IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 2, February 2017

Wireless Sensor Networking in the Internet of Things

Rohini Anand Nimbekar[1]

Student, Computer Technology, Bharati Vidyapeeth Institute of Technology, Mumbai, India[1]

Abstract: Internet of the future known as the "Internet of Things" (IOT) is a global web of things that are uniquely addressable based on standard protocols. In the recent past years we have seen many technological evolution like the transition from the analog world into its digital world and from centralized wired to distributed and then into pervasive wireless systems. In our everyday lives wireless sensor networks are increasing tremendously. Applications such as control networks, enhanced-living scenarios, health-care, industrial and production monitoring and in many other sectors are growing widely. Wireless sensor network likely to be integrated into "Internet of Things" and the sensors nodes connects internet dynamically in order to cooperate and achieve their tasks. In this paper, we appraise various methods to combine WSNs into the Internet and shape a set of challenges in the upcoming future.

Keywords: Networks, Internet of Things, Internet, Security, wireless sensor networks (WSN).

I. INTRODUCTION

The IOT is an intelligent network which provide services to interact and exchange data through the sensing devices. It accomplish the aim of tracking, monitoring, smart identifying and managing things [1]. Internet of things (IOT) is set of everyday object consists of sensors which sense the information based on the context and transfer it to the central database system through wired network or wireless network such as Bluetooth, wireless Fidelity(Wi-Fi), 3G or 4G. The interaction between computer system, people and the nearby environment is sensed and controlled by wireless sensor network [2].

In the growing Internet of Things, each and every thing that are around us will turn into proactive actors of Internet, generating and consuming information. Wireless sensor networks is an important component of Internet of Things. The benefits of interconnecting both WSN and other IOT component can collaborate and can provide facilities as heterogeneous information systems [3].

Now a days IOT is achieving popularity just because of improved technology, efficient analytical tools, low cost sensors and reduced storage. Due to the adoption of a digital communication interface the exchange of information and single interaction media by various devices is become possible. Centralized approach has brought measurement solution where many devices are connected to the sensors which are linked with central acquisition and processing system. By using WSN the object's information is widely shared across each and every object using internet and even they can be accessed from a remote area [4]. For the purpose of connecting devices, each device need unique IP address. But just having IP connection does not mean that every sensor node should be straight connected the internet. There may have many challenges which includes security that one must safely addressed.ss

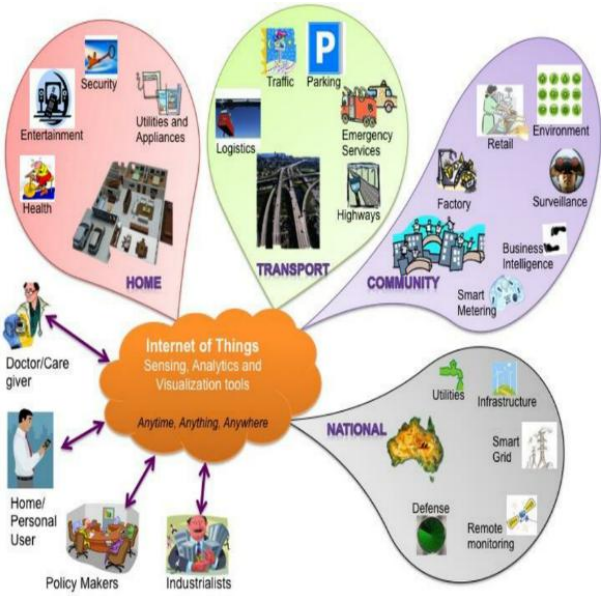

Fig.1. General Block diagram of working of IOT

II. SELECTED WSN APPLICATION

Internet of Things can be termed as a network of universal electronic devices where the interaction between people and sensing information take place without direct people interference. Device act as intelligent node in the network by sensing data and performing low-level signal processing in order to filter signals from noise and to decrease the bandwidth required for the interaction. To protect, process information, store and bounce actionable data to people in safe manner we required nodes to interact with a centralized database. Smart objects are connected to the internet and centralized cloud by using key technology which is been represented by low power wireless connectivity. Single technology is not ruled by wireless

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 2, February 2017

connectivity instead they liable on requirements and technology conditions which might need different software and hardware integrations [5]. Wireless sensor network application sector can be categorised into three main types.

