Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 41 (2016) 1-8 EISSN 2392-2192

Challenges in Integrating Wireless Sensor Network and Internet of Things for Environmental Monitoring

S. R. Vijayalakshmi* & **S. Muruganand**

Department of Electronics and Instrumentation, Bharathiar University,
Coimbatore - 641046, Tamil Nadu, India

*E-mail address: srvijisiva@gmail.com

ABSTRACT

Hardware technology developments and wireless communications enables the development of wireless sensor networks (WSNs). WSN will need to be connected to the Internet due to its variety of applications and their importance. This paper discusses the challenges in integrating WSN and IoT (Internet of Things). The best ways of integrating WSN and IoT for environmental monitoring are analyzed. The sensor node is developed to monitor environmental parameters such as temperature and humidity. The sensor SHT75 to sense the temperature and humidity of the environment, XBeePro to communicate with gateway, LCD to display information are interfaced with MSP430 Microcontroller. The microcontroller is used for processing, controlling and communicating the information. The sensor nodes are deployed to measure the parameter in the target area. The information is communicated to the world of Internet in one of the best integrating ways discussed in the paper.

***Keywords*:** Wireless Sensor Network, Internet of Things, Environmental monitoring, Temperature and humidity measurement

1. INTRODUCTION

The ways of getting information from the physical environment are changed by the wireless sensor network. The wireless sensor network consists of thousands to millions of tiny sensor nodes for sensing the environment with the limited computation and communication

(Received 01 February 2016; Accepted 10 February 2016; Date of Publication 11 February 2016)

capabilities. When they are networked together, these devices can provide highly precise and resolution knowledge about the sensed phenomenon. The task of integrating WSN to the existing Internet brings with it several challenges. This paper discusses the challenges and the best method to interface WSN with the IoT to monitor the environmental parameters are analyzed. The organization of this paper is as follows. The section 2 discusses about the background study. The wireless sensor network and its characteristics are studied in the section 3. The different methods of integrating WSN and IoT are analyzed in section 4. The results are discussed in section 5. Finally, conclusions are arrived at the last section.

2. BACKGROUND STUDY

Sudipta Bhattacharjee et al. [1] discussed wireless sensor network-based fire detection, alarming, monitoring and prevention system for Bord-and-Pillar coal mines. Daniela Ballari et al. [2] analyzed about a mobility constraint model to infer sensor behaviour in forest fire risk monitoring. Junguo ZHANG et al. [3] discussed about the forest fire detection system based on a ZigBee wireless sensor network. The Cetin Elmas and Yusuf Sonmez [4] analyzed the data fusion framework with novel hybrid algorithm for multi-agent decision support system for forest fire. The Andrey Somov et al. [5] discussed about the deployment and evaluation of a wireless sensor network for methane leak detection.

The Zujue Chen [6] et al. discussed about the design of wireless sensor network node for carbon monoxide monitoring. The Hakilo Sabit [7] et al. discussed about the wireless sensor network based wildfire hazard prediction system modeling. The Andrey Somov [8] et al. analyzed about the deployment and evaluation of a wireless sensor network for methane leak detection. Yeon-sup Lim et al. analyzed [9] Fire Detection and Rescue Support Framework with Wireless Sensor Networks. Daniela Ballari et al. [10] analyzed about a mobility constraint model to infer sensor behaviour in forest fire risk monitoring.

3. WIRELESS SENSOR NETWORK

A Wireless Sensor Network has little or no infrastructure. It has number of sensor nodes and can work together to monitor a region to obtain data about the environment. There are two types of WSNs called as structured WSN and unstructured WSN. Unstructured WSN contains dense collection of sensor nodes and often deployed in ad-hoc manner in field, i.e. nodes are deployed randomly in the target area. In structured WSN sensor nodes are deployed in pre-determined locations. These sensor nodes are energy limited and specific application oriented. Hence, the power management of sensor node is essential for effective network operation.

The characteristics of sensor networks are determined by the following two parameters.

3. 1. Data flow patterns

In sensor networks, each node is an independent data collection device. Periodically each sensor node in the wireless network sends its readings to central work station. Sometimes, the central workstation will be interested in specific information from nodes in such case it inserts the query into the network and it is propagated. Then nodes with the data will respond to the query with the relevant information.

3. 2. Energy constraints

The sensor nodes in the networks are battery operated with limited recharge capabilities. The primary network performance metric is the energy efficiency of operation.

4. INTEGRATING WSN AND IoT

The integration between the Internet and a WSN is classified in to three. They are (i) front end (ii) Gateway and (iii) TCP/IP. A WSN can be completely independent from the Internet (*Front-End*), be able to exchange information with Internet hosts (*Gateway*), or share a compatible network layer protocol (*TCP/IP*).

