

Master's Thesis 2011

Candidate: Rabin Bilas Pant

Title: Wireless Sensor Networking with Lab-Scale Intermediate Measurement Node for Extension of WSN Coverage

Telemark University College



Faculty of Technology

Kjølnes

3914 Porsgrunn

Norway

Lower Degree Programmes – M.Sc. Programmes – Ph.D. Programmes

TFver. 0.9



Telemark University College

Faculty of Technology

M.Sc. Programme

MASTER'S THESIS, COURSE CODE FMH606

Student: Rabin Bilas Pant

Thesis title: Wireless Sensor Networking with Lab Scale Intermediate Node for Extension of WSN Coverage

Signature:

Number of pages: 68

Keywords: WSN
Router
Coverage
Sensor Node

Supervisor: Saba Mylvaganam sign.:

2nd Supervisor: Hans-Petter Halvorsen sign.:

Censor: sign.:

External partner: Frode Skulbru (NI, Norway) sign.:

Availability: Open

Archive approval (supervisor signature): sign.: **Date :**

Abstract:

Wireless Sensor Networking (WSN) will be a leading solution for data communication for various monitoring and control applications in industries. However, the technology is not widely implemented due to some limitations. Improvement in transmission range, security issues, real time monitoring and control issues, system integration and coexistence are the fields in WSN, which require more investigations.

In this thesis, a comprehensive literature survey was done to understand existing standard of WSN elements; pros and cons of WSN; case studies of different WSN applications and security management. Two designs of WSNs were made using Wireless Fidelity (Wi-Fi) and Zig-bee. Wireless Distribution System (WDS) concept was used in Wi-Fi based design and router mode concept was used in Zig-bee based design. Zig-bee based design was economical but supports the lower sampling rate. Wi-Fi based design was expensive but supports the high sampling rate up to 51.2 K samples per second per channel.

WSN was setup using NI Zig-bee modules. NI WSN-3202 (sensor node) and NI WSN-9791 (Gateway) were connected in star network topology and multi-hop network topology. Using multi-hop topology, indoor transmission range was increased significantly from 23.1 meters to 47.1 meters with link quality more than 55%. Since the maximum sampling rate of Zig-bee modules is 1 sample per second per channel, physical quantity demanding high sampling rate are avoided in lab work. In both topology cases, temperature was measured.

Telemark University College accepts no responsibility for results and conclusions presented in this report.

Table of contents

- 1 INTRODUCTION 10**
 - 1.1 OBJECTIVES 11
 - 1.2 REPORT STRUCTURE 11
- 2 STANDARD SCENARIO OF WSN 12**
 - 2.1 STANDARD TRANSMISSION PROTOCOL..... 13
 - 2.1.1 *Bluetooth* 13
 - 2.1.2 *Zig-bee* 14
 - 2.1.3 *Wi-Fi* 14
 - 2.2 STANDARD NETWORK TOPOLOGY 15
 - 2.2.1 *Peer to Peer Network Topology* 15
 - 2.2.2 *Star Network Topology*..... 16
 - 2.2.3 *Mesh Network Topology*..... 16
 - 2.2.4 *Tree Network Topology*..... 17
- 3 EXTENSION OF WSN COVERAGE 19**
 - 3.1 DESIGNING WSN FOR COVERAGE EXTENSION 19
 - 3.1.1 *Design 1: Using Wi-Fi* 19
 - 3.1.2 *Design 2: Using Zig-bee* 22
 - 3.1.3 *Design Selection for Lab Work* 24
- 4 APPLICATION, ADVANTAGES AND DISADVANTAGES OF WSN..... 25**
 - 4.1 APPLICATIONS 25
 - 4.2 ADVANTAGES 26
 - 4.3 DISADVANTAGES 26
 - 4.4 INDUSTRIAL APPLICATIONS’ ISSUES 27
- 5 CASE STUDY 29**
 - 5.1 CASE STUDY I 29
 - 5.1.1 *Background* 29
 - 5.1.2 *System Architecture* 29
 - 5.2 CASE STUDY II 30
 - 5.2.1 *Background* 30
 - 5.2.2 *Network Architecture* 31
 - 5.2.3 *Data Acquisition Issues* 31
 - 5.3 CASE STUDY III 32
 - 5.3.1 *Background* 32
 - 5.3.2 *Existing Process Management System* 32
 - 5.3.3 *Coupling* 33
 - 5.4 CASE STUDY IV 34
 - 5.4.1 *Background* 34
 - 5.4.2 *Network Architecture* 34
 - 5.4.3 *Comparisons with Terrestrial WSN* 36
- 6 LAB WORK..... 37**

6.1	PHASE I- STAR NETWORK TOPOLOGY	37
6.1.1	<i>Configuration Steps</i>	37
6.1.2	<i>Determining Maximum Distance of Transmission</i>	39
6.1.3	<i>Temperature Sensor Setup</i>	41
6.1.4	<i>LabVIEW Code</i>	42
6.1.5	<i>Front Panel and Data Interpretation</i>	43
6.2	PHASE II- MULTI-HOP NETWORK TOPOLOGY	45
6.2.1	<i>Determining Operation of Mesh Router Mode</i>	46
6.2.2	<i>LabVIEW Programming and Data Interpretation</i>	48
7	WSN IMPLEMENTAION ISSUES	51
7.1	DEPLOYMENT	51
7.2	MOBILITY	51
7.3	COST, SIZE AND ENERGY	51
7.4	COMMUNICATION MODALITY	52
7.5	INFRASTRUCTURE.....	52
7.6	NETWORK TOPOLOGY AND COVERAGE.....	52
7.7	NETWORK SIZE.....	52
7.8	LIFE TIME.....	52
7.9	SAMPLING RATE.....	53
7.10	SECURITY	53
7.10.1	<i>Security Management</i>	53
7.10.2	<i>Security Management Requirements</i>	54
7.10.3	<i>Protocol Stacks, Security Threats and Prevention</i>	55
8	DISCUSSION	58
8.1	PROTOCOL AND TOPOLOGY	58
8.2	DESIGN 1 VS. DESIGN 2	58
8.3	TRANSMISSION DISTANCE	59
8.4	SECURITY	59
9	CONCLUSION AND FUTURE WORK	60
9.1	CONCLUSION.....	60
9.2	FUTURE WORK.....	60
10	REFERENCES	62
11	APPENDICES	66

Overview of tables and figures

- Table 2.1:Bluetooth Specifications[8]..... 14
- Table 2.2: Zig-bee specification..... 14
- Table 2.3: Wi-Fi specifications 15
- Table 3.1: Cost estimation of WSN using NI Wi-Fi Modules 21
- Table 3.2: Cost estimation of WSN using NI Zig-bee Modules 24
- Table 4.1: Advantages and Disadvantages of WSN 27
- Table 4.2: Source for Interference [22] 27
- Table 6.1: Elements used in LabVIEW code and their functions 43

- Figure 2.1: Detail structure of WSN [5]..... 12
- Figure 2.2: Peer to Peer Network Topology 15
- Figure 2.3: Star Network Topology 16
- Figure 2.4: Mesh Network Topology 16
- Figure 2.5: Mesh network using 8 sensor nodes 17
- Figure 2.6: Mesh network illustrating redundant feature after its node 4 fails 17
- Figure 2.7: Tree Network Topology 18
- Figure 3.1: NI devices used for design 1 20
- Figure 3.2: Radiation pattern of single WAP-3711 using omnidirectional antenna 20
- Figure 3.3: Connection diagram of Wi-Fi WSN using WDS system 21
- Figure 3.4: NI devices used for design 2..... 22
- Figure 3.5: Radiation pattern of single WSN-9791 using omnidirectional antenna 23
- Figure 3.6: Connection diagram of Zig-bee WSN using sensor node as router..... 23
- Figure 5.1: WSN based architecture for closed loop industrial plant energy evaluation and planning system [26] 30
- Figure 5.2: Sensor node layout on Golden Gate Bridge [31]..... 31
- Figure 5.3: Existing process management system and Wireless HART based process management system [34]..... 33
- Figure 5.4: Engineers busy on random installation of wireless HART in Yara, Porsgrunn 33
- Figure 5.5: Possible approach to underwater WSN node deployment [36] 35
- Figure 5.6: Two dimensional hierarchal topology using cluster concept 35
- Figure 6.1: Full configuration in a star network topology 37
- Figure 6.2: MAX window showing status of both sensor nodes detected by gateway..... 38

Figure 6.3: LabVIEW Project window showing both sensor nodes and its associated I/O variables	39
Figure 6.4: Time vs. Link quality graph to determine maximum distance of transmission.....	40
Figure 6.5: Top view of College to show where the sensor nodes and gateway were installed	40
Figure 6.6: Connection diagram of PT-100 elements, Transmitter and NI WSN 3202.....	41
Figure 6.7: Graph showing linear scaling to convert voltage to corresponding temperature ..	41
Figure 6.8: Block diagram of LabVIEW program used to measure temperature from 2 sensor nodes.....	42
Figure 6.9: Front panel consisting Temp & Link Qual. tab for both sensors.....	44
Figure 6.10: Front panel consisting Statistics tab for both sensors	44
Figure 6.11: Full configuration in a multi-hop network topology	46
Figure 6.12: MAX window showing Network Mode for both sensor nodes, where one sensor node is updated as Mesh Router.....	46
Figure 6.13: Top view of College to show where the sensor nodes and gateway were installed; and new path followed by end node after resetting.....	47
Figure 6.14: Time vs. Link quality graph to observe improvement in link quality after end node has been reset.....	47
Figure 6.15: MAX window showing Excellent link quality after the end node was reset.....	48
Figure 6.16: Top view of College to show where the sensor nodes and gateway were installed; and their separation distance	48
Figure 6.17: Block diagram of LabVIEW program used to measure temperature from end node	49
Figure 6.18 : Front panel consisting temperature statistics for end node and link quality statistics for both end node and router node.....	49
Figure 7.1: WSN Architecture with security components [43].....	54
Figure 7.2: Sensor node protocol stack [46]	55

Preface

This thesis is prepared as an obligatory requirement to be graduated as master in System and Control Engineering at the Telemark University College. The entire work was carried out in Sensor Lab, Flow Lab and Process Hall. The necessary technical information and equipment were provided by technical department of College. The main focus was given to understand the current standard scenario of WSN; its advantages and disadvantages; and security issues. Lab work was carried out to understand how intermediate sensor node configured as router node can help to extend the WSN coverage.

I would like to express my deep sense of gratitude to my supervisors Prof. Saba Mylvaganam and Assoc. Prof. Hans-Petter Halvorsen. I would also like to acknowledge invaluable support from National Instrument employees Frode Skulbru and Tom-Arne Danielsen. Special thank goes to employee from Yara nitric acid plant, Porsgrunn for organizing effective field visit of their WSN systems.

I would like to thank Telemark University College, Porsgrunn, Norway and National Instrument, Norway for giving me opportunity to work in this very interesting and relevant topic. It has been a great experience working on practical based project which has taken me to the new level of understanding the concept of WSN.

Finally, I would like to thank everybody who has supported me directly and indirectly.

Telemark University College, Porsgrunn, June 3,2011

Rabin Bilas Pant

Nomenclature

Abbreviations

AC	Alternative Current
AES	Advanced Encryption System
AP	Access Point
BAN	Body Area Network
BPSK	Binary Phase Shift Keying
CSS	Central Supervisory Stations
DAQ	Data Acquisition
DO	Dissolved Oxygen
DPSK	Differential Phase Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
ESF	European Science Foundation
GFSK	Gaussian Frequency Shift Keying
GSM	Global System for Mobile
IEEE	Institute of Electrical and Electronics Engineering
ISM	Industrial, Scientific and Medicine
ISO	International Organization for Standardization
ITS	Intelligent Transportation System
LOS	Line of Sight
MAX	Measurement and Automation eXplorer
MCC	Motor Control Centers
MEMS	Micro-Electro Mechanical system Sensors
NI	National Instruments
NPI	Name Plate Info
OQPSK	Offset Quadrature Phase Shift Keying
OSI	Open System Interconnection
pH	Potential of Hydrogen
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
SIG	Special Interest Group
TKIP	Temporal Key Integrity Protocol
VAC	Voltage Alternative Current
VDC	Voltage Direct Current
WAP	Wireless Access Point
WDS	Wireless Distribution System
Wi-Fi	Wireless Fidelity
WLS	WireLess Sensor
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WSN	Wireless Sensor Network

Letters and expressions

°C	Degree Centigrade
dBm	deciBels Milliwatt
hp	horse power
Is	Current
Kbps	Kilobits per second
Mbps	Megabits per second
MHz	Mega Hertz
mW	milli Watt
Rs	Resistance
Vs	Voltage
μG	micro Gravity

1 Introduction

A Radio Frequency (RF) network, which consists of transceivers, sensors, machine controllers, microcontrollers and user interface devices is called Wireless Sensor Network (WSN). Sensors are spatially distributed entities those cooperatively monitor physical or environmental conditions such as vibration, pressure, motion, temperature, etc. WSN consists of at least two nodes communicating each other through RF- medium. However, the numbers of nodes can be more than two, which depends upon the measurement strategies and environment.

WSN has attracted the attention of both the academic and industrial research companies from late 90's. Some famous smart sensors prototype like Berkeley motes and Smart Dust has been designed and implemented in such areas [1]. Smart sensors nodes are also commercialized by Crossbow, Philips, Siemens and National Instruments.

Since, there are lots of companies involved in designing and developing sensor nodes, a considerable amount of standardization is required in WSN field. For example, National Instrument (NI) WLS-9163 nodes are standardized with Institute of Electrical and Electronics Engineering (IEEE) 802.11 protocols [2] and NI WSN-3202 is standardized with IEEE 802.15.4 protocols [3] as a transmission medium.

WSN has been applied successfully in industries, health and environment sectors. It possesses some merits and demerits. Two of the major disadvantages are security and coverage area or transmission distance. Since, RF medium is used; the attackers can easily attack the physical medium and can extract valuable and sensitive information. Secured network is the need for today's applications. These days, many security measures are practiced so as to provide a hacker free network.

There are lots of implementation issues like deployment, mobility, topology, coverage area, life time, sampling rate, cost, energy, etc. WSN can be called perfect only when all the above mentioned implementation issues are addressed. Before designing any WSN, pre-study is required to understand its measurement type, its area of coverage, mobility requirement and budget. Then only design factors like topology, deployment, lifetime, sampling rate and transmission protocol are studied and investigated.

In some of the applications of WSN like underwater monitoring, bridge structural monitoring, etc., high transmission range is required in order to establish a link between measuring point to monitoring point. In most WSN, Industrial, Scientific and Medicine (ISM) band frequency is used. One of the limitations of ISM band is that output power of antenna cannot be more than 20 dBm [4] that means coverage area is limited. WSN using National Instrument Zig-bee devices can provide the highest range of 300 meters in America and 150 meters in Europe [3] at the cost of less sample rate as compared to Wireless Fidelity (Wi-Fi) devices.

Coverage area can be increased by using router node. Router node in WSN is a special type of measurement node, which acts as repeaters. These nodes are kept between end node and

gateway such that end measurement node first communicates with router node and then gateway. This is a case of multi-hop network. Multi-hop network can be changed to mesh network using more router nodes. Mesh network can provide redundancy to network. Another way for coverage extension is the use of multiple Access Point (AP) to create Wireless Distribution System (WDS). In WDS system, each AP can communicate with adjacent APs and its associated sensor nodes.

1.1 Objectives

The main objective of this thesis is to design and implement WSN in order to increase the transmission range by using intermediate router nodes that can communicate with sensor node and gateway. In order to achieve this, following sub-objectives are considered.

- a) Study of current standard scenario of WSN in terms of network topology and transmission protocol.
- b) Different applications, pros and cons of WSN. Deployment challenges of WSN in an industrial environment.
- c) Four case studies for different applications of WSN.
- d) Implementation issues of WSN, security threats and management.
- e) Lab work to verify improvement of transmission distance.
- f) Finally, documentations of lab result and theory.

The task description is given in Appendix 1.

1.2 Report structure

This report consists of nine chapters. Chapter one will give general introduction of WSN and objectives of a thesis. Chapter two will discuss about existing standard scenario of WSN in terms of transmission protocol and network topology. Chapter three will discuss about Wi-Fi and Zig-bee based design for coverage extension. Applications, advantages and disadvantages of WSN will be discussed in chapter four. Four case studies for different application of WSN will be presented and discussed in chapter five. Chapter six will present detail of lab work carried out in two phases. The phase I will deal with star network topology, and the phase II will deals with coverage extension using router mode sensor node. Chapter seven will discuss some WSN implementation issues, where security issues will be discussed more deeply. Discussion of lab work and major associated theories will be discussed in chapter eight. Chapter nine will point out the conclusion of a thesis along with its perspectives to elaborate it in the future.

2 Standard Scenario of WSN

The diversity in application areas and the specific properties of WSN demands some sort of regularization from sensing point to end users. These can be defined in terms of network topology, bandwidth offered, transmission protocols and sensor's compatibility. Following article deals with the current standard scenario of WSN and its essential technical details for transmission protocols and network topology.

Figure 2.1 is considered for a detailed structure of WSN. This figure is distinctly categorized into two sections, Classical Infrastructure and Sensor Networks.

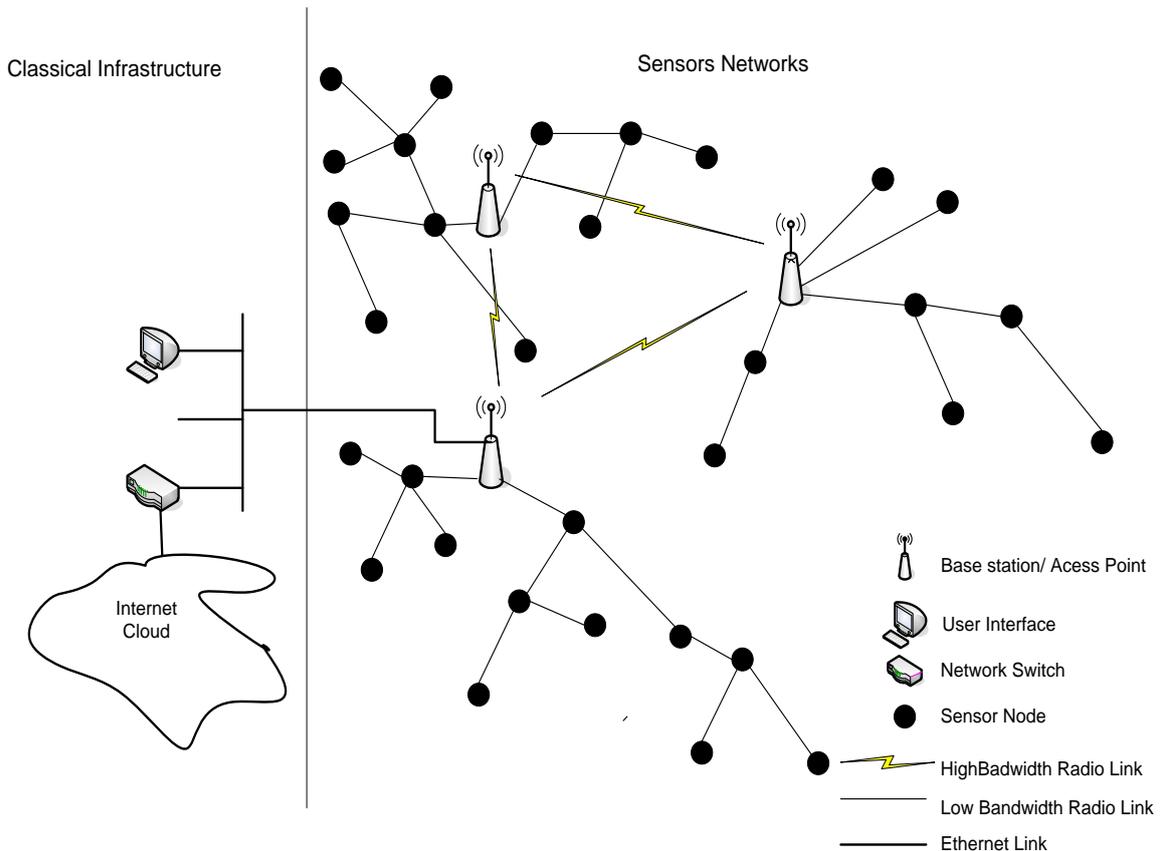


Figure 2.1: Detail structure of WSN [5]

Classical Infrastructure is the existing network structure which may or may not be connected to the internet. Simple private network of organizations or industries used for local communication and data exchange can be considered as classical structure. Sensor networks as defined earlier are spatially distributed autonomous sensors which are connected to each other forming a network topology (ad-hoc, Star, Mesh, etc.). The groups of sensors are connected to AP, which ultimately connect sensors to end users via some sort of display units or computers. End user can monitor and control the process if required. There are three APs interconnected to each other in *Figure 2.1*. Each AP is responsible for traffic and management flow for their group of sensors. One AP is connected to end user via classical infrastructure. Such that information from all nodes can be accessed by end-users.

