International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-5, Issue-12)

Research Article | **December 2016**

Evolution of Wireless Sensor Networks as the framework of Internet of Things- A Review

Keshav Kishore *
Ph. D Scholar,
Department of Computer Applications
Magadh University, Bodhgaya (Bihar) India

Shamneesh Sharma
IT- Head & Associate Professor
Department of Computer Science & Engineering
A P Goyal Shimla University, Shimla (H.P.) India

Abstract—

After the evolution of the wireless sensor networks, the next level of technology is Internet of Things (IoT)/Web of Things (WoT). Internet of things is not a very new concept but its applications are making it quite popular among the users over Internet. As the concept of IoT is applicable in numerous scientific fields, it is becoming universal application or one stop solution for every user's need. This paper presents a review of evolution of Wireless Sensor Networks Technology over the Internet of Things. Since WSN can act as core of IoT/WoT so the advantages of WSN can be directly utilized in IoT/WoT. Just as Wireless Sensor Networks, in Internet of Things, there is the encounter of monitoring of physical parameters, but desired outcomes are little different. As sensor nodes can be deployed and managed dynamically, IoT can act as Application/ service layer where as WSN can act as Network/Communication layer. The user can develop custom middleware according to its requirements. There are many layers in IoT which makes it flexible in term of usability, customization and choice of services. As the IoT is the evolving technology hence there is a certain amount of inevitable IoT components which can be different in each reference architecture.

Keywords— Wireless Sensor Networks, IoT, WoT, M2M, MEMS and Data Dissemination

I. INTRODUCTION TO INTERNET OF THINGS

In most of the organizations, information travels along proverbial routes. Proprietary information is wedged in databases and scrutinized in reports. Information also originates superficially gathered from public sources, harvested from the Internet. But the conventional conduits of information are changing: the physical world itself is becoming a type of information system. The Internet of Things (IoT) is a system of unified computing devices, mechanical and digital machines, objects, animals or people that are provided with inimitable identifiers and the ability to transfer data over a network without entailing human-to-human or human-to-computer interaction. In Internet of Things, a thing [1] can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network. It has come up with a general of network devices to sense and accumulate data from the world around us. After the data dissemination, it shares the collected data across the internet for further processing according to the user's desires. Basically Internet of Things is the network of physical objects proscribed and supervised over internet

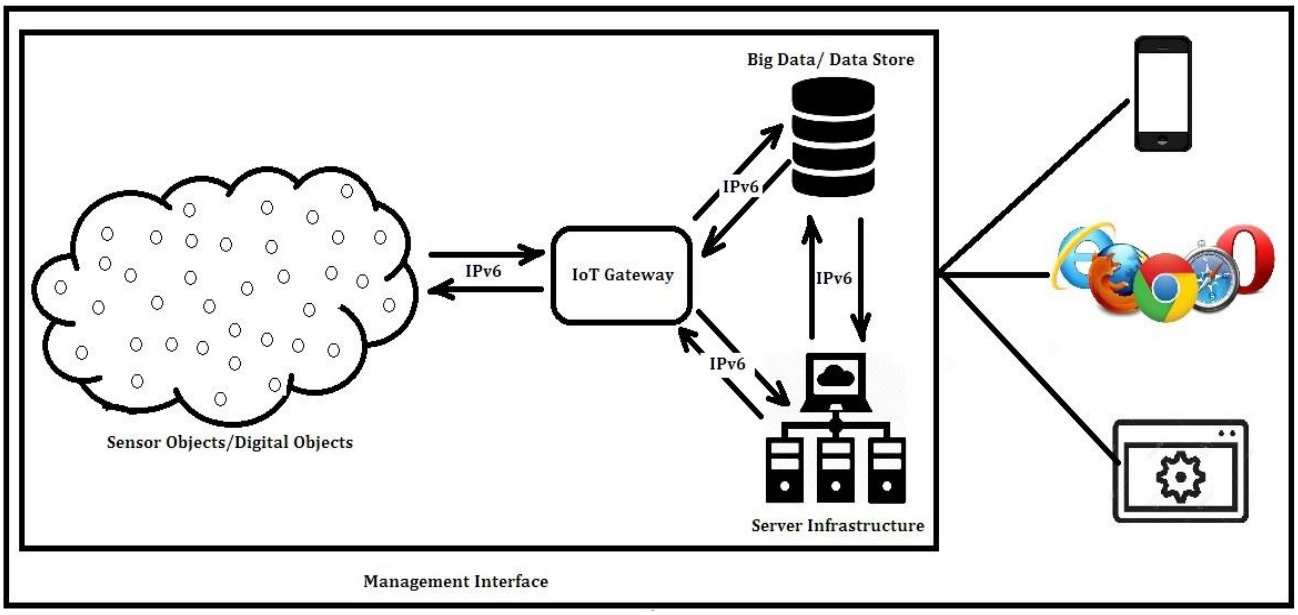

Fig. No. 1: Working of Internet of Things

IoT is more like as M2M [2] communication which is a form of data communication that involves one or more entities that do not necessarily require human interaction or intervention in the process of communication.

