International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Integration Approaches and Challenges of WSN for IoT

B. LasyaSri[1], L. Nirmala Devi[2]

[1]Deputy Manager,HAL, Hyderabad, Telangana, India
[2]Associate Professor, OUCE, Osmania University, Hyderabad, Telangana, India

---

Abstract: *Wireless sensor networks (WSNs) are finding a wide range of applications in various domains, including control networks, enhanced-living scenarios, health-care, industrial, production monitoring and in many other sectors. Internet of Things (IoT) ensures smart human being life, through communications between objects, machines together with peoples. Hence, Migration of Internet from People towards an Internet of Things (IoT) and integration 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 part of the Internet, we must carefully investigate and analyze 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.**

1. INTRODUCTION

The primary idea of IoT [1] is permanent 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 collaborate with their neighbors to reach common goals. Wireless sensor networks (WSNs) are ad hoc networks which consist of a large number of small sensor nodes with restricted resources and one or more base stations. If we wish to read the data from anywhere in the world, we need to integrate 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 investigation 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 advantages and benefits of such integration. This paper presents different approaches of integration of WSNs and Internet, issues and challenges. Summarization of this paper is as follows: we discussed 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 integration approaches are discussed 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

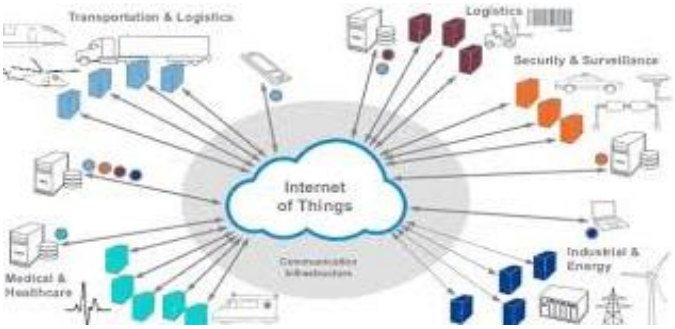

Fig.1: Internet of Things

A network of different electronic devices can be considered as Internet of Things (Fig.1) wherein without direct interference of the people the interaction takes place between people and sensing information. Here, sensing and processing of data for proper interaction will be performed by the Device which is acting as a intelligent 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 divided into different categories viz. Monitoring of space, objects and interactions between space and objects. Further the same can be extended 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 gathered using WSNs for different environments including mountains, forests and glaciers.

Observing particular objects like Structural monitoring becomes the second category. It detects the breakages of the structure and mechanical modifications 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 proposed classifications, monitoring human beings becomes the last category. In this case, the sensors can gather information on medical conditions using different physiological parameters and also can be used in monitoring the required data like in home care scenario, etc.

High diversity of WSN applications has been illustrated from the proposed 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 beneficial for the Internet of Things.

Development of IoT infrastructure around WSN is under development by different companies [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 adopted for connecting most of the WSNs to access the Internet, and also interaction between networks.

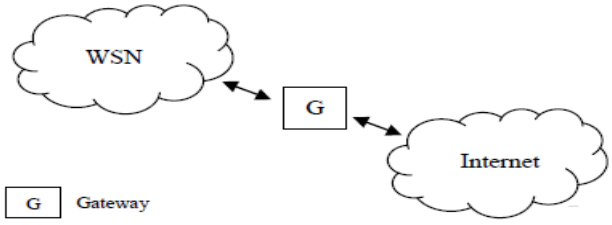

Fig.2: Approach of Independent Network

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

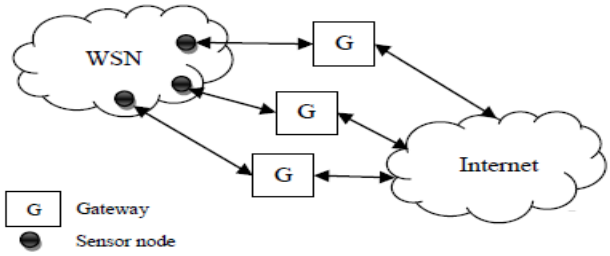

Fig.3: Approach of Hybrid Network

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.

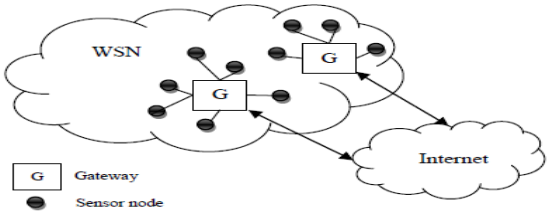

Fig.4: Approach of Access point Network

From the first approach it is noticeable that the failure of Gateway functioning leads to the breakdown of connection between Internet and WSN. However due to the multiple gateways exists in the other two approaches this type of network failure will not be noticeable. Hence depending on the WSN application scenario, one of these two approached would be preferred if network structure is supported 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 observed 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 responsibilities 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:

Depending 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 heterogeneous devices of the Internet of things. These heterogeneous 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 sufficient to utilize 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

Further to the security and QoS management, sensor nodes should be able to handle different tasks like managing their network configuration for new node joining the in the network [6] and ensuring self-healing capabilities 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 diversified application scenarios like monitoring environments and subjects to analyze the integration of WSNs into the Internet. Considering their main characteristics, three different integration approaches are analyzed[7]. However, it is observed 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 paradigm through providing intelligence to the sensor nodes. Further, three different challenges to be addressed are highlighted from this paradigm option: Security, QoS, and configuration management. By analyzing these challenges, it is noticed 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).