International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 2, February-2014, pp: (154-158), Impact Factor: 1.252, Available online at: www.erpublications.com

Wireless Sensor Network & their applications in Electrical System

Dr. Rajesh Goel[1], Sagar[2]
[1]Professor, [2]Department of Electrical & Electronics Engg.,
[12]Samalkha Group of Institutions, Samalkha, Panipat, India

Abstract: Wireless Sensor Network have been broadly familiar as a hopeful technology that can enhance various aspects of today's electric power systems, including generation, delivery, and utilization. Manual collection of data is very difficult & time consuming task and may be infeasible if the data terminals (nodes) are unreachable. Therefore, a wireless update mechanism is needed. The mentioned task is achieved by using Wireless sensor network. According to this concept, the power system will have such capabilities as to integrate micro producers of energy (possibly coinciding with customers), to perform automatic fault detection and self-reconfiguration according to supply and demand patterns. In order to allow these advanced functionalities, the power grid must first be sensorized, i.e. fit with sensors that are able to collect and deliver relevant measurements to the processing systems, as well as electro-mechanical actuators that are used to change the configuration of the grid. This paper presents a demonstrator developed within the scope of the WSN, which addressed the protection of critical infrastructures through the use of Wireless Sensor and Actuator Networks (WSAN). The demonstrator includes sensor nodes developed within the project. This paper focuses the hardware of the sensor nodes and presents the respective performance results, attesting the feasibility of the proposed solutions.

Introduction

As Sensors are very simple identical electronic devices equipped with a processor and small storage memory and a communication channel. The sensors can communicate to each other through wireless links, and most of the times they use radio frequency channels for the purpose of communication. In many applications the sensors perform measurements of specific metrics like temperature, pressure, movements or other physical values in a periodic or non-periodic way. Most of the times it is desired to collect the data of all sensors in a specific station for processing, archiving and other purposes. This station is a data sink, and it has enough processing power, storage space, and capability of communicating to the sensors. We will call this station the central node in the rest of the paper. For the purpose of communication to the central node, the sensors relay the packets of each other in a multi-hop way. Since the sensors operate on the battery power, it is very important to make efficient use of energy of sensors to increase the lifetime of the network. Most of the energy of sensors is spent for transmission of the data packets generated by that sensor or relaying the packets of the other sensors, so finding optimal transmission paths from each sensor to the destination is a very important task. A WSN is a system composed of numerous computing and sensing devices distributed within an environment to be monitored. In the past decades, WSNs have been applied to autonomous use of computing, sensing, and wireless communication devices for both scientific and commercial purposes.

Any communication protocol that involves synchronization between peer nodes incurs some overhead of setting up the communication. Obviously, each node could make the most informed decision regarding its communication options if they had complete knowledge of the entire network topology and power levels of all the nodes in the network. This should yield the best performance if the synchronization messages are not taken into account. However, since all the nodes would always have to know everything, it should be clear that there will be many more synchronization messages than data messages, and therefore ideal case algorithms are not feasible in a system where communication is very expensive. On the other hand, wireless links are not very reliable and nodes might stop operating at arbitrary points within the system's life; therefore, the routing protocol utilized must be able to handle arbitrary failure of nodes throughout the network. Such a network may operate in a standalone fashion, or it may be connected to other networks, such as the larger Internet.

Wireless Sensor Network for Power System Assets

Transmission system consists of towers, overhead power lines, underground power lines, etc., that are responsible for transportation of electricity from the generation sites to the distribution system. In the traditional power grid, the voltage is stepped up in order to reduce the losses at the transportation, and then, it is step down at the distribution system.

Distribution system consists of substations, transformers and wiring to the end-users. In the transmission and distribution segment, an equipment failure or breakdown may cause blackouts or it may even pose danger for public health. Moreover, these assets can be easily reached from outside, therefore they can be a target of terrorism. WSNs, once again, provide promising solutions for monitoring and securing the transmission and distribution segment.
WSNs provide a complete physical and electrical picture of the power system in real time and ease diagnosing faults. Moreover, power grid operators are provided with appropriate control suggestions in order to reduce the down time of the system. The authors employ a two-level hierarchy where short-range sensor nodes collect data from a component and deliver the collected data to a gateway. This gateway is called as Local Data and Communications Processor (LDCP). The LDPC has the ability to aggregate the data from the sensors, besides it has a longer-range radio which it uses to reach the other LDPCs that are several hundreds of meters away. The mechanical status of the transmission system is processed and delivered to the substation by the LDPCs. This hierarchical deployment increases the scalability of the WSN which emerges as a necessity when the large geographical coverage of the transmission system is considered. The communication services provided by WSNs have been shown to be useful for automation and remote metering applications. Power quality measurements include harmonics, voltage sags, swells, unbalanced voltage, etc

