is limited. To see the feasible number of hops in multi hop forwarding network the experiments were conducted by increasing the number of routing nodes in an open area of about a kilo meter distance. Because of logistic reasons the number of hops could not be increased beyond this. Increasing the number of nodes does not have any effect on the delivery ratio. But throughput will slightly comedown because of small latency introduced due to the routing nodes. However in the reactor the NNS signals have to be monitored once in 20 seconds. In this scenario the number of hops can be high.

Table 16. Packet Drop ratio (*10-5)

Day	NodeID 11	NodeID 13	NodeID 15	NodeID 18	NodeID 19	NodeID 22	NodeID 23	Average
24-07-12	0.00	2.31	2.31	0.00	0.00	0.00	0.00	0.66
25-07-12	2.31	4.63	0.00	2.31	0.00	-2.31	-2.31	0.66
26-07-12	0.00	2.31	2.31	0.00	0.00	0.00	-2.31	0.33
27-07-12	0.00	0.00	2.31	0.00	-2.31	0.00	-4.63	-0.66
28-07-12	0.00	2.31	2.31	0.00	0.00	0.00	-4.63	0.00
29-07-12	2.31	4.63	4.63	2.31	2.31	2.31	-2.31	2.31
30-07-12	0.00	2.31	2.31	0.00	0.00	0.00	-2.31	0.33
31-07-12	0.00	2.31	2.31	0.00	0.00	0.00	0.00	0.66
01-08-12	2.31	2.31	2.31	0.00	0.00	0.00	0.00	0.99
02-08-12	0.00	2.31	2.31	0.00	0.00	0.00	0.00	0.66
03-08-12	0.00	2.31	2.31	0.00	0.00	0.00	0.00	0.66
04-08-12	0.00	2.31	2.31	0.00	0.00	-2.31	-6.94	-0.66
05-08-12	0.00	4.63	2.31	0.00	0.00	0.00	0.00	0.99
06-08-12	0.00	2.31	2.31	0.00	-2.31	0.00	0.00	0.33
07-08-12	0.00	0.00	2.31	0.00	0.00	0.00	0.00	0.33
08-08-12	0.00	2.31	2.31	0.00	0.00	0.00	0.00	0.66
09-08-12	0.00	2.31	2.31	0.00	-2.31	0.00	0.00	0.33
Average	0.41	2.45	2.31	0.27	-0.27	-0.14	-1.50	**0.51**

Note: **Every node has been programmed to transmit a packet for every two seconds, thus contributing 43,200 packets theoretically for a day per node**

5.5. Analysis on Effect of Security Protocols

For evaluation of the developed Simple Security Protocol, it has been implemented in the TinyOS-2.x environment. The programs were written in nesC [108]. TinyOS is a lightweight operating system specifically designed for low-power wireless sensors [109][110]. TinyOS applications and systems, as well as the OS itself, are written in the nesC language. TinyOS has several important features that influenced nesC's design: a component-based architecture, a simple event-based concurrency model, and split-phase operations. nesC is a C dialect and is primarily intended for embedded systems such as sensor networks with features to reduce RAM and code size, and enable significant optimizations. It supports the TinyOS concurrency model, as well as mechanisms for structuring, naming, and linking together software components into robust network embedded systems. We deployed the code on IRIS motes.

The implementation of SSP is evaluated based on the code size, RAM size, overhead, packet delivery ratio and energy consumed by the nodes while incorporating the security features. For our evaluation, the application called *TestTinySec* was used.

5.6. Security Analysis

The reason for choosing a 4 byte MAC is that an adversary has to try about 2^{31} times and send 2^{31} packets in order to get a valid MAC. The relation between the radio bandwidth (B) and the time taken by the adversary to forge the MAC (T in days) is governed by the expression

$$T = (2^{n-1} * P_{size} * 8) / (B * 3600 * 24)$$

where n denotes the MAC size (in bits) and P_{size} denotes the packet size (in bits)

As an example IRIS node can deliver upto 250 Kbps application bandwidth and with a range of upto around 300m. Hence transmission of 2^{31} packets will take over nearly one month. Hence an adversary will need 32 days of continuous packet transmission to forge the MAC.

5.7. Memory Consumption

The base application without the key update code serves as reference and the results for ROM and RAM usage. Table 17 summarizes the memory overhead of the re-keying mechanisms.

Memory without Key Update : RAM = 4144 bytes ; ROM =22226 bytes

Table 17. Outline of Memory Overhead

Re-keying Mechanism	RAM (in bytes)	ROM (in bytes)	Difference (in bytes)		% increase	
			RAM	ROM	RAM	ROM
Serial	4341	24654	197	2428	4.826	10.924
Parallel	4407	24786	263	2560	6.346	11.518
Rotate	4333	24160	189	1934	4.560	8.701

The key update code adds only a considerable amount of overhead for both RAM and ROM per node. Hence the memory overhead is minimal and this scheme will be feasible on sensors with limited resource constraints.

5.8. Overhead Analysis

The most significant cost of security comes from the transmission of additional bytes, not cryptographic operations. The SSP's overhead comes solely from increased packet sizes. Fig. 71 shows a comparative study of the security overheads in the proposed protocol for both the modes namely – AUTH only and AUTH and Encrypt (AE) and how overhead increases from the existing TinyOS protocol stack.

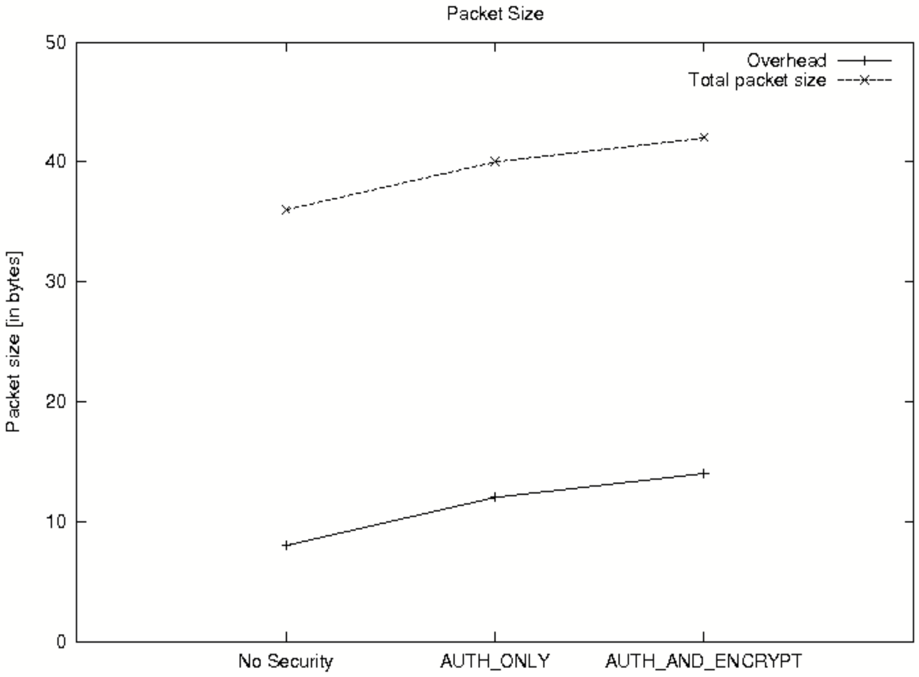


Fig. 71 Overhead Analysis

Auth only mode increases the packet overhead by 4 byte (4 byte MAC) and Auth and Encrypt mode increases the overhead by 6 bytes (2 for counter used in encryption and 4 for MAC).