The first approach is the *Front-End solution*. In this solution, the external Internet hosts and the sensor nodes never communicate directly with each other. In fact, the WSN is completely independent from the Internet, so it can implement its own set of protocols. All interactions between the outside world and the sensor network will be managed by a centralized device, such as a base station as shown in Fig. 1. This base station can store all the data streams coming from the WSN, and it can also provide these data streams to external entities through well-known interfaces. In addition, any queries coming from Internet hosts will always traverse the base station.

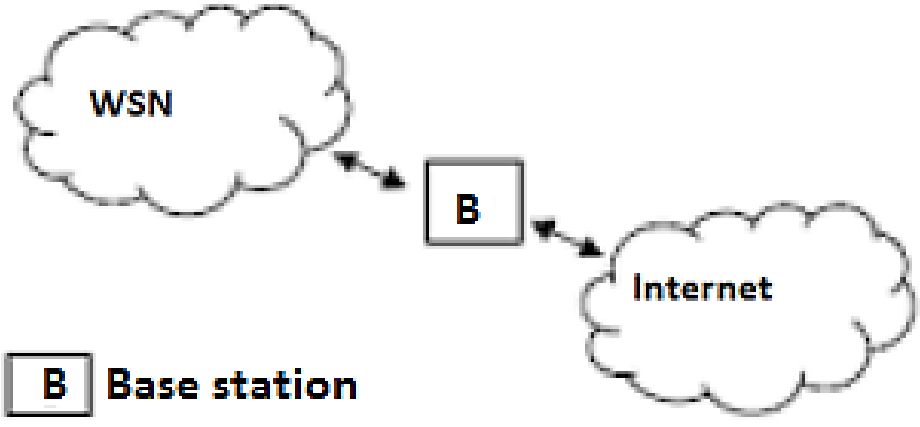

Figure 1. Front end solution for integrating IoT and WSN.

The second approach, the *Gateway solution*, considers the existence of a device (e.g. base station) that acts as an application layer gateway, in charge of translating the lower layer protocols from both networks (e.g. TCP/IP and proprietary) and routing the information from one point to another, as shown in Fig. 2. As a result, Internet hosts and sensor nodes can be able to address each other and exchange information without establishing a truly direct connection. In this solution, the WSN is still independent from the Internet, and all queries still need to traverse a gateway device. However, sensor nodes can be able to provide web service interfaces to external entities while maintaining their lower layer protocols.

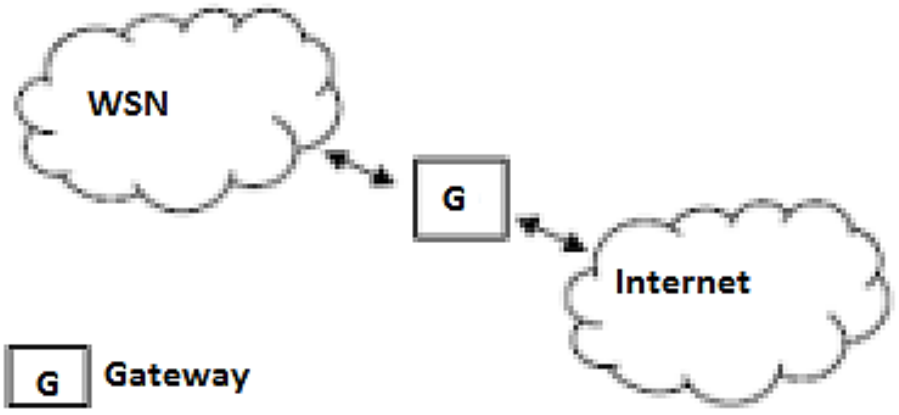

Figure 2. Gateway solution for integrating IoT and WSN.

As for the third approach, the *TCP/IP solution*, sensor nodes implement the TCP/IP stack thus they can be considered as full-fledged elements of the Internet. Any Internet host can open a direct connection with them, and vice-versa. In fact, this solution fully integrates the WSN with the IoT. A consequence of this approach is that sensor nodes are no longer able to use specific WSN protocols.

The Internet enabled nodes behave

i) as a front-end, effectively isolating the WSN sensors from the Internet, or

ii) as gateways, allowing direct data exchange between sensors and the central system.

There are multiple factors that must be taken into account before choosing a certain integration approach. The main factors are summarized in the following paragraphs:

1. *Resilience.* Any WSN that directly provides its services to external entities are quite vulnerable against attacks. Gateways and sensor nodes must be able to include security mechanisms that increase their robustness against attacks.

