Intermediate Measurement Node for Extension of WSN Coverage

Rabin Bilas Pant[1], Hans Petter Halvorsen[1], Frode Skulbru[2] and Saba Mylvaganam[1]

[1]*Faculty of Technology, Department of Electrical, Information Technology and Cybernetics, Department of Energy and Environmental Technology, Telemark University College, Porsgrunn, Norway; e-mail: saba.mylvaganam@hit.no*
[2]*National Instruments Norge Lensmannslia 4, 1386 Asker, Postboks 177, N-1371 Asker, Norway*

Received 15 January 2013; Accepted 3 June 2013

Abstract

Wireless Sensor Networks (WSN) are considered as viable options for data communication for various monitoring and control applications in industries. Improvements in transmission range, security issues, real time monitoring and control issues, system integration and coexistence with other WSN systems are some of the main issues limiting their widespread usage in the industries. After a brief literature survey on some of the recent WSN applications and security management, two designs of WSNs based on Wi-Fi and Zig-bee are presented in this paper. Wireless Distribution System (WDS) and router mode are used in Wi-Fi based and Zig-bee based designs respectively. Zig-bee based design was economic but supports lower sampling rate. Wi-Fi based design was expensive but supports 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 to 47.1 m with a link quality more than 55%. Since maximum sampling rate of Zig-bee modules is 1 Sample/s per channel, monitoring measurands

Journal of Cyber Security and Mobility, Vol. 2, 29–61.

demanding high sampling rates are deliberately avoided in this work. In both topologies, temperature is the only measuarand handled by both WSN solutions in the solutions presented here.

Keywords: WSN topologies, Wi-Fi, Zig-bee, multi-hop WSN, indoor transmission, sensor node.

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 Standarization
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
S/s or Sa/s	Sampling rate sample/se
SIG	Special Interest Group

TKIP	Temporal Key Integrity Protocol
TUC	Telemark University College
VAC	Voltage Alternating 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

1 Introduction

A radio frequency (RF) network consisting of sensors, transceivers, machine controllers, microcontrollers and devices facilitating user interfaces is frequently called a Wireless Sensor Network (WSN). Sensors in a WSN are spatially distributed entities monitoring process or environmental parameters such as flow, gas concentration, vibration, pressure, motion, temperature, etc. These parameters will be fused using different sensor fusion strategies at selected nodes or at a dedicated hub in the WSN. WSN has to have at least two nodes communicating with each other. However, in a typical WSN, the numbers of nodes are much than two depending upon the measurement strategies and environments being monitored.

WSN has attracted the attention of both the academia and industries from the late 90s. Some famous prototype smart sensors like Berkeley motes and Smart Dust and solutions based on them have already been implemented [1]. WSN solutions using smart sensors are also commercially available from Crossbow, Philips, Siemens and National Instruments.

Since there are many diverse actors and users involved in the design, development and use of WSN, there is an increasing need for standardization in the field of WSN. 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. In spite of the advantages in using WSN, two of the major disadvantages are security and coverage area or transmission distance. Since radio communication is used, unauthorized individuals can easily can get access to

valuable and sensitive information. A secured network is mandatory in most of the applications today.

There are some important implementation issues in conjunction with the commissioning of any WSN solution. Issues like deployment, mobility, topology, coverage area, life time, sampling rate, cost, energy, etc., have to be looked into when deciding for a WSN based solution for a given problem. Before designing any WSN, the user has to understand its measurement type, its area of coverage, mobility requirement, and budget and then consider design factors like topology, deployment, life time, sampling rate and transmission protocol.

In WSN-application areas like underwater monitoring, bridge structural monitoring, etc., transmission ranges required are much higher than in closed industrial fields, to achieve a strong enough signal link between measuring and monitoring locations.

In most WSN, ISM band frequency is used. One of the limitations of ISM band is the limitation on the output power of antenna 20 dBm [4], the consequence of which is the limits set on coverage areas for the different nodes. WSN using National Instrument Zig-bee devices can provide the highest range of 300 m in America and 150 m in Europe [3] at the cost of reduced 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. A mesh network can provide redundancy in the WSN based network. Another way for coverage extension is the use of multiple Access Point (AP) to create a Wireless Distribution System (WDS). In a WDS system, each AP can communicate with adjacent APs and its associated sensor nodes.

2 Standard Scenario of WSN

Depending on the application areas and the prevailing specific demands on the different properties of WSN, some standardization needs to be strived for, particularly from the point of view of the end-user. Very often, network topology used, bandwidth offered or needed for a particular application, transmission protocol and compatibility of sensors to be integrated in the planned WSN are the main factors to be considered. Figure 1 shows schem-

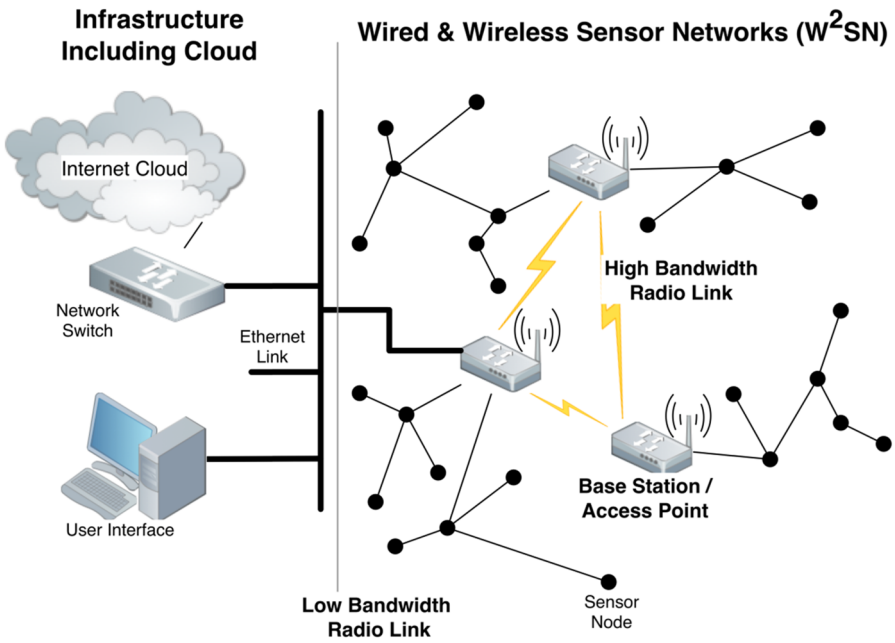

Figure 1 A classical infrastructure with a WSN Standard Transmission Protocol.

atically some of the implications of these demands on WSN in the context of a possible integration of two sub-modules: classical infrastructure and wired and wireless sensor networks.

Classical infrastructure is very often an already existing network structure (predominantly wired with some elements of wireless architecture) with or without internet connectivity. Classical structure may be a simple private or enterprise specific network used for communications and data exchange. Sensor networks as understood in the context of WSN are generally entities spatially distributed, autonomous and connected to each other in an appropriate topology. The different groups of sensors are connected to access points connecting the sensors to end users. End user can monitor and control the process if required. Each access point takes care of the signal traffic and management of signal flow for its group of sensors. In Figure 1, one access point is shown to be connected to end user.

Numbers of sensor nodes and access points differ depending on the type of measurements, environment and coverage area.

Table 1 Zig-bee specifications; Binary Phase Shift Keying (BPSK, Offset Quadrature Phase Shift Keying (OQPSK).

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

Handling scalar data such as temperature, humidity, pressure, and vibration can be done at low sampling rates, although vibration data will involve relatively higher sampling rates compared to the other parameters. Obviously, image and video data will need still higher sampling rates. As a consequence WSNs are normally used with measurands needing lower sampling rates. The advantages of low scanning rates in a given WSN based measurement are low power and low bandwidth requirements. These are some of the reasons for the deployment of Industrial, Scientific and Medicine (ISM) band in WSN applications. ISM band (2.4 GHZ band) needs no special license and is the choice of Wi-Fi, Zig-bee, Bluetooth and Wireless Hart. As our study uses Zig-bee and Wi-Fi, the following description addresses only these two protocols.

2.1 Zig-bee

Zig-bee is a low cost solution, based on IEEE 802.15.4 standard with ultra-low complexity, and extremely low-power wireless connectivity for portable devices [9]. Important features of Zig-bee are summarized in Table 1.

2.2 Wi-Fi

Wi-Fi is based on IEEE 802.11 protocols operating in ISM bands of 2.4 GHz and 5 MHz [10]. There are five types of Wi-Fi protocols: 802.11, 802.11a, 802.11b, 802.11g, 802.11n. Their ranges vary from 30 to 125 m and data rate varies from 2to 54 Mbps. The newest technology is now 802.11ac (although not commonly available) with even higher data rate. Wi-Fi specifications are summarized in Table 2.

2.3 Standard Network Topology

Arrangement and connection of nodes (circuit elements, sensors, computers, etc.) with each other is called a network topology. A WSN network topo-

Table 2 Wi-Fi specifications.