5.9. Summary

Performance analysis is done for various sizes of wireless sensor networks in terms of throughput, packet delivery ratio, delay/latency in delivering the packets to ensure that the networks are working satisfactorily and as per the theoretical backing. It has to be realized that some time is required for transferring the data from micro controller to the transmitter on the transmission side and receiver to the micro controller at the receiver side. This will influence the throughput and the delay/ latency. The experiment conducted to find out the time required for different packet rates with different baud rates viz. 9600 baud rate and 115 K baud rate had clearly indicated that the time required for 115 K baud is less when compared to 9600 baud rate by almost twelve times. Also increasing the packet transmission rates from one packet per second to 10 packets second had increased the time required by the same factor. This proves that the performance is as expected and according to theory.

Similarly throughput experiments were conducted for 15 bytes payload and 66 bytes payload for different packet rates (transmission rates). The throughput was more when packet transmission rates are increased from one packet per second to 5 packets per second in the same rate. Also the throughput had increased in the same ratio when the payload size is increased from 15 byes to 66 bytes. This proves that the network is working satisfactorily as expected and as per the theoretical basis. This is possible because the maximum throughput is still less than the channel capacity.

Similarly packet delivery ratio experiments for different packet transmission rates were conducted for 15 bytes payload and 66 bytes payloads for 8 node network. Packet delivery ratio was almost 100% for different packet rates because of the available channel capacity. Similarly when experiments were conducted with security enabled transmission, there is some overhead and reducing the packet delivery ratio to that extent. It is as expected. When the network size is increased to 25 node network and the experiment is conducted packet delivery ratio is 100% for transmission rates up to 680 msec. The maximum throughput in a 25noded network is 26.65 KbPS of useful data without taking in to account the overheads. These figures can be validated theoretically taking in to account the actual data and overhead data. Also it was found that the delay is zero second for almost 100% of the packets. This again is because of available channel capacity.

CHAPTER 6

6. Conclusions

The advances in digital electronics, wireless communication and the miniaturized sensors have led to the advent of wireless sensor networks that have many advantages and applications. The advantages are no cables and cabling cost, easy and fast deployment, ability to automatically reconfigure the networks. The applications are many and left to the imagination and ingenuity of the designer. Some of them are process monitoring, military surveillance, health care monitoring, environmental monitoring, structural monitoring, home automation etc. However there are many challenges viz. low processing power, low memory, smaller range, limited bandwidth, low battery life, etc. However the advantages outweigh the challenges and the challenges have to be met through focused research and development efforts.

The nuclear power reactors offer a clean energy source without any green house gas emissions. However the safety of nuclear reactors is paramount because of the radiation effects incase of any incident. Hence the reactor designer is looking for technologies which improves safety and reduce unit energy cost. The researcher is of the strong opinion that wireless sensor networks offer the solution for improving the safety and reduce unit energy cost. Hence the topic of “Wireless Sensor Networks for Nuclear Reactor Applications” has been chosen for research.

The nuclear facilities are constructed with thick walls of high density concrete. Hence the range of the wireless sensor nodes cannot be taken as the name plate value nor can be mathematically modeled as the structures which are used for nuclear facilities are quite different and varies with each facility depending on the radiation levels handled in that facility. Hence research studies have been carried out through actual deployment to find out the signal penetration in different environments and find out the ranges permitted. This has been confirmed through measurement of RSSI values.

Then experiments have been carried out using the commercially available IRIS motes based on ATMEL ATMEGA processor. Different signal conditioning circuit boards for measuring temperature, level, smoke etc. have been developed and tested. Using commercially available nodes, experiments have been conducted to find the number of nodes needed to cover the maximum linear distance of around 200 m, almost the entire laboratory area in RCL building. The nodes are configured to work at 2410MHz frequency which is channel 11 in the frequency spectrum defined by IEEE 802.15.4 standard. Experiments were started with simulated radiation source instead of real one and it is found that 18 numbers of nodes are needed to cover the entire RCL building. Penetration studies were carried out to find the ability of the 2.4GHz signal to pass through various structures like (i) Led mini cell, where the thickness of the glass shield is 400 mm and the lead brick thickness is around 200 mm; (ii) hot cell, where the thickness of the glass shield is 1.5 m and the average density is 2.5 gm/cc; and (iii) Reactor Containment Building in Fast Breeder Reactor where the concrete wall is 1.0 m. thick. Studies have been conducted for identifying the relation between RSSI and distance practically.

From the observations of the pre-deployment experiments in various nuclear environments, it has been concluded that the commercially available nodes would not be suitable for establishing robust wireless sensor networks in reactor environment. So, it was decided to develop wireless sensor nodes in house to suit the reactor environment. The first node developed was with ARM 7 architecture based LPC 2138 controller, X-Bee transceiver and with mains power. The nodes were used in various deployments. However, it is noticed that this node has limited processing power and for data aggregation and for implementing encryption algorithms we require more processing power. Hence another node based on CORTEX M3 LPC 1768 controller was developed and used in further deployments. Then, with the experience that was obtained, it was found that for deploying the nodes in harsh and high temperature environments, industrial grade nodes with IP 54 enclosure, design for EMI/EMC compliance, industrial grade electronic components to withstand high temperature were designed and developed. These nodes were fully deployed in different nuclear environments including the Fast Breeder Test Reactor. Thus different types of microcontroller based nodes such as sensor node, router node, cluster head node, actuator node and base station node have been developed for various functionalities and applications. Sensing systems have also been developed to interconnect the existing sensors to WSN nodes.

Software stack based on 802.15.4 MAC has been developed for in-house developed WSN nodes. Embedded OS based design has been chosen for the software stack design. Hardware based component of this implementation has been separated to provide the future portability of this stack to newer platforms. This software stack is useful for development of higher layer WSN mechanisms and protocol.