Number of sensor nodes and AP differs as per user's interest of measurement, environment and coverage area. Deploying mesh topology one should be very careful to know the supportability of multi-hop structure (node talking to adjacent node) by selected devices. For example, NI-WSN 3202 and Wireless HART support internode communication whereas nodes like NI-WLS 9163 can be configured only in star topology.

Advantages of multi-hop network topology are, it helps to increase the distance of communication and adds redundancy feature. It is also true that use of multiple AP can also increase distance in star network topology.

2.1 Standard Transmission Protocol

The scalar data such as temperature, humidity, pressure, vibration have low sampling rate. Vibration data have relatively high sampling rate compared to others. However, they are considered to be less as compared to video and picture data. WSNs mainly deal with such data having less scan rate (sampling rate). The advantage of low scan rate data is that WSN can be designed based on low power and low bandwidth transmission protocols. It gives clear concept of why ISM band is deployed in WSN as transmission protocol. ISM band is license free 2.4 GHz band used by Wi-Fi, Zig-bee, Bluetooth and Wireless HART.

2.1.1 Bluetooth

Bluetooth is a low powered, low cost and short-range protocol governed by IEEE 802.15.1 standard. Bluetooth is promoted by Bluetooth Special Interest Group (SIG) [6]. There are 5 different versions of Bluetooth namely, V 1.0/b, V1.1, V1.2, V2.0 and V 3.0. First three versions use Gaussian Frequency Shift Keying (GFSK) as a modulation scheme and fourth version uses GFSK, $\pi/4$ Differential Quadrature Phase Shift Keying (DQPSK) and 8 Differential Phase Shift Keying (8DPSK) as modulation scheme. The maximum data rate supported by V 1.0/b, V1.1, V1.2 is 1 Mbps. V2.0 supports up to 3 Mbps and latest version V3.0 supports up to 24 Mbps. Maximum transmission range of Bluetooth is 100m. Technical overview of Bluetooth in terms of raw data rate, version and modulations scheme is included in *Table 2.1*.

Bluetooth has low latency, high throughput operation with minimum channel hopping period of 600 microseconds [7]. Since it has very less channel hopping period, all nodes should be synchronized very fast, this adds complication in some WSNs where nodes send data very slowly. Bluetooth based WSN takes 2.4 seconds for connection establishment that is its disadvantages.

Table 2.1:Bluetooth Specifications[8]

Version	V 1.0/b	V 1.1	V 1.2	V 2.0
Modulation	GFSK	GFSK	GFSK	GFSK $\pi/4$ DQPSK 8DPSK
Raw rate	1 Mbps	1 Mbps	1 Mbps	1 Mbps 2 Mbps 3Mbps
Expires	17.01.2007	09.08.2007

2.1.2 Zig-bee

Zig-bee is based on IEEE 802.15.4 standard which provides ultra-low complexity, low cost and extremely low-power wireless connectivity for inexpensive and portable device [9].

Zig-bee uses 868 MHz in Europe, 915 MHz in USA and Australia and 2.4 MHz in other parts of world. The data rate ranges from 20 Kbps to 250 Kbps, modulation scheme is either Binary Phase Shift Keying (BPSK) or Offset Quadrature Phase Shift Keying (OQPSK). Zig-bee consumes less power than Bluetooth and Wi-Fi. Technical specifications of Zig-bee are given in Table 2.2.

Table 2.2: Zig-bee specification

Band (MHz)	Frequency (MHz)	Bit Rate (Kbps)	Symbol Rate (Ksymbol/S)	Modulation
868	868-868.6	20	20	BPSK
915	902-928	40	40	BPSK
2400	2400-2835	250	62.5	O-QPSK

2.1.3 Wi-Fi

Wi-Fi is based on IEEE 802.11 protocols, which works on ISM bands of 2.4 GHz and 5 MHz [10]. These are more secured and high bandwidth transmission techniques. The bandwidth and range of transmission depends upon the types IEEE 802.11 that are used by Wi-Fi devices. Five types IEEE 802.11 standard are 802.11, 802.11a, 802.11b, 802.11g, 802.11n. Their ranges vary from 30m to 125m and data rate varies from 2 Mbps to 54 Mbps. The

newest technology; 802.11n supposed to have data rate up to 100 Mbps to 200 Mbps [11]. Modulation scheme, frequency band, range and data rate are given in *Table 2.3*.

Table 2.3: Wi-Fi specifications

Types	Range (meter)	Bit Rate (Mbps)	Modulation	Band (GHz)
IEEE 802.11	30	1 or 2	FHSS,DSSS	2.4
IEEE 802.11.a	30	54	OFDM	5
IEEE 802.11.b	30	11	DSSS	2.4
IEEE 802.11.g	30	20 to 54	OFDM/DSSS	2.4
IEEE 802.11.n	125	100 to 200	OFDM	2.4

2.2 Standard Network Topology

Network topology defines the arrangement and connection of computers or nodes with each other. WSN network topology describes how sensor nodes are connected to other sensor nodes or hubs or base stations. Computer topologies include Star, Ring, Fully Connected, Bus, Tree and Mesh [12]. This chapter focuses mainly on following four standard WSN data network topologies.

- a) Peer to peer Network Topology
- b) Star Network (single point to multipoint) Topology
- c) Mesh Network Topology
- d) Tree Network Topology

2.2.1 Peer to Peer Network Topology

In this type of topology each nodes can communicate directly with another node without usage of any centralized infrastructure or hub. *Figure 2.2* shows how three sensor nodes are connected on peer to peer network topology.

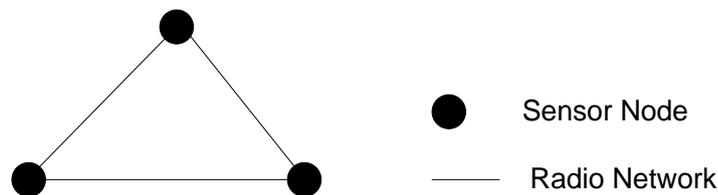


Figure 2.2: Peer to Peer Network Topology

2.2.2 Star Network Topology

Star network topology is a technology in which numbers of remote nodes can send or receive data to single base station. Unlike peer to peer network, nodes are not permitted to send and receive message to and from each other. Routing algorithm for this topology is simpler than other topologies. There are some disadvantages also; first, remote nodes must be in radio range of base station. Second, due to dependability of all remote nodes on a single base station, redundancy and robust structure are hard to achieve. Base station is core part of this network as it is responsible for message handling, routing and decision making. *Figure 2.3* shows how 5 sensor nodes are connected to single base station in star network topology.

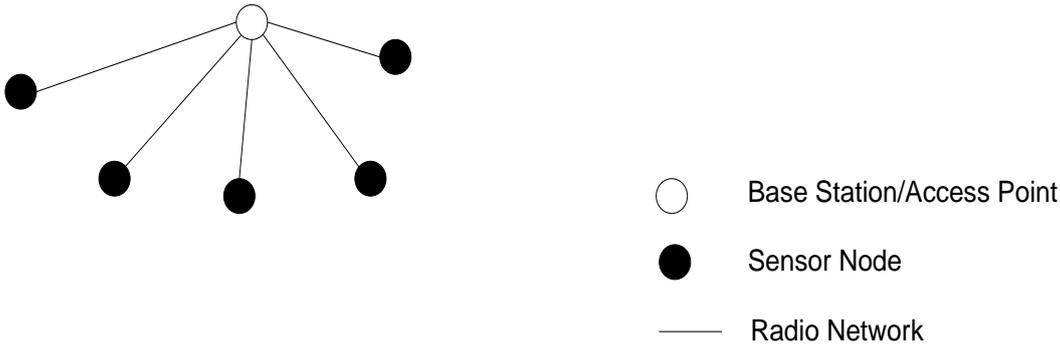


Figure 2.3: Star Network Topology

2.2.3 Mesh Network Topology

Mesh networks are distributed networks, which allow any node in the network to talk to any other nodes in the same network within its coverage area. Mesh network can be suitable for large scale distributed network of sensors over geographic region like personal or vehicle security surveillance systems [12].

Mesh network topology has the advantages of fault tolerance and load balancing; and disadvantages of scalability [13]. For an instance, if an individual node fails, a remote node still can forward message to desired node by communicating to any other nodes in its transmission range. Typical example of mesh network topology is given in *Figure 2.4*.

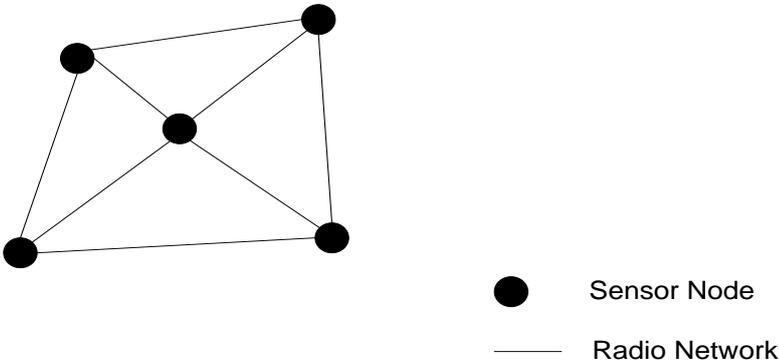


Figure 2.4: Mesh Network Topology

In order to illustrate redundancy feature in mesh network topology, *Figure 2.5* is considered. It consists of eight sensor nodes, each connected on multi-hop structure.

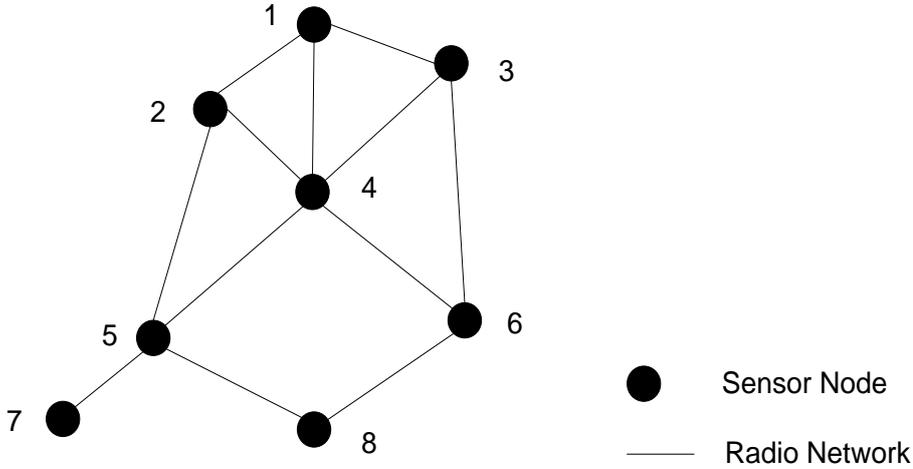


Figure 2.5: Mesh network using 8 sensor nodes

If measurement taken by node 8 has to be transferred to node 1, it can take either of following paths: path 8-5-2-1 or path 8-5-4-1 or path 8-5-4-3-1 or path 8-6-4-2-1 or path 8-6-4-1 or path 8-6-4-3-1 or path 8-6-3-1. For an instance, assume that current path used to flow signal from node 8 to node 1 is path 8-5-4-3-1, all of sudden node 4 fails to work. Then mesh network automatically switch path 8-6-3-1 or path 8-5-2-1 giving redundant features. This is illustrated in *Figure 2.6* from the figure it can see that node 4 is failed and its corresponding paths are broken.

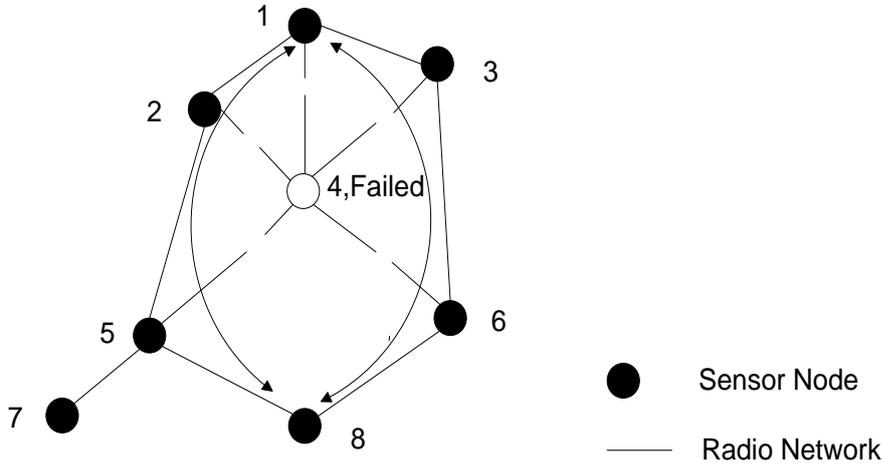


Figure 2.6: Mesh network illustrating redundant feature after its node 4 fails

2.2.4 Tree Network Topology

The hybrid combination of peer to peer network and star network topologies is a tree network topology. Tree network topology consists of root node and central hub. Central hub is responsible for communicating with sensor nodes connected to them and root node is

responsible for merging and managing central hub in a common central point. Simple example of tree network topology is given in *Figure 2.7*.

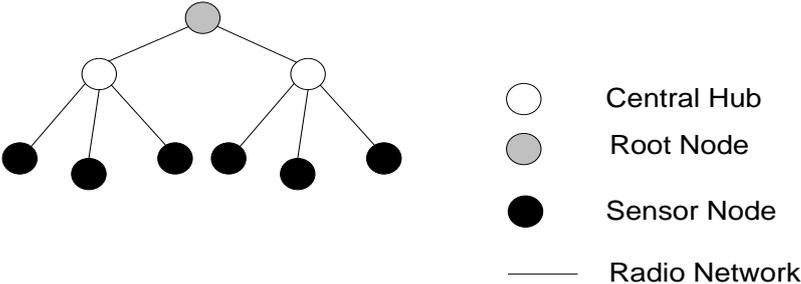


Figure 2.7: Tree Network Topology

3 Extension of WSN coverage

The range between source (sensor node) and sink (monitoring node) depends upon transmission protocol used. Zig-bee protocol offers highest transmission range at the cost of lower sampling rate. Zig-bee devices have coverage up to 300 meters. Wi-Fi devices have coverage up to 30 meters (802.11.n is newest technology with 125 meters range).

One way to increase range is to use high power directional antennas. However, different countries' policies to limit the maximum output power in ISM bands restrict the use of high power directional antennas. Maximum output power limitation in USA is 50mW. Thus the maximum range supported by Zig-bee is 300 meters. For Europe and Asia, maximum output limitation is 10mW and the corresponding maximum range supported is 150 meters [14].

Another way to increase the range is to place infrastructure in between source and sink nodes. This infrastructure acts as a repeater. Basically, AP can be used as an intermediate infrastructure in Wi-Fi based WSN whereas router can be used in Zig-bee based WSN. These two methods are studied and technical overview is presented in the following sub chapters.

3.1 Designing WSN for Coverage Extension

In order to design the extension of WSN coverage, task is defined at first. The task is to measure any physical quantity, which is placed more than 300 meters far from monitoring station.

The overall concept of these designs will be to study all the technical constraints and budget requirements. Comparisons between the designs will be made and one design will be chosen for lab work.

3.1.1 Design 1: Using Wi-Fi

This design is based on the concept of WDS. WDS is a system where new AP is placed between existing sensor node and AP. By doing this, the overall range of the system is increased approximately by twice. More APs can be used to create more WDS such that each intermediate AP acts as repeater. Many Wi-Fi vendors are using IEEE 802.11a/b/g multimode AP. IEEE 802.11 b/g mode is mainly used to connect sink AP with computer or monitoring station. IEEE 802.11 a mode is mainly used to connect two APs in order to form WDS [15]. In this case, for both purposes, the device supporting IEEE 802.11 b/g multimode will be used.

3.1.1.1 Technical Specification of Device Used

Proposed devices for design using Wi-Fi are from National Instruments. NI WLS-9163 C-series carrier along with NI WLS-9234 I/O module is used as sensor nodes. This device supports 4 input channels with 24 bit resolution and maximum sampling rate of 51.2 K

samples per second per channel. It requires 220 Volt Alternative Current (VAC) power supply [16]. NI WAP-3701/3711 is used as access point which can support Wi-Fi b/g standard. The range of transmission is 30 meters and uses 24 Volt Direct Current (VDC) external power supply [17]. *Figure 3.1* shows the NI devices used for design 1.



Figure 3.1: NI devices used for design 1

3.1.1.2 Proposed Network Architecture

When single WAP-3711 is configured, it can communicate with sensor nodes WLS-9163 up to 30 meters range. Omnidirectional antenna is used in such device; therefore, radiation pattern will be circle of 60 meters diameter approximately. *Figure 3.2* shows the radiation pattern of single WAP-3711 using omnidirectional antenna.

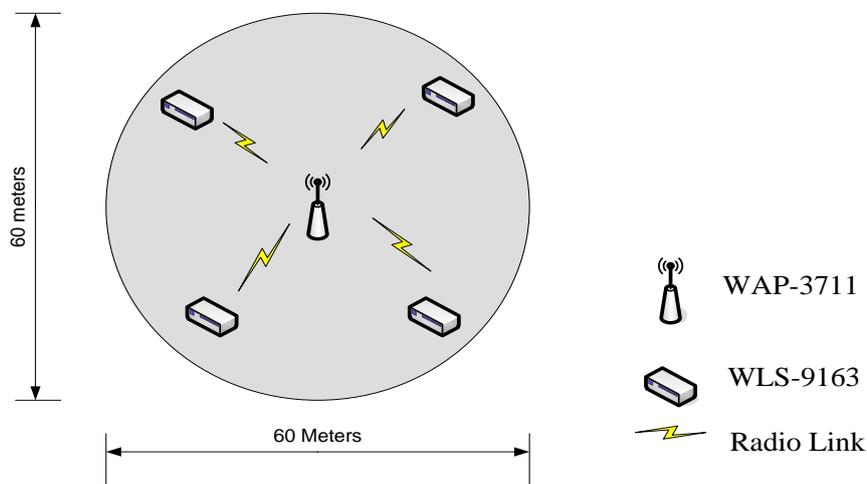


Figure 3.2: Radiation pattern of single WAP-3711 using omnidirectional antenna

Advantage of omnidirectional antenna and WDS system are combined together to extend the coverage. Maximum numbers of WDS that can be used are 6 [18]. Each WDS has overlapping distance of 5 meters; such that first WAP-3711 has range of 55 meters and second, third, fourth, fifth have range of 50 meters. The last WAP-3711 has range of 25 meters. Last WAP-3711 has 25 meters range as only one side can be used. This last WAP-3711 is connected to the computer. *Figure 3.3* shows the overall connection diagram.