Types	Range (m)	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
IEEE 802.11ac		500 to 1000	256-QAM	5 GHz

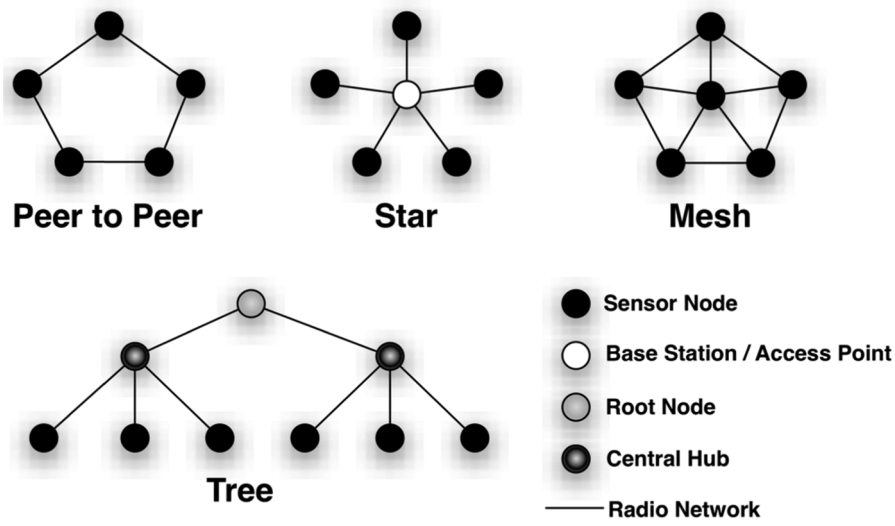

Figure 2 Main network technologies used in WSN applications.

logy indicates how sensor nodes are connected to each other or hubs or base stations. Network topologies include star, ring, fully connected, bus, tree and mesh [12]. Our focus is on peer to peer, star (single point to multipoint), mesh and tree network topologies, which are schematically presented in Figure 2.

In peer to peer topology, each node can communicate directly with another node without any centralized infrastructure or hub.

Remote nodes in a star network can send or receive data to a single base station. In contrast to the operation of peer to peer network, nodes in star network are not permitted to send and receive messages to and from each other. A routing algorithm is simpler in star than those used in other topologies. Some of the disadvantages in star configuration are: mandatory presence of remote nodes within radio range of base station, somewhat reduced redund-

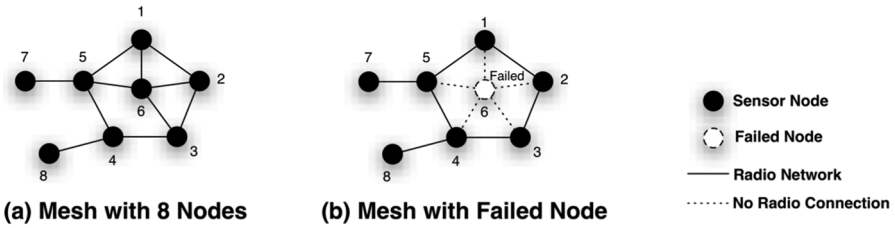

Figure 3 A mesh network with 8 nodes and functionality preserved even with failed nodes.

ancy and robustness. Base stations are central in star topology as they handle messages, routing as well as make the key decisions.

Mesh networks are distributed networks allowing any node in the network to talk to any other node in the same network, of course within the coverage area of the network. Mesh network is appropriate for large scale distributed network of sensors over geographic regions. Personal or vehicle security surveillance systems using mesh networks are described in [12].

Tree network topology is a hybrid of peer to peer network and star network topologies. A tree network topology shown in Figure 2, consists of root node and central hub. Central hub communicates with sensor nodes connected to it and root node is responsible for merging and managing central hub.

However, mesh network topology has the advantages of fault tolerance and load balancing and disadvantages of scalability [13]. As shown in Figure 3, if an individual node fails, a remote node can forward message to desired nodes via any other node in its range.

While deploying a 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 that it helps to increase the distance of communication and adds redundancy feature. It is also true that use of multiple access points can also increase distance in star network topology.

2.4 Extension of WSN Coverage

As described above, the accessible range between source (sensor node) and sink (monitoring node) varies with the transmission protocols used. Zig-bee protocol offers highest transmission range at the cost of lower sampling rate.

Zig-bee devices have coverage up to 300 m. Wi-Fi devices have coverage up to 30 m (802.11ac is the newest, range depending on power levels can approach a couple of km). One obvious method of increasing coverage range is to use higher transmitting power and antennas with more directionally enhanced characteristics. Different countries have varying limits on the maximum output power allowed to be transmitted in ISM bands thus restricting the use of high power directional antennas. Maximum output power allowed in the USA is 50 mW thus extending the maximum range with Zig-bee to 300 m. In Europe and most of Asia the allowed maximum output is 10 mW with an associated maximum range of 150 m [14].

Coverage range can also be extended by adding an additional module in the existing infrastructure between source and sink nodes. This additional module functions as a repeater or router. Access point can be used as an intermediate module in Wi-Fi based WSN and router in Zig-bee based WSN. These two methods are presented in this paper.

2.5 Designing WSN for Coverage Extension

In conjunction with the extension of WSN coverage, the task is to measure any physical quantity at points 300 m away from monitoring stations.

3 Design Alternative Using Wi-Fi

In this design, the concept of WDS is used. WDS is based on the introduction of a new AP between existing sensor node and AP, whereby the overall range of the system is almost doubled. By interlacing the existing WSNs with more APs the wireless distribution is spatially extended. Each intermediary AP acts as a 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 802.11a mode is mainly used to connect two APs in order to form WDS [15]. In the cases presented here, devices supporting IEEE 802.11 b/g multimode are used.

3.1 Technical Specification of Device Used

Devices used in the Wi-Fi design methodology are from National Instruments. NI WLS-9163 C- series carrier along with NI WLS-9234 I/O module are used as sensor nodes. This device supports 4 input channels with 24 bit resolution and maximum sampling rate of 51.2 KS/s per channel using 230

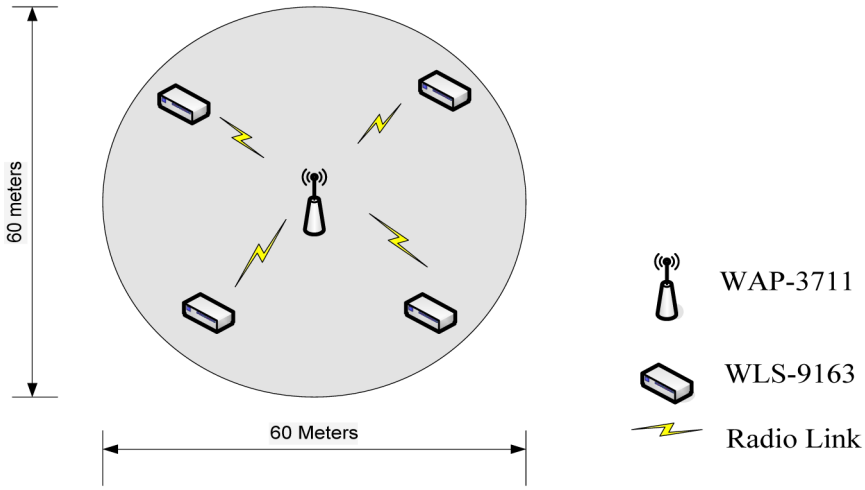

Figure 4 Radiation pattern of single WAP-3711 using omnidirectional antenna.

Volt (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 m and uses 24 Volt Direct Current (VDC) external power supply [17].

3.2 Proposed Network Architecture

When single WAP-3711 is configured, it can communicate with sensor nodes WLS-9163 up to 30 m. Omnidirectional antenna is used in this module, thus giving a circular radiation pattern of approximately 60 m in diameter, as shown in Figure 4.

WDS with omnidirectional antenna can be advantageously used to extend the coverage range. NI limits the number of WAP-3711 modules to 6 [18]. Each WDS has an overlapping distance of 5 m, such that first WAP- 3711 has range of 55 m and second, third, fourth, fifth have range of 50 m and the last WAP-3711 has range of 25 m. Last WAP-3711 has a range of 25 m because we can use only one side of the circular pattern facing the other modules as shown in Figure 5. This last WAP-3711 is connected to the computer. First WAP-3711 is used to communicate with sensor node WLS-9163 and all the other WAP-3711 modules are used as repeaters. The overall distance of measurement is not more than 330 m in the direction of Line of Sight (LOS).