Pre-deployment and commissioning methodologies have been developed. These methodologies are useful in detecting the in-site interference and identification of routing patterns and behaviors of the future network. These studies also help to identify the scope and method of integration and interoperation with the existing plant network. Special hardware and software solution has been developed for pre-deployment, commissioning, monitoring and management methodologies. These solutions can further be developed for automatic network diagnostic decision, based on the network parameters collected by network manager and/or network coordinator. Monitoring and management solutions are important during network operation. These solutions show the current network behavior and traffic pattern in the network and also help to identify and debug the problems in network operation.

Long term wireless sensor networks have been deployed at various facilities at IGCAR such as Computer Centre, INSOT, SADHANA and FBTR in addition to various test networks in radiological laboratories. At computer centre, initially WSN is deployed for monitoring the temperature and humidity at High Performance Computing cluster system. The flat architecture has been chosen for WSN. This network consists of two sensor nodes with temperature sensors, two routing nodes and a base station. All nodes were configured to work at 2450MHz frequency in channel ‘14’ with 3dbm power level. The ¼ wave dipole antenna is used. The WSN has been expanded for monitoring the room temperature and humidity of the whole computer centre [CCNET] with the sensor nodes placed at Simulator room, Server room, Campus Backbone area, HPC cluster Air inlet and HPC rack. The expanded WSN setup consists of 4 sensor nodes and 3 router nodes with Xbee transceiver and a base station. Web based GUI has been developed for continuous monitoring from anywhere in network. Further the CCNET has been enhanced by replacing the USB connectivity base station with the Ethernet based gateway, designed using Wiznet module. This established setup has been effectively maintained and working well for more than 2 years.

At INSOT, initially WSN was deployed for Sodium Leak detection for 9 numbers of leak signals with 3 nodes and one base station. Since the alarm has to be activated while detecting Sodium leak, the actuator node has been designed, developed and added in the control room. This test network with independent leak detectors was running successfully for 6 months. After the successful testing, a 15 noded WSN with 13 sensor nodes connected to 50 leak signals and one base station, one actuator node has been established in INSOT facility. The transceiver XBee-Pro radio chips are configured for 2410 MHz at channel ‘C’ of IEEE 802.15.4 Standard, with a power of 1mW. The network is distributed across three floors of the building covering nearly 80 m² area. One router node is placed in each of the three floors to provide redundant path. The base station was connected to a PC through USB port and receives the field data from the sensor nodes. The status of the leak detectors was displayed on the PC monitor. Actuator node for actuating buzzer in case of sodium leak was installed in the control room. This network was made as a permanent setup to provide diverse path for detecting the sodium leak along with the wired leak detector systems. It is running successfully for the past one year

.

At SADHANA, the WSN is deployed vertically across multiple floors to measure temperature and humidity. Flat architecture has been chosen for this network and it consists of two sensor nodes and a base station. All nodes were configured to work at 2425MHz frequency in channel ‘F’ with 3dbm power level. Omni directional 2dBi dipole high gain antenna is used and oriented vertically in all nodes. One sensor node is located in 11th floor (chimney outlet at terrace of Hall-III building) with two K-type thermocouples and one humidity sensor connected to it. Another sensor node has been placed in 5th floor (chimney inlet) with one humidity sensor connected to it. The two sensor nodes data was collected by the base station through two router nodes in the control room and displayed on the PC monitor. For that, GUI has been developed using Laboratory Virtual Instrumentation Engineering Workbench (LabVIEW). The network is running successfully for the past 16 months.

To explore the potential of WSN technology in reactor environment, WSN was deployed in Fast Breeder Test Reactor (FBTR). Initial experiments in FBTR were mainly concentrated on the evaluation of RF profile of FBTR complex and ranging capabilities of in-house developed WSN systems in FBTR environment. Based on these experiments, WSN is deployed for measuring temperature and vibration and monitoring. Zigbee based WSN is configured at 2410 MHz, Channel ‘C’. Sensors connected to the network contain both, independent and intra-system sensors from FBTR. Router nodes have been placed in between to route the sensor data towards base station, which has been placed in FBTR control room. The locations of these nodes were determined based on the initial experiments. To manage and configure wireless sensor network from a remotely located base station, Wireless Network Management Station (WNMS) has been developed. This network is successfully working from past 18 months and different performance evaluation experiments have been carried out. Readings from intra-system FBTR sensors also have been verified with plant sensor readings and found to be matching. Presently FBTR WSN has been expanded with 25 nodes, which includes 5 sensor nodes for temperature (12 signals), 7 sensor nodes for vibration (7 signals), 1 sensor node for flow rate (2 signals), 1 base station node and 11 router nodes.

When different wireless sensor networks were deployed, it became necessary to mange the networks to ensure that the networks are working smoothly. Towards this it is required to know, the topology view, indicating the path of data transfer ie. which sensor node is using which router nodes to transmit the data to the final base station, status view of the healthiness of each of the nodes, the table view, which indicates the sensor signal name, tag number and the sensed value etc. Hence a Wireless Sensor network Management Station has been developed. The successful operation of this WNMS was tested. It became a very useful tool for measuring the healthiness of the network and for debugging purposes.

From the deployed networks, the performance analysis has also been done with the parameters such as throughput, packet drop ratio, packet delivery ratio, effect of interference and battery backup duration. Throughput experiments were conducted at WSN lab with 15 byte and 66 byte payload for varying transmission rates, with and without security enabled. The packet delivery ratio was measured for 25 noded network and found that for a tolerance of 2.5% loss in packets, maximum achievable throughput was 26.64 Kbps. Performance analysis was conducted for WSN deployed at INSOT and FBTR and the results were explained in the respective chapters.

Another important issue related to WSN is the data security. Network security is also an evolving field and some of the solutions can be applied to WSN. However the encryption algorithms used in wired networks cannot be deployed in WSNs because of the constraints in processing power and memory. Thus WSN poses different challenges than the traditional networks hence the careful application of these security solutions are required. Some of these solutions have been applied to deployment and their effects on the WSN node and network have been observed.

With the design and deployment of multiple wireless sensor networks using indigenously developed nodes, their successful operation was observed for many months. The results from the field are compared with the measured and transmitted values at the base station. A very good matching of results over the complete period is found. With the wireless network management station data flow is observed and the automatic reconfigurability of the router nodes is successfully verified by switching off and switching on different router nodes. The table view gave a complete view of the sensed signals in the control room where ever the wireless network management station is deployed.