2. *User authentication and authorization.* It is essential for some Internet-enabled sensor nodes applications to implement security mechanisms that control who are accessing their services.

3. *Security of the communication channel.* It is necessary to analyze how mechanisms such as TLS could be used to offer an end-to-end secure channel. In fact, it is also necessary to study the different key exchange mechanisms that should be used.

4. *Accountability.* For an Internet-enabled WSN, it might be interesting to develop a distributed system that is able to record the interactions with the users of the system. By storing all interactions, we can be able to recreate security incidents and abnormal situations.

5. *Functionality.* There might be some applications where the sensor nodes do not need to be aware of the Internet. For example, WSN whose tasks are limited to collect information and answer users queries do not need to contact any Internet service.

6. *Hardware.* A specially constrained sensor node might not be able to be directly connected to the Internet due to the memory requirements of the different security mechanisms.

7. *Inherent weaknesses.* Internet-enabled sensor nodes are vulnerable to many different types of attacks, ranging from DoS attacks to exploit attacks. This particular factor is actually quite important on choosing whether certain applications should completely isolate their sensor nodes from the Internet, filtering all traffic at the edge of the network.

8. *Network redundancy.* A group of sensor nodes may offer the same functionality for redundancy purposes, but in a TCP/IP environment an external host will request services from specific nodes through their IP addresses. This means that it is necessary to develop specific mechanisms in TCP/IP environments to deal with exceptional circumstances (e.g. unreachable nodes).

9. *Protocol optimizations.* Most WSN-specific protocols include certain mechanisms that allow a network to self heal itself and to optimize its internal behaviour.

After describing the different integration approaches, it would seem that the TCP/IP solution is the best solution to successfully integrate WSN and the Internet. Not only any external system can directly access the information provided by the nodes, but also the nodes are aware of the existence of the Internet and are able to query any of its services. In other solutions, such as the Front-End solution, the nodes can only access those services that are implemented in the central system. In fact, it is actually more challenging to assure the security of WSN that make use of the TCP/IP solution. But for considering the environmental monitoring Front end solution is the simple, easy and effective way of integration. For measuring the environmental parameters the data will be minimized by the base station. The data which is necessary to monitor only send to the Internet.

5. RESULT AND DISCUSSION

The sensor node is designed to monitor environmental parameters. The temperature and humidity are measured by the sensor SHT75. This SHT75 sensor is interfaced with MSP430 microcontroller IIC peripheral unit. The LCD module to display information is interfaced with the microcontroller. The information after processing is send to the base station by the XBeePro. This XBeePro transceiver is interfaced with the SPI peripheral module of the microcontroller.

The sensor node is communicating the information to the base station. The base station has internet facility and team viewer software for viewing information at distance. Through the Internet the information is shared to the outside world. The developed sensor node module and designed base station is shown in Fig. 3. The sensor node will measure the temperature and humidity at the target area and communicated to the base station. The information displayed at base station is shown in Fig. 4.

The front end solution is easy to implement to monitor the environmental parameters. The TCP/IP solution need security implementations. The gateway solution is more expensive than the front end solution. We have designed the base station and sensor node. The base station could communicate with the sensor node through the transceiver unit. The designed Transceiver unit is shown in Fig. 5.

The authenticated information is communicated to the sensor node from the base station before receiving the environmental parameters.