First category includes the environmental monitoring such as monitoring object, monitoring space and interaction between this both. Second category includes observing certain objects and by sensing through acoustic emissions, responses to stimuli, vibration the issues can be detected [6]. The third and the last category mainly focus on observing human being especially in terms of medical area, monitoring elderly people, etc.

III. INTEGRATION APPROACHES

From the network point of view a WSN is partially integrated or completely integrated to the Internet or not must be checked for this initially it important to know what type of integration approach can be applicable in order to connect stack based and topology based structures. In fig.2 the integration approaches are shown in two different types: stack-based [7] and topology-based [8]. The first approach is stack based approach, in this approach according to similarities between their network stacks the integration among WSN and the Internet takes place. With the help of single gateway WSN and the Internet are connected. A WSN can exchange data with Gateway (Internet hosts) even they can share a well suited network layer protocol (TCP/IP). The second approach is topology based approach this forms a hybrid network which consists of independent network from where sensor nodes can access the Internet. In this approach the integration of nodes mainly depends on the real location in order to give access to the Internet. In the first approach we may face certain problems that might take place because of weak gateway.

Due to failure of gateway the connection between WSN and the Internet can be disconnected and this may cause problems. The second approach is adopted because WSN can conserve such organization by having a centralized gateway rather than having common individual base station without Internet access. Nevertheless, in topology approach the hybrid network and access point network provides static network configuration. Now a days many upcoming new devices try to connect to the Internet for this time consuming gateway reprogramming is needed.

For this purpose the flexibility is expected by the future which cannot be achieved by this recent form. So to satisfy and accomplish this expectation "IP to the Field" model can be used [9]. In this model sensor nodes are expected to be smart network elements which will have no limitations for sensing tasks. By passing the control of sensor nodes, the gateways process would be restricted to protocol translation and repetition. Subsequently, dynamic network configuration could be attained and no more operations required for gateway reprogramming.

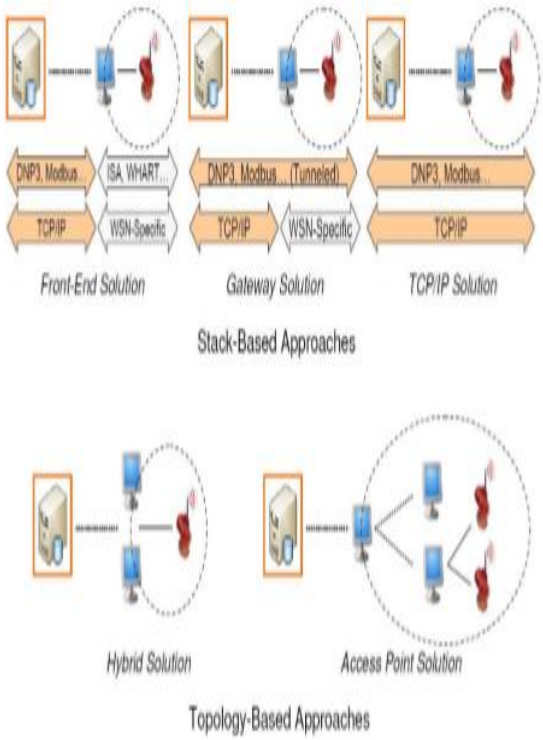

Fig.2. Integration Approach

IV. CHALLENGES OF WSN'S IN AN INTERNET OF THINGS

WSN is permitted to become an essential of IOT various security challenges should be measured. The user acceptance and security mechanism are main challenges of integration. These challenges are part of WSN but those can be used in other terms of IOT [10]. IOT security need to be assumed from a global point of view. IOT should satisfy the need of user without breaking their trust. It has introduced "IP to the field paradigam" which includes many tasks to sensor node along with their normal sensing functionality. To focus and deliberate the challenges the three tasks that sensor node should complete that are security and quality of service management, and network configuration.