The research and development activities that measured the packet delivery ratio, packet drop ratio at different scan rates, over heads because of enabling security etc. has proved the successful working of the networks. All this research gave enough confidence that wireless sensor networks can be successfully deployed in nuclear reactor environment and it is a potential technology that can increase the safety of the nuclear reactors and eventually reduce the unit energy cost. A cost analysis study was done to prove that the wireless networks cost less when compared to wired networks. The cost analysis was given in Table 18. Accordingly it is being planned to establish Wireless Sensor Networks in future reactors for process monitoring.

Table 18. Cost comparison between Wired network and Wireless Sensor Network for transmitting 20 Process Monitoring Signals in FBTR (A Typical Network)

	Wired set up at FBTR	**Wireless set up at FBTR**
Source side	signal conditioning : Rs 500 X 20 = Rs 10000/-	Sensor node (Industrial grade components, IP54 rated, EMI/EMC qualified) Rs 35,000/- *3[#] =Rs 1,05,000/-
Transmission	Cable & Cable laying cost: Rs 600/- per meter.	Router cost: Rs 16,000/- per 60 meter
Destination side	Processing electronics Rs 15000/- * 20 = Rs 3,00,000	Base station Rs 2000/- per network
For Single Hop (60 meters)	Rs 10000 + 600 * 60 + 300000 = Rs 3,46,000	Rs 105000 + 0 + 2000 = Rs 1,07,000
For 2 hops	Rs 10000 + 600 * 60*2 + 3,00,000 = Rs 3,82,000	Rs 105000 + 16000 + 2000 = Rs 1,23,000
For 3 hops	Rs 10000 + 600 * 60*3 + 3,00,000 = Rs 4,18,000	Rs 105000 + 16000 *2+ 2000 = Rs 1,39,000
For 4 hops	Rs 10000 + 600 * 60*4 + 3,00,000 = Rs 4,54,000	Rs 105000 + 16000 *3 + 2000 = Rs 1,55,000

- #: Each WSN node can take care of 8 signals.
- For single hop no router is required as sensor node will directly transmit to Base Station. For two hops, one router node is required. In FBTR from field to control room 4 hops are required.

- The **distance** used for calculation is considered as “**Line of sight**” (straight line – minimum distance). In Wired setup, the cable routing does not follow the straight line path. The approximate cable required for transmitting the 20 signals from field to Control Room in FBTR will be around 500 meters of 20 pair shielded cable. However the line of sight distance is only included. Also in wired network, the cable tray cost, it’s installation cost has to be included.
- Thus Wireless Sensor Network costs out to be much cheaper than Wired Network.

CHAPTER 7

7. Future Scope

The design & development of various WSN nodes and their deployment in various nuclear facilities including the Nuclear Reactor has given enough confidence to the designers that it is a viable and economical solution for monitoring various plant parameters. However some more works need to be done to convince the regulatory authorities. They are listed below as a future scope.

1. Though the WSN nodes have been designed and fabricated with EMI/EMC compatibility, signal integrity and thermal integrity tools, they need to be tested for EMI/EMC in an accredited Laboratory.

2. The nodes have to be radiation hardened by designing the nodes with radiation hardened Components, so that they work well even in incident conditions when radiation levels are expected to be high.

3. It is required to measure the radiation levels in and around radiation facilities like nuclear reactors, reprocessing facilities etc. So, it is planned to establish a radiation monitoring wireless sensor network few kilo meters around the reactor complex. For such a network, it is not possible to provide electrical supply for all the nodes and it will be difficult to change batteries often. Hence the development of solar powered nodes is required.
4. For improving the security Advanced Encryption Standard with 256 bit key length needs to be implemented. The required light weight Security protocol is required to be developed.

5. For improving the real time response, efficient real time routing protocols need to be developed.

6. Some of the existing deployments especially in Fast Breeder Test Reactor were established as parallel network, by tapping the process parameter for use in wired as well as wireless sensor network. Further network deployments without parallel connection needs to established and their robustness has to be shown to get them approved by regulatory authorities.

7. Further wireless sensor networks with large number of nodes ie. more than hundred nodes need to be deployed and interference studies have to be carried out.

8. Multiple wireless sensor networks in multiple channels of 2.4 GHz ISM band with large number of nodes in each channel need to be established in the same area and the interference studies have to be done.

9. The through put analysis shall also be carried out for such networks having more than hundred nodes.

10. The networks shall also be established in high radiation environments and their performance over a long period has to be studies.

REFERENCES

[1] Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards, Paolo Baronti , Prashant Pillai , Vince W.C. Chook , Stefano Chessa Albert,Gotta , Y. Fun Hu. Computer Networks 52 (2008) 2292–2330.

[2] Embedded Everywhere: Research Agenda for Networked Systems of Embedded computers The National Accademics Press, Washington, D.C. , 2001

[3] Wireless Sensor Networks: A Survey, Akyildiz I.F., Su W., Sankarasubramaniam Y., Cayirci E., Computer Networks, Vol .3 No. 4, pp. 393-422, 2002

[4] Sensor Networks: An Overview, Archana Bharathidasan, Vijay Anand Sai Ponduru, Department of Computer Science, University of California, Davis, CA 95616.

[5] Wireless sensor network survey, Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, Computer Networks 52 (2008) 2292–2330.

[6] Lessons In Industrial Instrumentation, Tony R. Kuphaldt, Version 0.4 – Released January 11, 2009

[7] Wireless Sensor Networks for Industrial Process Monitoring and Control: A Survey, Gang Zhao, Network Protocols and Algorithms, ISSN 1943-3581, Vol. 3, No. 1,2011

[8] Wireless Sensor Networks: Principles and Practice; Fei Hu, Xiaojun Cao;CRC Press Taylor & Francis Group, ISBN: 978-1-4200-9215-8.

[9] Wireless Sensor Networks, Raghavendra, C.S, Krishna M. Sivalingam, Ty Znati, Springer Academic Publishers, 2004.

[10] An Introduction to Wireless Sensor Networks, Bhaskar Krishnamachari, Tutorial Presented at the Second International Conference on Intelligent Sensing and Information Processing (ICISIP), Chennai, Jan 2005.

[11] Wireless sensor networks: Technology, protocols and Applications, Kazem Sohraby, Daniel Minoli, Taieb Znati, A John Wiley& Sons, INC., Hoboken, New Jersey, 2007.

[12] Design challenges for short-range wireless networks, A. Sikora, WLAN Systems and Interworking, IEE Proceedings on Communication, Vol. 151, No. 5, October 2004

[13] Wireless sensor networks: applications and challenges of ubiquitous sensing, Puccinelli D, Haenggi. M , IEEE Circuits and Systems Magazine, Volume: 5, Issue: 3, Pg 19 - 31 2005.

[14] Wireless Sensor Networks: Architectures and Protocols; Edgar H.Callaway.Jr, Auerbach Publications; ISBN 0-8493-1823-8.

