Low Power Secure Wireless Protocol Design Using RFID System

[1]Hemant Agrawal,[2]Priyanka Bari,[3]Brijesh Chopda, [4]Dhrumen Dharani, [5]Bhavesh Asodariya
[1,2,3,4] B.E. Student, [5]Assistant Professor
[1,2,3,4,5]Department of Electronics & Communication Engineering
[1]Shree Swami Atmanand Sarswati Institute of Technology, Surat,India

***Abstract*—In today's global competitive world, there is necessity of developing a Low Power consuming Wireless Protocol and full functional nodes and to deploy Wireless Secure Network for Industrial parameter monitoring. As we know that modern wireless communication systems require the deployment of increasingly complex protocols that satisfy tight requirements at low implementation cost, especially in terms of size and power consumption. A most important stage of this thesis work is to develop sensor nodes for collecting sensor data and acquires data on master node which has MIWI wireless protocol stack. A system prototype is implemented using Microchip RF 433MHz Transceiver module with microchip microcontroller, RFID system and other systems to build a network and test its main parameters. The designed system is constituted of three adapter powered functional MIWI Slave Secure Nodes structured to be wirelessly networked. Wireless Secure Network protocol suitable for measuring industrial parameter considering energy demands, data rates, physical dimensions, costs and other important aspects. Wireless secure network can reorganize themselves to form a network and convey meaningful data. These nodes have the capability to reorganize themselves into a network and transmit data that can range from measuring light, temperature, humidity or even motion. Communication of signals is carried out using radio frequency (RF) waves. The main advantages of wireless systems over wired systems is the considerable reduction in the cost and power consumption.**

***IndexTerms*—Wireless, Secure, Low Power consuming, Network, RFID (Radio Frequency Identification), MIWI.**

I. INTRODUCTION

A Wireless Secured Network consists of spatially and randomly distributed self-configurable autonomous secured nodes to cooperatively monitor physical conditions. Typical examples includes RFID system for detection. These three hardware ingredients e.g. microcontrollers, sensors, and low-power radios--make up a sensor node, or mote. A Wireless secured node is a battery-operated device, capable of sensing physical quantities. In addition to sensing, it is capable of Wireless communication, data storage, and a limited amount of computation and signal processing. Advances in integrated circuit design are continually shrinking the size, weight and cost of sensor devices, while simultaneously improving their resolution and accuracy. At the same time, modern Wireless networking technologies enable the coordination and networking of a large number of such devices. Hence, as a result of which the power requirement increases.

A WSN has one or more sinks (or Base Stations) which collect data from all sensor devices. These sinks are the interface through which the WSN interacts with the outside world. Wireless sensor nodes are networked via low power Wireless communications. It is the networking capability that fundamentally differentiates a sensor network from a mere collection of sensors, by enabling cooperation, coordination, and collaboration among sensor assets. Harvesting advances in the past decade in microelectronics, sensing, analog and digital signal processing, Wireless communications, and networking, Wireless sensor network technology is expected to have a significant impact on our lives in the twenty-first century.

The basic premise of a WSN is to perform networked sensing using a large number of relatively unsophisticated sensors, instead of the conventional approach of deploying a few expensive and sophisticated sensing modules. The potential advantage of networked sensing over the conventional approach can be summarized as greater coverage, accuracy and reliability at a possibly lower cost. The range of potential applications that WSNs are envisaged to support, is tremendous. In coming years, as advances in micro-fabrication technology allow the continuous drop of the cost of manufacturing sensor motes, increasing deployments of Wireless sensor Networks are expected with the network eventually growing to large numbers of motes. In general the WSN works on 2.4GHz or higher frequencies, as a result of which the different loses within the networks increases. Hence signal degradation and power loss increases. Hence low frequency module also reduces the power loss and improves the range of the system.