The problem is that people have limited time, interest and precision which means they are not very virtuous at incarcerating data about things in the existent world. If there will be computers that know everything and gather data without any help, we would be able to track and tally everything and significantly condense waste, loss and cost. In nutshell IoT is the network of physical digital objects being controlled and monitored over internet. It typically contains sensors, wireless radios, IPv6 and management tools. This technology is still in research and development phase.

II. INTRODUCTION TO WSN

A wireless network of sensor nodes for the communication is known as Wireless Sensor Network [3]. A sensor node is made up of four main components i.e. radio, processor, sensors and battery. The wireless sensor network is a network of Micro- Electro- Mechanical- System (MEMS) which has the following characteristics:

1) Self- Computation Capabilities.
2) Communication Capabilities.
3) Sensing Capabilities.

The working of the wireless sensor network is entirely based on its architecture or on the deployment method of sensor nodes. The initialization of the network is done by deploying the sensor nodes of same or different features; rest of the working depends upon the design of the node and the mode of application. Wireless sensor networks are very much application and system model dependent. Algorithms/protocols that are designed based on one system model usually do not produce the same results or show the same effectiveness when they are applied on another system model without modification.

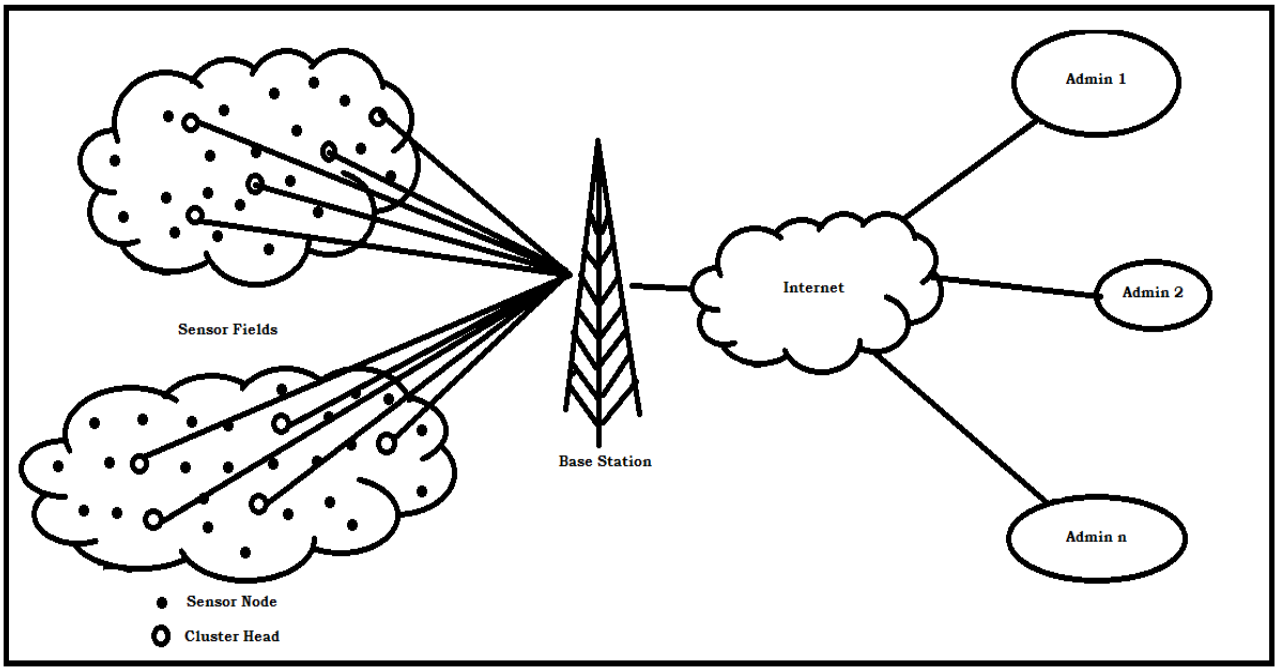

Fig. No. 2: Working of Wireless Sensor Networks

In nutshell WSN is the network of sensor nodes being controlled and monitored over wireless network. It is dynamic, low cost, battery powered and collection of various tested protocols or modules.