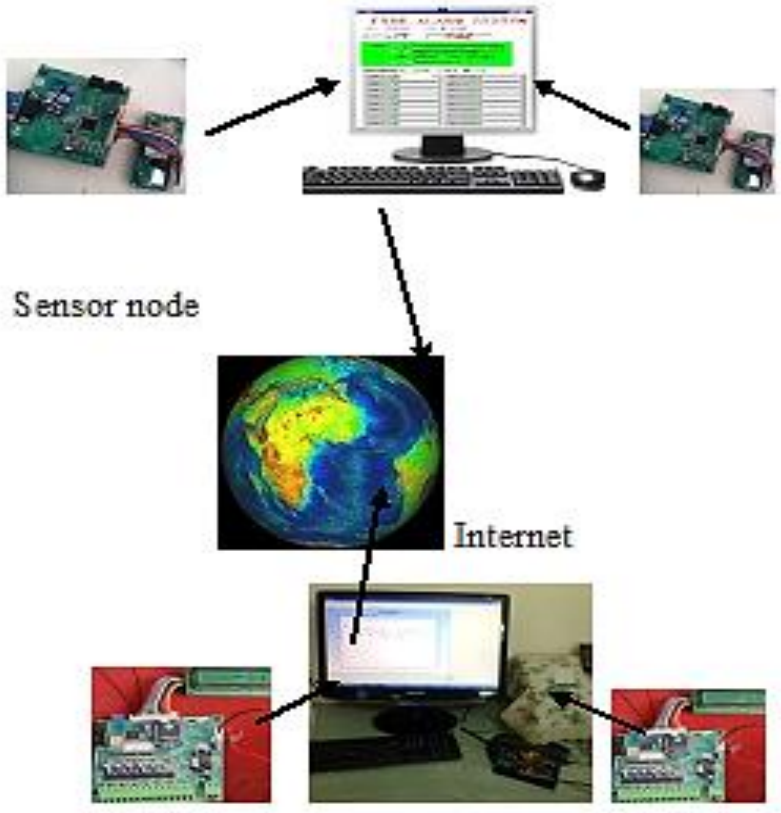

Figure 3. Sensor node and base station design.

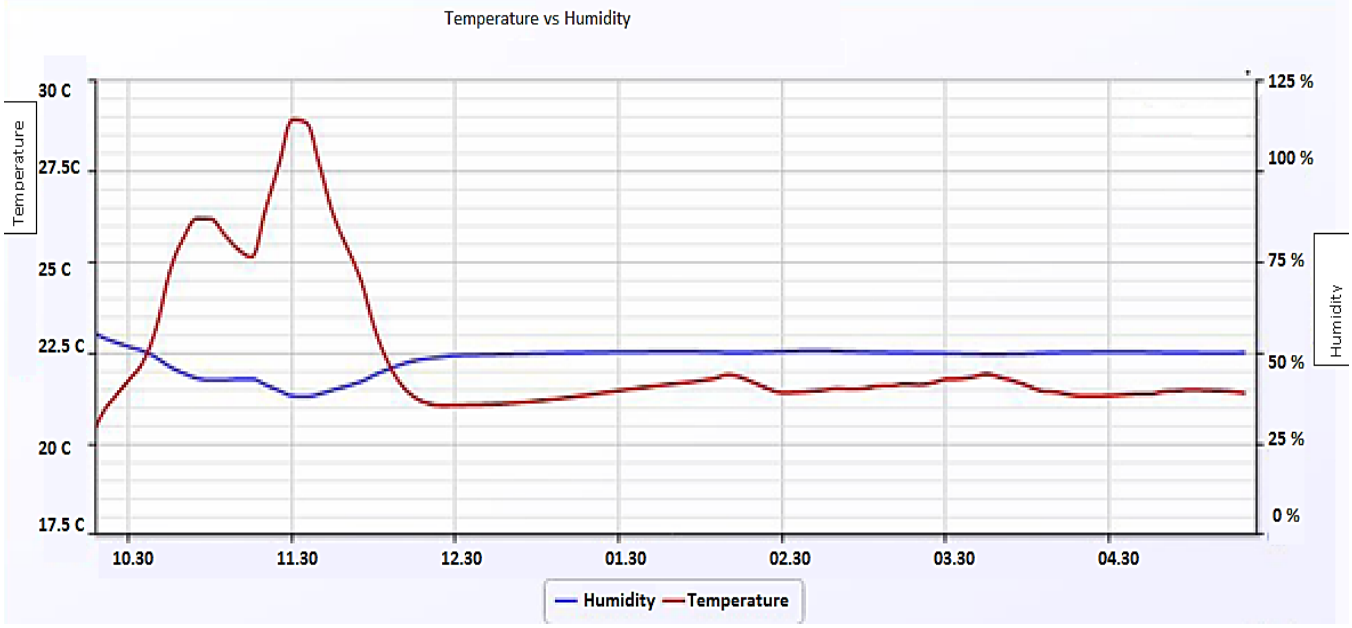

Figure 4. Display of temperature and humidity output at the base station.

