International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 10, Issue 2, March-April 2019, pp. 210-214. Article ID: IJARET_10_02_020
Available online at http://iaeme.com/Home/issue/IJARET?Volume=10&Issue=2
ISSN Print: 0976-6480 and ISSN Online: 0976-6499

METHODOLOGIES AND CHALLENGES OF WSN FOR IOT

Dr Syeda Gauhar Fatima
Professor ECE dept, Deccan College of Engineering and Technology,
Darussalam, Hyderabad, India

Syeda Kausar Fatima
Associate Professor, Shadan College of Engineering and Technology, Hyderabad, India

Syed Mohd Ali
Research Scholar, ECE dept, JNTUH, Kukatpally, Hyderabad, India

Naseer Ahmed Khan
Student, ECE Dept, Deccan College of Engineering and Technology,
Darussalam, Hyderabad, India

Syed Adil
Student, ECE Dept, Deccan College of Engineering and Technology,
Darussalam, Hyderabad, India

ABTRACT

Wireless sensor networks (WSNs) are discovering a wide range of applications in various fields, counting control networks, enhanced-living scenarios, health-care, industrial, production monitoring and in many other sectors. Internet of Things (IoT) confirms smart human being life, through communications between things, machines together with peoples. Hence, Relocation of Internet from People towards an Internet of Things (IoT) and addition of Wireless sensors in to Internet of Things enables sensors nodes connect internet dynamically in order to cooperate and achieve their tasks. However, when WSNs become a portion of the Internet, we must carefully examine and scrutinize the issues involved with this integration. In this paper, we evaluate various methods to combine WSNs into the IOT and discuss a set of challenges.

Keywords: WSN; IOT; Integration approaches; Issues; Challenges.

Cite this Article: Dr Syeda Gauhar Fatima, Syeda Kausar Fatima, Syed Mohd Ali, Naseer Ahmed Khan and Syed Adil, Methodologies and Challenges of WSN for IOT, *International Journal of Advanced Research in Engineering and Technology*, 10(2), 2019, pp. 210-214.
http://iaeme.com/Home/issue/IJARET?Volume=10&Issue=2

1. INTRODUCTION

The chief impression of IoT [1] is enduring presence for variety of objects such as radio-frequency identification (RFID) tags, sensors, actuators, mobile phones, etc.-which, having unique addressing schemes and are able to view each other and cooperate with their neighbors to reach mutual goal line. Wireless sensor networks (WSNs) are ad hoc networks which contain a big amount of small sensor nodes with limited resources and one or more base stations. If we wish to read the data from anyplace in the world, we need to assimilate the WSNs into the Internet as part of the IoT. A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations.

Since dynamically joining of Sensor nodes in to the Internet, careful examination is required while integrating WSN and IOT. Lot of issues are involved with this integration. These issues and challenges are required to be handled for getting compensations and reimbursements of such integration. This paper presents different methods of integration of WSNs and Internet, issues and challenges. Summarization of this paper is as follows: we discoursed WSN and Internet with a view that WSNs are part of the Internet of Things in Section I. WSN applications are discussed in Section II taking into consideration of issues involved with this integration. Different additional approaches are debated in Section III and critical challenges to be addressed to realize the full potential in integration of WSN into the Internet are discussed in Section IV. Finally in Section V, we summarize our discussion regarding integration approaches, issues and challenges of WSN for IOT.

2. WSN APPLICATIONS

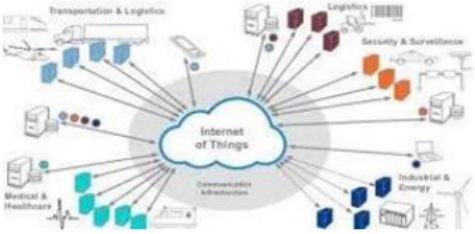

Figure 1 Internet of Things

A network of dissimilar electronic devices can be considered as Internet of Things (Fig.1) wherein without direct intrusion of the people the interaction takes place between people and sensing information. Here, sensing and processing of data for proper interaction will be achieved by the Device which is acting as a smart node in the network. Using key technology like low power wireless connectivity, Smart objects are connected to the centralized cloud and internet.

Applications areas of the wide wireless sensor network can be segmented into different groups viz. Monitoring of space, objects and communications between space and objects. Further the same can be prolonged to the additional category of monitoring human beings.

Environmental monitoring is an example for application area of the wireless sensor network. Environmental parameters like temperature, moisture or light sensor readings are collected using WSNs for different environments including mountains, forests and glaciers.

Observing particular objects like Structural monitoring becomes the second category. It detects the ruptures of the structure and mechanical adjustments of bridges or buildings by sensing the parameters like acoustic emissions, responses to stimuli and modes of vibration, etc.

Monitoring environmental threats like volcanic activities and floods can be considered as an example of the combined activity of Monitoring interaction between space and objects.