A. Security:-

In WSN's deprived of internet access sensor nodes act as main role to provide integrity, confidentiality, availability and authentication according to the sensitivity of an application. In addition to this novel location diversity, WSNs may address new threats such as malware, worms which is introduced by Internet and the attackers. WSN connected to Internet are secured by a central and unique powerful gateway provides efficient security [11]. IOT component provides security mechanism at network level as well as provide means of interaction between services and objects. To provide services efficiently IOT should combine different technologies. Security point of view basic infrastructure and objects must be capable of various identification. Such interaction between objects should be under control and should give numerous services to the

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 2, February 2017

world. Having safe interaction between objects and services is an interesting challenges in IOT [12]

B. Quality of Service:
In the gateway acting along with protocol translator and repeater, sensor nodes also take part in quality of service management enhancing the resource consumption of future devices of Internet of Things. In fact, resource differences may be exploited to share the current workload between nodes offering available resources. Improving the quality of service, such collaborative work is consequently promising for mechanisms requiring high amount of resources like security mechanisms. In WSNs present approaches provides quality of services in the Internet are not measured as many variations in features may lead to significant reconfiguration of the WSN topology.

C. Configuration
Along with the quality of service and security, sensor nodes also need to control the WSN configuration which have various tasks such as self-healing capabilities, address administration or handling their own features. However, self configuration of participating nodes is not a common feature in the Internet. Instead, the user is expected to install applications and recover the system from crashes.In contrast, the unattended operation of autonomous sensor nodes needs novel means of network configuration and management.

V. CONCLUSION

The aim of this chapter is to discuss few importances of WSNs. IOT is capable of interconnecting each and every intelligent gadgets in order to have interaction between people, share information, manage things, improve the quality of services. WSN provides us a new opportunity to handle every activities in a smarter way and gives us smart interaction standards which empowers setting up smart network capable of managing applications that evolve from user requirements. Sensor network will grow in future lives with the wide range of applications. Thus new security structure will improve security into WSN integration and IOT and as well as will help to put a great impact on our daily life.

ACKNOWLEDGMENT

This research was supported by teachers. We thank our colleagues who provided us various resources which assisted for research and help to complete this paper.

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] BRÖRING, A. et al. New generation sensor web enablement. Sensors, 11, 2011, pp. 26522699. ISSN 1424-8220. Available from: doi:10.3390/s110302652
[3] IBM: A Smarter Planet, http://www.ibm.com/smarterplanet/, Accessed on October 2010.
[4] Daqiang Zhang, Laurence T. Yang, Hongyu Huang, "Searching in Internet of Things: Vision and Challenges", Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications, 2011.
[5] http://www.st.com/content/ccc/resource/sales_and_marketing/promotional_material/brochure/d7/74/dc/eb/b4/f5/40/d5/brwireless_web.pdf/files/brwireless_web.pdf/jcr:content/translations/en.brwireless_web.pdf
[6] Talzi, A. Hasler, S. Gruber, and C. Tschudin, "PermaSense: investigating permafrost with a WSN in the Swiss Alps," in Proceedings of the workshop on Embedded networked sensors (EmNets), 2007.
[7] R. Roman, J. Lopez. Integrating Wireless Sensor Networks and the Internet: a Security Analysis. Internet Research, Vol. 19, no. 2, pp. 246-259, 2009.
[8] D. Christin, A. Reinhardt, P.S. Mogre, R. Steinmetz. Wireless Sensor Networks and the Internet of Things: Selected Challenges. 8th GI/ITG KuVS Fachgesprch "Drahtlose Sensornetze", 2009.
[9] Smart Energy Alliance, online, http://www.smart-energyalliance.com/solutions/ip-to-the-field/.
[10] C.P. Mayer. Security and Privacy Challenges in the Internet of Things. KiVS Workshop on Global Sensor Network, 2009.
[11] Crossbow Technology, online, http://www.xbow.com.
[12] J. Claessens. Trust, Security, Privacy, and Identity perspective. Panel on Future Internet Service Offer, 2008

BIOGRAPHY

Rohini Anand Nimbekar was born in Nagpur on 10th May 1998. Im currently pursuing Diploma in Computer Technology from Mumbai, India. I have published two paper in International journal. My area of intrest are security, Internet of Things,Wireless networks, Digital Techniques.