Since sensors are now small and cheap, they can be deployed on large scale. They become more and more important for applications like security, industrial parameter monitoring, traffic monitoring, agriculture, battlefield, etc. Most of those sensors are powered by batteries. The lifespan of an energy-constrained sensor is determined by how fast the sensor consumes energy. Sensors use energy to run circuitry and send radio signals. The later is usually a function of distance and takes a large portion of the energy. Researchers are now developing new routing mechanisms for sensor Networks to save energy and prolong the sensor lifespan. Four primary routing mechanisms are direct transmission, minimum energy transmission, static clustering, and dynamic clustering. Sensor lifespan is an important performance index for comparison of different routing mechanisms. Using the lower frequency of 433MHz also reduces the power consumption and increases the communication range of Communication.

Wireless Secured Networks are increasingly considered by the scientific community as the future of Environmental Monitoring:

Proposed applications of sensor network include environmental monitoring, natural disaster prediction and relief, home land, security, healthcare, manufacturing, transportation, and home appliances and entertainment.

II. The Research Objectives

- To compare and contrast existing Wireless Sensor Network protocol suitable for measuring industrial parameter considering energy demands, battery lifetime, data rates, physical dimensions, costs and other important aspects.
- To develop battery powered sensor nodes for collecting sensor data and acquire data on master node. There is need to develop hardware and software of sensor node for acquisition of sensor data and wirelessly transmit to master node.
- To create the Graphical User interface in LabVIEW development environment for API interfaced to application for acquisition and extracting sensor nodes information. The sensor nodes parameter graphically displayed on real time graphs. Finally, the testing phase Coordinator and Slave nodes tested in terms of indoor range, outdoor range, current consumption, reliability. This phase also test hardware and software implementation of nodes.

III. WSN Protocol

For selecting protocol for this application we concerns for the following:

- Hardware dimensions
- Memory requirements
- Data rate and other advantageous network features (‘Bandwidth and range’)
- Power consumption
- Reliability and security
- Costs

To be precise, for measuring in small devices the data rate demand is an insignificant parameter for comparisons e.g. the reliability or power consumption, in most cases, are in contradiction with high data rates.

We decided to omit following technologies from comparison as they obviously do not meet the requirements application needs

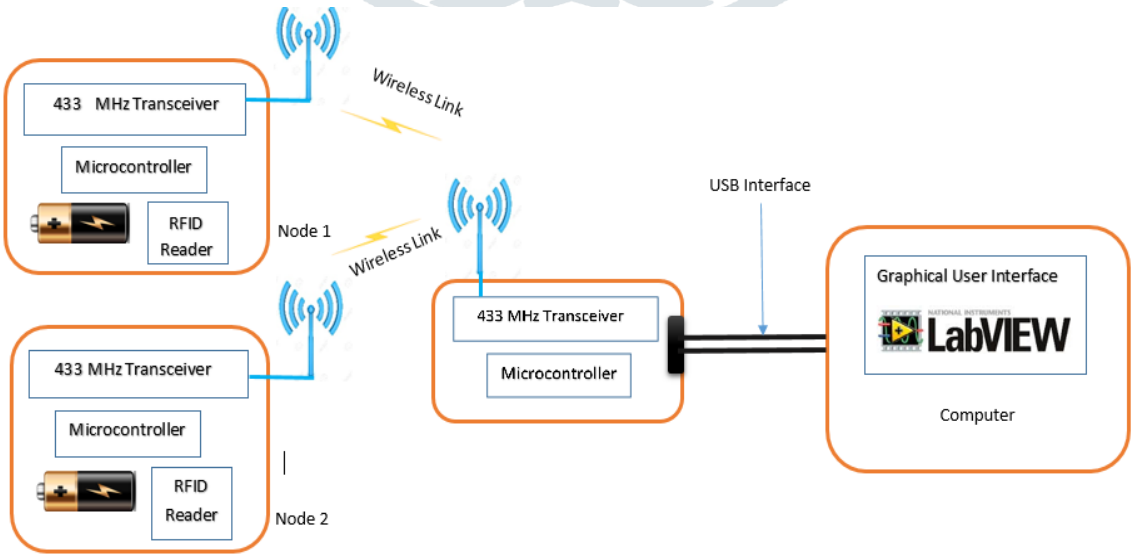
- Wireless technologies of cellular network (GSM, UMTS) as they do not provide enough independency in network construction and management.
- MAN / Distribution networks because of their inadequate nature.