[15] Mica: a wireless platform for deeply embedded networks, Jason L. Hill, David E. Culler, IEEE Micro, Volume 22 Issue 6, November 2002

[16] MICA2, Wireless Measurement System, Document Part Number: 6020-0042-04, Crossbow Technology, Inc

[17] MPR - Mote Processor Radio Board, MIB - Mote Interface / Programming Board User's Manual MPR500CA, MPR510CA, MPR520CA,PR400CB, MPR410CB, MPR420CB, MPR300CA, MPR310CA, IB300CA, MIB500CA,MIB510CA, MIB600CA, Rev. A, December 2003, Document 7430-0021-05, Crossbow Technology, Inc

[18] MICA2DOT, Wireless Microsensor Mote, Document Part Number: 6020-0043-03, Crossbow Technology, Inc

[19] MICAz, Wireless Measurement System, Document Part Number: 6020-0065-05 Rev A, MEMSIC Inc.

[20] IRIS, Wireless Measurement System, Document Part Number: 6020-0124-02 Rev A, MEMSIC Inc.

[21] MCS410, Cricket Wireless Location System, Document Part Number: 6020-0063-03 Rev A, MEMSIC Inc.

[22] RFM TR1000 data sheet, 916.50 MHz Hybrid Transceiver TR1000 - RF Monolithics, Inc., 2008-2012

[23] CC1000 datasheet, Single Chip Very Low Power RF Transceiver, Texas Instruments

[24] CC2420 data sheet, 2.4 GHz IEEE 802.15.4 / ZigBee-Ready RF Transceiver, SWRS041, Texas Instruments

[25] AT86RF230 Datasheet: Low Power 2.4 GHz Transceiver for ZigBee, IEEE 802.15.4, 6LoWPAN, RF4CE and ISM Applications

[26] MTS/MDA Sensor and Data Acquisition Board User's Manual, Rev. B, April 2005 Document 7430-0020-03

[27] The intel® mote platform: a bluetooth*-based sensor network for industrial monitoring, Lama Nachman, Ralph Kling, Robert Adler, Jonathan Huang, Vincent Hummel, Corporate Technology Group Intel Corporation

[28] Imote2, High-performance Wireless Sensor Network Node, Document Part Number: 6020-0117-02 Rev A, MEMSIC Inc.

[29] A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, Elizabeth M. Royer, Santa Barbara, Chai-Keong Toh, IEEE Personal Communications, Pg 46 -55, April 1999

[30] Routing techniques in wireless sensor networks: a survey, Al-Karaki, J.N., Kamal, A.E., IEEE Wireless Communications, 11(6), 6–28, 2004.

[31] A survey on routing protocols for wireless sensor networks, Kemal Akkaya, Mohamed Younis, Ad Hoc Networks 3 325–349, 2005.

[32] Energy-Efficient Communication Protocol for Wireless Microsensor Networks**,** Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan, Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000, ISBN:0-7695-0493-0/00 (c) 2000 IEEE.

[33] Analysis of security protocols for wireless, M. Swathy, Jemimah Ebenezer, E.N. Ganesh S.A.V. SatyaMurty, International Journal of Computer Applications in Engineering, Technology and Sciences (IJ-CA-ETS), April 2009

[34] Security Issues in Wireless Sensor Networks, Jemimah Ebenezer K.Vijaykumar S.A.V.SatyaMurty S. Athinarayanan P.Swaminathan, Proceedings of International Conference on Trends in Intelligent Electronic Systems (TIES 2007), July 2007

[35] Secure routing in wireless sensor networks: Attacks and countermeasures, C. Karlof and D. Wagner, Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, September 2003.

[36] Security in wireless sensor network, Adrian Perrig, John Stankovic, David Wagrer, Communications of the ACM, Vol. 47, No. 6, pg 53 -55, June 2004

[37] Tinysec: A link layer security architecture for wireless sensor networks, C. Karlof, N. Sastry, and D. Wagner, Second ACM Conference on Embedded Networked Sensor Systems (SensSys 2004), pages 162–175, November 2004

[38] MiniSec: A Secure Sensor Network Communication Architecture, Mark Luk, Ghita Mezzour, Adrian Perrig, Virgil Gligor, In Proceedings of the Sixth International Conference on Information Processing in Sensor Networks (IPSN 2007), April 2007.

[39] IEEE 802.15 Working Group for WPAN, [online] Available at: http://www.ieee802.org/15/

[40] IEEE Std 802.15.4™-2003, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)

[41] IEEE Std 802.15.4e™-2012, (Amendment to IEEE Std 802.15.4™-2011), Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), Amendment 1: MAC sublayer

[42] Towards IEEE 802.15.4e: A Study of Performance Aspects, Feng Chen, Reinhard German and Falko Dressler

[43] IEEE Std 802.15.4g™-2012, (Amendment to IEEE Std 802.15.4™-2011), Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), Amendment 3: Physical Layer (PHY) Specifications for Low- Data-Rate, Wireless, Smart Metering Utility Networks

[44] ZigBee Wireless Networks and Transceivers: Shahin Farahani, Newnes, An Imprint of Elsevier; ISBN: 978-0-7506-8393-7

[45] ZigBee Specification, ZigBee Document 053474r17, January 17, 2008, ZigBee Alliance

[46] Zigbee Wireless Networking, Drew Gislason, Newnes

[47] Wireless communication network and communication profiles – WirelessHART™, IEC 62591, Edition 1.0 2010-04, Industrial communication networks

[48] ISA-100.11a-2011, An ISA Standard Wireless systems for industrial automation: Process control and related applications

[49] Fieldbus specifications – WIA-PA communication network and communication profile, IEC 62601, Edition 1.0 2011-11 Industrial communication networks

[50] TSMP: Time Synchronized Mesh Protocol, Kristofer S. J. Pister, Lance Doherty, Proceedings of the IASTED International Symposium on Distributed Sensor Networks (DSN08), November 2008, Orlando, Florida, USA.