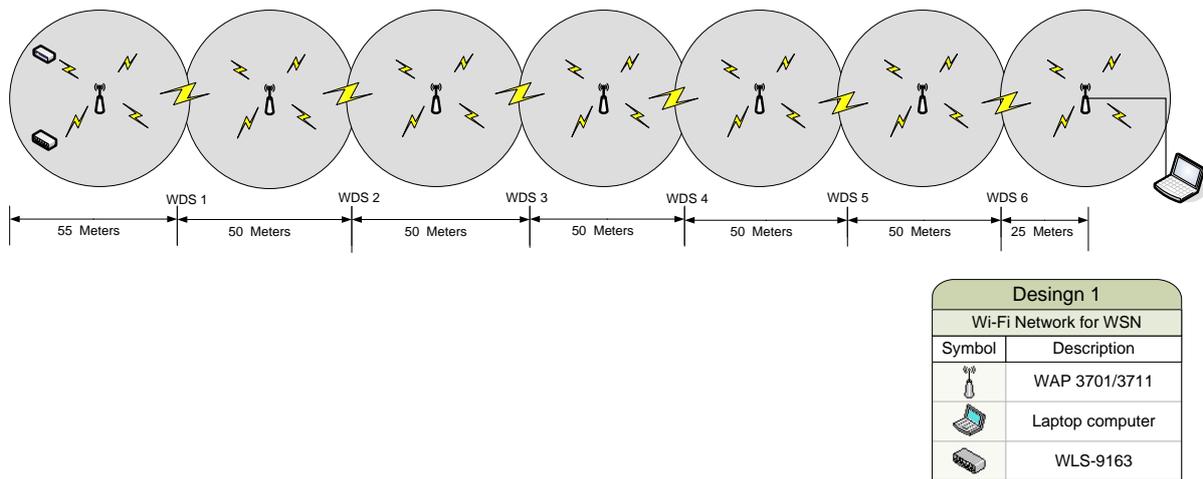


Figure 3.3: Connection diagram of Wi-Fi WSN using WDS system

First WAP-3711 is used to communicate with sensor node WLS-9163 and all other WAP-3711s are used as repeaters. The overall distance of measurement is not more than 330 meters in Line of Sight (LOS).

3.1.1.3 Cost Estimation

Device implemented in first design, their individual cost and grand total after VAT and discount is given in the Table 3.1.

Table 3.1: Cost estimation of WSN using NI Wi-Fi Modules

Cost Estimation for Design 1: Wi-Fi Network using NI devices			
Devices	Price per unit(NOK)	Unit requirement	Total price (NOK)
NI WLS-9163 IEEE 802.11b/g Carrier for C Series Modules	3699,00	2	7398,00
NI WLS-9234	12999,00	2	25998,00
NI PS-15 Power Supply, 24 VDC, 5 A, 100-120/200-240 VAC Input	1699,00	7	11893,00
NI WAP 3711/3701	6999,00	7	48993,00
Other Accesories	1000,00	1	1000,00
VAT			23820,00
Grand total			119102,00

Total cost for Wi-Fi based design is approximately 119102, 00 NOK. This cost has been calculated with the reference to price list provided by National Instruments, which is given in Appendix 2.

3.1.2 Design 2: Using Zig-bee

In this design, concept of intermediating AP used as repeater is avoided; instead, intermediate sensor node is configured as a router. One more sensor node is placed in between the existing sensor node and gateway. Such that overall coverage will be sum of both. This design is based on the concept of multi-hop network. Measuring sensor node transfers data to the intermediate sensor node, which is responsible to update and boost the signal and transfer it to nearby gateway. For this design, Zig-bee (IEEE 802.15.4) protocol and its features are used. The advantage of using Zig-bee is its high coverage range than that of W-Fi. As a result, cost effective network using minimum devices can be designed.

3.1.2.1 Technical Specification of Device Used in Design

Proposed devices for design using Zig-bee are from National Instruments. NI WSN-3202 is used as measurement node and router node. This device supports 4 analog input channels with 16 bit resolution and maximum sampling rate of 1 sample per second per channel. It requires 30V DC power supply when configured as router and standard battery when configured as measurement node. NI WSN-3202 is also facilitated with 4 digital input/output channels [3]. NI WSN-9791 gateway is used as a sink node, where we can connect our measurement station. It uses 9 to 30V DC external power supply. Communication range is 300 meters in USA and 150 meters in Europe. It can support 8 end nodes in star topology and 36 end nodes in Mesh topology [14]. *Figure 3.4* shows NI devices used for design 2.



Figure 3.4: NI devices used for design 2

3.1.2.2 Proposed Network Architecture

When a single WSN-9791 is configured, it can communicate with sensor nodes configured as measurement nodes or router nodes. Maximum communication distance is up to 150 meters. Because of omnidirectional antenna used in such device, radiation pattern will be a circle of 300 meters diameter approximately. *Figure 3.5* shows the radiation pattern of single WSN-9791 using omnidirectional antenna.

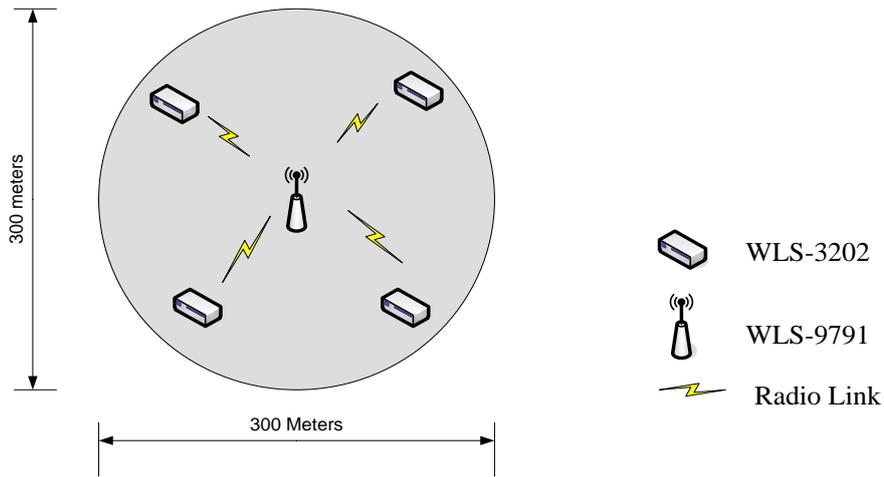


Figure 3.5: Radiation pattern of single WSN-9791 using omnidirectional antenna

Advantage of omnidirectional antenna and property of sensor nodes that can be configured as router nodes are used together to extend the coverage. For extending distance up to 300 meters, two sensor nodes are sufficient. One sensor node is configured as router and other is configured as measurement node. Overlapping distance of 5 meters between router node and gateway is maintained such that WSN-3202 router node has range of 295 meters and WSN-9791 has range of 145 meters. WSN-9791 gateway has 145 meters of range because only one side of its coverage area can be used. Monitoring station or computer is connected to gateway. Figure 3.6 shows the overall connection diagram. The overall distance of measurement is not more than 450 meters in LOS.

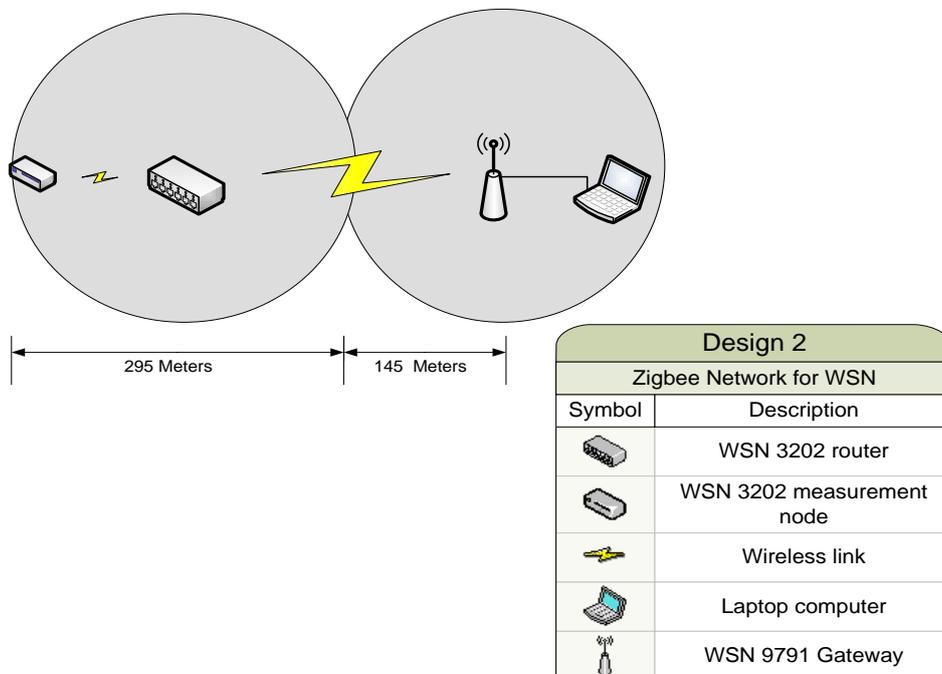


Figure 3.6: Connection diagram of Zig-bee WSN using sensor node as router

3.1.2.3 Cost Estimation

Device going to be implement in second design, their individual cost and grand total after VAT and discount is given in the *Table 3.2*.

Table 3.2: Cost estimation of WSN using NI Zig-bee Modules

Cost Estimation for Design2: Zigbee Network using NI devices			
Devices	Price per unit(NOK)	Unit requirement	Total price (NOK)
NI WSN 3202	2789,00	2	5578,00
NI WSN 9791 gateway	5669,00	1	5669,00
NI PS-15 Power Supply 5 A, 24 VDC	1529,00	2	3058,00
Sum			14305,00
VAT			3826
Grand Total			18131,00

Total cost for design based on Zig-bee is approximately 18131, 00 NOK. This cost has been calculated with the reference to price list provided by National Instruments which is included in Appendix 2.

3.1.3 Design Selection for Lab Work

Cost for Design 2 is very less as compared to Design 1. Design 2 is best suited in the context where low sample data rate are required to be measured. Design 2 can be easily modified to mesh network topology but this is not possible in Design 1. Apart from these, Design 2 consists of less number of devices giving advantages of less installation time, less labor, reduced complexity, etc. Due to these reasons, Design 2 seems to be best option for a lab work.

4 Application, Advantages and Disadvantages of WSN

WSN has various applications in home, industries, health sector and environmental monitoring. There are also some merits and demerits of WSN. Since radio medium is used for the transmission of data, WSN comprises all the advantages and disadvantages of wireless communications.

4.1 Applications

Major applications of WSN are described below.

- a) Home, buildings and traffic security application: Home and building surveillance for intrusion, fire detection can be done easily using WSN. Moreover, WSN can be used in traffic surveillance technologies. Data are updated constantly to provide historical and real time data of traffic count, speed, classification and re-identification. These data are then sent to Intelligent Transportation System (ITS) for the further processing [19].
- b) Automobile application: In modern automobiles, large number of sensors is installed for monitoring machineries' conditions and health. Large number of cables is used to interconnect these sensors with main cabinet. These cables are replaced by using WSN technology. By using WSN, designer can reduce volume and weight of automobiles.
- c) Industrial application: WSN is used in industries to monitor temperature, level, and pressure of ovens, pipes or tanks. Furthermore, health conditions of machineries can also be monitored. For control purposes, WSN is integrated with process management units.
- d) Health monitoring application: WSN is used as Body Area Network (BAN) [20]. BAN consists of several sensors placed in different parts of human body. These sensors measure heartbeat, blood pressure, neural activities, etc. WSN can be combined with Global System for Mobile (GSM) or internet for telemedicine purposes.
- e) Structural monitoring application: WSN is used to detect the damage in buildings, stadium, tower, bridge, ships, aircrafts and vehicles. This is done by monitoring the response to ambient or force excitation created on the structure.

- f) Military application: Deploying WSN in battlefield provides the awareness of situation in the field. This helps operational forces to make valuable decision. Aircraft is used to scatter micro-sensor nodes randomly in the battle field and intelligence information are received in base camp.

4.2 Advantages

WSN has wide range of operational environment. It provides advantages in cost, size, power, flexibility and intelligence compared to wired sensor networks. Some advantages of WSN are described below.

- a) It avoids lots of wiring and risk of cutting the bus connecting sensors that persists in field bus or other wired technologies.
- b) WSN uses Micro-Electro Mechanical Systems Sensors (MEMS). MEMS technology has low cost, small size, and low power requirements [21].
- c) In situations, where cabling is very difficult, dangerous and impossible; WSN can be used to avoid cable installations.
- d) Relocation and restructuring of wireless network is easier than that of wired network.
- e) Radio signals can easily penetrate the buildings and walls. It avoids the need of drilling and making hole during wire installation.

4.3 Disadvantages

Some disadvantages of WSN are given below.

- a) WSN provides low speed of communications as compared to wired sensor network.
- b) In some cases, hackers can hack the information if proper security policies are not implemented on the networks.
- c) Most of WSN uses ISM band and vendors for multiple applications also use the same spectrum. In such case, there exists problem of co-existence due to interference.
- d) Some sensor nodes are required to be installed in the remote places and unattended for number of years. These nodes are powered by battery. So there may be power problem after some years of deployment.

- e) WSN are relatively more complex to configure than that of wired system and there is always problem of bandwidth for special measurement cases.

Abovementioned advantages and disadvantages of WSN are summarized and presented in *Table 4.1*.

Table 4.1: Advantages and Disadvantages of WSN

Advantages	Disadvantages
Avoids wires	Low speed compared to wired network
Low cost, small size and less power consumption	Security issues, less transmission range
Easy installation compare to wired network	Coexistence problem
Relocation and restructuring is easy	Battery drained after long use
Avoids drilling in walls	Bandwidth problem

4.4 Industrial Applications' Issues

WSN operating in industrial applications may suffer from co-channel interference, adjacent channel interference, multipath propagation, reflection, scattering and diffractions. There are potential chances to degrade reliability of data by noise generated by heavy equipment, by multipath propagation [22] and by interference by other devices using ISM bands [23]. There are two types of interference, broadband interference and narrowband interference. *Table 4.2* summarizes all possible interference sources that can exist in industrial environments.

Table 4.2: Source for Interference [22]

Broadband interference	Narrowband Interference
Motors	Cellular telephone
Inverters, Silicon-Control Rectifier (SCR) circuits	Radio and TV transmitter
Computer, ESD	Signal generator
Ignite system	Local oscillator, UPS system
Voltage regulator	Test equipments
Lightning electromagnetic pulses	Microwave and ultrasonic equipments
Arc/ vapor lamps	Electronics ballasts
Pulse generators	Medical equipments
Thermostats	Microprocessor systems
Welding equipments	Pager transmitter
Frequency converters	High frequency generators

Interference caused by other devices using ISM band gives co-existence problem. Wireless HART use many methods to avoid co-existence problem [23]. These methods are:

- a) Network Segmentation
- b) Spectrum isolation
- c) Low power
- d) Spacial hopping
- e) Channel hopping
- f) Direct sequence spread spectrum coding
- g) Time synchronized mesh protocol

5 Case Study

Four case studies related to different industrial applications of WSN were studied and presented in this chapter.

5.1 Case Study I

In this case study, WSN based closed loop industrial plant energy evaluation and planning system has been studied. In a closed loop system, a sensor collects status information of a process and feeds it to a controller. Controller monitors the process information and takes necessary action by allowing actuators to act. Traditionally, these functions are realized in a wired system using Field bus and Profibus [24]. These days, WSN based non-intrusive methods are also practiced.

5.1.1 Background

In industries, motor driven systems consume most of the energy used. Research reveals that, 98% of motors used in industries are below 200 hp and consume 85% of overall energy used in industries [25]. This adds the importance of study on industrial plant energy evaluation and planning. In many cases, motors do not operate on full load condition, which results in the reduction of efficiency and waste of energy. Average load consumed by motors in industries is 60% of rated capacity [26]. Moreover, motor condition monitoring helps to prevent unexpected motor shut downs, decrease energy consumption and increase efficiency. This information gives the plant manager valuable information for planning a scheduled maintenance. WSN based close loop industrial plant energy evaluation and planning system uses non-intrusive methods for efficiency estimation. This WSN transfer only motor terminal voltages and currents.

5.1.2 System Architecture

The system architecture is divided into two parts, Motor Control Centers (MCC's) and Central Supervisory Station (CSS). Terminal qualities measurements are done at MCC's and transferred to CSS through WSN. These data are collected and processed on CSS. Non-intrusive methods are used to process information in CSS and energy usage evaluation, motor health conditioning and monitoring can be made for each motor in the plant. Terminal quantities transferred to CSS from MCC's are generally current (I_s) and Voltage (V_s). I_s , V_s , speed estimator and resistor estimator are used to estimate corresponding speed (S_s) and resistance (R_s). For energy uses evaluation, V_s , I_s , S_s , R_s and (Name Plate Info) NPI are needed. NPI has information of motor types, their operation range and rating. By studying, Machine Condition Prediction and Energy Plant Usage Evaluation, plant manager can make a decision for replacing faulty and oversized motors; and can work on the efficiency

improvement of under load motors. *Figure 5.1* gives the overall architecture of WSN based system architecture for closed loop industrial plant energy evaluation and planning system.

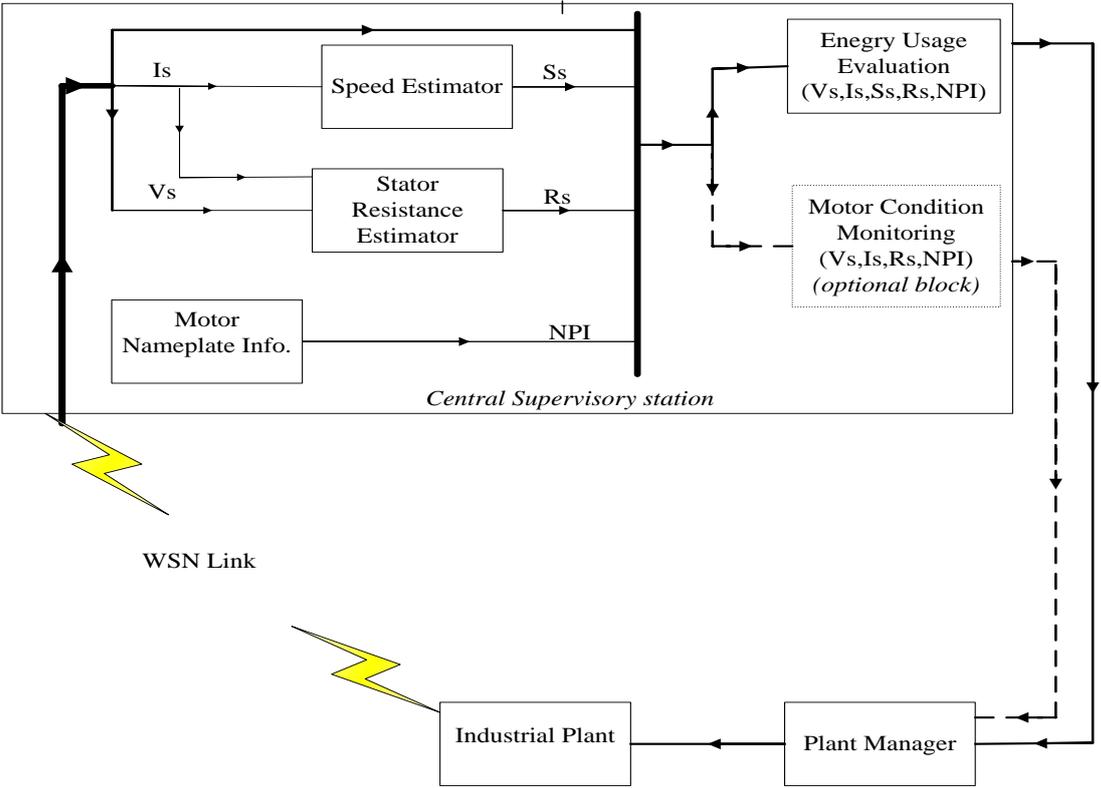


Figure 5.1: WSN based architecture for closed loop industrial plant energy evaluation and planning system [26]

5.2 Case Study II

This study is related to the work done to measure and monitor a physical dynamics like vibration and displacement in order to determine the structural health condition of a bridge.