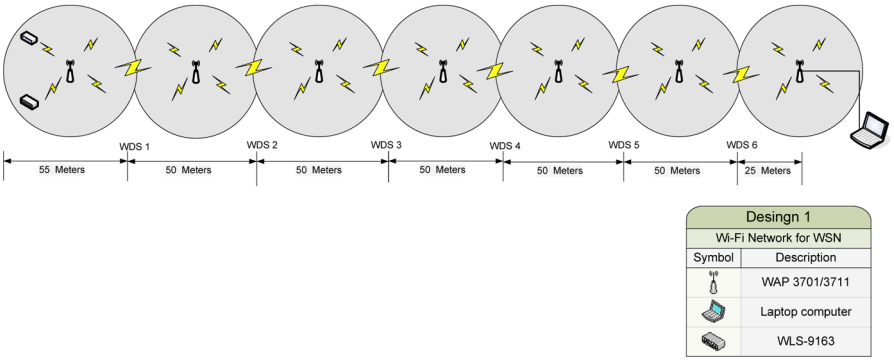

Figure 5 Connection diagram of Wi-Fi WSN using WDS system.

3.3 Design Alternative Using Zig-bee

In this design, the concept of intermediary AP used as repeater is avoided; instead, sensor node is configured as a repeater. An additional sensor node is placed in between the existing sensor node and the gateway. As a result, overall coverage range will be the sum of the coverage ranges of both. This design is based on the concept of multi-hop network. Measuring sensor nodes transfer data to the intermediary sensor nodes, which update and boost the signals and transfer them to the nearest sensor node. In the application presented here, Zig-bee (IEEE 802.15.4) protocol is used and its features are exploited in the design of the system. The advantage of using Zig-bee is mainly in its larger coverage range and cost, compared to the Wi-Fi based solution.

3.4 Technical Specification of Device Used in Design

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 S/s per channel. It requires 30 VDC 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]. As such, it requires 9 to 30 VDC external power supply. In addition, NI WSN-9791 gateway is used as a sink node, to which the measurement station is connected. The communication range is 300 m in USA and 150 m in Europe. It can support 8 end nodes in star topology and 36 end nodes in mesh topology [14].

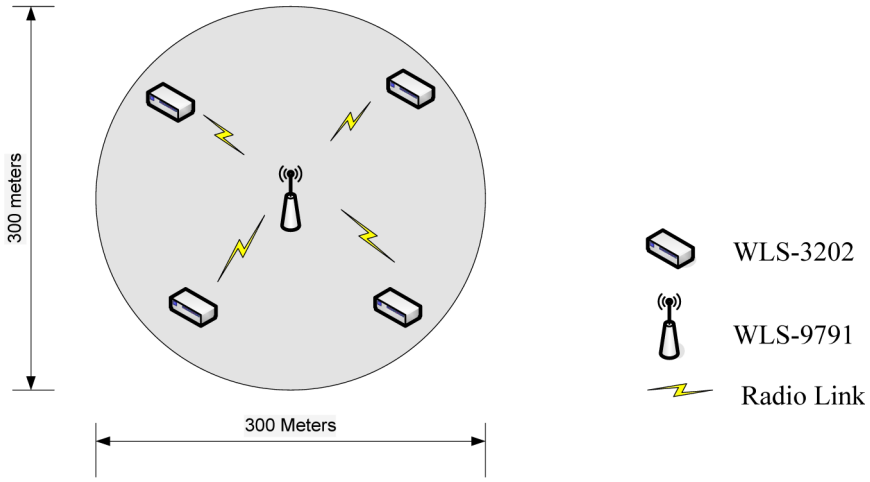

Figure 6 Radiation pattern of single WSN-9791 using omnidirectional antenna.

3.5 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 m. Because of omnidirectional antenna used in such device, radiation pattern will be a circle of approximately 300 m diameter. Figure 6 shows the radiation pattern of single WSN-9791 using omnidirectional antenna.

The omnidirectional antenna and property of sensor nodes can be used as router nodes to extend the coverage range. To test performance of coverage range extension, two sensor nodes are used thus extending the coverage range to 300 m. One sensor node is configured as router and other as measurement node. We maintain overlapping distance of 5 m between router node and gateway such that WSN-3202 router node has a range of 295 m and WSN-9791 has a range of 145 m. WSN-9791 gateway has a range of 145 m because we can use only one side of its coverage area. A monitoring station or computer is connected as shown in Figure 7, which shows the overall connection of the modules. The overall distance of measurement is not more than 450 m in LOS.

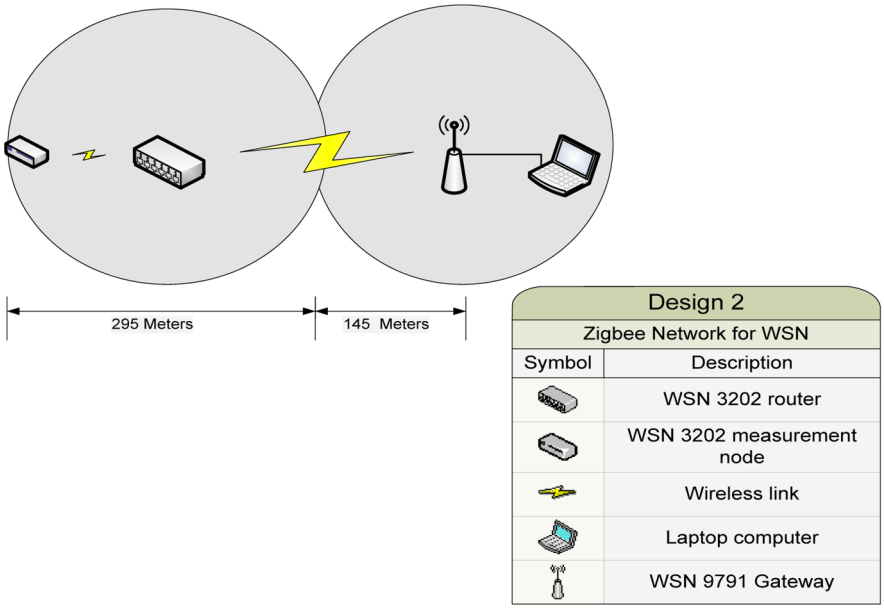

Figure 7 A connection diagram of Zig-bee WSN using sensor node as router.

3.6 Star Network Topology

Full configuration of WSN in a star network topology is given in Figure 8. Both sensor nodes directly communicate with gateway, which in turn, can be monitored by using LabVIEW program in computer. Straight Ethernet cable is used to connect gateway with a laptop computer.

The modules are configured in the LabVIEW platform. After configuring the modules and running the LabVIEW project with them, the system gives rise to the status screen for the sensor nodes and the list of analog and digital signals available in the LabVIEW project as shown in Figures 9 and 10 respectively.

3.7 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. The mobile sensor node was slowly taken away from the gateway and the link quality was monitored in LabVIEW program. National

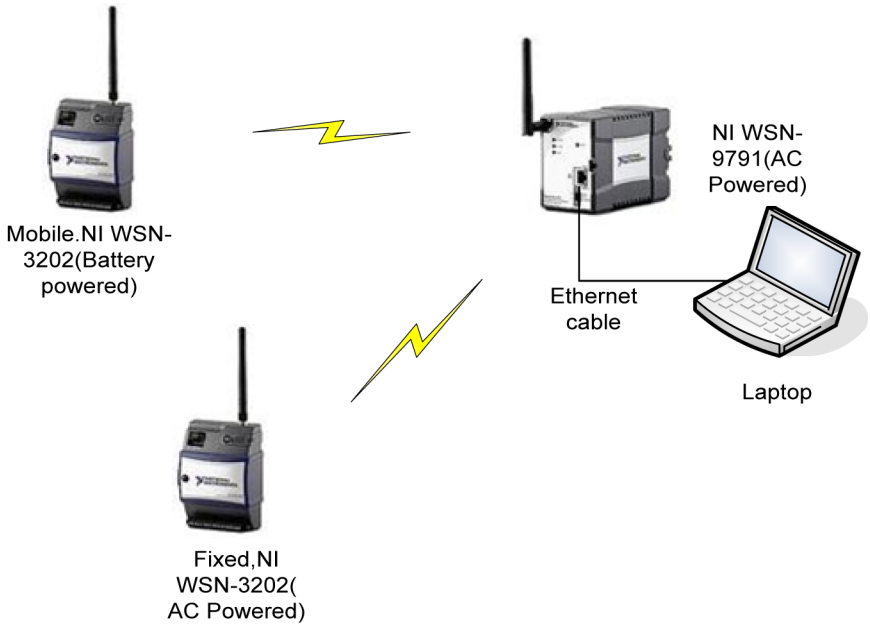

Figure 8 Full configuration in a star network topology using NI modules.