[51] IETF Working Group for IPv6 over Low power WPAN (6LoWPAN), [online] Available at: http://datatracker.ietf.org/wg/6lowpan/charter/

[52] RFC4919, August 2007 : IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals; [online] Available at: http://tools.ietf.org/html/rfc4919

[53] RFC4944, September 2007 : Transmission of IPv6 Packets over IEEE 802.15.4 Networks, [online] Available at: http://tools.ietf.org/html/rfc4944

[54] The 6LoWPAN Architecture: Geoff Mulligan, 6LoWPAN Working Group, IETF, EmNets '07: Proceedings of the 4th workshop on Embedded networked sensors, ACM, 2007

[55] Energy Harvesting Wireless Sensor Solutions and Networks from EnOcean, [online] Available at: http://www.enocean.com/en/home/

[56] Wireless Short-Packet (WSP) protocol optimized for energy harvesting - Architecture and lower layer protocols, ISO/IEC 14543-3-10:2012 : Information technology -- Home Electronic Systems (HES) -- Part 3-10:

[57] IEEE 1902.1-2009 - IEEE Standard for Long Wavelength Wireless Network Protocol, Print ISBN: 978-0-7381-5898-3, March 2009

[58] Rubee Technology, Real-Time Asset Visibility, [online] Available at: http://www.rubee.com/Techno/index.html

[59] Pantex: Advanced Inventory and Material Management at Pantex, [online] Available at: http://www.rubee.com/Work/WhitePapers/PantexReport/ AIMMPresentationINMM.pdf

[60] DASH 7 Alliance, [online] Available at : http://www.dash7.org/

[61] Nuclear Power Plant Instrumentation and Control, H.M.Hashemian, Chapter 3 in InTech book, Nuclear Power – Control, Reliability and Human Factors, European Open Access Publisher, [online] Available at: http://www.intechweb.org. Nuclear Power / Book 4, ISBM 979-953- 307-855-6, pp. 49-66 (September 2011).

[62] Radiation detection with distributed sensor networks, Brennan, S,M., Angela M. Mielke, David C. Torney and Arthur B. Maccabe, (2004), IEEE Computer Magazine, vol. 37, pp. 57-58, August 2004.

[63] Radioactive source Detection by Sensor Networks, Brennan, S, M.,. Mielke A, M.and. Torney D, C,. (2005), Transaction on Nuclear Science, Vol.52, No.3, June 2005

[64] Wireless Sensor Networks to Control Radiation Levels, Gascón, D., Yarza, M. (2011) [online] Available at: http://www.libelium.com/libeliumworld/articles/11-21.

[65] Radiation Detection and Measurement, 3rd Edition,Glenn ,F,K. (2000) , John Wiley & Sons, Inc.

[66] Design and Implementation of Radiation Dose Monitoring System Based on Wireless Sensor Network, Huang,F., Sun,T., (2011), International Conference on Future Information Technology IPCSIT, Vol.13, 2011.

[67] INIT (2001) ‘Health Physics Instrumentation’, Proceedings of BRNS Symposium on Intelligent Nuclear Instrumentation-2001 (Invited Talks) – INIT-2001, Feb.6-9,2001, pp. 44-53.

[68] Radiation Detection with Distributed Sensor Networks, Mielke, A., Jackson, D., Brennan, S.M., Smith, M.C., Torney, D.C., Maccabe, A.B. and Karlin, J.F., (2005) SPIE Defense and Security Proceedings 2005.

[69] Application of wireless sensor networks in personnel dosage monitoring system of nuclear power plant, Yonghong,C., Dafa,Z., Wei,J. (2007), Chinese Journal of Nuclear Science and Engineering, Vol 27 No.4.

[70] Experimental Deployment of Wireless Sensor Network for Radiation Monitoring, S.A.V. SatyaMurty Baldev Raj Krishna M. Sivalingam Jemimah Ebenezer R. Parthasarathy D. SaiSubalakshmi, Journal of Nuclear Engineering & Technology, April 2012

[71] Wi-Spy Data Sheet [online] Available at: http://files.metageek.net/marketing/Wi-Spy_2.4x/MetaGeek_Wi-Spy_24x_datasheet.pdf

[72] The Fast Breeder Test Reactor -Design and Operating Experiences, G. Srinivasan, K.V. Suresh Kumar, B. Rajendran, P.V. Ramalingam, Nuclear Engineering and Design 236 Pg 796–811, 2006

[73] Twenty five years of operating experience with the Fast Breeder Test Reactor, K.V. Suresh Kumar, A. Babu, B. Anandapadmanaban & G. Srinivasan, Asian Nuclear Prospects 2010, Energy Procedia Vol-7, Pg. 323–332, 2011

[74] Wireless Sensor Network in Fast Breeder Test Reactor, S.A.V. SatyaMurty, Baldev Raj, Krishna M. Sivalingam, S.Sridhar, Jemimah Ebenezer, Kalyan Rao Kuchipudi, Journal of Nuclear Engineering & Technology, Volume 3, Issue 1, ISSN: 2277-6184, April 2013

[75] XBee®/XBee- PRO® ZB RF Modules datasheet © 2010 Digi International, Inc.

[76] Experimental Analysis of RSSI-based Location Estimation in Wireless Sensor Networks, Mohit Saxena, Puneet Gupta, Bijendra Nath Jain; 3rd International Conference on Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008.

[77] Is RSSI a Reliable Parameter in Sensor Localization Algorithms – An Experimental Study, Ambili Thottam Parameswaran, Mohammad Iftekhar Husain, Shambhu Upadhyaya, 28th International Symposium on Reliable Distributed Systems; September 27-30, 2009.

[78] IRIS mote Data Sheet, [online] Available at: http://www.xbow.com/Products/Product pdf files/Wireless pdf/IRIS Datasheet.pdf

[79] Localization Algorithms in Wireless Sensor Networks: Current Approaches and Future Challenges, Amitangshu Pal, Network Protocols and Algorithms, ISSN 1943-3581; 2010, Vol. 2, No. 1

[80] Experimental Analysis of RSSI for Distance and Position Estimation, Vinita Daiya, Jemimah Ebenezer, S.A.V. SatyaMurty, Baldev Raj, Proceedings of International Conference on Recent Trends in Information Technology [ICRTIT'11], June 2011

[81] LPC2131/2/4/6/8 user manual, Rev.4 - April 2012, [online] Available at: http://www.nxp.com/documents/user_manual/UM10120.pdf

[82] Analog devices, AD7327, 2006, [online] Available at: http://www.analog.com/static/importedfiles/data_sheets/AD7327.pdf

[83] Document No.: FT_000053 FT232R USB UART IC Datasheet Version 2.10, 2010, [online] Available at: http://www.ftdichip.com/Support/Documents/DataSheets/ICs/DS_FT232R.pdf

[84] AT86RF230 Datasheet: Low Power 2.4 GHz Transceiver for ZigBee, IEEE 802.15.4, 6LoWPAN, RF4CE and ISM Applications, [online] Available at: http://www.atmel.in/images/doc5131.pdf

[85] Cortex™-M3, Revision: r1p1, Technical Reference Manual, ARM Ltd., ARM DDI 0337E, [online] Available at: http://chess.eecs.berkeley.edu/eecs149/sp09/docs/CortexM3_TRM.pdf

[86] UM10360, LPC17xx User manual, Rev. 01 — 4 January 2010, NXP Ltd, [online] Available at: http://laboratorios.fi.uba.ar/lse/curso_intensivo/practicas_laboratorio/user.manual.lpc17xx.pdf

[87] USB Complete, The Developer's Guide, Jan Axelson, Lakeview Research; June 2009, 506 pages; ISBN 9781931448116

[88] Wireless Sensor and Actuator Networks: Technologies, Analysis and Design, Roberto Verdone, Davide Dardari, Gianluca Mazzini and Andrea Conti, Academic press, Elsevier Ltd 2008 edition.