5.2.1 Background

Structural condition of a bridge is affected by different factors like, external forces, wind, seismic activity and traffic passing through it. An application of WSN is to monitor structural health conditions in order to know how structures perform over a long period under changing environmental conditions. Dense wireless sensor solutions as used in suspension bridge at St. Lawrence County, New York [27] are practiced in many cases of structural monitoring. In Dense wireless sensor solutions, large numbers of sensor nodes are distributed throughout the bridge structure. Factors such as strain, vibration, acceleration and displacement measurement are analyzed at the same time. However, there are also many cases where single nodes can be used to monitor particular location of a bridge. The University of Sheffield succeeded in monitoring longitudinal movement of Tamar Bridge using single measurement node [28].

5.2.2 Network Architecture

WSN deployed in Golden Gate Bridge, USA, for structural health monitoring is similar to the concept of dense wireless sensor solutions. 64 sensor nodes were installed on 4200 ft. long main span and the tower located at the southern end of the bridge. Out of 64 nodes, 46 nodes were made hop network for routing data from farthest sensor nodes to the monitoring station. Vibration measurement was taken at 1 KHz rate [29]. Two types of accelerometer sensors were used for collecting the vibration data from a bridge. These were ADXL 202E and SD 1221L. Each type of accelerometer sensors was responsible for the different range of vibration detection. Mica2 motes were used as sensor nodes for storing and communicating data. Mica2 consists of ATmelATmega 128L microprocessor, 128 KB of programmable memory, 4KB of RAM, Chipcon CC1000 radio chips, and operates at 8 MHz with data rate of 28.4 Kbaud [30]. Sensor layout on the Golden Gate Bridge is shown in *Figure 5.2*.

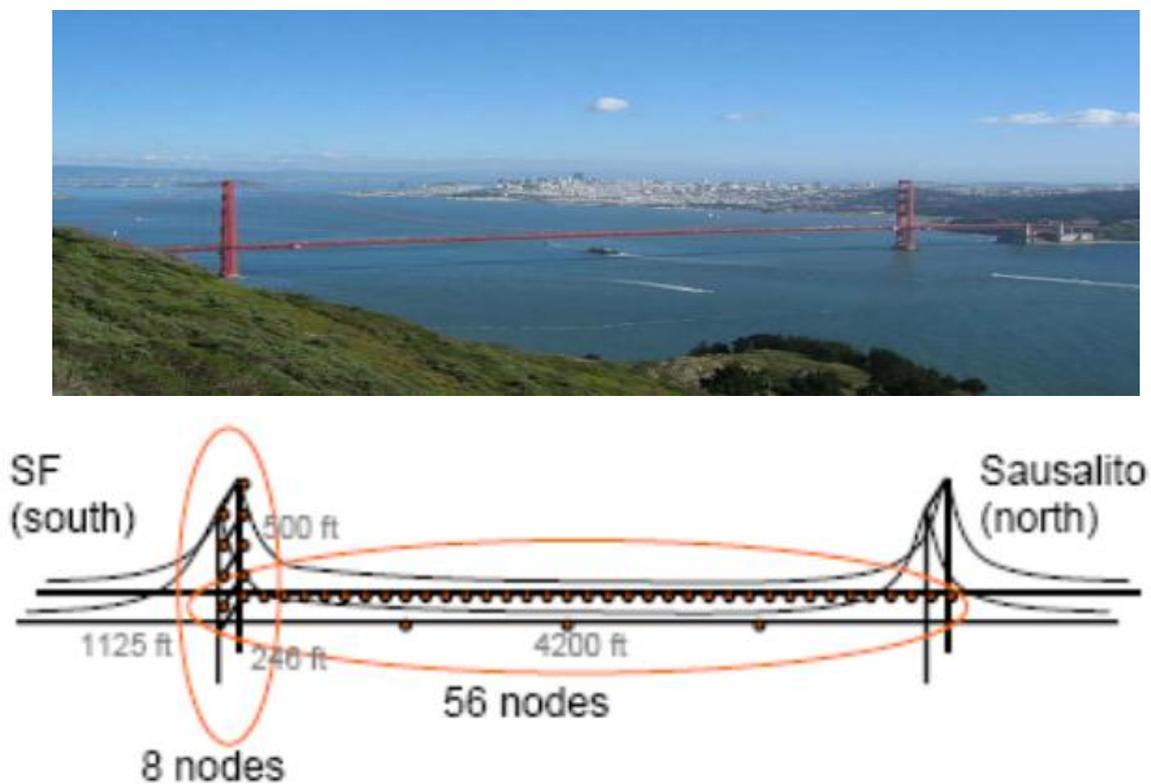


Figure 5.2: Sensor node layout on Golden Gate Bridge [31]

5.2.3 Data Acquisition Issues

Some data acquisition issues [30] related to structural health monitoring are given below.

- a) For every sensor reading, static noise is associated with it. Less static noise floor gives high accuracy measurement. Structural health monitoring application required the detection of signal down to $500\mu\text{G}$ for a distortion less measurement.

- b) Structural health monitoring applications require high frequency sampling in order to avoid the variations in sampling interval (jitter).
- c) In order to monitor a large area, multi-hop network is established. In such cases, if any node fails to work, then monitoring station may get a wrong picture of the situation.

5.3 Case Study III

This case study is based on the industrial field visit in Yara nitric acid plant, Porsgrunn. The main purpose of the field visit is to understand how Wireless HART is integrated with DELTA V in order to monitor and control the process. A team of an Engineer from Emerson, Yara and TUC were involved for the coupling of devices.

5.3.1 Background

Wireless HART is a global International Electro-technical Commission (IEC) standard (62591) for wireless communication in process industries [23]. It is used for real time industrial process measurement and control applications. Using Wireless HART, one can implement self-organizing mesh topology WSN. Gateway, host system, wireless adaptor, wireless field devices and wireless repeater are used to develop complete WSN system for process measurement and management. DELTA V is a digital system used for the easy way to control, supervise and data acquisition system in process industries [32]. DELTA V is given a specific name of “host system” in Wireless HART based WSN system. DELTA V communicates through open standards (OPC, OPC.NET 3.0) to integrate with other plant functions and applications for real time and historical data transfer [33].

Traditional process management system used Profibus or Field bus to connect sensors and actuators to the DELTA V system. Development and research on WSN enable the feature of using wireless technology to replace cabling installation, such that relocation and installation have become very easy.

5.3.2 Existing Process Management System

YARA has installed DELTA V for process management. All the sensors were connected to DELTA V process management system through a wired system like an optical fiber, field bus, etc. In order to avoid cable and make the process management system more robust, non-critical process data monitoring was planned to be replaced by wireless link. They have chosen Wireless HART system based WSN. Integrating Wireless HART allows devices to communicate wirelessly with existing DELTA V system. Self-organizing mesh network was created and data from all sensors were transferred to DELTA V system. *Figure 5.3* gives an overview of existing process management system and Wireless HART based process management system.

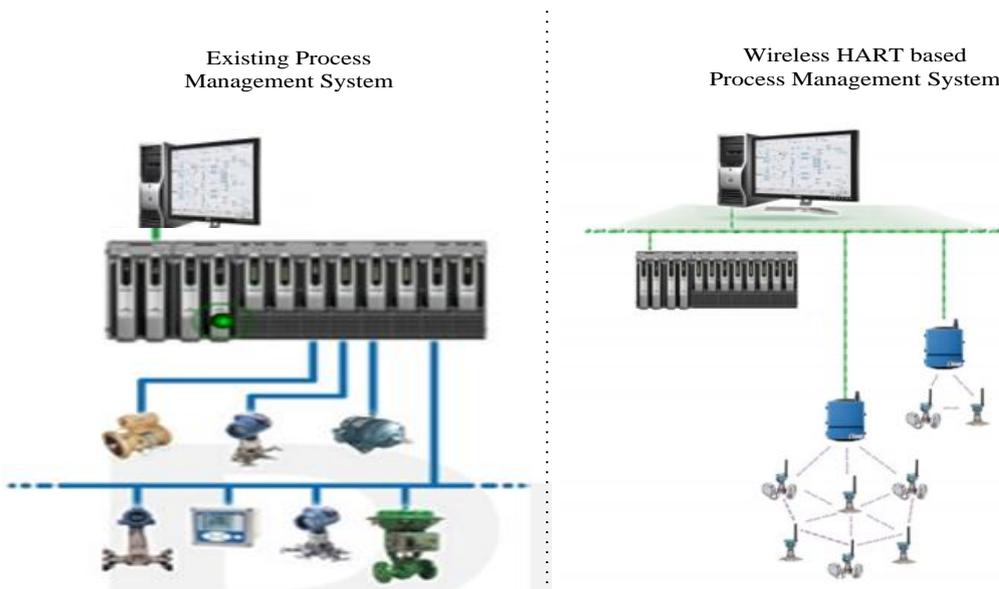


Figure 5.3: Existing process management system and Wireless HART based process management system [34]

5.3.3 Coupling

Engineers first tried to install Wireless HART sensors randomly. The gateway was placed on the room, which was located on the 4th floor of the plant building, and sensor nodes were placed on the roof of 7th floor where pumps and other machineries were installed as shown in Figure 5.4. The rough distance between sensor nodes and gateway was about 60 meters. One sensor node with vibration sensors was installed on the top of the tower. Second sensor node with temperature sensor was placed on one corner of the floor, and third sensor node was placed on the corridor.



Figure 5.4: Engineers busy on random installation of wireless HART in Yara, Porsgrunn

First of all, Engineers tried to form a star network topology. During testing, it was found that gateway could not receive signal form any of the sensors installed. This could be because of

obstacles like walls of the buildings and huge machines causing diffraction or deep fading of the radio signals. Due to this, Engineers decided to put a sensor node in between the gateway and measurement points such that multi-hop network is formed, and signals can be received in the gateway. This approach was found successful. Later on complete mesh topology was formed by installing multiple intermediate sensor nodes and measuring nodes.

5.4 Case study IV

In this case study, underwater WSN for water quality monitoring has been studied. Underwater sensor networks have wide applications in industries. They help in water quality monitoring, ocean graphic data collection, disaster detection & prevention and oiled field monitoring.

5.4.1 Background

To control physical, chemical and biological characteristics of water, water quality monitoring is required. Industries found it very important because it helps to check contaminations of water, discharge of toxic chemical from industrial process and pollution.

Varieties of sensors are available for underwater monitoring. In most cases, following measurement are made; 1) Potential of Hydrogen (pH), 2) Dissolved Oxygen (DO), 3) Temperature, 4) conductivity/TDS, 5) Turbidity. pH measurement gives an idea of concentration of hydrogen ions in water. DO measurement gives milligrams per liter (mg/l) of oxygen availability in water. Temperature measurement gives warmth or coldness of the water, which in turn, gives an idea about the amount of oxygen available. Cold water can dissolve more oxygen. Conductivity/TDS gives an idea of the ion concentration. Precisely, it measures the ability of water to conduct the electricity. Turbidity determines the cleanliness of water. It gives a fair idea about how many particles are floating in the surface of water, and how much sun light can reach beneath the surface of ocean and lakes.

5.4.2 Network Architecture

Basically, there are two types of underwater WSN architecture [35].

- a) Two dimensional
- b) Three dimensional

In two dimensional communication architecture, the coverage area needs to be covered fully by sensor nodes, and each node need to establish a multi-hop path to the gateway. In three dimensional architecture, sensor nodes float at different depth of ocean in order to observe different seismic phenomena. Sensor nodes are attached to buoy by means of wires and length of wires are adjusted as per requirement. Two dimensional architecture may not observe these

phenomena as sensors are installed at the bottom of sea level. *Figure 5.5* gives one possible approach to underwater WSN installation.

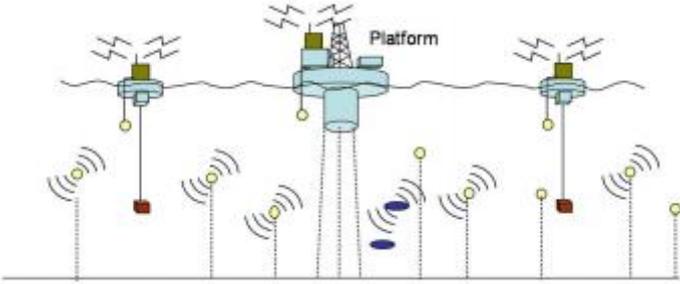


Figure 5.5: Possible approach to underwater WSN node deployment [36]

Large numbers of sensor nodes are installed at the bottom of the sea level. These nodes are battery powered and remain in sleep mode in order to save power. At the top layer, control nodes are installed in offshore or onshore platform. For large area coverage, super nodes are installed. Super nodes have access to lower level sensor nodes and upper level base stations [36].

In underwater WSN, hierarchical topologies are inevitable as nodes are deployed in the bottom of sea level [37]. For this, multiple sink nodes (AP) are installed. Each AP can talk only with the group of sensor nodes called cluster and super nodes. *Figure 5.6* is a hierarchical topology developed after combining two dimensional architecture and cluster concept (shown by dotted line).

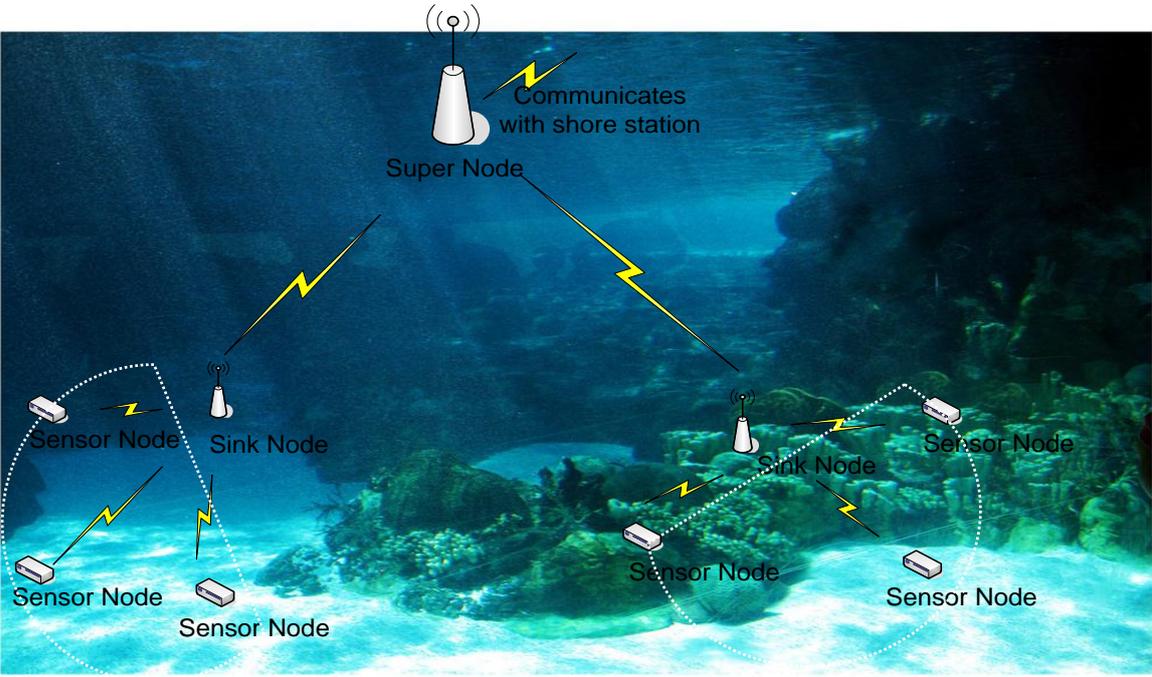


Figure 5.6: Two dimensional hierarchal topology using cluster concept

5.4.3 Comparisons with Terrestrial WSN

Underwater WSN is more problematic than terrestrial WSN in terms of radio propagation, fault, battery backup and signal attenuation [38]. Comparisons of underwater WSN with terrestrial WSN are listed below.

- a) Radio communications inside water always suffers from long propagation delay, fading and multipath fading problems. Terrestrial radio communications have lower signal degradation as compared to underwater radio communications.
- b) Commercial water quality sensors are expensive than other general terrestrial sensors.
- c) In salty water, radio signals degrade significantly. Hence, there is always a problem in designing WSN.
- d) Underwater sensors have fewer lifetimes because of corrosion. Maintenance and replacement of faulty parts are difficult.

6 Lab Work

Lab work was carried out in two phases. In the first phase, star network topology was created with gateway and two sensor nodes. The maximum distance of wireless transmission between sensor node and gateway was determined and temperature measurement from both sensor nodes was monitored. In the second phase, distance of transmission was increased by configuring one sensor node as an intermediate router node and temperature was measured. This is the case of multi-hop network topology. Lab work in the second phase was based on the Design2 described in the Chapter 3.1.2. Two numbers of NI WSN-3202 were taken as sensor nodes and one NI WSN-9791 was taken as a standard gateway. Four standard AA size batteries were used to power one sensor node. NI PS-15 was used to power another sensor node and gateway. These WSN devices work on Zig-bee standard.

6.1 Phase I- Star Network Topology

Full configuration of WSN in star network topology is given in *Figure 6.1*. Both sensor nodes were directly communicating with gateway, which in turn, can be monitored by using LabVIEW program in computer. Straight Ethernet cable was used to connect gateway with Laptop.

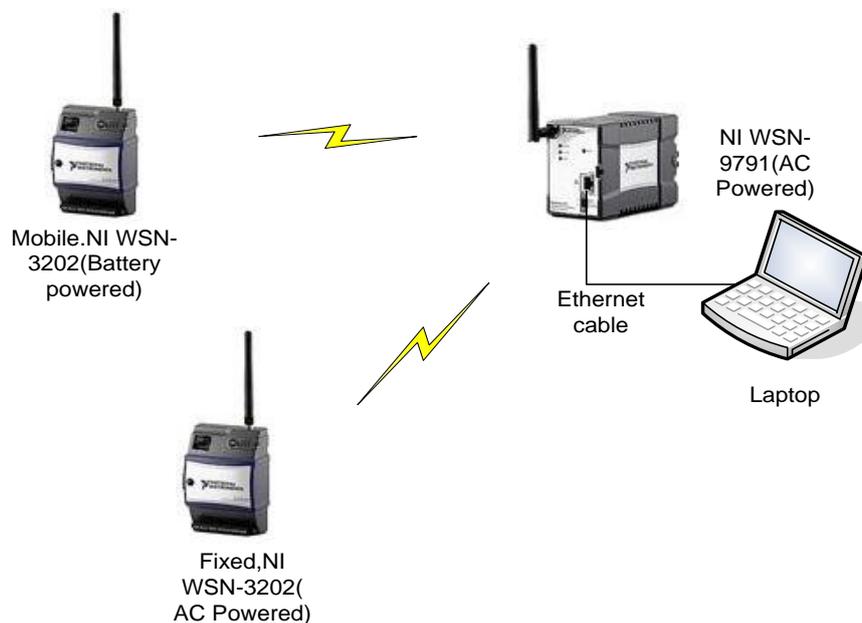


Figure 6.1: Full configuration in a star network topology

6.1.1 Configuration Steps

Coupling of WSN devices and its monitoring through LabVIEW programming are given step wise below.