Further to the projected classifications, monitoring human beings becomes the last category. In this case, the sensors can gather information on medical conditions using different functional parameters and also can be used in monitoring the mandatory data like in home care scenario, etc.

High diversity of WSN applications has been demonstrated from the projected category of applications like monitoring environments and subjects, etc. Integration of WSN into the Internet through suitable approach by considering this scenario of diversity will be useful for the Internet of Things.

Development of IoT substructure around WSN is under development by different corporations [2]. Examples are 'A Smarter Planet' project by IBM for utilizing sensors for water management systems and intelligent cities and CeNSE project for deployment of a worldwide sensor network to create a "central nervous system for the Earth" by HP Labs.

3. INTEGRATION APPROACHES

Three main approaches are discussed here for Connecting WSNs to the Internet, which is mainly considering the WSN integration degree into the Internet structure. In first approach (Fig. 2) a single gateway is used to connect the independent WSN to the Internet. This approach is accepted for connecting most of the WSNs to access the Internet, and also interaction between networks.

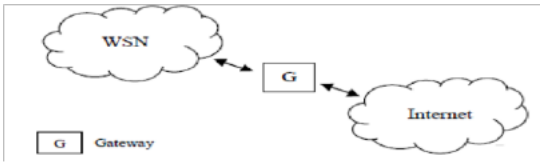

Figure 2 Approach of Independent Network

From the cumulative integration degree point of view, the second approach (Fig.3) of hybrid network formed which consists of two independent network structures but rare dual sensor nodes can access of the Internet.

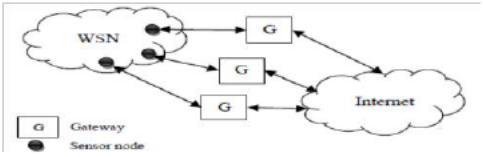

Figure 3 Approach of Hybrid Network

In Fig.4 , the last approach multiple sensor nodes are joining the Internet in one hop. It is similar to the WLAN structure and forms 802.15.4 access point network.

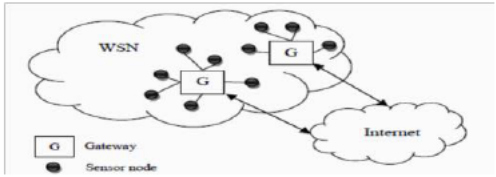

Figure 4 Approach of Access point Network

From the first approach it is obvious that the failure of Gateway functioning leads to the breakdown of connection between Internet and WSN. However due to the several gateways exists in the other two approaches this type of network failure will not be clear. Hence depending on the WSN application scenario, one of these two approached would be favored if network structure is maintained by the required application. As per distance point of view, and for the WSNs organized in Mesh topology the second approach is preferable. As per the WSN

application classifications discussed in the previous section, "monitoring space" and the "monitoring interactions between objects and space" prefers this Hybrid network approach.

Since using the third and last approach Internet can be accessed in one hop, WSN applications requiring low latency prefers this access point approach. Hence, as per the proposed WSN applications for monitoring of objects and human beings this approach is preferred.

It has experiential the static network configuration from the second and third integration approaches. As it is known that gateway reprogramming is required for the new device to join the network. Hence, this requirement cannot be achieved in the existing form from both the approaches. To fulfill this requirement "IP to the Field" paradigm may be proposed. As per this model, sensors nodes are provided with the intelligence apart from the sensing tasks. Protocol translation and forwarding functionalities are only given to the Gateway. From this, dynamic network configuration would be attained and reprogramming of gateway operations are no longer be required.

4. CHALLENGES FOR WSNS IN AN INTERNET OF THINGS

In addition to their usual sensing functionality sensor nodes are assigned with the additional tasks with this "IP to the Field" paradigm. Accordingly, new tasks or challenges are to be faced by the sensor nodes with this additional responsibility. Out of these, three potential tasks are discussed here: Security, quality of service (QoS) management, and network configuration.

4.1. Security

on the sensitivity of application WSNs has the capability to provide data confidentiality, authentication, integrity and availability without having internet access. To introduce malicious nodes in the existing network or jamming or capturing, the physical presence near the WSN is required by the attacker. However, this opening of WSNs into the internet enables attackers to perform their malicious activities [3] from everywhere. Hence, the issues developed by this internet connection like malware and others should be definitely addressed by the WSNs. To ensure efficient protection by the current WSNs they are provided with central and unique powerful gateway. However, due to the scarce of computational resources, energy and memory constraints it is difficult to reuse the existing security mechanism. In fact, common Mica2 motes offer 7.3 MHz 8-bit microcontrollers with 128 Kbytes of reprogrammable flash memory, 4 Kbytes of RAM and 4 Kbytes of EEPROM. Similar to the other Internet services, sensor nodes are yet to support the cryptography with key lengths like RSA-1024 for better confidentiality. Further, to avoid different attacks arising from Internet, it is required to develop better security mechanisms[4] taking into account of the existing resource constraints.