[89] Choosing the best system software architecture for your wireless smart sensor design: [online] Available at: http://www.embedded.com/design/prototyping-and-

development/4007255/Choosing-the-best-system-software-architecture-for-your-wireless-smart-sensor-design-Part-1

[90] The Contiki Operating System, [online] Available at: http://www.sics.se/contiki/

[91] Porting Contiki: [online] Available at: http://www.sics.se/~adam/contiki-workshop-2007/workshop07porting.ppt

[92] Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors: Adam Dunkels, Bj¨orn Gr¨onvall, Thiemo Voigt, Swedish Institute of Computer Science

[93] A Study of the Behaviour of the Simple Network Management Protocol, Colin Pattinson, 12th International Worshop on Distributed systems: Operations and Management, DSOM'2001

[94] Intelligent Management Center Wireless Services Manager Software Datasheet, [online] Available at: http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-0720ENW.pdf

[95] RFC 2571: An Architecture for Describing SNMP Management Frameworks, [online] Available at: http://www.ietf.org/rfc/rfc2571.txt

[96] Packetostatics: Deployment of massively dense sensor networks as an electrostatics problem, Toumpis, S., and Tassiulas, L., Mar. 2005, Proc. IEEE INFOCOM, Miami, FL.

[97] CBC-MAC, [online] Available at: http://en.wikipedia.org/wiki/CBC-MAC

[98] Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks, Woo Kwon Koo, Hwaseong Lee, Yong Ho Kim, Dong Hoon Lee 2008, International Conference on Information Security and Assurance.

[99] Handbook of Applied Cryptography, A. Menezes, P. van Oorschot, and S. Vanstone.

[100] Wireshark Network Protocol Analyzer, [online] Available at: http://www.wireshark.org/

[101] Zena Network Analyzer, [online] Available at: http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1406&dDocName=en520682

[102] SmartRF™ Packet Sniffer User Manual, Texas Instrument, SWRU187F

[103] Perytons™ Protocol Analyzers - Wireless product suite, [online] Available at: http://www.perytons.com/products/general-wireless-page/#TextTop

[104] Wireshark User's Guide: for Wireshark 1.7 by Ulf Lamping, Richard Sharpe, and Ed Warnicke

[105] RZRAVEN USB Stick (Jackdaw), [online] Available at: http://www.sics.se/~adam/contiki/docs-uipv6/a01108.html

[106] Wireshark Zigbee Utility, [online] Available at: http://sourceforge.net/projects/wiresharkzigbee/

[107] WSBridge,[online] Available at: http://freaklabs.org/index.php/WSBridge.html

[108] ARM Compilation tools, [online] Available at: http://www.keil.com/arm/realview.asp

[109] X-CTU Configuration & Test Utility Software User guide, [online] Available at: http://ftp1.digi.com/support/documentation/90001003_A.pdf

[110] Introduction to LabVIEW 8.5 by Finn Haugen 31. August 2008, [online] Available at: http://techteach.no/labview/lv85/labview/index.htm

[111] Operating Experience of High Temperature Sodium Loops for Material Testing, Shanmugavel, M., Vijayaraghavan, S., Rajasundaram, P., Chandran, T., Shanmugasundaram, M., Rajan, K.K., Kalyanasundaram, P., Energy Procedia, 7, 609-615. 2010.

[112] Operating experience of In-Sodium Test facility, Vijayaraghavan, S., Shanmugasundaram, M., Shanmugavel, M., Rajan, K.K., Venugopal, S., Bhanusankara Rao, K. Rajan, M., 2006. Proceedings of the National conference on Operating Experience of Nuclear Reactors and Power Plants –OPENUPP-2006, Mumbai.

[113] Developments in sodium technology. Kale, R.D., Rajan, M., 2004. Current Science, 86(5), 668-675.

[114] Performance evaluation of PFBR wire type sodium leak detectors, Nuclear Engineering and Design, Vijayakumar, G., Rajan, K.K., Nashine, B.K., Chandramoul, S., Madhusoodana, K., Kalyanasundara, P., 2011. 241(6), 2271-2279

[115] Wireless sensor network for sodium leak detection, S.A.V. Satya Murty, Baldev Raj, Krishna M. Sivalingam, Jemimah Ebenezer, T.Chandran, M. Shanmugavel, K.K. Rajan; Nuclear Engineering and Design, Volume 249 (2012) 432– 437

[116] Major Sodium Facilities in FRTG, [online] Available at: www.igcar.ernet.in/facility/Sodium_facilities.pdf

[117] Current Status of Fast Reactors and Future Plans in India, S.C.Chetal, P.Chellapandi, P.Puthiyavinayagam, S.Raghupathy, V.Balasubramaniyan, P.Selvaraj, P.Mohanakrishnan, Baldev Raj, Asian Nuclear Prospects 2010,Energy Procedia 7 (2011) 64–73.

[118] Twenty five years of operating experience with the Fast Breeder Test Reactor, K.V. Suresh Kumar, A. Babu, B. Anandapadmanaban & G. Srinivasan, Asian Nuclear Prospects 2010, Energy Procedia 7 (2011) 323–332

[119] Construction, Commissioning and Operation Summary, Reactor Operation and Maintenance Group, FBTR, [online] Available at: http://www.igcar.ernet.in/igc2004/romg/fbtrcons.htm

[120] The Fast Breeder Test Reactor - Design and operating experiences, G. Srinivasan, K.V. Suresh Kumar, B. Rajendran, P.V. Ramalingam, Nuclear Engineering and Design 236 (2006) 796–811

[121] The nesC Language: A Holistic Approach to Networked Embedded Systems, David ,G., Levis,P., Behren,R,V., Welsh,M., Brewer,E., and Culler,D. (2003),In Proceedings of Programming Language Design and Implementation (PLDI) 2003, June 2003.-nesC ref

[122] TinyOS Programming, Philip Levis and David Gay, [online] Available at: http://csl.stanford.edu/~pal/pubs/tos-programming-web.pdf

[123] TinyOS Tutorials, [online] Available at: http://docs.tinyos.net/index.php/TinyOS_Tutorials.