1. PC containing LabVIEW program was taken.

2. NI WSN software that came along with device package was installed.
3. NI WSN-9791 was connected to PC using straight Ethernet cable.
4. Measurement and Automation eXplorer (MAX) was clicked from the tools button of LabVIEW window.
5. Remote Systems in MAX was expanded and NI WSN-9791 was detected by MAX.
6. NI WSN-9791 gateway was selected, WSN nodes tab was clicked and after that, add node tab was clicked.
7. Type of sensor node i.e. NI WSN-3202 device was selected, serial number of the device from device sticker was typed and in ID Number, 1 was entered. After this, Finish button was clicked.
8. Another NI WSN-3202 was added by clicking Add Another button and step 7 was repeated again, but in ID Number, 2 was entered. ID number ranges from 1 to 50 and each device were given with unique ID number.
9. Now, nodes were connected automatically to the gateway. *Figure 6.2* is the screen shot of MAX screen when both sensor nodes were detected.

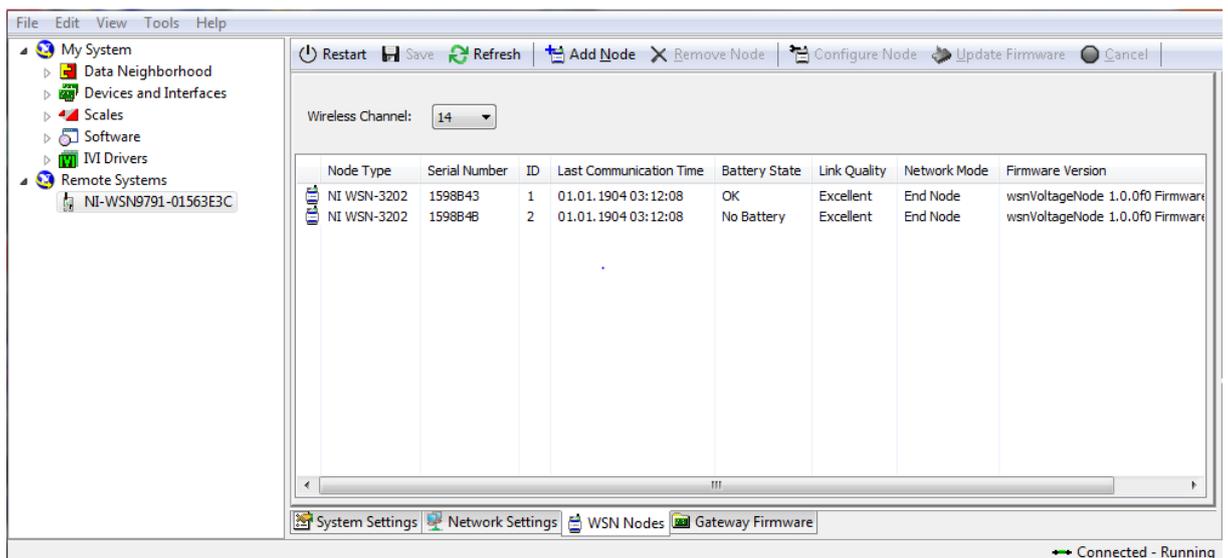


Figure 6.2: MAX window showing status of both sensor nodes detected by gateway

10. After that, devices were configured in LabVIEW.
11. New LabVIEW project was opened.
12. Project name was right clicked and New>> Targets & Devices were selected.
13. Existing target or device was selected and WSN gateway folder was expanded.
14. After certain scanned time, NI WSN-9791 was detected; OK button was clicked so that gateway was added to the Project Explorer window.
15. In order to see associated nodes, NI WSN-9791 was expanded. Each node was expanded and all I/O variables were seen. Screen shot of LabVIEW project and its associated I/O variables for both sensor nodes were given in *Figure 6.3*.

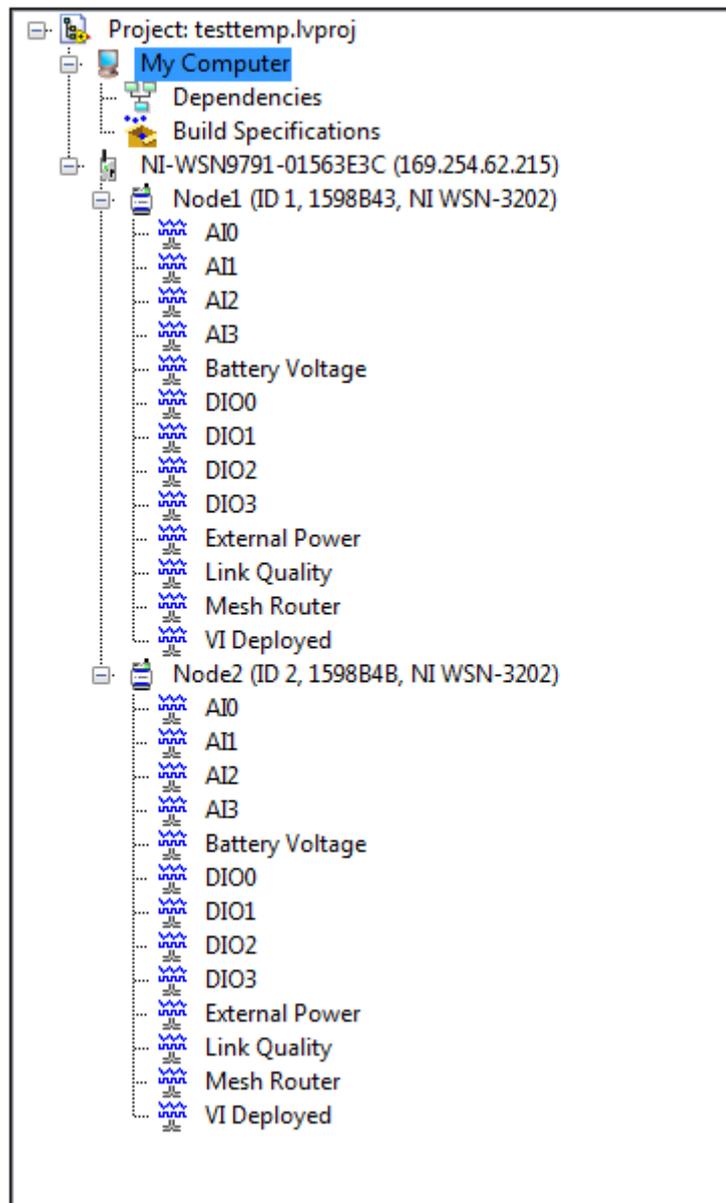


Figure 6.3: LabVIEW Project window showing both sensor nodes and its associated I/O variables

16. New VI was created, I/O variables were dragged and dropped to the block diagram, and indicators for each I/O variables were created.

6.1.2 Determining Maximum Distance of Transmission

After the coupling and configuration of sensor nodes with gateway, second step was to determine maximum wireless distance that WSN devices can support without traffic interruption. For this, sensor node powered with battery was made mobile. Mobile sensor node was slowly taken away from the gateway and link quality was monitored in LabVIEW program. 55% of link quality was supposed to be minimum signal strength as instructed by National Instruments and regarded as a fair signal that corresponds to signal strength of 2 bar highlight in the sensor nodes [39].

A sensor node was moved away further up to the distance, where signal strength decreased to 60%. Measurement of link quality was done in LabVIEW simultaneously. When signal strength reached to 60 %, sensor node was kept stationary in that place. The distance where a sensor node was kept stationary was measured to be 23.1 meters. Link quality fluctuation was measured up to 1024 samples and found that most of the time, link quality ranges from 55% to 60 %. Thus, maximum indoor distance of transmission was determined to be 23.1 meters with the link quality from 55% to 60%. *Figure 6.4* shows LabVIEW plot for link quality measurement. Up to 168 samples, sensor node was mobile, then it was fixed in particular location and other samples were measured.

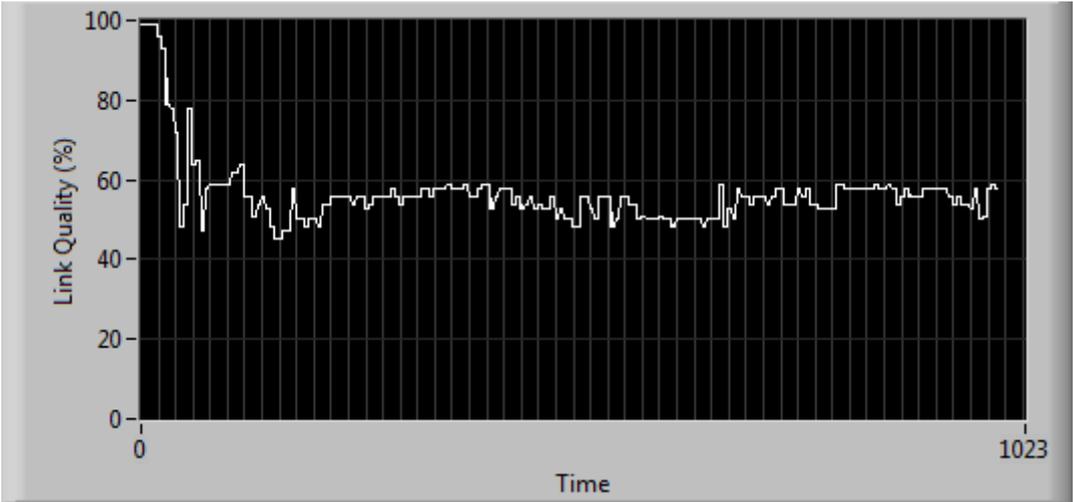


Figure 6.4: Time vs. Link quality graph to determine maximum distance of transmission

Sensor node powered with Alternative Current (AC) was kept stationary at 7.9 meters away from the gateway. *Figure 6.5* shows the top view location of both sensor nodes installed and their distance from gateway.



Figure 6.5: Top view of College to show where the sensor nodes and gateway were installed

6.1.3 Temperature Sensor Setup

Two PT-100 temperature sensors were connected to first analog I/O (ai0) of each sensor nodes and temperature fluctuations were measured through LabVIEW program. Transmitter, 250Ω resistor, +24VDC power supply and PT-100 element were combined together to form a complete set of temperature sensor. This set was then connected to sensor node as in *Figure 6.6*.

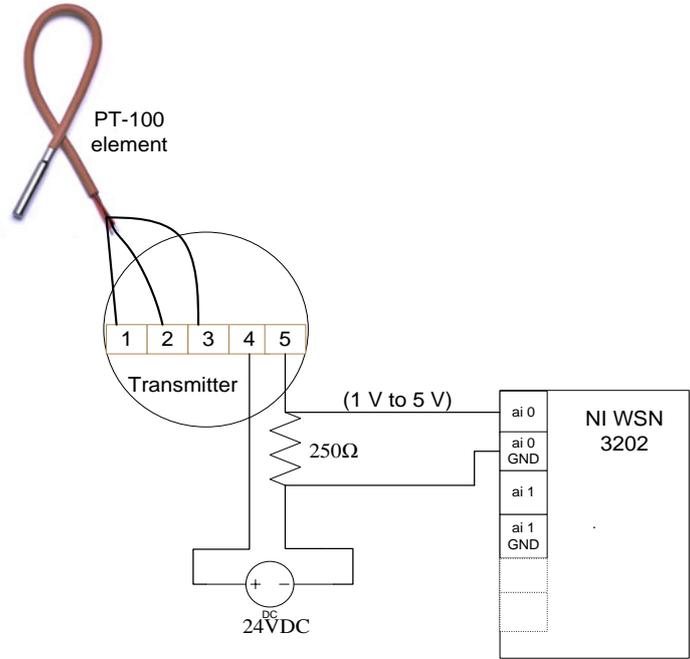


Figure 6.6: Connection diagram of PT-100 elements, Transmitter and NI WSN 3202

Transmitter operating range is 0 to 50 °C. Due to this limitation, any temperature below and above this range cannot be measured. The voltage drop between resistor points was always 1 to 5 V. 1 V corresponds to 0 °C and 5V corresponds to 50 °C. A linear scaling was done in a LabVIEW program in order to convert voltage measurement to corresponding temperature measurement.

Figure 6.7 shows a linear scaling graph for the corresponding temperature measurement at the different voltage level.

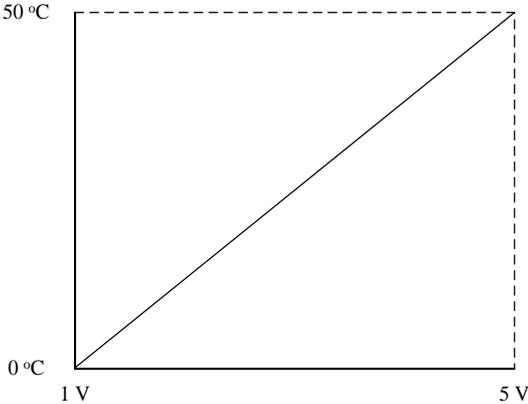


Figure 6.7: Graph showing linear scaling to convert voltage to corresponding temperature

6.1.4 LabVIEW Code

The program code was made in a block diagram as shown in *Figure 6.8*. The code was written in a while-loop. All the interested I/O variables were dragged and dropped to the block diagram from a LabVIEW project window. Indicators for each variable were created. Some of the important elements of code and their functions are given in *Table 6.1*. Voltage measurement from sensor nodes was converted to temperature measurement by linear scaling. For signal analysis, Create Histogram Express VI and Statistic Express VI were used. Indicator and Scope for each parameter were created. Shift register and Build array were used to store and process the values in every loop in order to calculate arithmetic mean, maximum value, time of maximum value, minimum value, time of minimum value and histogram.

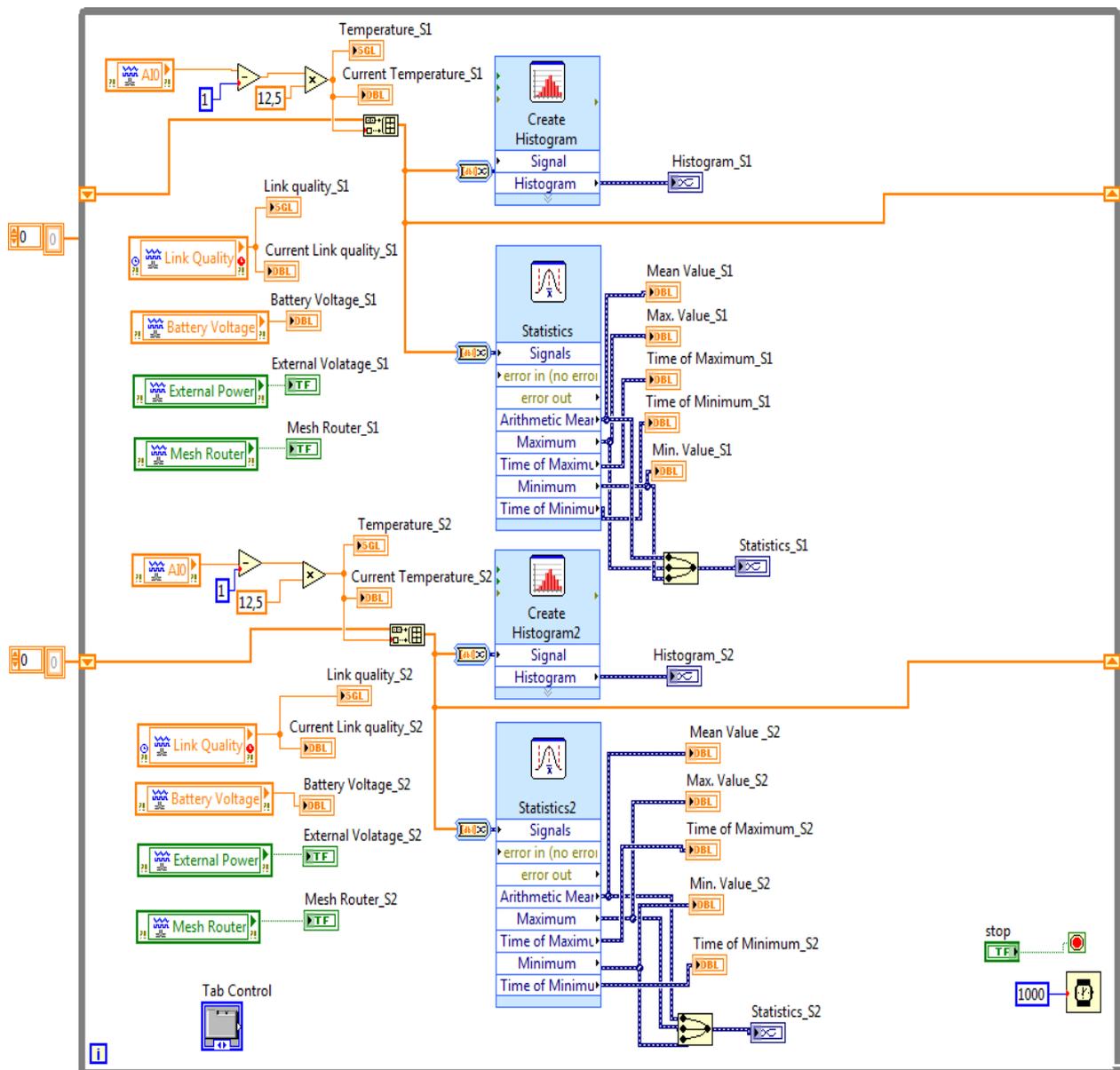
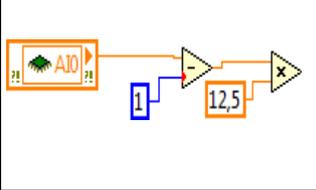
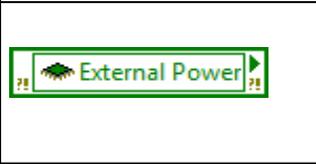
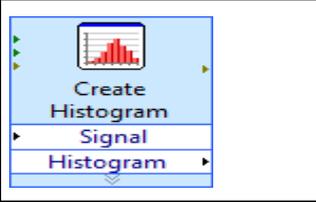
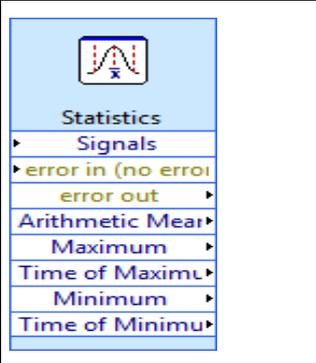


Figure 6.8: Block diagram of LabVIEW program used to measure temperature from 2 sensor nodes

Table 6.1: Elements used in LabVIEW code and their functions

	<p>Output of AIO is 1V-5V, linear scaling is done to convert voltage measurement to corresponding temperature measurement. 1 V corresponds to 0 deg.Cent. and 5V corresponds to 50 deg.cent. Temperature measurement is shown by numerical indicators and waveform graph.</p>
	<p>The output of Link Quality variable is between 1 to 100, this output is shown by numerical indicators and waveform graph. This shows how good is the the air-link quality between sensor nodes and gateway.</p>
	<p>The output of Battery Voltage variable is between 1 to 6, this output is shown by numerical indicators. 1 means very less battery voltage and 6 means full battery voltage condition.</p>
	<p>The output of External Power variable is either TRUE or False, this output is shown by boolean indicators. If TRUE, sensor node is power by external source and booleana indicators is highlighted in front panel.</p>
	<p>The output of Mesh Router variable is either TRUE or False, this output is shown by boolean indicators. If TRUE, sensor node is configured as router mode and booleana indicators is highlighted in front panel.</p>
	<p>Inbuilt function Create Histogram Express VI is used to create Histogram of temperature measurement throughout the monitored time period. Histogram is plotted on waveform chart. Data in each loop are stored in 1-Dimensional array and then passed to next loop by using Shift register.</p>
	<p>Inbuilt function Statistics Express VI is used to calculate mean value, maximum value, minimum value of temperature throughout the monitored time period. Furthermore, sample time when minimum value and maximum value occurred is also calculated by this VI. These values are shown by numerical indicators and waveform chart. Merge signal function is used to concatenate and show all data in single graph. Data in each loop are stored in 1-Dimensional array and then passed to next loop by using Shift register.</p>

6.1.5 Front Panel and Data Interpretation

Front panel of LabVIEW program was divided into two tab control. Temp & Link Qual. tab as shown in *Figure 6.9*, consists of scope for temperature and link quality measurement for both sensor nodes. Measurement plot can be seen on the scopes. This tab also consists of the current value of link quality, temperature, battery status. Sensor node mode of configuration (end node or mesh router node) and presence of external power supply was indicated by Boolean indicators.