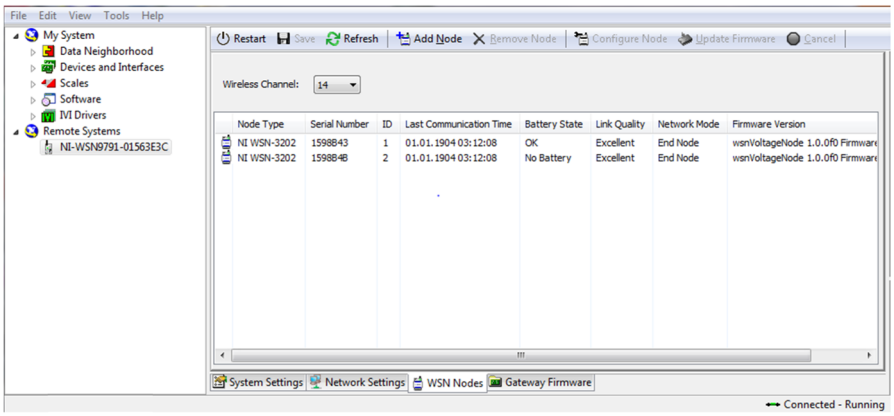

Figure 9 MAX window showing status of both sensor nodes detected by gateway. MAX (Measurement & Automation Explorer) is a graphical user interface provided by NI, to configure IVI (three types of NI drivers). MAX is usually installed with one of the NI application development environments such as LabVIEW or Measurement Studio, or with NI hardware product drivers such as NI-488.2 or NI-DAQ.

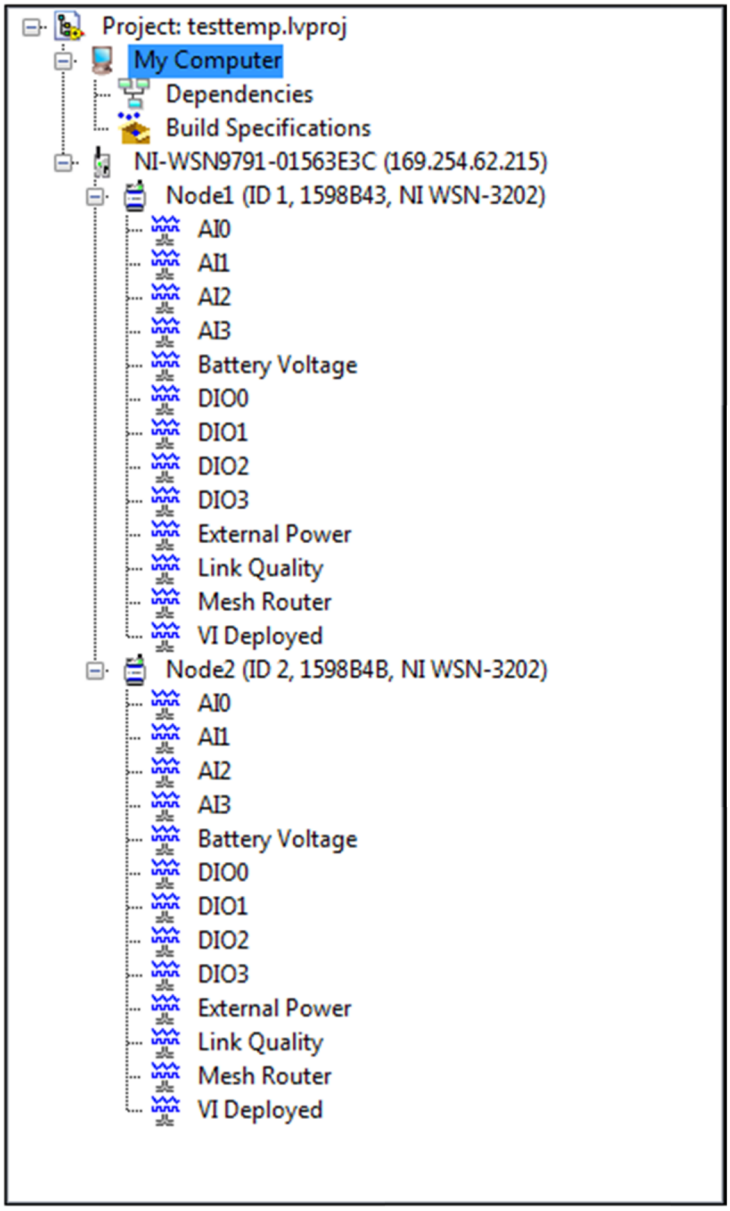

Figure 10 LabVIEW Project window showing both sensor nodes and its associated I/O.

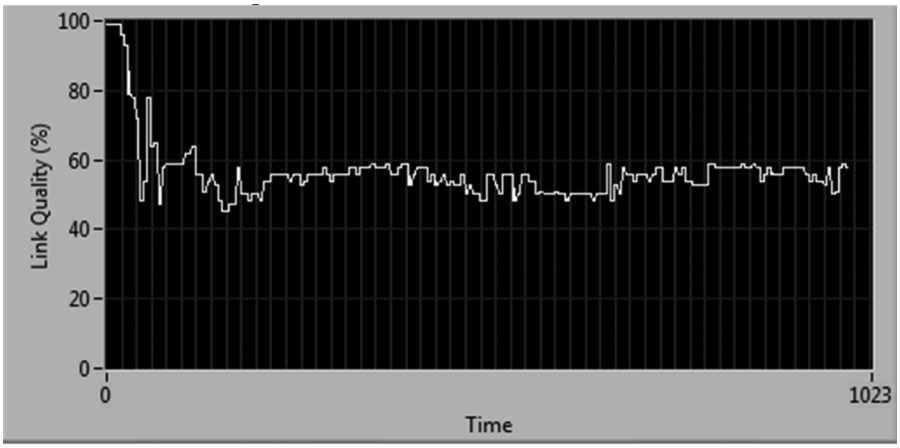

Figure 11 Time vs. link quality graph to determine maximum distance of transmission.

Instruments instructs that 55% of the link quality is supposed to be minimum signal strength and regarded as a fair signal that corresponds to a 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 the link quality was done in LabVIEW simultaneously. When the signal strength reached to 60%, the sensor node was kept stationary in that place. The distance where the sensor node was kept stationary was measured to be 23.1 m. The link quality fluctuation was measured up to 1024 samples and it was found that most of the time link quality ranges from 55 to 60%. The measurements were based on random selections. Thus, the maximum indoor distance of transmission was determined to be 23.1 m with a link quality from 55 to 60%. Figure 11 shows a LabVIEW plot for a link quality measurement. Up to 168 samples, the sensor node was mobile, then it was fixed in a particular location and other samples were measured.

Sensor node powered with AC was kept stationary at 7.9 m away from the gateway. Figure 12 shows the top view location of both sensor nodes installed and their distance from gateway.

3.8 LabVIEW Programming and Data Interpretation

The program code is presented using the block diagram as shown in Figure 13. The code was written in a while-loop. All the interested I/O variables

Figure 12 Top view of TUC building to show where the sensor nodes and gateway were installed.

were dragged and dropped to the block diagram form a LabVIEW project window. Indicators for each variable were created. 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 order to calculate arithmetic mean, maximum value, time of maximum value, minimum value, time of minimum value and histogram.

Statistics tab as in Figure 14, consists of scope for different parameters of temperature measurement like, maximum value, minimum value, arithmetic mean, and histogram for both sensors. Numerical values for these measurements along with sample time for maximum and minimum values are also presented.

1024 samples of temperatures 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 big hall, where probability of temperature fluctuations was small.

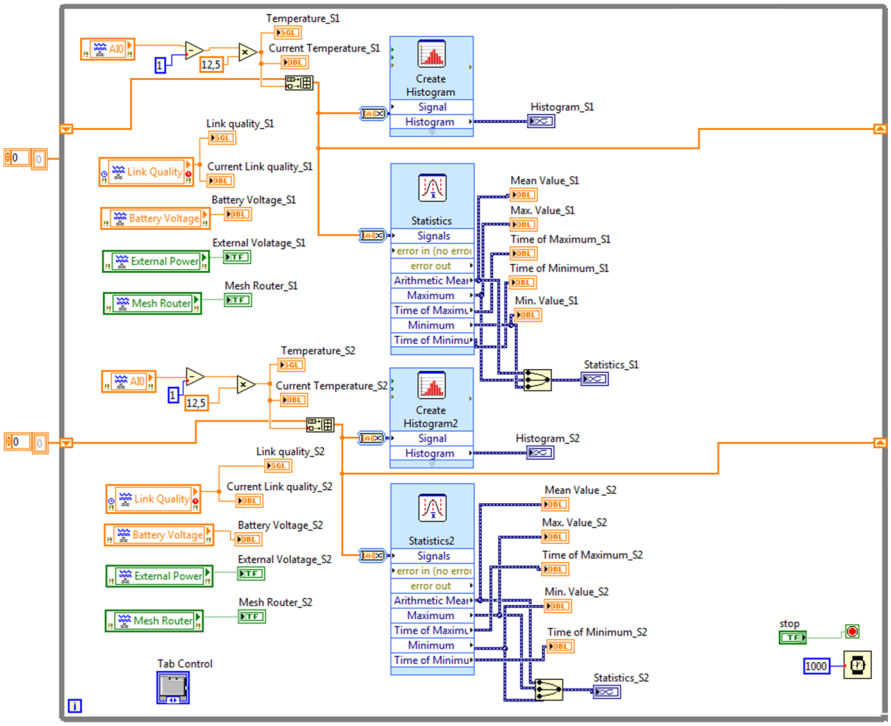

Figure 13 A block diagram of LabVIEW program used to measure temperature from two sensor nodes. NB: This VI is from a set of trial VIs from different student projects and is not an optimized or professional version.