Publications from the Work

Journal Publications

1. Title: Wireless Sensor Network in Fast Breeder Teat Reactor

Authors: **S.A.V. Satya Murty**, Baldev Raj, Krishna M. Sivalingam, S.Sridhar, Jemimah Ebenezer, Kalyan Rao Kuchipudi

Journal: Journal of Nuclear Engineering & technology, Volume 3, Issue 1, ISSN: 2277-6184, Apr 2013

2. Title: Wireless Sensor Network for Sodium Leak Detection

Authors: **S.A.V. Satya Murty**, Baldev Raj, Krishna M. Sivalingam, Jemimah Ebenezer, T Chandran, M Shanmugavel, K.K. Rajan

Journal: International Journal of Nuclear Engineering and Design, Vol 249, PP432-437, Aug 2012.

3. Title: Experimental Deployment of Wireless Sensor Network for Radiation Monitoring

Authors: **S.A.V. Satya Murty**, Baldev Raj, Krishna M. Sivalingam, Jemimah Ebenezer, R. Parthasarathy, D. SaiSubalakshmi,

Journal: Journal of Nuclear Engineering & Technology, Volume 2, Issue 1, ISSN: 2277 – 6184, Apr 2012

Conference Publications

International

1. Title: Real Time Routing Protocols for Wireless Sensor Networks : A Survey
   Authors: Pradeep Chennakesavula, Jemimah Ebenezer, **S.A.V. Satya Murty**

   Conference: Fourth International Conference on Wireless and Mobile Networks (WiMo-2012) at Avinasalingam University, Coimbatore Oct 26-28, 2012.

2. Title: Experimental Analysis of RSSI for Distance and Position Estimation
   Authors: Vinita Daiya, Jemimah Ebenezer, **S.A.V. Satya Murty**, Baldev Raj

   Conference: International Conference on Recent Trends in Information Technology (ICRTIT) at MIT, Chennai, June 2011.

3. Title: Low Latency and Energy Efficient Routing Protocols for Wireless Sensor Networks
   Authors: D. Baghyalakshmi, Jemimah Ebenezer, **S.A.V. Satya Murty**

   Conference: International Conference on Wireless Communication and Sensor Computing [ICWCSC] at SSN College of Engg, Chennai, Jan 2010

4. Title: Low Latency Energy efficient MAC protocols for Wireless Sensor Networks
   Authors: G. Sandhya Rani, Jemimah Ebenezer, **S.A.V. Satya Murty**

   Conference: International Conference on Sensors and Related Networks at VIT University, Vellore, Dec 7-10, 2009

5. Title: Architecture for Real Time Communication in Wireless Sensor Networks
   Authors: D. Baghyalakshmi, Jemimah Ebenezer, **S.A.V. Satya Murty**

Conference: International Conference on Sensors and Related Networks at VIT University, Vellore. Dec 7-10, 2009

6. Invited Talk: Security issues in Wireless Sensors Networks

Speaker: **S.A.V. Satya Murty**

Conference: International Conference on Sensors and Related Networks (SENNET-07) at VIT University, Vellore, Dec 12-14, 2007.

7. Invited Talk: Wireless Sensor Networks: Security Concerns

Speaker: **S.A.V. Satya Murty**

Conference: In pre conference tutorial of International Conference on Sensors and Related Networks (SENNET-07) at VIT University, Vellore, Dec 10-11, 2007.

NATIONAL

1. Invited Talk: Wireless Sensor Networks for Process Monitoring in Power Plants

Speaker: **S.A.V. Satya Murty**

Conference: National Workshop on Sensors for Power Plant process & Equipment by NTPC at Noida, 21st June 2013.

2. Invited Talk: Wireless Sensor Networks in Nuclear Facilities

Speaker: **S.A.V.Satya Murty**

Meeting: BRNS theme Meeting on Electronics and Security at BARC, Mumbai, 27th Feb, 2013

3. Invited Talk: Wireless Sensor Networks: The Emerging Technology

Speaker: **S.A.V. Satya Murty**

Conference: Theme meeting on Novel and Innovative Measurements in Non Destructive Evaluation, Feb 23-24, 2012.

4. Title: Deployment Challenges of Wireless Sensor Network for Nuclear Applications
Authors: Jemimah Ebenezer, D.Baghyalakshmi, G. Sandhya Rani, **S.A.V. Satya Murty**

Conference: Sangoshthi-2012, BHAVINI, Kalpakkam, Dec 21-23, 2012

5. Title: Management Issues of Wireless Sensor Networks
Authors: T.S. Shrikrishnan, Sukant Kothari, Jemimah Ebenezer, K. Kuriakose, **S.A.V. Satya Murty**

Conference: Sangoshthi-2012, BHAVINI, Kalpakkam, Dec 21-23, 2012

6. Title: Study on Effect of Radiation Shield RCB Wall on RF Signal
Authors: Vinita Daiya, Jemimah Ebenezer, K. Kuriakose, **S.A.V. Satya Murty**

Conference: Sangoshthi-2012, BHAVINI, Kalpakkam, Dec 21-23, 2012

7. Title: Design and Development of 802.15.4 based media access control
Authors: Sukant Kothari, Jemimah Ebenezer, K. Kuriakose, **S.A.V. Satya Murty**

Conference: Sangoshthi-2012, BHAVINI, Kalpakkam, Dec 21-23, 2012

8. Title: Test bed based Throughput Analysis in a Wireless Sensor Network
Authors: Anand Kumar, P. Gireesan Namboothiri, Sarang Deshpande, Sreejith Vidhyadharan, Krishna M. Sivalingam, **S.A.V. Satya Murty**

Conference: National Conference on Communications (NCC), Kharagpur, Feb. 2012.

9. Invited Talk: Wireless Sensor Networks and its Applications
Speaker: **S.A.V. Satya Murty**

Meeting: Theme Meeting on Instrumentation for Nuclear Facilities at IGCAR, Kalpakkam, 30th Dec 2008.

Other Publications from the related work

Book Chapters

1. Title: Security Trends and Challenges in Wireless Sensor Networks

Authors: **S.A.V. Satya Murty**, P. Gireesan Namboodri, Krishna M. Sivalingam

Book: Hand Book on Sensor Networks edited by Yang Xiao, Hui Chen, Frank Haizhon Li and published by World Scientific.

2. Title: Networking of Sensors

Authors: **S.A.V. Satya Murty**, A.Sivagami, Jemimah Ebenezer, P. Swaminathan

Book: Science and Technology of Sensors (In Press)

Co- Editor of International Proceedings

1. Co-edited the International Conference Proceedings on “Sensors and Related Networks” held by VIT University, Dec 7-10, 2009.

2. Co-edited the International Conference Proceedings on “Sensors and Related Networks” held by VIT University, Dec 12-14, 2007.