4.2. Quality of Service

Considering the Intelligence provided to the sensor nodes, they are also required to contribute to quality of service by utilization of all mixed devices of the Internet of things. These mixed devices make the possibility of the workload distribution between the nodes with the available resources. Due to dynamic network configurations and link characteristics, it is not adequate to operate the existing approaches of QoS available on the Internet [5]. Hence, better approaches are required to be developed to avoid latency and loss of data, etc.

4.3. Configuration

Additional to the security and QoS management, sensor nodes should be able to handle diverse tasks like handling their network configuration for new node joining the in the network [6] and ensuring self-healing competences through detection and elimination of faulty nodes and address administration to ensure scalable network constructions, etc. However, in the Internet it is not a common feature of joining of new node through self-configuration. Hence, for smooth operation of this network configuration, required applications are to be installed by the user and necessary precautions to be taken to avoid the system crashes.

5. CONCLUSION

Here, we considered selected expanded application scenarios like monitoring environments and subjects to examine the integration of WSNs into the Internet.

Considering their main features, three different integration approaches are examined [7]. However, it is practical that these approaches are not supporting the requirement of dynamic network configuration of Internet of Things for new node joining the network in the existing form. Hence, as a solution to this, we considered IP to the Field pattern through providing intellect to the sensor nodes. Further, three different challenges to be addressed are highlighted from this pattern option: Security, QoS, and configuration management. By analyzing these challenges, it is observed that the existing solutions in the Internet are not suitable for these sensor networks having dynamic network configurations [8]. Hence, better mechanisms are to be developed and adapted considering the constraints of WSNs.

REFERENCES

[1] J. A. Stankovic, "Research directions for the Internet of Things," IEEE Internet Things J., vol. 1, no. 1, pp. 3–9, Feb. 2014.

[2] IBM: A Smarter Planet, http://www.ibm.com/smarterplanet/, Accessed on October 2010.

[3] J. Claessens. Trust, Security, Privacy, and Identity perspective. Panel on Future Internet Service Offer, 2008

[4] C.P. Mayer. Security and Privacy Challenges in the Internet of Things. KiVS Workshop on Global Sensor Network, 2009.

[5] R. Roman, J. Lopez. Integrating Wireless Sensor Networks and the Internet: a Security Analysis. Internet Research, Vol. 19, no. 2, pp. 246-259, 2009.

[6] M. A. Ezechina, K. K. Okwara, C. A. U. Ugboaja. The Internet of Things (Iot): A Scalable Approach to Connecting Everything. The International Journal of Engineering and Science 4(1) (2015) 09-12.

[7] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems 29.7 (2013): 1645-1660.

[8] A. Menon1, et al. " Implementation of internet of things in bus transport system of singapore" Asian Journal of Engineering Research (2013).

[9] T. Aravinda Babu and K.S.R.S. Jyothsna, IOT Based Smart Vehicle and Smart Parking System: International Journal of Electrical Engineering & Technology, 9(3), 2018, pp. 121–136.

[10] Sharmila Nath, Jayanta Kumar Nath and Kanak Chandra Sarma, IoT Based System for Continuous Measurement and Monitoring of Temperature, Soil Moisture and Relative Humidity. International Journal of Electrical Engineering & Technology, 9(3), 2018, pp. 106–113

[11] IOT Based Toll Collection System Using Image Processing, Malvik Patel, Bharavi Joshi, Kajal Bhagat and Hetakshi Desai and Jekishan K. Parmara. International Journal of Computer Engineering & Technology, 9(3), 2018, pp. 132– 139.

[12] Mr. N. Sampathraja, Dr. L. Ashok Kumar, Mr. K. Vishnu Murthy, Ms. V. Kirubalakshmi and Ms. C. Muthumaniyarasi, Iot Based Underground Cable Fault Detector, International Journal of Mechanical Engineering and Technology 8(8), 2017, pp. 1299–1309.

[13] Ganesh Babu Loganathan, Dr.E.Mohan and R.Siva Kumar, Iot Based Water and Soil Quality Monitoring System, International Journal of Mechanical Engineering and Technology, 10(02), 2019, pp. 537–541

[14] M. Tanooj Kumar, S.L. Narayana Reddy, B. Katyayini and Sk. Shabana Azmi, Optimized and Secured Storage Approach For IOT Based Applications, International Journal of Mechanical Engineering and Technology 8(12), 2017, pp. 699– 702.

[15] G.Sasi, P.G.Akila, R.ambika and Dr.G.Athisha, Performance Analysis of IOT Based Smart Sensors In Agriculture, International Journal of Mechanical Engineering and Technology (IJMET), Volume 9, Issue 11, November 2018, pp. 1936-1942.

[16] Snehal R. Shinde, A. H. Karode and Dr. S. R. Suralkar, Review onIOT Based Environment Monitoring System, International Journal of Electronics and Communication Engineering and Technology, 8(2), 2017, pp. 103–108.