3.9 Multi-hop Network Topology

Sensor node with external power supply was placed stationary at 23.1 m away from the gateway. A distance of 23.1 m was found in the first phase of lab work and this was the maximum distance supported by one sensor node with a 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 end node such that, end node first communicates 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 16. The gateway is connected to a laptop PC using straight Ethernet cable.

In MAX, sensor node with serial number 159884B was selected, Update Firmware tab was clicked and then from drop down menu, Mesh Router was

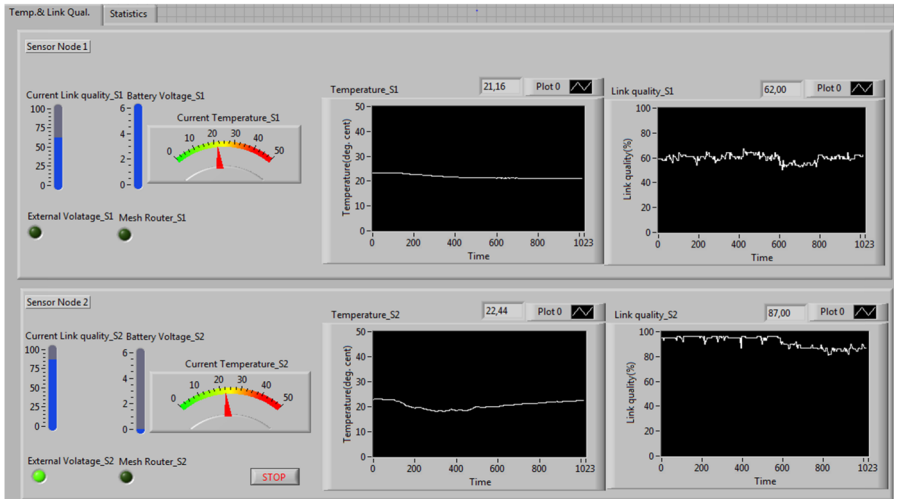

Figure 14 Front panel consisting Temp & Link Qual. tab for both sensors.

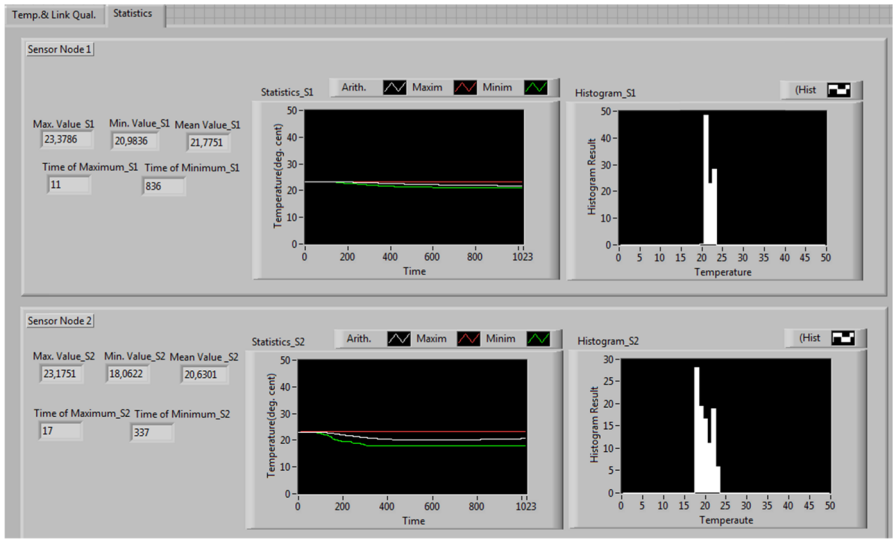

Figure 15 Front panel consisting Statistics tab for both sensors.

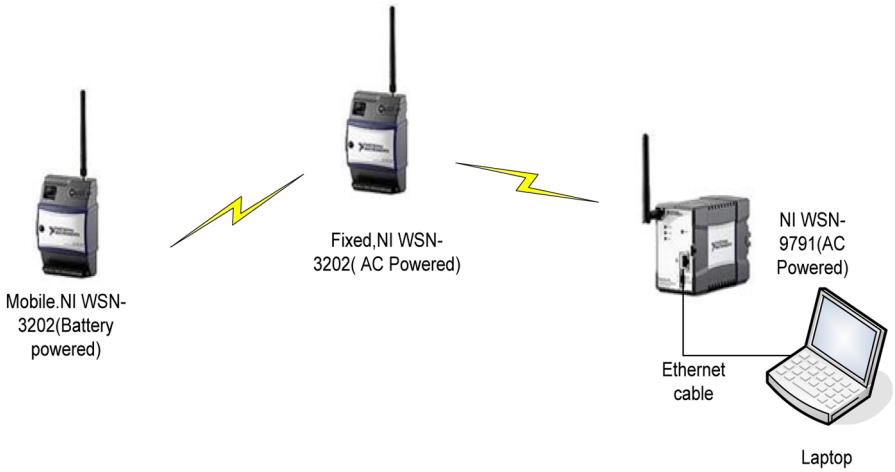

Figure 16 Full configuration in a multi-hop network topology.

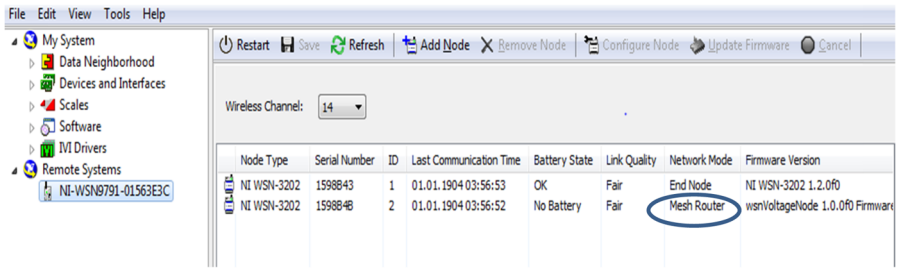

Figure 17 MAX window showing Network Mode for both sensor nodes, where one sensor node is updated as Mesh Router.

selected. Sensor node took some time before it was configured to router node. Figure 17 shows the screen shot of MAX screen when one sensor node is updated as router mode. Circle in screen shot clearly indicates Mesh Router mode.

3.10 Determining Operation of Mesh Router Mode

In order to determine the operation of mesh router node, battery powered sensor node was kept closed to router node placed at 23.1 m away from gateway as shown in Figure 18. At first, both nodes communicate directly with gateway with the link quality ranging from 55 to 65%. Reset button of end node was pressed for more than 5 seconds and released. After this,

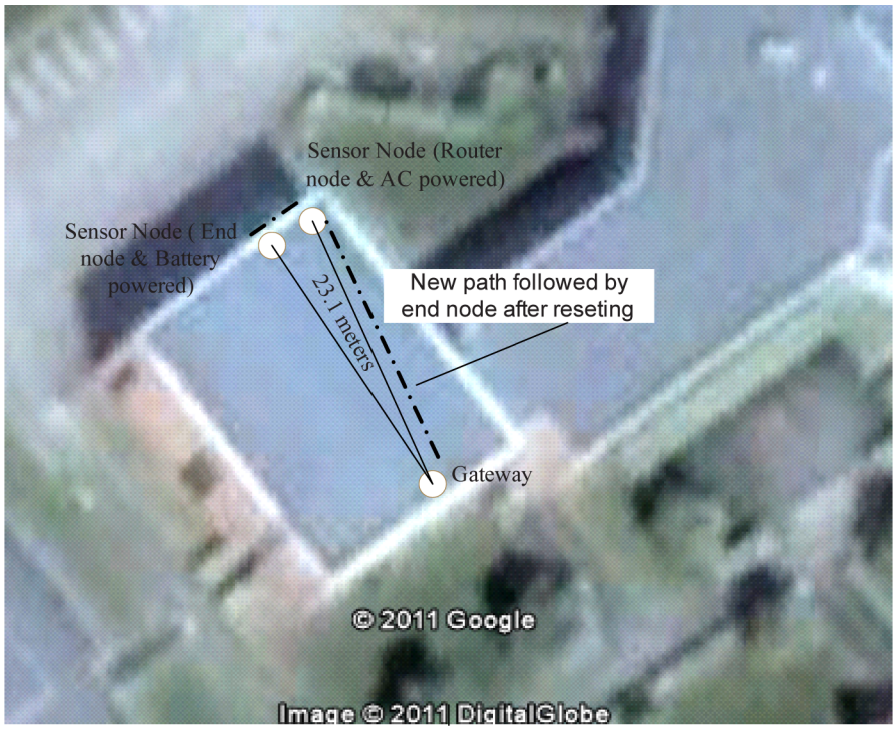

Figure 18 Top view of TUC to show where the sensor nodes and gateway were installed; and new path followed by end node after resetting.