Four of the remaining technologies were chosen to be further discussed. They are all wellknown, widely commercially exploited L AN/PAN standards with industry-driven development and support, manufactured in large-scale and equipped in wide range of applications. They are

- Bluetooth
- ZigBee
- Wi-Fi
- Wireless HART
- MIWI^{TM}

Any of these hardly is chosen in advance as the most suitable, as they all do have both advantages and disadvantages. They range from mid-range LAN to high-rate PAN, provide various network topologies. The features are indeed wide and the final solution seems to be in certain compromise between the requirements the features offered by these technologies.

IV. Block Diagram



The Master Node must be configured to API Coordinator ZNet 2.5 before we use it for LabVIEW GUI. Master Node is The Master Module (MM) is the part of the application directly controlled by the user and has a Graphical User Interface (GUI) especially designed to

obtain the user inputs easily and present the results to the user. Through the MM front panel, the user can monitor sensor nodes, view graphical history of each monitored sensor, enable or disable the monitoring status of a particular sensor, view the current value of each sensor numerically and graphically. When the Master Module starts, it goes through an initialization stage and then starts three concurrent threads that will be kept alive until the application is closed by the user.

MIWI SPECIFICATION

Microchip MiWi™ P2P Wireless Protocol is one of the wireless protocols that are supported in MiWi DE (Development Environment). It is a variation of IEEE 802.15.4, using Microchip's IEEE 802.15.4 compliant and other proprietary RF transceivers, which are controlled by Microchip 8, 16 or 32-bit microcontroller with a SPI(Serial Peripheral Interface).
The MiWi P2P Wireless Protocol has the following features:

- Operates on Microchip PIC18, PIC24, dsPIC33 and PIC32 platforms
- Supports Microchip C18, C30 and C32 compilers
- Functions as a state machine (not RTOS-dependent)
- Supports a sleeping device at the end of the communication
- Enables Energy Detect (ED) scanning to operate on the least-noisy channel
- Provides active scan for detecting existing connections
- Enables frequency agility (channel hopping)
- Supports all of the security modes defined in IEEE 802.15.4.

LAB VIEW

- LabVIEW empowers you to build your own solutions for scientific and engineering systems.
- LabVIEW gives you the flexibility and performance of a powerful programming language without the associated difficulty and complexity.
- By using LabVIEW to prototype, design, test, and implement your instrument systems, you can reduce system development time and increase productivity by a factor of 4 to 10.
- You can use LabVIEW to easily communicate with several hardware interfaces such as data acquisition, vision, and motion control devices, as well as GPIB, PXI, VXI, USB, Ethernet, RS232, and RS485 instruments and plug-in data acquisition devices.
- LabVIEW provides us with an excellent set of tools for examining all sorts of DSP (digital signal processing) and digital communication topics. Its graphical nature allows us to quickly and efficiently get to the core of a communication problem, without all the overhead that generally accompanies a digital communication system
- Using LabVIEW, you can create 32-bit compiled applications that give you the fast execution speeds needed for custom data acquisition, test, measurement, and control solutions. You can set breakpoints, animate program execution, and single-step through the program to make debugging and development easier.

V. SUMMARY

By studying all the above points we can say that WSN technique is having wide scope of applications, and not limited to only one organization or industry. A number of objectives can be achieved by using WSN. For achieving these objectives one can uses the protocols like MIWI and the software like Lab-VIEW. And the major problem in such network creating and data collecting is the security issue. If proper security is not maintained the tampering and hacking of the data takes place. The other factor is the power requirement. By lowering down the frequency we can decrease the power requirement and hence improves the life time of the device.

VI. CONCLUSION

In this paper the available literature on VSM has been categorized yearly focusing on their aim and finding after implementation of WSN. Based on the literature we can say that WSN works for keeping the records secured and improving human efficiency and reducing human efforts and saving time. WSN should not be end with one improvement; it should be continued with continuous improvements.

VII. ACKNOWLEDGMENT

We feel great pleasure in expressing our deep sense of gratitude towards Prof. Mahesh B. Hasani, EC Department, Shree Swami Atmanand Saraswati Institute of Technology (Surat) and Vipulkumar Patel, Team Leader in Embedded System, Spectra Techno-vision (Ahmedabad) for their guidance and constant supervision till the completion of Project.