Nodes of Wireless Sensor

Some applications of sensor networks might require a diverse mixture of sensor nodes with different types and capabilities to be deployed. Data from different sensors, can be generated at different rates, network can follow different data reporting models and can be subjected to different quality of service constraints. Such a heterogeneous environment makes routing more complex. Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. If many nodes fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection base stations. This require actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption, or rerouting packets through regions of the network where more energy is available. Therefore, multiple levels of redundancy may be needed in a fault-tolerant sensor network

A. Design of Wireless Sensors Node

The wireless sensor node design on a pole transformer. The block diagram in Figure 1 illustrates the components, consisting of wireless sensor node, and their interactions with one another. Through the 3-phase transformer part, power quality is measured periodically. Measurements are carried out once every second, which is sufficient to provide the power quality monitoring service. Assuming that we store 3,600 data per hour, each hour requires a little over 500 Kbytes of space. This implies that 640 Kbytes of flash RAM are sufficient to store the data. The microprocessor has a number of functions: processing data collection from the sensing part, interfacing the data to the physical radio layer, and managing the radio network protocol. We use the OEM wireless Ethernet module with a range of about 500 meters for peer transfers among neighboring pole transformers.

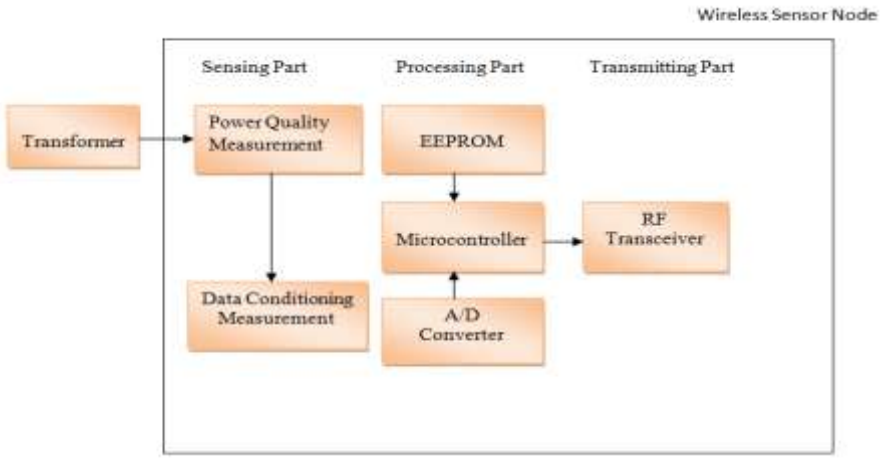


Figure 1: Wireless Sensor Network Block Diagram

Security in Wireless Sensor Network

Because sensor networks use wireless communication, they are vulnerable to attacks which are more difficult to launch in the wired domain. Many wired networks benefit from their inherent physical security properties. It is unlikely that an adversary will dig up the Internet backbone and splice into the line. However, wireless communications are difficult to protect; they are by nature a broadcast medium. In a broadcast medium, adversaries can easily eavesdrop on, intercept, inject, and alter transmitted data. In addition, adversaries are not restricted to using sensor network hard- ware. They

can interact with the network from a distance by using expensive radio transceivers and powerful workstations. Sensor networks are vulnerable to resource consumption attacks. Adversaries can repeatedly send packets to drain the nodes' batteries and waste network bandwidth. Since sensor networks will be deployed in a variety of physically insecure environments, adversary can steal nodes, recover their cryptographic material, and pose as authorized nodes in the network. However, we do not address these threats. Our focus is on guaranteeing message authenticity, integrity, and confidentiality. We do not address resource consumption attacks, physical tamper resistance, or node capture attacks.
A link layer security protocol should satisfy three basic security properties: access control, message integrity, and message confidentiality.

A. Access Control & Message Integrity

Access control means the link layer protocol should prevent unauthorized parties from participating in the network. Legitimate nodes should be able to detect messages from unauthorized nodes and reject them. Closely related to message authenticity is message integrity: if an adversary modifies a message from an authorized sender while the message is in transit, the receiver should be able to detect this tampering. We provide message authentication and integrity by including a message authentication code with each packet.