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 gateway. The new connection path is shown by the dotted line in Figure 18.

The link quality of end node was measured in LabVIEW throughout the testing period. Figure 19 shows the link quality of end node before and after it has been reset. At first the link quality was seen to be 55–60%. After resetting it was observed that the end node link quality increased sharply and reached almost 100%. This was because of the new link that was established between the end and router nodes.

A significant change in MAX window at this point was observed. The Fair link quality of end node changed to Excellent. This also proves the improvement in link quality after the end node was reset. Figure 20 shows the change in the MAX window when the end node was rested.

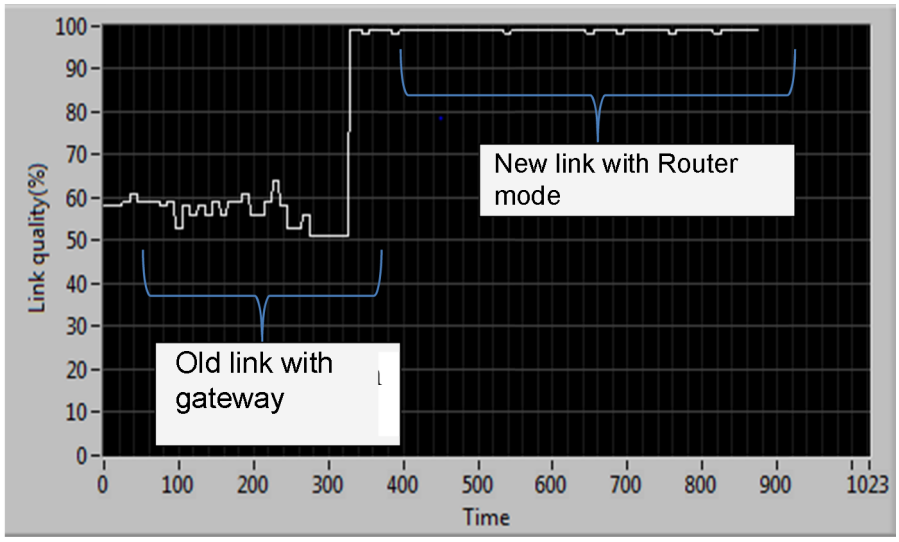

Figure 19 Time vs. link quality graph to observe improvement in link quality after end node has been reset. Note Link quality improvement by almost 50% after 300 s.

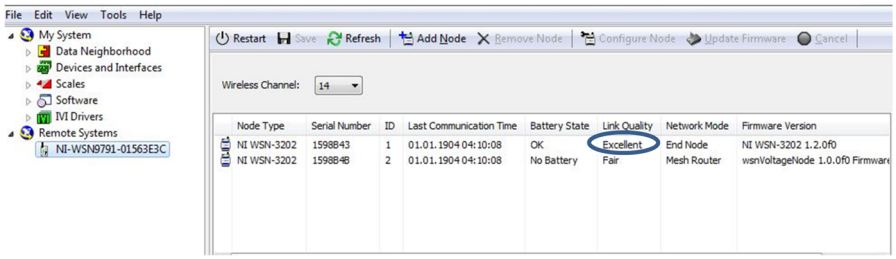

Figure 20 MAX window showing 'Excellent' link quality after the end node was reset. It is important to emphasize that this is only the link quality between the node and the router.

Taking advantages of the improved link quality, the end node was moved away from the router node until its link quality reached around 55%. Thus, the overall distance of transmission increased. Figure 21 shows the location of the end and router nodes and their distance from the gateway. The end node was kept 24 m away from router node, thus the total transmission range was measured to be 47.1 m.

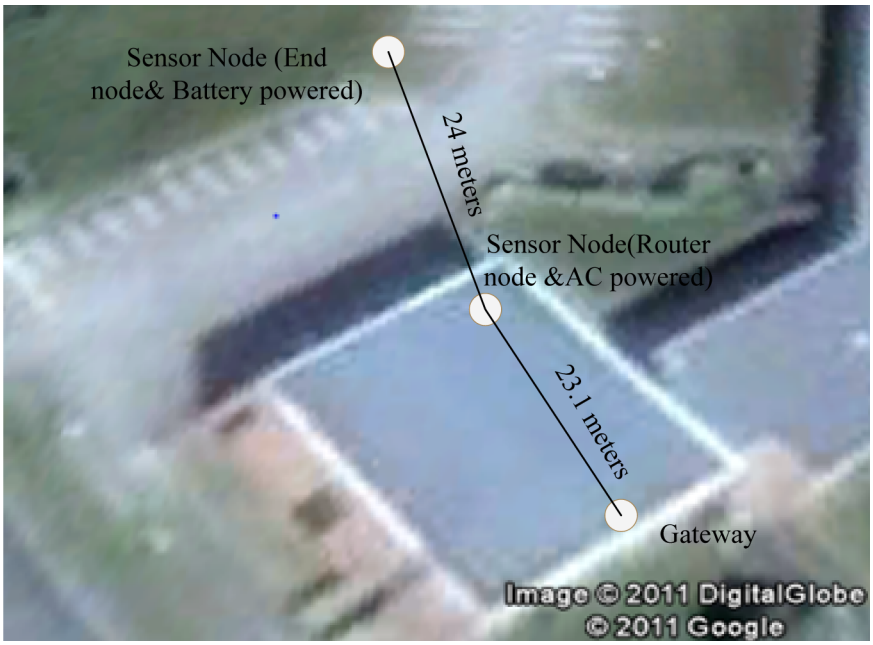

Figure 21 Top view of TUC to show where the sensor nodes and gateway were installed, and their separation distance.

3.11 LabVIEW Programming and Data Interpretation

LabVIEW code used for phase-I of lab work was modified with the provision of measuring temperature statistics for only end node. Since there were no significant variations in temperature, histogram analysis was removed. Code still has provisions for link quality monitoring, battery voltage monitoring along with Boolean indicators for external voltage and mesh router mode for both nodes. Figure 22 shows the code and Figure 23 shows the front panel of LabVIEW program used in this phase of lab work.

4 WSN Implementation Issues

The European Science Foundation (ESF) organized a workshop in April 2004 in order to investigate research in WSN and its practical implications in Europe. Academic researchers and representative form different European country were participated and concluded with important dimensions of the sensor network design [40]. Some of the dimensions of WSN design are

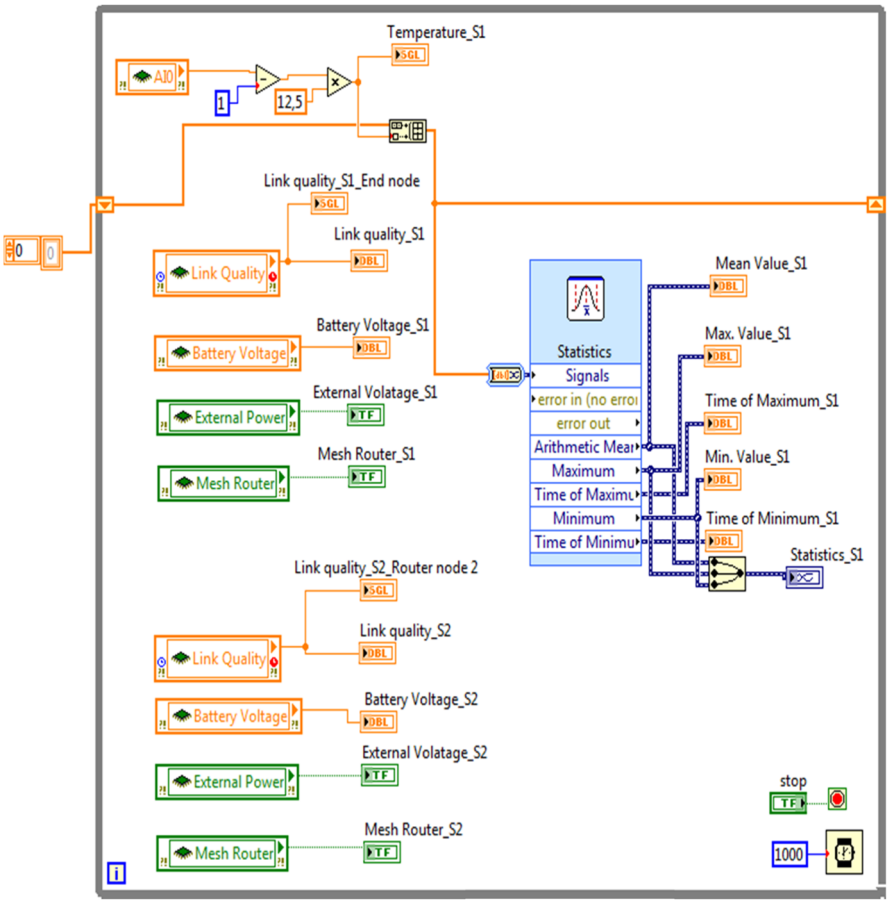

Figure 22 Block diagram of LabVIEW program used to measure temperature from end node.

deployment, mobility, cost, size, energy availability/usage and security. As there are some techniques of handling security with NI modules, this paper focusses on security issues.