Statistics tab as indicated in *Figure 6.10*, consists of scope for different parameters of temperature measurement like, maximum value, minimum value, arithmetic mean, and histogram for both sensors. Numerical value for these measurements along with sample time for maximum and minimum value were also present in this tab.

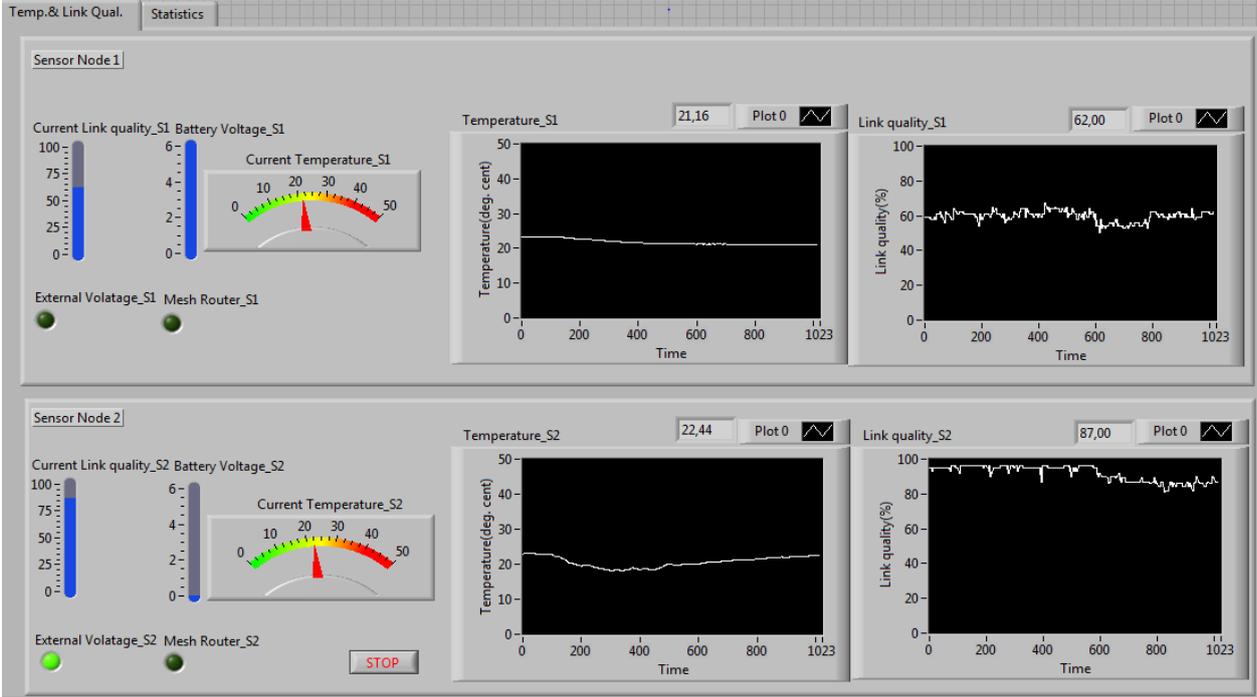


Figure 6.9: Front panel consisting Temp & Link Qual. tab for both sensors

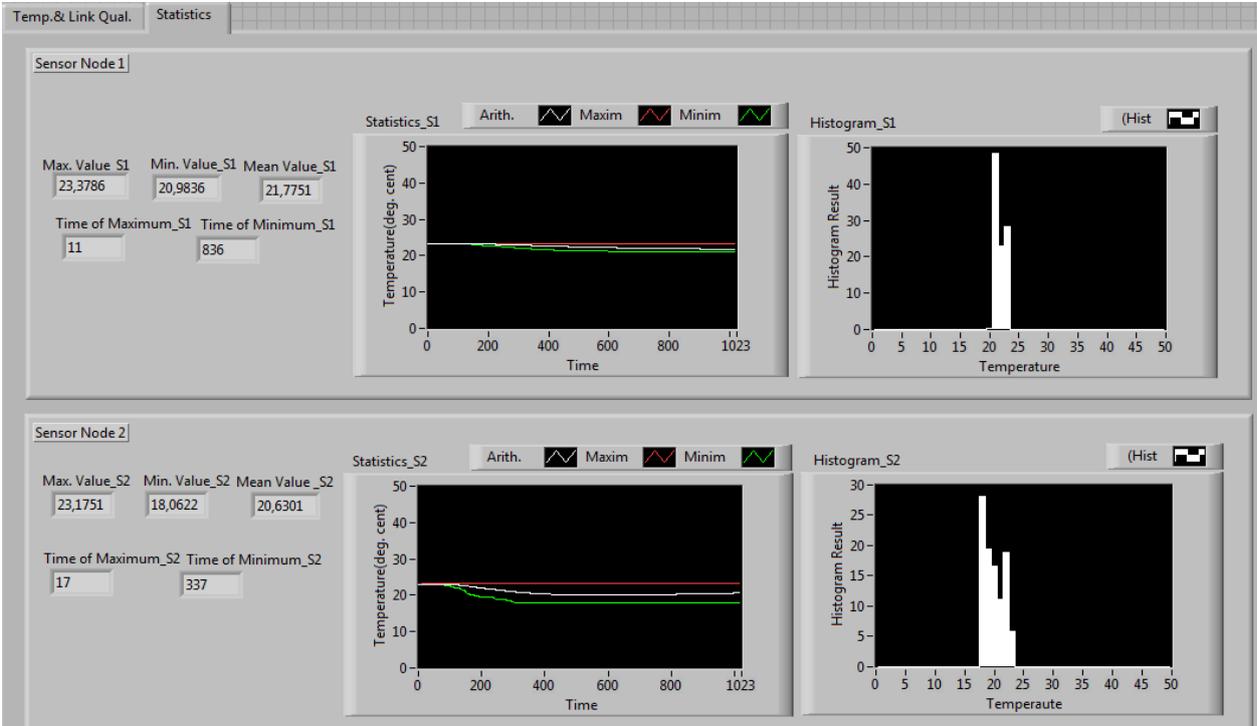


Figure 6.10: Front panel consisting Statistics tab for both sensors

1024 samples of temperature were measured. For the temperature variation, window was opened and closed in a room where sensor node 2 (AC powered sensor node) was kept.

Sensor node 1 (battery powered sensor node) was kept in a big hall, where the probability of temperature fluctuations was very less. From *Figure 6.9*, it can be seen that, temperature measurement for sensor node 2 fluctuated from 18 °C to 23.1 °C for the samples 0 to 1023. After 100 samples measurement, the window of room was opened as a result, temperature decreased. After 500 samples' time, window was closed and temperature started to increase again. Similarly, link quality of sensor node 2 fluctuated from 85 % to 95 %. The reason behind link quality fluctuation was due to opening and closing of a door as people entered the room. The current temperature, current battery voltage, current link quality for sensor node 2 were measured to be 22.4 °C, 6 V, 87 % respectively. External Voltage Boolean indicator was highlighted which indicated as sensor node2 was powered by external AC power supply, but Mesh router Boolean indicator was not highlighted, that means sensor node 2 was configured in end node mode not at the mesh router.

Temperature measurement for sensor node 1 fluctuated constantly around 20.9 °C to 23.3 °C. Link quality fluctuated from 55% to 65%. The current temperature, current battery voltage, current link quality for sensor node 1 were measured to be 21.1 °C, 0 V and 62 % respectively. Both the Boolean indicators for sensor node 1 were not highlighted, that means there was no external power supply to node and node was configured in end node mode not mesh router mode.

From *Figure 6.10*, statistical interpretations for both sensor nodes were studied. It can be seen that the maximum temperature for sensor node 2 was measured to be 23.1 °C at 17th sample time and minimum temperature was measured to be 18 °C at 337th sample time. Mean value of temperature was found to be 20.63 °C. Histogram for sensor node 2 suggested that, temperature around 18 °C occurred most of the time and temperature around 23 °C occurred least of the time of observations. The maximum temperature for sensor node 1 was measured to be 23.3 °C at 11th sample time and minimum temperature was measured to be 20.9 °C at 836th sample time. Mean value of temperature was found to be 21.77 °C. Histogram for sensor node 1 suggested that, the maximum occurrence was 21 °C and the minimum occurrence was 22 °C. There were much variations of temperature in sensor node 2 than sensor node 1. Statistical scopes for both sensors consist of green, red and white color. These represent minimum value, maximum value and arithmetic mean value respectively.

6.2 Phase II- Multi-hop Network Topology

Sensor node with external power supply was placed stationary at 23.1 meters away from gateway. 23.1 meters distance was found in first phase of lab work, and that was the maximum distance supported by one sensor node with link quality of 55% or more. In this phase, stationary sensor node was configured as mesh router mode and battery powered sensor node was configured as an end node such that, end node first communicated with intermediate router node and then gateway. Thus, the overall distance of transmission was

increased. Full configuration of WSN in multi-hop network topology is given in *Figure 6.11*. Gateway was connected to Laptop by using straight Ethernet cable.

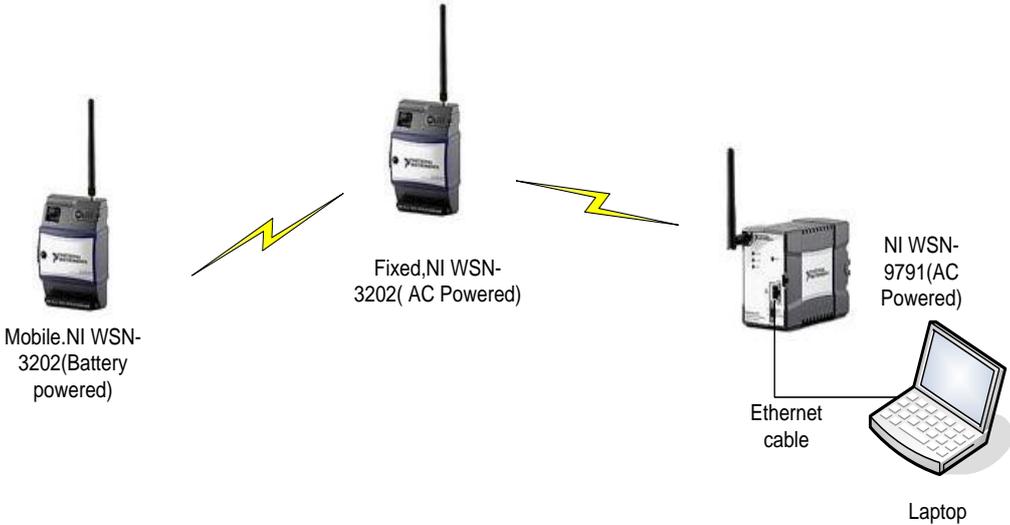


Figure 6.11: Full configuration in a multi-hop network topology

In MAX, sensor node with serial number 159884B was selected, Update Firmware tab was clicked and then from the drop down menu, Mesh Router was selected. Sensor node took some time before it was configured to router mode. *Figure 6.12* shows the screen shot of MAX screen when one sensor node is updated as a router mode. Circle in the screen shot clearly indicates Mesh Router mode.

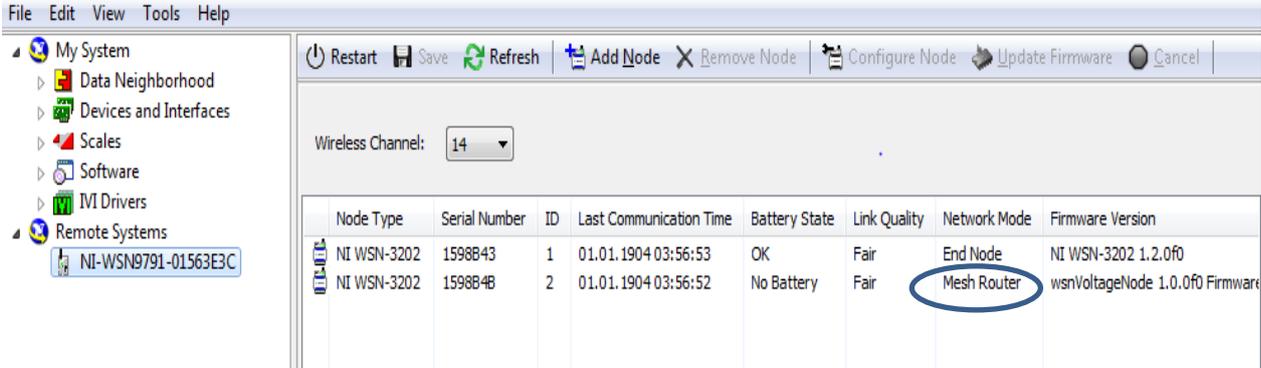


Figure 6.12: MAX window showing Network Mode for both sensor nodes, where one sensor node is updated as Mesh Router

6.2.1 Determining Operation of Mesh Router Mode

In order to determine the operation of a mesh router node, battery powered sensor node was kept close to router node placed at 23.1 meters away from gateway as shown in *Figure 6.13*. At first, both nodes were communicating directly with gateway with link quality ranges from 55 % to 65 %.

Reset button of an end node was pressed for more than 5 seconds and released. After this, end node searched for the strongest link nearby. Since, the nearest link would be the waves

propagated by router node, it was connected to router node rather than the gateway. The dotted line in *Figure 6.13* shows the new connection path.

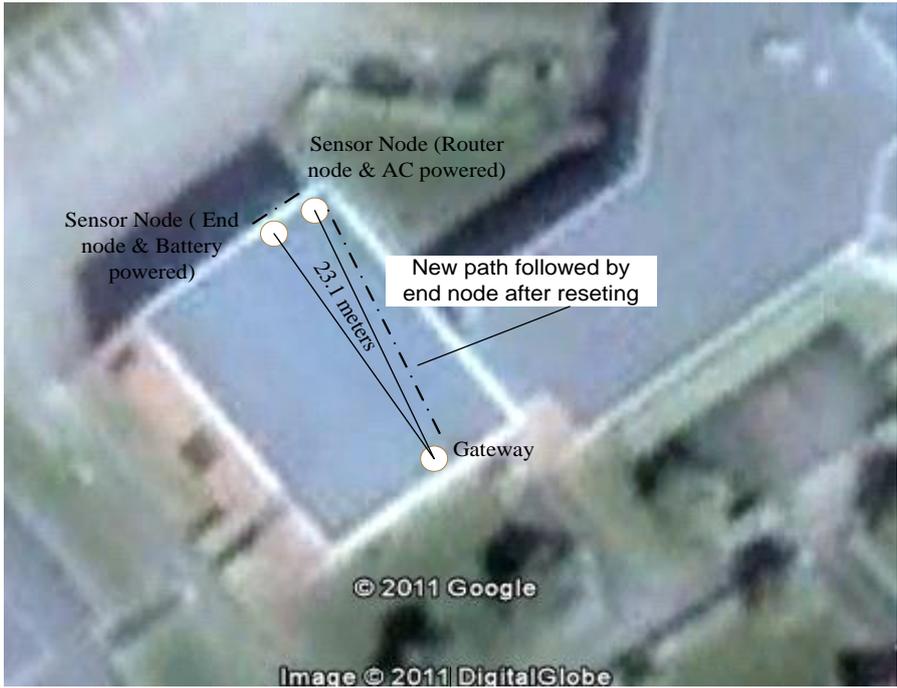


Figure 6.13: Top view of College to show where the sensor nodes and gateway were installed; and new path followed by end node after resetting

Link quality of the end node was measured in LabVIEW throughout the testing period. *Figure 6.14*, shows the link quality of the end node before, and after it has been reset. At first the link quality was seen to be 55 % to 60 %. After resetting it was observed that, end node link quality increased sharply and reached to almost 100%. This was because of a new link that has been established between the end node and router node.

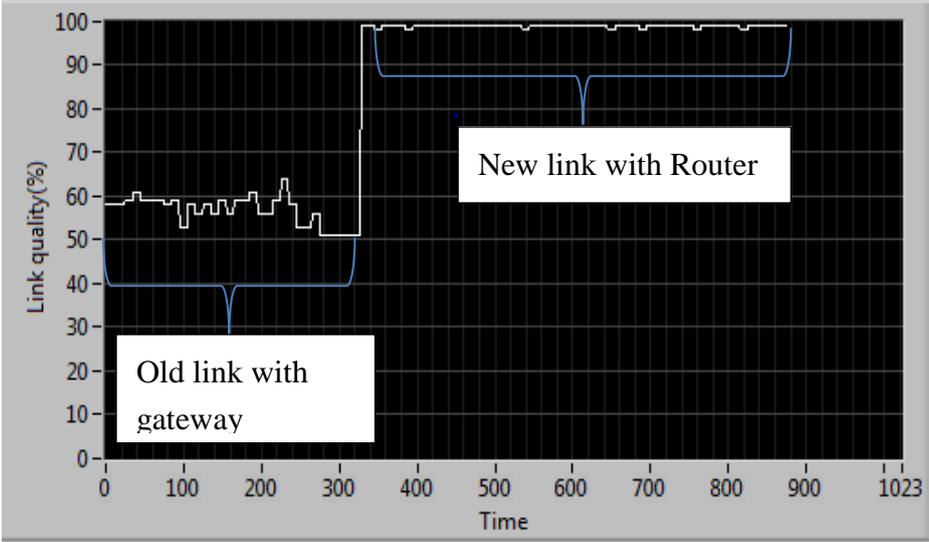


Figure 6.14: Time vs. Link quality graph to observe improvement in link quality after end node has been reset

A significant change in MAX window at this point was observed. Fair link quality of the end node as in *Figure 6.12* was changed to Excellent. This also proved the improvement in link quality after the end node was reset. *Figure 6.15* shows the change in MAX window when the end node was reset.

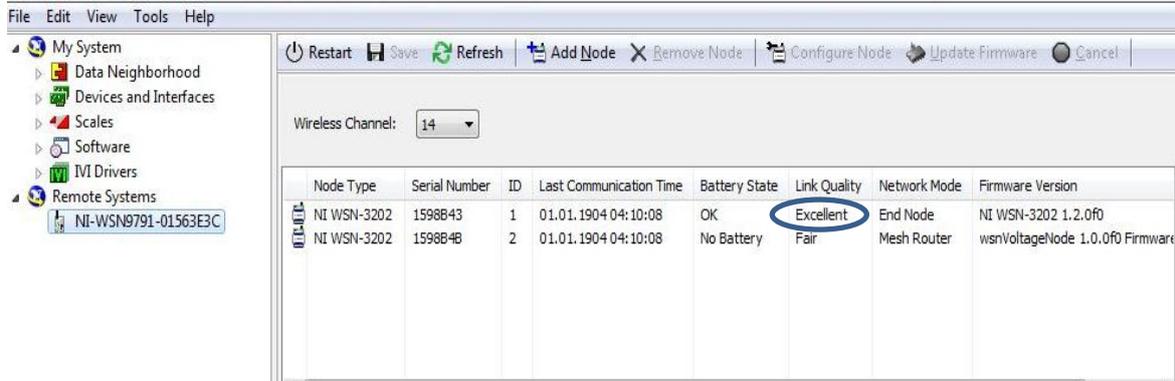


Figure 6.15: MAX window showing Excellent link quality after the end node was reset

Taking advantages of improved link quality, end node was moved away from router node until its link quality reached around 55%. Thus, overall distance of transmission was increased. *Figure 6.16* shows the location of the end node and router node and their distance from gateway. The end node was kept 24 meters away from router node. Thus total transmission range was measured to be 47.1 meters.