III. MAPPING OF WSN IN IOT

In the field of Computer Science and Information Technology, there is a convergence of different technologies such as cognitive computing [4], sensors, cloud [5], machines and humans; with a goal to intelligently improve health, wealth and lifestyle. These technologies made the computer applications reach over various and diverse domains such as building monitoring & surveillance, health care, home-automation, energy management and last but not least industrial automation. Making use of association among nodes, WSN can improve progressive efficiency, draw out system lifetime, handle dynamics, detect and correct errors and increasing the reliability of the user application. Moreover, WSNs are also basic elements of recently suggested collaborative Internet of Things (IoT) technologies that allow creating novel invasive and smart environments. The hypothetical model of mapping of WSN with IoT is described in Fig. No.3. It includes four common layers i.e. Hardware Layer, Communication Layer, Middleware and Application Layer out of which first two belongs to WSN and rest two belongs to IoT. Hardware layer is responsible for the working of all the hardware associated with WSN and IoT. Communication layer is responsible for the mapping and integration of WSN protocols to Internet (TCP/IP) [6] so that it can be used in IoT. Middleware is the key layer which amalgamates both the technologies i.e. WSN and IoT for data analytics, visualizations and Machine Learning. This layer gives the custom

solution with the integration of both the technologies. The Last layer is Application layer which is responsible for the End user applications which can be Web applications, Mobile Applications or Cloud based solutions. The major objective of this model is to create smart universal solution for every application domain.

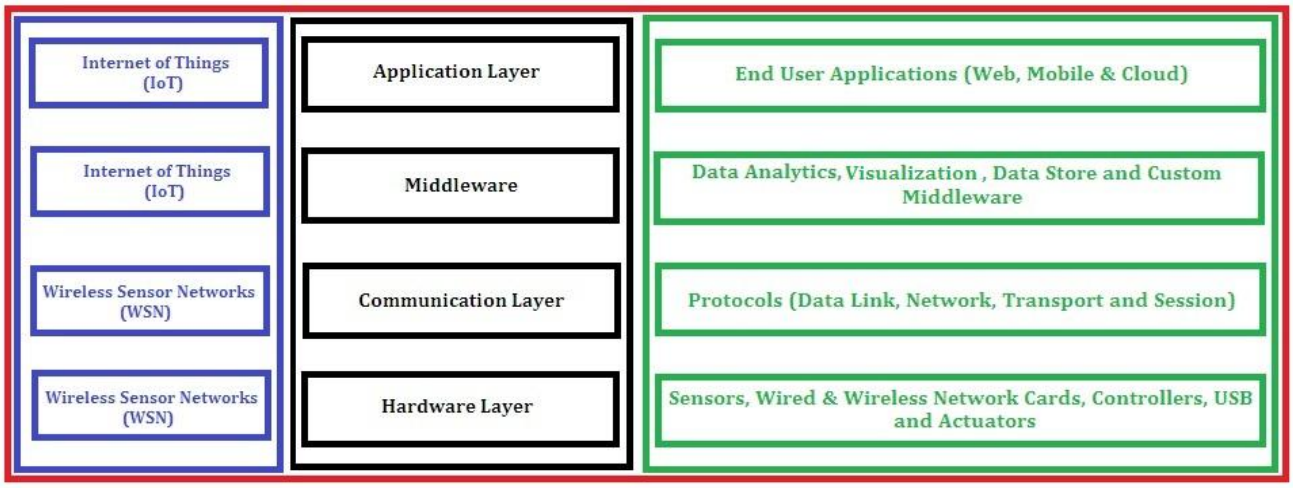

Fig. No3: Logical correlation between IoT and WSN

IV. CHALLENGES OF USING WSN IN IOT

The Internet of Things (IoT) world may be exciting, but there are serious technical challenges that need to be addressed properly. Since the applications of IoT are under development phase so there are several challenges which encounters; some of them are listed below:

Deployment Standards to the definition and implementation: We need to develop, deploy, common model for protocols, communication and hardware. However several standard bodies have developed protocols to provide connectivity between physical sensing systems and the Internet.

Anywhere computing: Most of the devices in IoT and WSN technologies falls under ubiquitous devices category and are typically based on low power and wireless technologies. To ensure flexible and cost-effective deployments, every node in an industrial WSN should be able to run on batteries for at least five years, as this offers the ultimate flexibility to users in coverage for Industrial IoT applications.