4.1 Security

WSN uses RF signal as a physical transmission medium. 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

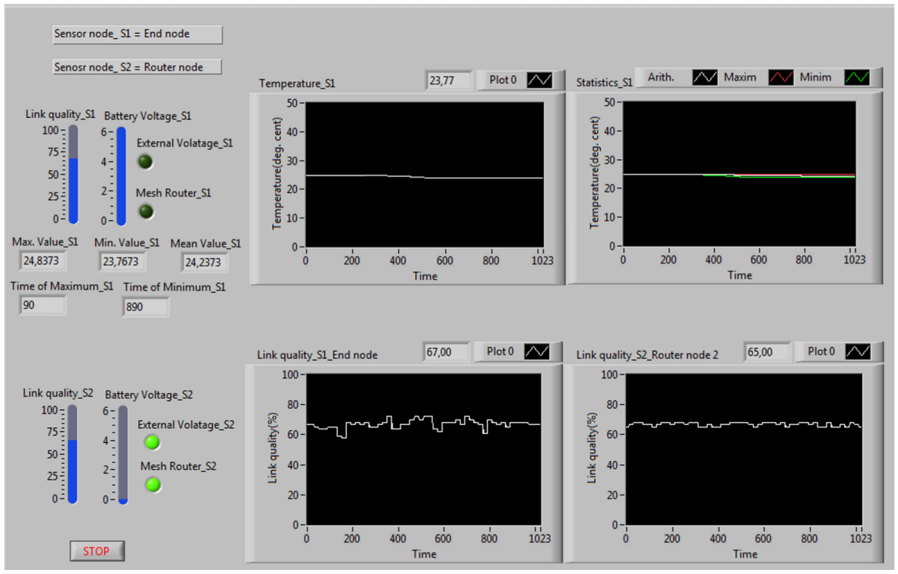

Figure 23 Front panel consisting temperature statistics for end node and link quality statistics for both end node and router node.

security practices, these practices are based on network security components like wireless security protocols, encryption, authentication, etc.

4.2 Security Management

Management of security is done by incorporating appropriate security components as per the nature of networks (public/private, Wi-Fi/Zig-bee). Figure 24 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 vital role to maintain secured networks by authenticating network devices and by generating, storing and managing encryption keys.

Different transmission protocols have different security types. For example, NI Wi-Fi DAQ 9163 device can supports 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]. The most sensitive Wi-Fi WSN

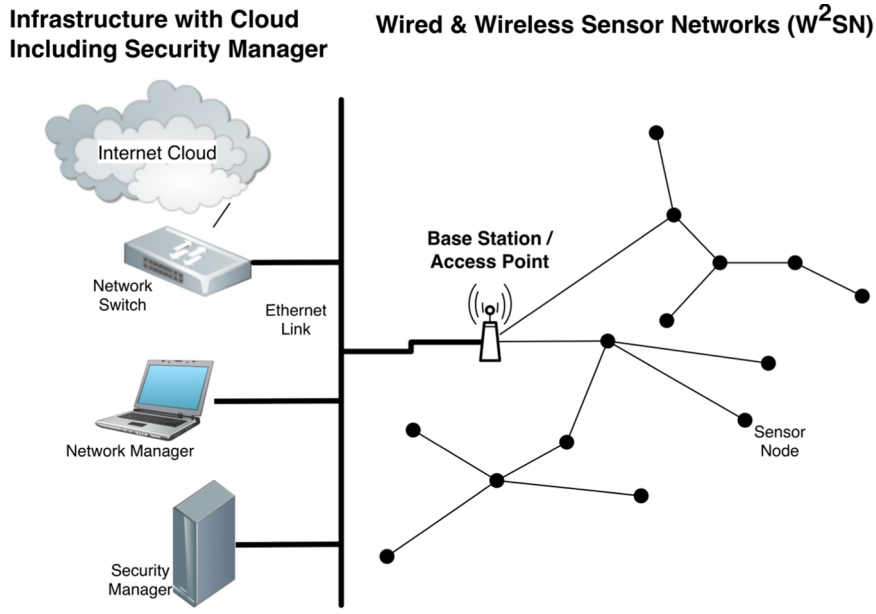

Figure 24 WSN architecture with security components. Adapted with some modifications from [43].

networks in military and industrial application use advanced security management policies with at least one authentication server running a Remote Authentication Dial-In User Service (RADIUS). Less sensitive Wi-Fi WSNs use simple network security; that means that protocols could be WEP or WPA rather than IEEE 802.11i and the encryption key could be Temporal Key Integrity Protocol (TKIP) rather than AES.

5 Design Summaries

- *Protocol and topology*
  Zig-bee seems to be the best protocol if range and power are considered and Wi-Fi seems to be the best protocol if data rate is considered. Zig-bee supports range up to 150 m 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 m. It is important to note that SEA modules for CompactRIO are available for up to 270 meters (inside)0.9 GHz (not for use in EU). The new 802.11ac standard, according to pcmag.com, article 2 of April

9, 2013, supports even up to 1.3 Gbps. Bluetooth has a moderate data rate of 3 Mbps with a maximum range of 100 m.
Mesh network topology have redundant feature. Mesh topology is 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 large geographical area. Other network topology like star, tree and point to point cannot give redundant feature and their coverage area are limited to the range of AP.

- *Wi-Fi based vs. Zig-bee based WSNs*
  For any transmission range of 300 m, both designs can be used. However, design 1 seems more expensive. The total approximated cost for design 1 implementation is around NOK 119100, whereas the cost for implementing design 2 is much lower, and is around NOK 18100 (all 2011 prices). Design 1 uses Wi-Fi DAQ, it provides high bandwidth and sampling rate of 51.2 K samples per second per channel. However, design 2 uses Zig-bee DAQ, which provides a much lower sampling rate 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 m, design 1 fails. This suggest that implementation of WSN in the area which demands both range and sampling rate is practically difficult to design, especially when we consider ISM band and vibration is our interest of measurement.
  To tradeoff between range and sampling rate can be solved by modifying our 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 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.
- *Transmission distance*
  In star network topology, the maximum distance of communication between sensor node and gateway was found to be 23.1 m with a link quality not lower than 55%. Theoretical transmission distance is 150 m at LOS. But experiment was setup inside the hall, where LOS between sensor nodes and gateway was not possible to maintain. Instruments, machineries placed in hall and closed surface of room where gateway was placed, creates diffraction, reflection, refraction, scattering, shadowing and multipath fading of a signal such that their link quality

degrades and overall transmission distance was decreased to 23.1 m rather than 150 m. In order to increase the transmission distance, we need at least two sensor nodes. One sensor node act as router and other node act as end node. Router node acts as repeater that links the end node and gateway. In this mode, the link quality of end node is not dependent on the position of gateway; it entirely depends on position of router node. Hence, end node can be moved away from router node till the link quality between 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 form router node to gateway. The total transmission distance was increased from 23.1 to 47.1 m at a fair link quality of 55%. Thus, coverage extension was successfully achieved using router node concept.

- *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 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 transport layer. They are prevented by client puzzle techniques and proper authentication techniques.

6 Conclusion and Future Work

This work is based on experimental work involving predominantly NI hardware and software to test performance quality and limitations of intermediate nodes in sensor networking with focus on continuity of the crucial functions of the network. The study was done in-campus environments with a

lot of structures hindering line of sight communications. However, the basic results indicate the feasibility of achieving improved performance of sensor networks with the help of intermediate nodes. Following the methodology used here might help beginners to learn the basic principles of hardware and software system integration in conjunction with the implementation of intermediate node based sensor networking. After successfully testing the nodes with and without intermediate nodes, the technological possibilities available with NI modules are discussed.

6.1 Conclusion

- Zig-bee provides high range of transmission but less data rate, Wi-Fi provides high data rate but less transmission distance.
- Mesh network topology support multi-hop networking where node can talk to adjacent nodes. This feature allows redundancy in the system. Mesh topology is used when WSN needs to be implemented in large geographical region.
- Wi-Fi based WSN design is expensive as it demands a large number of AP. For the same transmission distance, Zig-bee based design is cheap but suffers less sampling rate problem.
- Tradeoff between sampling rates and transmission distances can be solved by using National Instrument module CompactRIO along with Wi-Fi DAQ and third party Zig-bee transmission module.
- It is useful to see if there are any relationship between time of day and signal strength (disturbance from Wi-Fi phones, radio transmissions, etc.).
- The theoretical range of 150 m was not achieved due to nature of operating environment. LOS cannot be maintained between gateway and sensor node and signal suffers reflection, refraction, scattering, multipath fading, etc.
- Authentication and Encryption are two key security components of wireless networks. Each layer of ISO OSI suffers different types of attack.