B. Confidentiality

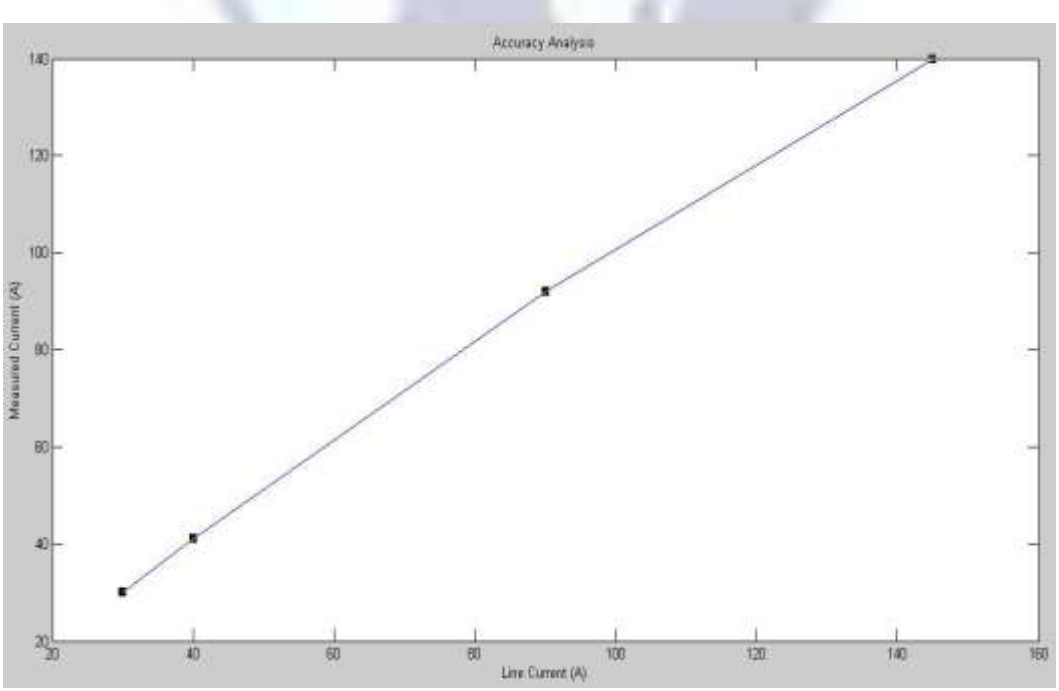
Confidentiality means keeping information secret from unauthorized parties. It is typically achieved with encryption. Preferably, an encryption scheme should not only prevent message recovery, but also prevent adversaries from learning even partial information about the messages that have been encrypted. This strong property is known as semantic security [8]. Semantic security implies adversaries should have no better than a 50% chance in correctly answering any yes or no question about an encrypted message

Test and Results

The current sensor was tested separately at special lab facilities before the WSAN integrated tests and trial deployment. This was due to the harsh electromagnetic conditions to which it would be subject during the trial, as well as the high costs of retrieval and redeployment. This section will cover the individual sensor performance tests.

A. Medium Voltage Current Sensing Node

In order to find potential EMC (Electro Magnetic Compatibility) problems, the wireless current sensor node was tested under exposure to the electromagnetic fields generated by the 15 kV power line. Firstly, the node behavior was tested for voltages of 9kV, 13 kV and 20 kV. No problems were detected on the wireless communication or on the node functionality. Only for 20 kV, the corona effect starts to be noticed. Accuracy was also analyzed in the medium voltage environment. Measured values present an offset to the theoretical values. Calibration was then done by software