Installation challenges: The IoT is the industrial form of WSN so the installation of this network needs experts from the field. The maintenance of these networks needs a special training too.

Design Challenges: The development of new WSN architectures specifically for Internet of Things and we need to design flexible Cross-layer design for Internet of Things/Web of Things and Wireless Sensor Networks.

Assurance quality of information: We need to develop models which ensure efficient delivery, aggregation and processing [7] of data. It should provide reliable autonomous control and management facilities. It should also ensure prompt and accurate results according to the user's needs. The model should be robust and scalable.

Security Issues: We need to develop cryptographic models [8] which should ensure security, privacy, and system integrity of data communication for Internet of Things.

V. BENEFITS OF WSN IN IOT

Wireless Sensor Networks are an important element in IoT paradigm in terms of facilitating the collaboration of heterogeneous information systems and services. These followings are the benefits of using WSN Technology in the IOT:

Reliable and Tested Technology: Since WSN have many implemented and tested models in industry, it can be harnessed in IoT directly. WSN provides many flexible cross layer models for reuse in IoT.

Integration of Protocols: The WSN is independent of internet so it designs its own protocols for the communication where as IoT is internet dependent. The Wireless Sensor Network model presents the compatible network layer protocol and its use in IoT as back end technology made the whole process easy by integrating the WSN and TCP/IP protocols together.

Secure Backend Data: As there is a lot of work done on the security issues of WSN Technologies since its birth so there are fewer chances of data preach in these networks. Now as WSN is used in the IoT at its backend so the initial data collected is much secure which increase the accountability over security incidents and abnormal situations.

Multi Layer Architecture: WSN contains many layers which provide many options for developers to customize the serve model for IoT.

VI. CONCLUSION & FUTURE WORK

With the emerging concept of "anywhere computing", we want to achieve robust and low cost service oriented platform solution for our daily computation needs. As communication, computing and micro-electro-mechanical technologies evolve; the notion of the Internet of Things (IoT) exerts a pull on attention of the researchers and academicians. The applications of IOT/WOT should be universal in nature. The Internet of Things (IoT) is mounting rapidly and wireless sensor networks (WSNs) are providing significant backend services to extend the reach of the

Internet infrastructure to "everything." The Internet of Things also can support complex human planning and decision making. The technology requirements include the magnificent storage and computing resources associated with highly developed software systems that engender a variety of graphical exhibit for exploring the data. There are traces of futurism in this technology and early warnings too. There is a need to develop the powerful industrial applications and business models to promote this technology in future.

ACKNOWLEDGMENT

Blessed are those that can give without remembering and receive without forgetting. As we express our gratitude, we must never forget that the highest appreciation is not to utter words, but to live by them. My heart and soul feels greatly honoured to find this opportunity to be in thankfulness before Almighty for his constant innumerable blessings and also for bestowing the enough strength and courage to complete my thesis work. We have been amazingly fortunate to have an advisor who gave us guidance to recover whenever my step faltered and had helped and cared me throughout the research. We also thank Dr. Ashok Kumar Raghav- Vice Chancellor A P Goyal Shimla University, Shimla, H.P. India for his guidance and support. We thank all our colleagues of department for sitting besides us to be the part of fruitful discussions. A special thanks to Dr. Purnima Bali, Mr. Sonit Singh and Mr. Pankaj Kajla for their assistance in proof reading of this review paper.

REFERENCES

[1] Ivy Wigmore, "Internet of Things", HTML Text, Retrieved from http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT on 24th December, 2016 at 01:21 PM.

[2] "Internet of Things", HTML Text, Retrieved from http://www.etsi.org/technologies-clusters/technologies/internet-of-things on 27th December, 2016 at 10:30 AM.

[3] Shamneesh Sharma, Keshav Kishore & Vandana Chaudhary, " Review on Wireless Sensor Networks: Total Technology Yesterday, Today and Tomorrow", International Journal of Computer Science & Technology, 2013 Vol- 4, spl.-3.

[4] Nilesh Jain, "IoT Is Reshaping Lives", Business World, November, 2016 Issue.

[5] P. Mell, T. Grance, "The NIST definition of cloud computing", Commun ACM 2010; 53(6):50.

[6] Kristofer Pister and Jonathan Simon, "Secure Wireless Sensor Networks Against Attacks," Retrieved from http://electronicdesign.com/communications/secure-wireless-sensor-networks-against-attacks on 29th December, 2016 at 12:16 PM.

[7] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[8] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.