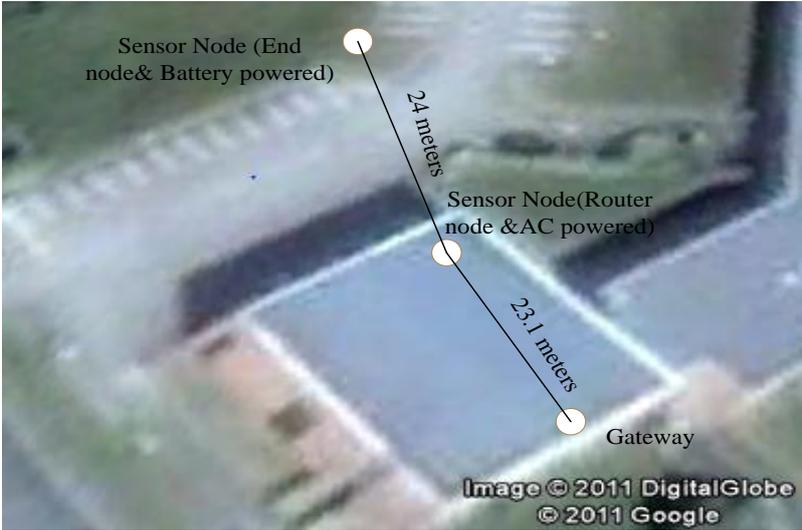


Figure 6.16: Top view of College to show where the sensor nodes and gateway were installed; and their separation distance

6.2.2 LabVIEW Programming and Data Interpretation

LabVIEW code used for phase-I of lab work was modified with the provision of measuring temperature statistics only for end node. Since there were no significant variations in temperature, histogram analysis was removed. Code still has provisioned of link quality monitoring, battery voltage monitoring along with Boolean indicators for external voltage and

mesh router mode for both nodes. *Figure 6.17* shows the code and *Figure 6.18* shows the front panel of LabVIEW program used in this phase of lab work.

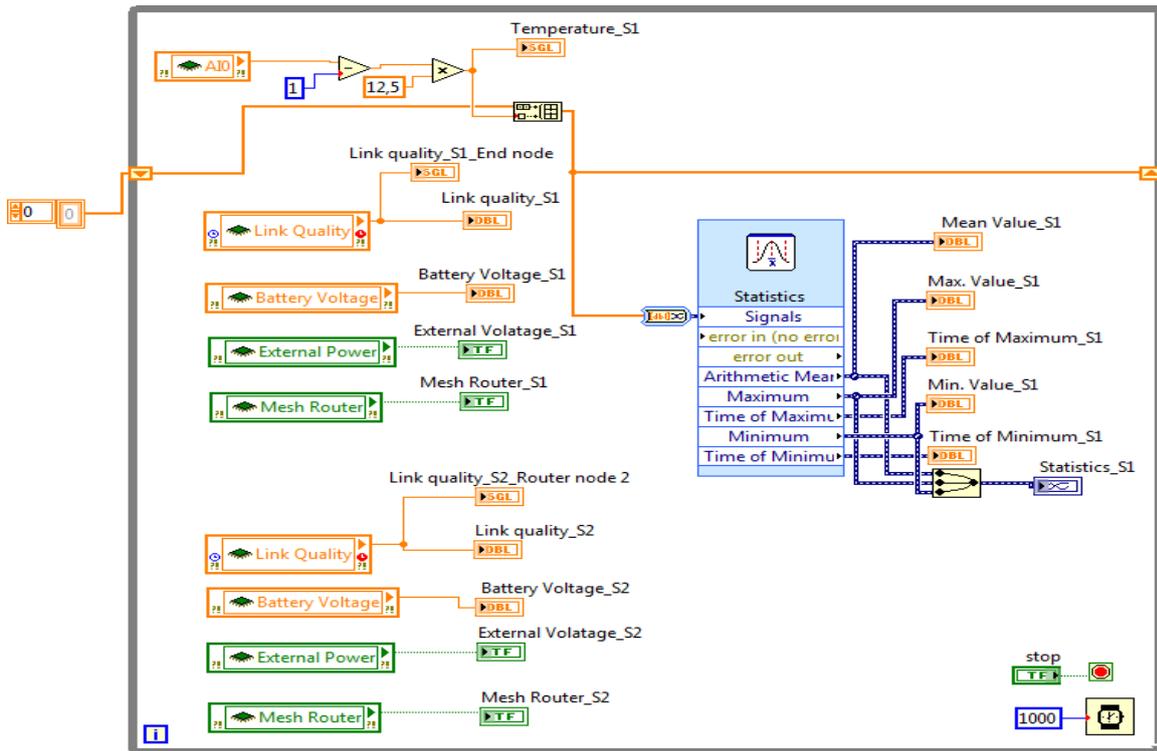


Figure 6.17: Block diagram of LabVIEW program used to measure temperature from end node

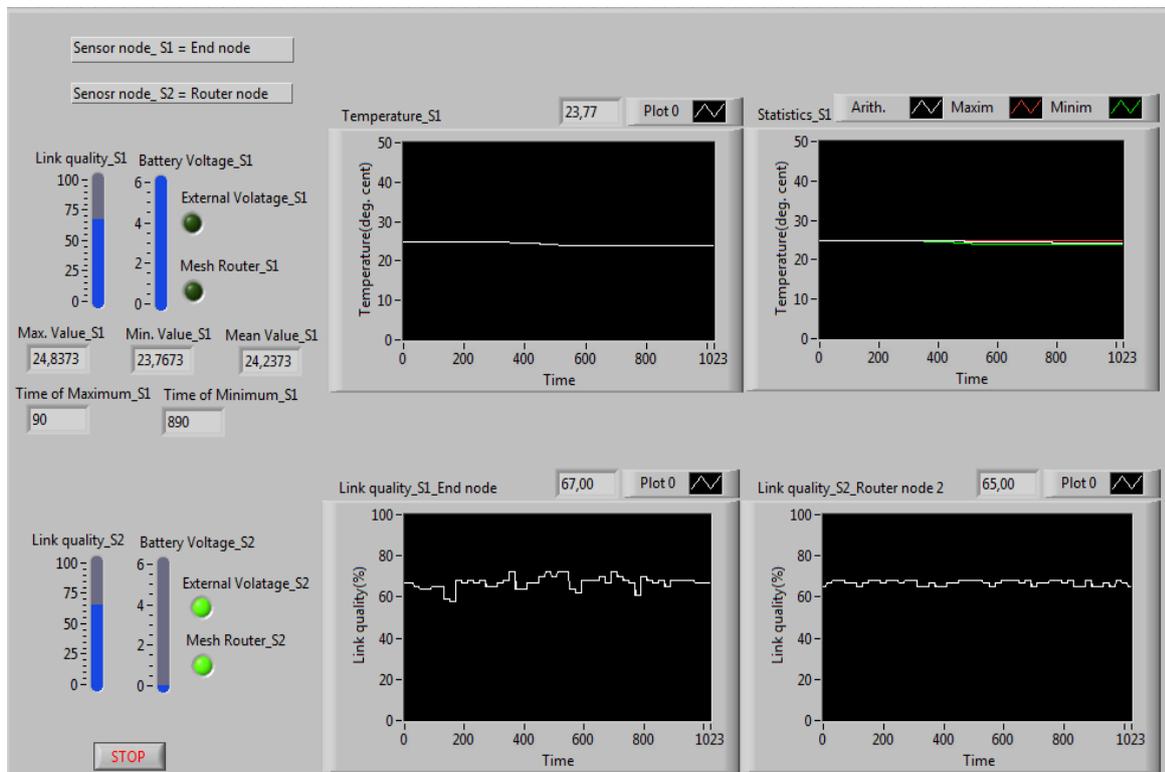


Figure 6.18 : Front panel consisting temperature statistics for end node and link quality statistics for both end node and router node

Mesh router boolean indicator for sensor node 2 was highlighted indicating the operation of router mode and that of sensor node 1 was not highlighted indicating the operation of the end node. Link quality of both nodes were more than 55%, indicating fair link quality. Statistical analysis for end node showed that, maximum environmental temperature was 24.8°C at 90th sample time, minimum temperature was 23.7 °C at the 890th sample time and average temperature throughout observation duration was found to be 24.2 °C. Current link quality for end node 1 and 2 were 67% and 65 % respectively. A Boolean indicator for external voltages indicates that, router node was operated by external power supply. Battery voltage of the end node was found to be 6 V. Statistical scopes for end node consist of green, red and white color. These represent minimum value, maximum value and arithmetic mean value respectively.

7 WSN Implementaion Issues

European Science Foundation (ESF) has organized a workshop in April 2004 in order to investigate research in WSN and its practical implications in Europe. Academic researchers and representative from different European country were participated and concluded with important dimensions of the sensor network design [40]. Some of these dimensions of WSN design are discussed below. These dimensions are the issues that need to be addressed while implementing WSN.

7.1 Deployment

The deployment of nodes in a given environment can be done in two ways. They are random deployment and fixed deployment. If nodes are installed haphazardly throughout the physical environment then they are considered to be random deployment, whereas, if nodes are installed with proper calculation and budgeting in a predefined location then it is considered as fixed deployment. Nature of deployment is either continuous (more nodes are deployed at any time during the operation of network) or fixed time.

7.2 Mobility

In WSN, the individual sensor nodes are assumed to be static. However, use of WSN in moving equipment demands the mobility feature. When a sensor changes its position during operation time, particular mobile node is allowed to use another frequency transmitted by adjacent AP. This means, nodes use the concept of hand-over used in cellular technology [41]. Mobility in WSN leads change in working environment and has more or less impact on WSN network architecture design, working protocols, range and power of transmission.

7.3 Cost, Size and Energy

The cost, size and energy of WSN depend on the application. Some applications require microscopic sensor nodes, whereas some require relatively big nodes with local processing and storing features. Microscopic sensors are used in military applications. They are cost effective, small and consume less power but do not support local processing. Local processing features on the nodes help to reduce communication overhead, especially over low bandwidth links by pre-processing, extracting and transferring useful processed data rather than whole raw data [42]. Big node with local processing and storing features are expensive and consume more energy.

7.4 Communication Modality

The common communication modality for WSN design is radio waves. However, there are numbers of other modalities such as diffuse light, laser, inductive and capacitive coupling and sound. Most used modality is a protocol using ISM band. Protocols using ISM bands are IEEE 802.11, IEEE 802.15.4, and IEEE 802.15.1. Zig-bee (IEEE 802.15.4) standard has a wide range and consumes less power so it is mostly used WSN communication modality.

7.5 Infrastructure

Designing sensor network is based on the infrastructure used. Sensor nodes can communicate with each other either using infrastructure or without using infrastructure for e.g. sensor node NI WLS-9163 can be connected either using infrastructure like NI WAP-3711 or using ad-hoc mode with computer. Infrastructure is simple AP or gateways installed in industries, schools and public areas.

7.6 Network Topology and Coverage

WSN using single infrastructure are considered to be in star network topology, where coverage for WSN depends entirely on its infrastructure coverage area. In a multi-hop network, the coverage for WSN depends on the sum of range supported by their sensor nodes and their spatial distributions. Using multi-hop, the network topologies that can be created are mainly; mesh, extended star and tree.

Moreover, coverage of WSN depends upon output power of the transmitter. Different countries have different regulations defined for maximum output RF-power. Output power of ISM band ranges from 0 dBm to 20 dBm [8].

7.7 Network Size

Network size of WSN varies from few nodes to numbers of sensor nodes. The number of sensor nodes, in particular, WSN depends upon interest of measurement, quality of WSN, environment and coverage area. WSN with fewer sensor nodes is flexible to relocate, to manage traffic, to upgrade and troubleshoot. Implementing WSN with large numbers of sensor nodes demands more research in designing communication protocols and routing algorithms.

7.8 Life Time

In WSN, the sensor nodes are generally placed out in the field and unattended for months or years. So, WSN deployed are expected to have certain life time. Energy supplied to the nodes

can either be managed locally by using battery or managed by supplying external power supply. WSN in a real time system and security system demands every node must last for many years. Single node failure may lead vulnerability in the networks.

Apart from above mentioned implementation issues, factors like sampling rate also play vital role in WSN implementations.

7.9 Sampling Rate

All sensor nodes have their own sampling rate specification. Sampling rate is the time used by sensor to measure the physical quantities. Generally, sampling rates are less if a single node is considered, but it has considerable effects when multiple nodes are implemented.

In WSN, parent node must handle data from its child node. If there are 40 child nodes then parent node is responsible to transmit and receive 40 times as much as it would have been a single child node. Due to this, sampling rate has more impact on topology design. For example, National Instrument device NI-WSN 3202 has the sampling rate of 1 samples/sec [3]. If 20 such nodes are connected to gateway then overall sampling rate will be 20 samples/sec, which may not be practically feasible. Another problem would be, if high sampling rate data like picture, video and vibration are to be measure, WSN design fails.

Some solutions can be implemented in order to measure the physical parameters with a high sampling rates. They can be followings:

- a) Various forms of spatial and temporal compression of data can be done before transmitting. These compressed data are recovered in receiving sections.
- b) Temporary storing of data can be done in local nodes and allowed to transmit over network when bandwidth becomes free.

7.10 Security

WSN uses RF signal as a physical transmission medium. A wireless medium adds security challenges than that of wired system. Due to this, sensitive data needs to be protected from unauthorized access. There are many common security practices, which are based on network security components like wireless security protocols, encryption, authentication, etc.

7.10.1 Security Management

Management of security is done by incorporating appropriate security components as per the nature of networks (public/private, W-Fi/Zig-bee). *Figure 7.1* shows the secured WSN architecture. This architecture comprises of WSN, Network Manager and Security Manager. AP or Gateway is connected to Network Manager and Security Manager. Security Manager plays a vital role to maintain secured networks by authenticating network devices and by generating, storing and managing encryption keys.

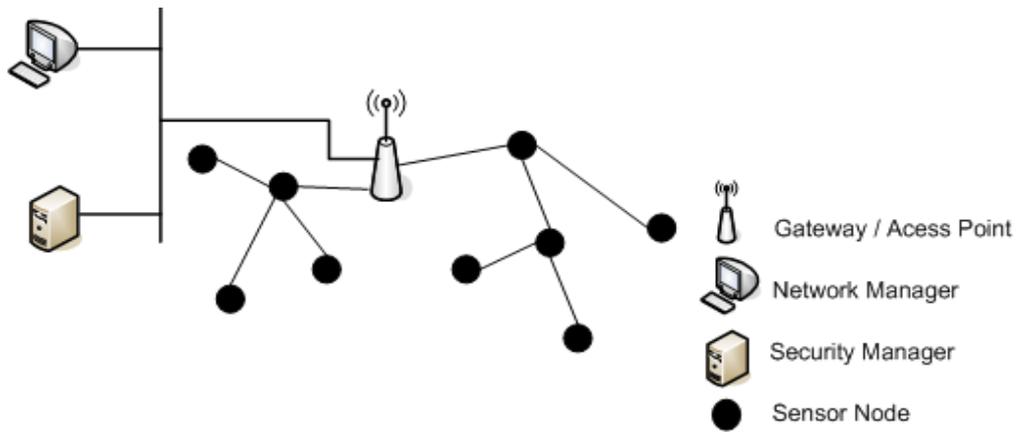


Figure 7.1: WSN Architecture with security components [43]

Different transmission protocols have different security types. For example, NI Wi-Fi DAQ 9163 device can support up to the highest commercially available security IEEE 802.11i known as Wi-Fi Protected Access 2 (WPA2) Enterprises along with IEEE 802.1X authentication and Advanced Encryption Standard (AES) encryption algorithm. However, lower security features like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) are also available for this device [44]. Most sensitive Wi-Fi WSN networks in military and industrial application uses advanced security management policies with at least one authentication server running a Remote Authentication Dial-In User Service (RADIUS). Less sensitive Wi-Fi WSN uses simple network security that means, protocols could be WEP or WPA rather than IEEE 802.11i and encryption key could be Temporal Key Integrity Protocol (TKIP) rather than AES.

7.10.2 Security Management Requirements

Unsecured WSNs can suffer unauthorized access to the resource, data and information. Person or system attempting unauthorized access is called attackers, and the process is called attack. Managing WSNs security in order to avoid attack demands following requirements to be addressed [45].

7.10.2.1 Authentication

Authentication is the way to validate and identify user, device or client of the networks. Each device needs to be authenticated in order to use the resources. Authentication helps a receiver to ensure data and control information are originated from valid source.

7.10.2.2 Encryption

Process to modify data or information such that it can be read or identified by intended user, device or client is called encryption. Strong encrypted keys and effective key management scheme are used to encrypt data prior to transmission. At the receiving section, receiver needs to know the proper decrypted keys to decipher the encrypted message.

7.10.2.3 Integrity and Data Freshness

Integrity refers to the change of data before it reaches to an intended receiver. Data change may occur due to communication environment, faulty nodes or intended attack by attackers. Data's freshness ensures that receiver is receiving new data in each cycle and no old data are replayed at the receiver. To ensure data freshness, time stamp is added in each packet of data.

Other requirements that are equally important for security management are listed below.

- a) Sensor nodes are capable of avoiding the intentional jamming that makes a sensor unavailable.
- b) Sensor nodes are capable of self-organizing and self-healing in different adverse environment and attack.
- c) Location information is core part of WSN. Unsecure localization scheme in WSN allows an attacker to manipulate false signal strength.

7.10.3 Protocol Stacks, Security Threats and Prevention

Protocol is the set of rules used by communication devices to exchange data. In WSN, sensor nodes used layer based protocol stack based on International Organization for Standardization (ISO) - Open System Interconnection (OSI) protocol [46]. However, there are lots of researches going on to determine perfect protocol stack for WSN. Sensor node protocol stack based on ISO- OSI protocol is given in *Figure 7.2*.

Wood and Stankovic conducted research to outline the possible attacks and prevention in first 4 layers of the protocol stack [47].

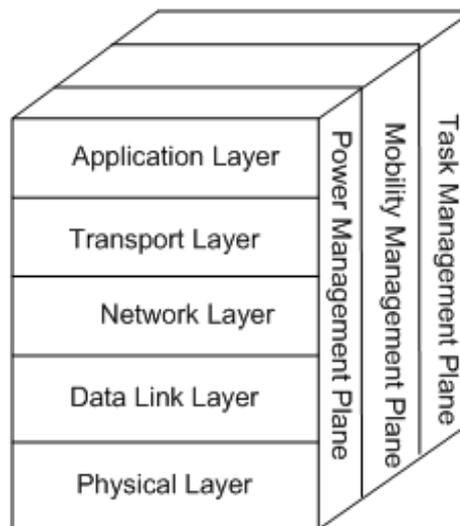


Figure 7.2: Sensor node protocol stack [46]

7.10.3.1 Physical Layer Attacks

Attacks on the physical layer can be done by two ways.

- a) Jamming: Jamming is the process to interfere sensor frequency by transmitting same frequency in sensor operational area. By doing this, sensor node suffers deep interference, and data are jammed.
- b) Tampering: Tampering is the intentional way to damage and replace the existing sensor node. Physical access to sensor node and electronic tampering may reveal sensitive information like encryption keys.

Jamming can be prevented by using spread- spectrum technique or code spreading techniques. Tampering can be prevented by using special packaging for the nodes. These packaging are tampering free and very costly.

7.10.3.2 Data link layer Attacks

The possible attacks in data link layer are collisions and unfairness.

- a) Collisions: Collision is process to collide two data packets; it is somehow similar to jamming. In collision, whole packets can be damaged.
- b) Unfairness: MAC priority scheme is harmed or ill-treated such that, sensor node cannot maintain the real time deadlines causing service degradation.

Collision can be prevented by using collision detection technique or error correcting codes. Unfairness is prevented by using small frames such that, channels are captured only for small time interval and released very soon.