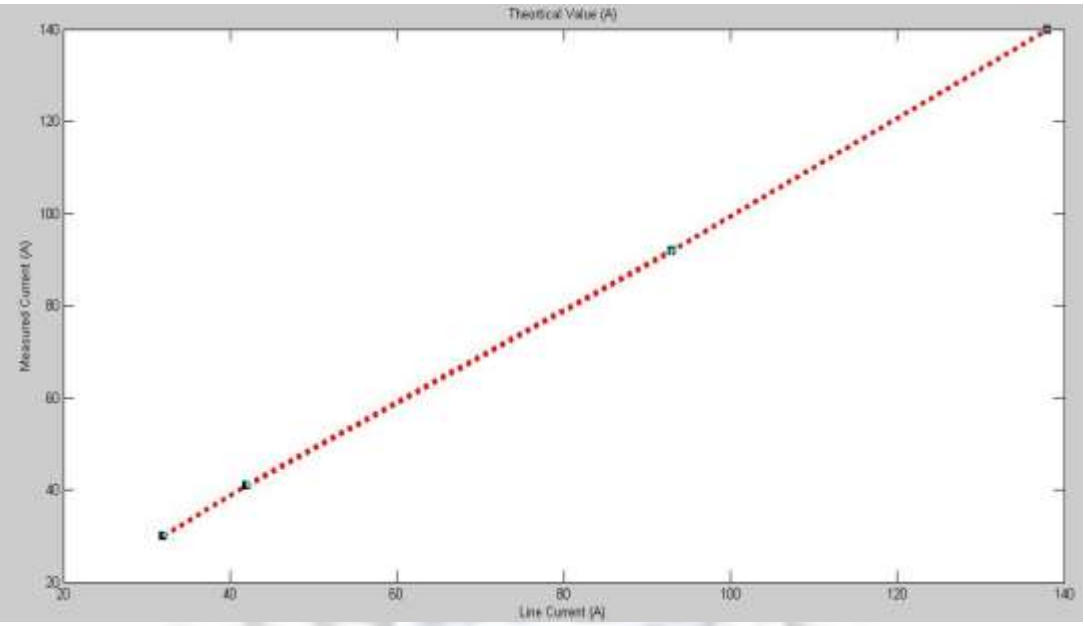


Figure 2: Accuracy analysis for MV

B. Accuracy Test

For the current measurement tests, extra current was externally injected in the LV lines by the EDP technicians and the sensor reports were confronted against the known current injection values. For the trip-coil, on-demand tests were performed while the trip-coil was operational. Then, the 110 V terminals were disconnected from the trip-coil to check whether the malfunction was automatically detected. The on-demand test was also repeated under this condition.
For the intrusion and hotspot detection tests, the respective situations were simulated by the EDP and INOV team. The tests entailed the transmission of images from the LV/MV power transformer to the primary substation. For the hotspot detection, a soldering iron was placed in front of the camera, while for intrusion detection, a member of the EDP team simulated intrusions in a secondary substation.
Regarding the temperature measurements, the precision is high, with an average error of 1% and maximum of 3%. For the power line current measurements, the average error was 4.58% with peaks of 10.83%. This precision is enough to detect breakdown spots in the power-lines as well as to provide coarse reports about the distribution of current consumption within the EDP network. The remaining components feature a high precision.

Conclusion/Results

This paper has presented the sensor node hardware that was developed and deployed in the demonstrator of FP7 project WSAN4CIP. Besides standalone tests, the sensors were also tested as nodes of the WSAN, both in-lab and in the deployed pilot system. Results of performed tests show that sensors performance is adequate. The energy harvesting mechanism implemented to recharge the WSAN node batteries demonstrated to be effective in powering sensors to measure MV power line activity.
.

References

[1]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” Comput. Netw., vol. 38, no. 4, pp. 393–422, Mar. 2002.
[2]. S. M. Amin and B. F. Wollenberg, “Toward a smart grid,” IEEE Power Energy Mag., vol. 3, no. 5, pp. 34–41, Sep./Oct. 2005.
[3]. L. Angrisani, M. Bertocco, D. Fortin, and A. Sona, “Experimental study of coexistence issues between IEEE 802.11b and IEEE 802.15.4 wireless networks,” IEEE Trans. Instrum. Meas., vol. 57, no. 8, pp. 1514–1523, Aug. 2008.
[4]. L. L. Bello, O. Mirabella, and A. Raucea, “Design and implementation of an educational testbed for experiencing with industrial communication networks,” IEEE Trans. Ind. Electron., vol. 54, no. 6, pp. 3122–3133, Dec. 2007.
[5]. U.S. Department of Energy, “The smart grid: An introduction, ” Washington, DC, Sep. 2008
[6]. V. C. Gungor and G. P. Hancke, “Industrial wireless sensor networks: Challenges, design principles, and technical approaches.
[7]. Lu and V. C. Gungor, “Online and remote motor energy monitoring and fault diagnostics using wireless sensor networks,” IEEE Trans. Ind. Electron., vol. 56, no. 11, pp. 4651–4659, Nov. 2009.
[8]. V. C. Gungor, B. Lu, and G. P. Hancke, “Opportunities and challenges of wireless sensor networks in smart grid,” IEEE Trans. Ind. Electron. vol. 57, no. 10, pp. 3557–3564, Oct. 2010.
[9]. U.S. Dept. of Energy, “Communications Requirements of Smart Grid Technologies,” tech. rep., Oct. 2010.

[10]. Y. Gobena et al., "Practical Architecture Considerations for Smart Grid WAN Network," Proc. Power Systems Conf. and Exposition, Mar. 2011, pp. 1–6.
[11]. M. Erol-Kantarci, H. T. Mouftah, "Wireless Multimedia Sensor and Actor Networks for the Next-Generation Power Grid," accepted for publication, Elsevier Ad Hoc Networks Journal, 2011. DOI 10.1016/j.adhoc.2010.08.005.
[12]. O. Asad, M. Erol-Kantarci, H. T. Mouftah, "Sensor Network Web Services for Demand-Side Energy Management Applications in the Smart Grid," IEEE Consumer Communications and Networking Conference (CCNC'11), Las Vegas, USA, January 2011.
[13]. M. Erol-Kantarci, H. T. Mouftah, "Prediction-Based Charging of PHEVs from the Smart Grid with Dynamic Pricing," First Workshop on Smart Grid Networking Infrastructure in LCN 2010, Denver, Colorado, U.S.A, October 2010.
[14]. S. Paudyal, C. Canizares, and K. Bhattacharya, "Optimal operation of distribution feeders in smart grids," IEEE Trans. Ind. Electron., vol. 58,no. 10, pp. 4495–4503, Oct. 2011.