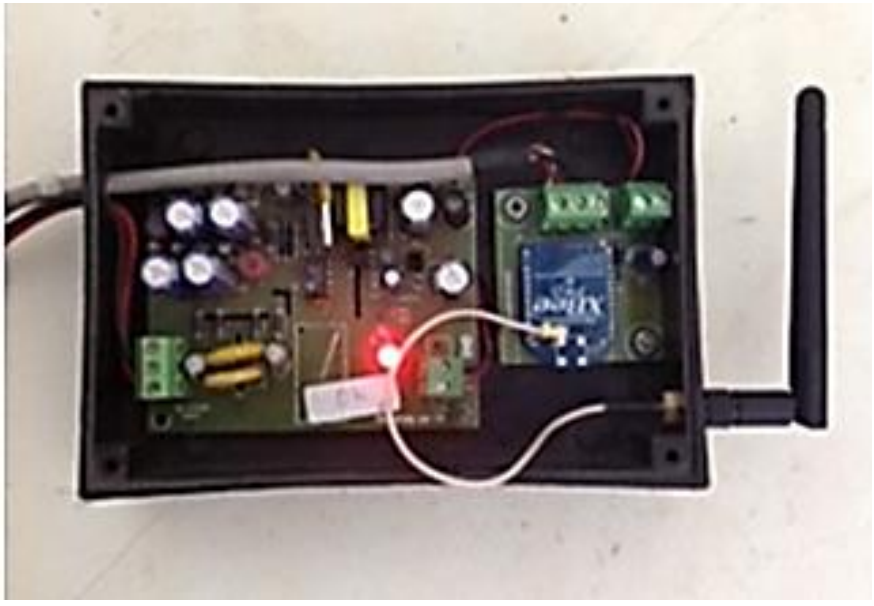

Figure 5. Transceiver unit.

6. CONCLUSION

The development of wireless sensors networks with the integration of Internet of Things arise new challenges in several fields. This system includes two aspects, hardware and software. The hardware is composed of one base station with RS232 & XBeepro and several sensor nodes. The sensor node and base station control module are designed. The software aspect mainly consists of one monitoring center/ base station that can supervise all the location, through the information given by all the nodes inside the whole network. The front end solution is the easy way to integrate the IoT and WSN for environment monitoring.

ACKNOWLEDGMENT

This work is supported by the University Grants Commission, Government of India under grant no. F.151/2014-15/PDFWM-2014-15-OB-TAM-24657.

AUTHORS

S. R. Vijayalakshmi is a Post Doctoral research Fellow in Department of Electronics and Instrumentation in Bharathiar University. She received her B.Sc. M.Sc. M.Phil. and Ph.D in Electronics from the Bharathiar University and also received M.Sc. in Computer Science from Bharathiar University and M.Phil. in Computer Science from Avinashilingam University. She has experience in the teaching field and also in research. Her research interests include digital image processing, embedded systems, real time systems, wireless sensor networks and Microprocessors. She completed one DST-WOS-A project funded by Government of India.

S. Muruganand is an Assistant Professor in Department of Electronics and Instrumentation in Bharathiar University. He received his M.Sc. Physics from Madras University, M.Ed. from Annamalai University and Ph.D from Bharathiar University. He has 25 years of experience in the teaching and research field. His research interests include digital image processing, embedded systems, nano science, power electronics, wireless sensor networks,

thin films, biomedical and Microprocessors. He completed one UGC - Minor project funded by Government of India. He is author of many papers in the referred journals.

References

[1] Sudipta Bhattacharjee et al., Wireless sensor network-based fire detection, alarming, monitoring and prevention system for Bord-and-Pillar coal mines. *The Journal of Systems and Software*, 85 (2012) 571-581

[2] Daniela Ballari et al., A mobility constraint model to infer sensor behaviour in forest fire risk monitoring. *The Journal Computers, Environment and Urban Systems*, 36 (2012) 81-95.

[3] Junguo Zhang et al., Forest fire detection system based on a ZigBee wireless sensor network. *Journal front for China*, 3 (2008) 369-374

[4] Cetin Elmas and Yusuf Sonmez, Data fusion framework with novel hybrid algorithm for multi-agent Decision Support System for Forest Fire. *Expert Systems with Applications*, 38 (2011) 9225-9236

[5] Andrey Somov et al., Deployment and evaluation of a wireless sensor network for methane leak detection. *Sensors and Actuators*, 202 (2013) 217-225

[6] Zujue Chen et al., Design of wireless sensor network node for carbon monoxide Monitoring. *Telecommunication Systems*, 53 (2013) 7-53

[7] Hakilo Sabit et al., Wireless Sensor Network Based Wildfire Hazard Prediction System Modeling. *Procedia Computer Science*, 5 (2011) 106-114

[8] Andrey Somov et al., Deployment and evaluation of a wireless sensor network for methaneleak detection. *Sensors and Actuators*, 202 (2013) 217-225

[9] Yeon-sup Lim et al., A Fire Detection and Rescue Support Framework with Wireless Sensor Networks. *International Conference on Convergence Information Technology*, (2007) 135-138

[10] Daniela Ballari et al., A mobility constraint model to infer sensor behaviour in forest fire risk monitoring. *The Journal of Computers, Environment and Urban Systems*, 36 (2012) 81-95