7.10.3.3 Network layer Attacks

Attacks in the network layer give some serious misinformation, which results in packet dropping, wrong routing information and misdirection.

All the possible attacks in the network layer can be avoided by following methods.

- a) Use of link layer encryption and authentication
- b) Use of redundant network to form a multi-path routing
- c) Use of unique key in order to establish communication between a nodes and base stations

7.10.3.4 Transport layer attacks

Flooding and de-synchronization are the terms used to describe the attacks in the transport layer.

- a) Flooding: By flooding attacks, attackers send many connection establishment requests. System responds to each request by allocating memory. As the result, memory resources of the system are exhausted.
- b) De-synchronization: In this type of attacks, control flags and sequence numbers are modified; this may lead infinite cycle of retransmitting previous erroneous message.

In order to avoid flooding, client puzzle technique can be used. In this technique, client must solve the puzzle send by the server each time they demand connection. De-synchronization can be avoided by a proper authentication scheme.

8 Discussion

This chapter discusses the result obtained in this study. The discussion is mainly focused on, protocol and topology, comparison between design 1 and design 2, transmission distance and security issues.

8.1 Protocol and Topology

Zig-bee seems to be the best protocol if range and power are considered while Wi-Fi seems to be the best protocol if data rate is considered. Zig-bee supports range up to 150 meters at the cost of lower data rate of 250 Kbps, whereas Wi-Fi supports data rate up to 54 Mbps at the cost of lower range of 30 meters. However, newest Wi-Fi technology can support 125 meters range with data rate of 200 Mbps, but this technology is not widely implemented. Bluetooth has moderate data rate of 3 Mbps with a maximum range of 100 meters.

Mesh network topology has redundant feature. Mesh topology is the combination of numbers of multi-hop networks where any node can talk with other nodes in the network. Thus, it is used in such WSN, where nodes are to be distributed in the large geographical area. Another network topology like star, tree and point to point cannot give the redundant feature and their coverage area are limited to the range of AP.

8.2 Design 1 vs. Design 2

For any transmission range of 300 meters, both designs can be used. However, Design 1 seems more expensive. The total approximated cost for Design 1 implementation is around 119102,00 NOK, whereas, the cost for implementing Design 2 is very less, and is around 18131,00 NOK. Design 1 uses Wi-Fi DAQ, which provides high bandwidth and sampling rate of 51.2 K samples per second per channel. Nevertheless, Design 2 uses Zig-bee DAQ, which provides very fewer sampling rates of 1 sample per second per channel.

For any physical quantity demanding high sampling rate Design 2 fails and for any measurement that requires transmission distance more than 330 meters, Design 1 fails. This suggests that, implementation of WSN in the area that demands both range and sampling rate is practically difficult to design, especially when ISM band is considered and vibration is the interest of measurement.

The tradeoff between a range and sampling rate can be solved by modifying the design. Use of National Instruments CompactRIO device along with third party modules [48] can give both high transmission range and high sampling rate. Doing this we can have a high sampling rate of Wi-Fi Data Acquisition (DAQ) as Design 1, high transmission distance of Zig-bee as in Design 2 and new design will be cost effective. For this, NI WLS 9234 can be used as DAQ device and SEA cRIO Zig-bee [49] can be used as transmission modules.

8.3 Transmission Distance

In star network topology, the maximum distance of communication between sensor node and gateway was found to be 23.1 meters with link quality not less than 55%. Theoretical transmission distance is 150 meters at LOS. Experiment was set up inside the hall, where LOS between sensor nodes and gateway was not possible to maintain. Instruments, machineries placed in the hall and closed surface of room where the gateway was placed, creates diffraction, reflection, refraction, scattering, shadowing and multipath fading of a signal such that their link quality degraded and overall transmission distance was decreased to 23.1 meters rather than 150 meters.

In order to increase the transmission distance, at least two sensor nodes are needed, where one sensor node act as a router and other node act as an end node. Router node that acts as the repeater links the end node and gateway. In this mode, the link quality of the end node is not depend on the position of gateway; it entirely depends on position of the router node. Hence, end node can be moved away from router node until the link quality between the end node and router node becomes 55%. The overall transmission distance was found to be sum of distance from end node to router node and distance from router node to gateway. The total transmission distance was increased from 23.1 meters to 47.1 meters at fair link quality of 55%. Thus, coverage extension was successfully achieved using a router node concept but range suggested by design 2 was not achieved.

8.4 Security

In order to use WSN in application like industrial control and monitoring, military purposes, etc., network requires minimum level of security to avoid attacks. Data needs to be sufficiently encrypted, properly authenticated and any change or replay of data during transmission needs to be identified and stopped. Jamming, tampering, collisions, unfairness, misdirection, misinformation, flooding, de-synchronization were identified as different possible attacks when referred to ISO-OSI protocol.

Jamming and tampering are physical layer attack and can be avoided by spread spectrum technique and tampering free packaging. Data link layer attacks like collision, and unfairness can be prevented using collision detection techniques and making small frame of data such that they occupy channels for very less time. Network layer attacks like packet dropping and misrouting can be prevented by encryption, authentication, multi-path routing and use of unique key. Flooding and de-synchronization are identified as major attacks in the transport layer. They are prevented by client puzzle techniques and proper authentication techniques.

9 Conclusion and Future work

After achieving thesis requirements to certain level, important conclusions were drawn out. Apart, this work also gives ideas about how this thesis can be used in future in more elaborated and innovated form.

9.1 Conclusion

The following conclusions are drawn from this study.

- a) Zig-bee provides high range of transmission but less data rate, Wi-Fi provides high data rate but less transmission distance. Bluetooth range and data rate are moderate as compared to other two.
- b) Mesh network topology support multi-hop networking where a node can talk to adjacent nodes. This feature allows redundancy in the system. Mesh topology is used when WSN needs to be implemented in the large geographical region.
- c) Wi-Fi based WSN design is expensive as it demands the large number of AP. For the same transmission distance, Zig-bee based design is cheap but suffers from less sampling rate problem.
- d) Tradeoff between sampling rate and transmission distance can be solved by using National Instrument module CompactRIO along with Wi-Fi DAQ and third party Zig-bee transmission module.
- e) 23.1 meters of transmission range between two WSN-3202 sensor nodes and WSN 9791 gateway in star topology was significantly increased to 47.1 meters using multi-hop topology where one sensor node was configured as the router node.
- f) Single node theoretical range of 150 meters was not achieved due to nature of an operating environment. LOS cannot be maintained between a gateway and sensor nodes, and signal suffers reflection, refraction, scattering, multipath fading, etc.
- g) Authentication and Encryption are two key security components of wireless networks. Each layer of ISO-OSI suffers different types of attack.

9.2 Future work

Following future work are suggested to elaborate the findings of this study.

- a) Existing wired system installed in any applications can be replaced by WSN for reliability and performance testing, co-existence problems can be studied by installing Zig-bee based WSN near to any other WSN based in ISM bands.
- b) Monitoring application can be elaborated to monitoring and control application by integrating WSN with DELTA V process management system.
- c) Small Network Management Protocol (SNMP) can be implemented in order to access data from any remote computers.

- d) LABVIEW program can be improved by adding data logging facility, database facility, and alarm handling facility.
- e) Mesh network topology can be established between sensor node and gateway by adding one more router node.

10 References

- [1] Santi P. Topology Control in Wireless Ad Hoc and Sensor Networks, John Wiley & Sons Ltd, First Edition, England, 2005; 9-10.
- [2] National Instruments. User guide and specifications NI WLS/ENET-9163, National Instruments Corporations, USA, Feb 2010.
- [3] National Instruments. User guide and specifications NI WSN-3202, National Instruments Corporations, USA, Nov 2010.
- [4] Loy M; Karingattil R; Willams L. ISM-Band and Short Range Device Regulatory Compliance Overview, TEXAS INSTRUMENTS, USA, May 2005.
- [5] Villegas M A E; Tang S Y; Qian Y. Wireless Sensor Network Communication Architecture for Wide-Area Large Scale Soil Moisture Estimation and Wetlands Monitoring, University of Puerto Rico, Puerto Rico, Aug 2005.
- [6] Bray J; Sturman C F. BLUETOOTH 1.1 Connect Without Cables, Prentice Hall Inc., Second Edition, USA, 2002; 2-4.
- [7] Hill J L. System Architecture for Wireless Sensor Networks, University of California, USA, 2007.
- [8] Castino J G. Algorithms and Protocols Enhancing Mobility Support for Wireless Sensor Networks Based on Bluetooth and Zigbee, Malardalen University, Sweden, Sep 2006.
- [9] Gutierrez J A; Callaway E H Jr; Barrett R L Jr. Low-Rate Wireless Personal Area Networks, IEEE Standards Information Network/IEEE Press, Second Edition, Jan 2007.
- [10] Wi-Fi Alliance. Discover and Learn, 2011, http://www.wi-fi.org/discover_and_learn.php, [Feb 2011]
- [11] Javvin. WLAN: Wireless LAN by IEEE 802.11, 802.11a, 802.11b, 802.11g, 802.11n, 2011, <http://www.javvin.com/protocolWLAN.html>, [Feb 2011]
- [12] Lewis F L. Wireless Sensor Networks, Smart Environments: Technologies, Protocols and Applications, University of Texas, USA, 2004.
- [13] Akyildiz I F; Wang X; Wang W. Wireless mesh network: a survey, Computer Networks, 2005;47:445-487.
- [14] National Instruments. User guide and specifications NI WSN-9791 Ethernet Gateway, National Instruments Corporations, USA, Nov 2010.
- [15] Huang J H; Wang L C; Chang C J. Deployment of Access Point for Outdoor Wireless Local Area Networks, National Chiao Tung University, Taiwan, 2003.
- [16] National Instruments. Operating instructions and specifications NI 9234, National Instruments Corporations, USA, Aug 2008.

- [17] National Instruments. NI WAP-3701/3711 User Manual, National Instruments Corporations, USA, Sep 2007.
- [18] National Instruments. Wireless Data Acquisition: Range versus Throughput, National Instruments Corporations, USA, Jun 2007.
- [19] Cheung S Y; Varaiya P. Traffic Surveillance by Wireless Sensor Networks: Final Report, University of California, USA, Jan 2007.
- [20] Tavares J; Velez F J; Ferro J M. Application of Wireless Sensor Networks to Automobiles, Measurement Science Review, 2008; 8: 65-70.
- [21] Garcia L R; Lunadei L; Barreiro P; Robla J I. A Review of Wireless Sensor Technologies and Application in Agriculture and Food Industry: State of The Art and Current Trends, Sensor, 2009; 9: 4728-4750.
- [22] Paavola M. Wireless Technologies in Process Automation-Review and an Application Example, University of Oulu, Finland, Dec 2007.
- [23] Wireless HART. IEC 62591 WirelessHART System Engineering Guide, Emerson Process Management, Revision 2, Oct 2010.
- [24] Khakpour K; Shenassa M H. Industrial Control using Wireless Sensor Networks, K.N. Toosi University of Technology, Iran, 2007.
- [25] Department of Energy. Industrial Wireless Efficiency & Renewable Energy Report, USA, Dec 2002.
- [26] Gutierrez J A; Durocher D B; Lu B; Harley R G; Habetler T G. Applying wireless Sensor Network in Industrial Plant Energy Evaluation and Planning Systems, The 2006 IEEE IAS Pulp and Paper Industries Conference, USA, 2006.
- [27] Gangone M V; Whelan M J; Janoyan K D. Deployment of a dense hybrid wireless sensing system for bridge assessment, Structure and Infrastructure Engineering: Maintenance, Management, Life-Cycle Design and Performance, 2011;7: 369-378.
- [28] Battista N D. Wireless Monitoring the Longitudinal Movement of a Suspension Bridge Deck, University of Sheffield, UK, 2010.
- [29] Sukun K; Pakazad S; Culler D; Demmel J; Fenves G; Glaser S; Turon M. Health Monitoring of Civil Infrastructures Using Wireless Sensor Networks, Information Processing in Sensor Networks, Apr 2007; 254-263.
- [30] Kim S. Wireless Sensor Networks for Structural Health Monitoring, University of California, USA, 2005.

- [31] Melo M; Taveras J. Structural Health Monitoring of Golden Gate Bridge using Wireless Sensor Network- Progress Report, University of Massachusetts Lowell, Aug 2009.
- [32] DeltaV. The DeltaV System Overviewed, Emersion Process Management, 2002.
- [33] DeltaV. DeltaV OPC.NET Server, Emersion Process Management, Jan 2011.
- [34] DeltaV. Smart Wireless Gateway, Emersion Process Management, 2009.
- [35] Pompili D; Melodia T; Akyildiz I F. Deployment Analysis in Underwater Acoustic Wireless Sensor Networks, Georgia Institute of Technology, USA, Sep 2006.
- [36] Heidemann J; Li Y; Sayed A; Wills J; Ye W. Underwater Sensor Networking: Research Challenges and Potential Applications, USC/Information Science Institute, USA, 2005.
- [37] Khodadoustan S; Hamidzadeh M. Tree of Wheels: A New Hierarchical and Scalable Topology for Underwater Sensor Networks, Sharif University of Technology, Iran, 2011.
- [38] Dong B. A survey of Underwater Wireless Sensor Networks- localization system design, Texas A&M University, USA, 2007.
- [39] National Instruments. Why Am I Losing Data When My Node Indicates an Excellent WSN Link Quality?, May 2010,
<http://digital.ni.com/public.nsf/allkb/C0B57DBB7A7512C0862575EF0058C6C9> ,
 [Mar 2011]
- [40] Romer K; Mattern F. The Design Space of Wireless Sensor Networks, Institute for Pervasive Computing ETH, Switzerland, 2004.
- [41] Molish A F. Wireless Communications, John Wiley & Sons Ltd, First Edition, England, 2005; 386-387.
- [42] Chen M; Kwon T; Yuan Y; Leung V C M. Mobile Agent Based Wireless Sensor Networks, JOURNAL OF COMPUTERS, Apr 2006; 1:14-21.
- [43] Kalita H K; Kar A. Wireless Sensor Network Security Analysis, International Journal Of Next-Generation Networks, Dec 2009; 1:1-10.
- [44] Bakken T; Pant R B; Xie P; Shrestha A. Wireless Sensor Networks Using NI Modules, Telemark University College, 2010, Norway.
- [45] Mohanty P; Panigrahi S; Sarma N; Satapathy S S. Security Issues in Wireless Sensor Networks Data Gathering Protocols: A Survey, Journal of Theoretical and Applied Information Technology, 2010; 14-26.
- [46] Kaplantzis S. Security Models for Wireless Sensor Networks, Monash University, Australia, Mar 2006.
- [47] Wood A D; Stankovic J A. Denial of Service in Sensor Networks, Computer, Oct 2002; 35:54-62.

[48] National Instruments. CompactRIO Third-Party Modules, National Instruments Corporation, USA, Dec 2010.

[49] SEA. Zigbee, <http://www.sea-gmbh.com/en/products/compactrio-products/sea-crio-Modules/wireless-technology/zigbee/>, [Apr 2011].

11 Appendices

Appendix 1: Task description.



Telemark University College

Faculty of Technology

FMH606 Master's Thesis

Title: Wireless Sensor Networking with lab-scale intermediate measurement node for extension of WSN Coverage

TUC supervisor: Saba Mylvaganam, Hans p. Halvorsen, Frode Skulbru NI

External partner: National Instruments

Task description:

This study will have focus on wireless sensor network. However to facilitate the implementation of wireless networking an overview of existing standards in wireless networking will be essential. The topics to be addressed for an in depth study and demonstration are:

- (1) Overview of the current standards scenario with essential technical details
- (2) Pros and cons of wireless networking and especially wireless sensor networking in the industries
- (3) At least four case studies of wireless sensor networking as practised in the industries
- (4) Lab scale demo unit consisting of two wireless nodes communicating with an intermediate measurement node as a router
- (5) Identifying and describing issues related to implementation of wireless sensor networking, management of and their security
- (6) Delivery of written thesis following the guidelines from TUC

Task background:

Wireless networking has already penetrated the industries in various forms, for data transfer, communication and sensor networking. With the increased interest for wireless networking in general in the industry, naturally there is a need for looking into strategies of enhancing performance of wireless networking with respect to the possibility of integrating wireless networking with existing wired networks, extending coverage distance of wireless networks etc. Industrial users are interested predominantly in the following areas of study in wireless networking in general: standards and their convergence to a form accepted by major actors in

Adress: Kjølnes ring 56, NO-3918 Porsgrunn, Norway. **Phone:** 35 57 50 00. **Fax:** 35 55 75 47.



the industries, implementation of wireless networking, management of wireless networks and their security

Student category:

For SCE students with communication background and with good knowledge of National Instruments Wireless Sensor Networking Modules and their practical applications using LabVIEW.

Practical arrangements:

EIK / HiT has the latest NI Wireless Sensor Networking Modules and has close interaction with the National Instruments, Norway. Necessary hardware and software will be provided by HiT. Work will be performed in Sensor Lab and Flow Lab. Possible interaction with organisations and research groups working with similar problems in Norway and abroad.

Filename FMH606_WSN_Saba_Mylvaganam_6.rtf

Signatures:

Student (date and signature):

Supervisor (date and signature):

Agmt 01.02.2011

M. Kanary

01.02.11

Appendix 2: National Instruments price list.



National Instruments Norge
Postboks 177
1371 ASKER
Tlf nr: 66 90 76 60
Fax nr: 66 90 76 61

1 / 3

Høgskolen i Telemark
Rabin Bilas Pant
Kjølnes Ring 56
3918 PORSGRUNN

Asker 31-01-2011

Tilbudsnr. 1235753 - 1

Vi har gleden av å tilby Dem følgende;

Alt.	Antal	Artikelnr	Beskrivelse	Listepris	Rabatt	Total pris
1	1	780997-11	NI WSN-3202, 4-Ch, 16-bit, $\pm 10V$ Analog Input Node - International w/ 4 DIO channels. Provides selectable input ranges and external sensor power up to 12V, 20mA. Leveringstid Ca: 5 - 10 dager for lagerførte artikler Opprinnelsesland : HUNGARY	3.099	10.00%	2.789 NOK
2	1	780996-11	NI WSN-9791, WSN Ethernet Gateway, 9-30V powered - International Version, 9-30V DC powered, Industrial temperature and shock & vibe ratings. Outdoor range up to 1000m with line of sight. Leveringstid Ca: 5 - 10 dager for lagerførte artikler Opprinnelsesland : HUNGARY	6.299	10.00%	5.669 NOK
3	1	780471-01	cRIO-9073 8-Slot Integrated 266 MHz Real-Time Controller and 2M Gate FPGA Leveringstid Ca: 1 - 2 dager for lagerførte artikler Opprinnelsesland : HUNGARY	12.599	10.00%	11.339 NOK
4	1	781093-01	NI PS-15 Power Supply, 24 VDC, 5 A, 100-120/200-240 VAC Input Leveringstid Ca: 2 - 5 dager for lagerførte artikler Opprinnelsesland : China	1.699	10.00%	1.529 NOK
5	1	780507-01	NI WLS-9234 IEEE 802.11b/g Wireless Dynamic Signal Analyzer, SW Selectable IEPE & AC/DC Input, 4 Ch, 51.2 kS/s/ch, 24-Bit, $\pm 5 V$, and NI-DAQmx Software Leveringstid Ca: 12 - 20 dager for lagerførte artikler Opprinnelsesland : HUNGARY	16.399	10.00%	14.759 NOK
SUM						38.086 NOK
Frakt						164 NOK
VAT						9.062 NOK
Totalt						45.312 NOK

Betalingsbetingelser 30 dager etter godkjent kredittsjekk
Gyldig til og med 02-03-2011
Leveringstid Ca. 2-3 dager for lagerførte artikler, eller 2-4 uker
Se vedlagte salgsvilkår: Neste side