6.2 Future Work

- 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.
- Monitoring application can be elaborated to monitoring and control application by integrating WSN with, e.g. a DELTA V process management system.
- Small Network Management Protocol (SNMP) can be implemented in order to access data from any remote computers.
- LabVIEW program can be improved by adding data logging facility, database facility, and alarm handling facility.
- Reliability considerations with data transmission in the 2.4 GHz band.

Acknowledgements

Our thanks are due to Tom-Arne Danielsen of National Instruments of Norway for his valuable comments. We are grateful to Ms. Ru Yan, former PhD research student of TUC for her help with most of the graphics in this paper. Hardware assembly and mechanical work associated work were done by our lab engineers Mr. Eivind Fjelldalen and Mr. Talleiv Skredtvedt. Rabin has now joined the industries in Nepal.

References

[1] P. Santi. Topology Control in Wireless Ad Hoc and Sensor Networks (1st ed.), pp. 9–10. John Wiley & Sons England, 2005.
[2] National Instruments. User guide and specifications NI WLS/ENET-9163. National Instruments Corporations, USA, February 2010.
[3] National Instruments. User guide and specifications NI WSN-3202, National Instruments Corporations, USA, November 2010.
[4] M. Loy, R. Karingattil, and L. Willams. ISM-Band and Short Range Device Regulatory Compliance Overview. Texas Instruments, USA, May 2005.
[5] M.A.E. Villegas, S.Y. Tang, and Y. Qian. Wireless Sensor Network Communication Architecture for Wide-Area Large Scale Soil Moisture Estimation and Wetlands Monitoring, University of Puerto Rico, Puerto Rico, August 2005.
[6] J. Bray and C.F. Sturman. BLUETOOTH 1.1 Connect without Cables (2nd ed.), pp. 2–4. Prentice Hall Inc., USA, 2002.
[7] J.L. Hill. System Architecture for Wireless Sensor Networks. University of California, USA, 2007.
[8] J.G. Castino. Algorithms and Protocols Enhancing Mobility Support for Wireless Sensor Networks Based on Bluetooth and Zigbee. Malardalen University, Sweden, September 2006.

[9] J.A. Gutierrez, E.H. Callaway Jr., and R.L. Barrett Jr. Low-Rate Wireless Personal Area Networks (2nd ed.). IEEE Standards Information Network/IEEE Press, January 2007.
[10] Wi-Fi Alliance. Discover and Learn, 2011, http://www.wi-fi.org/discover_and_learn.php, February 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, February 2011.
[12] F.L. Lewis. Wireless Sensor Networks, Smart Environments: Technologies, Protocols and Applications, University of Texas, USA, 2004.
[13] I.F. Akyildiz, X. Wang, and W. Wang. Wireless mesh network: A survey. Computer Networks, 47:445–487, 2005.
[14] National Instruments. User guide and specifications NI WSN-9791 Ethernet Gateway, National Instruments Corporations, USA, November 2010.
[15] J.H. Huang, L.C. Wang, and C.J. Chang. 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, August 2008.
[17] National Instruments. NI WAP-3701/3711 User Manual, National Instruments Corporations, USA, September 2007.
[18] National Instruments. Wireless Data Acquisition: Range versus Throughput, National Instruments Corporations, USA, June 2007.
[19] S.Y. Cheung and P. Varaiya. Traffic Surveillance by Wireless Sensor Networks: Final Report, University of California, USA, January 2007.
[20] J. Tavares, F.J. Velez, and J.M. Ferro. Applicaiton of wireless sensor networks to automobiles. Measurement Science Review, 8:65–70, 2008.
[21] L.R. Garcia, L. Lunadei, P. Barreiro, and J.I. Robla. A review of wireless sensor technologies and application in agriculture and food industry: State of the art and current trends. Sensor, 9:4728–4750, 2009.
[22] M. Paavola. Wireless Technologies in Process Automatation – Review and an Application Example. University of Oulu, Finland, December 2007.
[23] Wireless HART. IEC 62591 WirelessHART System Engineering Guide. Emerson Process Management, Revision 2, October 2010.
[24] K. Khakpour and M.H. Shenassa. 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, December 2002.
[26] J.A. Gutierrez, D.B. Durocher, B. Lu, R.G. Harley, and T.G. Habetler. Applying wireless sensor network in industrial plant energy evaluation and planning systems. In Proceedings of the 2006 IEEE IAS Pulp and Paper Industries Conference, USA, 2006.
[27] M.V. Gangone, M.J. Whelan, and K.D. Janoyan. Deployment of a dense hybrid wireless sensing system for bridge assessment. Structure and Infrastructure Engineering: Maintenance, Management, Life-Cycle Design and Performance, 7:369–378, 2011.
[28] N.D. Battista. Wireless Monitoring the Longitudinal Movement of a Suspension Bridge Deck. University of Sheffield, UK, 2010.
[29] K. Sukun, S. Pakazad, D. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon. Health monitoring of civil infrastructures using wireless sensor networks. Information Processing in Sensor Networks, April:254–263, 2007.

[30] S. Kim. Wireless Sensor Networks for Structural Health Monitoring. University of California, USA, 2005.
[31] M. Melo and J. Taveras. Structural Health Monitoring of Golden Gate Bridge Using Wireless Sensor Network – Progress Report. University of Massachusetts Lowel, Aug 2009.
[32] DeltaV. The DeltaV System Overviewed, Emersion Process Management, 2002.
[33] DeltaV. DeltaV OPC.NET Server, Emersion Process Management, January 2011.
[34] DeltaV. Smart Wireless Gateway, Emersion Process Management, 2009.
[35] D. Pompili, T. Melodia, and I.F. Akyildiz. Deployment Analysis in Underwater Acoustic Wireless Sensor Networks. Georgia Institute of Technology, USA, September 2006.
[36] J. Heidemann, Y. Li, A. Sayed, J. Wills, and W. Ye. Underwater Sensor Networking: Research Challenges and Potential Applications. USC/Information Science Institute, USA, 2005.
[37] S. Khodadoustan and M. Hamidzadeh. Tree of Wheels: A New Hierarichal and Scalable Topology for Underwater Sensor Networks. Sharif University of Technology, Iran,2011.
[38] D. Dong. 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, March 2011.
[40] K. Romer and F. Mattern. The Desing Space of Wireless Sensor Networks, Institute for Pervasive Computing. ETH, Switzerland, 2004.
[41] A. F. Molish. Wireless Communications, pp. 386–387. John Wiley & Sons Ltd, England, 2005.
[42] M. Chen, T. Kwon, Y. Yuan, and V.C.M. Leung. Mobile agent based wireless sensor networks. Journal of Computers, 1:14–21, April 2006.
[43] H. K. Kalita and A. Kar. Wireless sensor network security analysis. International Journal of Next-Generation Networks, 1:1–10, December 2009.
[44] T. Bakken, R.B. Pant, P. Xie, and A. Shrestha. Wireless Sensor Networks Using NI Modules. Telemark University College, Norway, 2010.
[45] P. Mohanty, S. Panigrahi, N. Sarma, and S.S. Satapathy. Security issues in wireless sensor networks data gathereing protocols: A survey. Journal of Theoretical and Applied Information Technology, 14–26, 2010.
[46] S. Kaplantzis. Security Models for Wireless Sensor Networks. Monash University, Australia, March 2006.
[47] A.D. Wood and J.A. Stankovic. Denial of service in sensor networks. Computer, 35:54–62, October 2002.
[48] National Instruments. CompactRIO Third-Party Modules. National Instruments Corporations, USA, December 2010.
[49] SEA. Zigbee, http://www.sea-gmbh.com/en/products/compactrio-products/sea-crio-Modules/wireless-technology/zigbee/, April 2011.
[50] http://www.broadcom.com/press/release.php?id=s637241, accessed 18 June 2013.

Biographies

Rabin Biplab Pant did his Master degree in the Department of Electrical Engineering, IT and Cybernetics of TUC and has joined the industry in Nepal.

Hans-Petter Halvorsen is Research/Senior Engineer in the Department of Electrical Engineering, IT and Cybernetics of TUC. He works with Research and Development, Programming and System Development, Laboratory Work and Data Acquisition within the fields Measurement and Control Systems. He has worked in industrial IT projects involving LabVIEW and many other programing languages in the Norwegian IT companies CARDIAC and Braze Technology.

Frode Skulbru belongs to the management team of NI in Norway.

Saba Mylvaganam is professor in Process Measurements and Sensorics at TUC.