REFERENCES

[1] PranaySharma ,Overview and setup of a ZigBee wireless sensor network.
[2] ThamerAlajlan, Microchip MiWi Wireless Protocol Stack
[3] Yingshu Li, My T. Thai, Weili Wu, "Wireless Sensor Networks and Applications", Springer Science Media, LLC, 2008.
[4] Yifeng Yang, "*MiWi™ P2P Wireless Protocol Stack*", AN1204,(DS01204B), Microchip Technology Inc., 2010.
[5] MihaelaCardei, Yinying Yang, and Jie Wu, "Non-Uniform Sensor Deployment inMobile Wireless Sensor Networks", Department of Computer Science and EngineeringFlorida Atlantic University

[6] Ivan Stojmenovic and NejibZaguiaSITE ,"Bluetooth Scatternet formation in ad hoc wireless networks", University of Ottawa

[7] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen, "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi", Information & Communications Research Labs Industrial Technology Research Institute (ITRI), The 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON) Nov. 5-8, 2007, Taipei, Taiwan

[8] Qinghua Wang and IlangkoBalasingham, Wireless Sensor Networks - An Introduction", Norwegian University of Science and Technology, Norway

[9] Guangchao GAO, Heng ZHANG, Li LI ,"A Reliable Multipath Routing Strategy forWirelessHART Mesh Networks Using Subgraph Routing", Computer and Information Science College, Southwest University, China, Journal of Computational Information Systems 9: 5 (2013) 2001–2008

[10] Yifeng Yang, AN1371, "*MiWi™ pro Wireless Networking Protocol* ", Microchip Technology Inc., 2011.

[11] David Flowers and Yifeng Yang, AN1066, "*MiWi™ Wireless Networking Protocol Stack*"Microchip Technology Inc., 2010.

[12] Mark A. Perillo and Wendi B. Heinzelman,Wireless Sensor Network Protocols, Department of Electrical and Computer Engineering, Rochester, NY, USA.

[13] Protocol Design and Implementation for Wireless Sensor Networks, Masters' Degree Project, Stockholm, Sweden April 2008.

[14] Alan Mainwaring1 Joseph Polastre2 Robert Szewczyk2 David Culler1,2 John Anderson3,Wireless Sensor Networks for Habitat Monitoring,*WSNA'02,* September 28, 2002, Atlanta, Georgia, USA.

[15] Microchip Application Note AN1283, *"Microchip Wireless Media Access Controller – MiMAC"* http://www.microchip.com/miwi

[16] Microchip Application Note AN1284, *"Microchip Wireless Application Programming Interface – MiAPP"* http://www.microchip.com/miwi

[17] Victor H. Li, Zhi-Qiang Liu, and Steven H. Low. Enhancing tcp performance over wireless networks.

[18] L. Doherty, K. Pister, and L. Ghaoui. Convex position estimation in wireless sensor networks. In Proceedings of the Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), 2001.

[19] S. Tilak, N. Abu-Ghazaleh, and W. Heinzelman. Infrastructure tradeoffs for sensor networks. In Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications (WSNA), 2002.

[20] M. Perillo and W. Heinzelman. Sensor management. In C. Raghavendra, K. Sivalingam, and T. Znati, editors, Wireless Sensor Networks, pages 351–372. Kluwer Academic Publishers, 2004.

[21] C. Wan, A. Campbell, and L. Krishnamurthy. PSFQ: A reliable transport protocol for wireless sensor networks. In Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications (WSNA), 2002.

[22] W. Chen, J. Hou, and L. Sha. Dynamic clustering for acoustic target tracking in wireless sensor networks, 2003.

[23] IEEE Std 802.154.4-2003, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area networks (WPANs). New York: IEEE, 2003.

[24] Yifeng Yang, "Microchip Wireless (MiWi™) Media Access Control – MiMAC", Microchip technology Inc., 2009.

[25] Yifeng Yang, "Microchip Wireless (MiWi™) Application Programming Interface – MiApp", Microchip Technology Inc., 2009.