JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

WIRELESS SENSOR NETWORKS AND IOT : A NEW ERA OF SENSOR NETWORKS

[1]Amardeep Bajwa, [2]Daljeet Singh Bajwa, [3]Raminder Singh Uppal
[1] Research Scholar, [2]Trainer and Assessor, [3]Associate Professor
[1]Electronics Department, [2]Automotive Engg. Department, [3]Electronics & Comm. Engg. Department
[1]SGGSWU, Fatehgarh Sahib, India, [2]Durban International College, Adelaide, SA, BBSBEC, Fatehgarh Sahib, India

Abstract : Internet of Things has effortlessly replaced network of People on the internet (IoT). The processing of interoperability between the heterogeneous Internet items, such as RFIDs (Radio Frequency Identification), mobile portable devices, and wireless sensors, is complicated by such relocation. The Internet of Things idea has been integrated into WSN to address this circumstance (IoT). It has been observed recently that IoT-based WSNs had developed quickly in a number of industries. The Internet of Things (IoT) is a system that allows unattended communication between physical items, machinery, sensors, and other hardware. A key element of the Internet of Things (IoT), which has rapidly expanded into a variety of real-time scenarios, is the WSN (Wireless Sensor Network). Nowadays, the IoT and WSNs have several essential and non-critical applications that affect almost every facet of our daily lives. We shall outline the many characteristics, difficulties, and some particular IoT applications of wireless sensor networks in this post.

***IndexTerms* - WSN, IoT, Communication, Devices, Technology, Sensors.**

I. INTRODUCTION

With the development of wireless network infrastructure, every aspect of our daily lives has changed substantially. One of the technologies that is developing the fastest in the future is the Internet of Things (IoT). With the addition of IoT, several devices can be connected in the real world, effectively altering our daily lives. As a result, there is an urgent demand for communications everywhere and at all times, particularly in industries with high activity. The Internet of Things has been described as the fusion and interconnection of sentient objects (things). The dominance of IoT helps develop new technologies and applications. These sensors and actuators typically come with a variety of transceivers, micro-controllers, and standards for exchanging sensor and controller information. [1]

Due to the large number of communication devices, data produced by various devices affects the network's overall effectiveness. Unsustainable increases in the amount of energy used and carbon emissions have been caused by the dramatically faster communication and information transmission. The amount of energy consumed by the sensors is the main component that defines how long the application will run, and the presence of dead nodes can affect the dependability and accuracy of data in contrast to the interconnection of devices. [2]

The processing element, the sensing/identification component, the communication module, and the unit that provides power are the four main units that make up a sensor node. [3] Filters, amplifiers, transducers, comparators, and other secondary elements are included with these primary components. Information from the workspace is collected by the sensor device. The master node sends data at the base stations, while the power unit—typically a battery-limited one—provides energy to all other devices. The processing element performs various data manipulation activities, such as data gathering.

The exact energy consumption of a sensor network depends on its working environment, which might be one of 3 states: active, sleeping, or idle. When in active mode, the node consumes the most energy. During sleeping, when the node doesn't carry out any processing activities and the communication module is switched off, far less energy is lost. However, there are other sources of power losses, including packet collisions, node failures, physical channel defects, frame interrupting, overhead protocols, and overhead computing. As a result, the IoT community has been motivated to create energy-efficient and renewable IoT solutions.

In modern IoT networks, gadgets are typically powered by batteries, therefore energy economy is of course of utmost importance for system administration. Battery-operated sensors' energy efficiency and maintenance with regard to a particular WSN domain have long been research concerns [4], where Medium Access Control (MAC) protocols place an emphasis on optimising sensor node operation and routeing layer protocols are created for data aggregation and transmission from multiple-to-one. Figure 1 lists the sensor node's components.

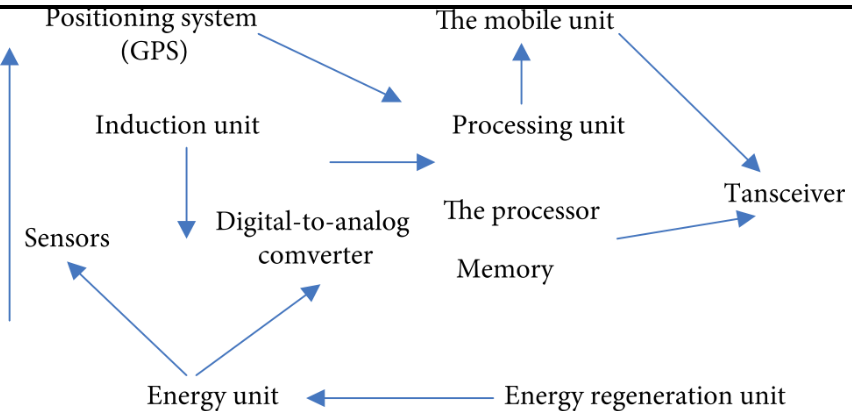

figure 1: components of sensor node

II. Role of IOT in WSN

IoT is referred to as a self-configuring wireless sensor network with the aim of connecting everything. Through the interaction created by rfid chips (RFID), sensors, and two-dimensional patterns on items, it connects to the wireless network. IoT makes it possible to communicate with both people and things. Appreciable, internet-connected, and intelligent are the three fundamental qualities of the Internet of Things [5]. Information gathering, two-way communication, processing, and adaptive control are the four fundamental components of the Internet of Things.

There is a large use of the Internet of Things. It has applications in nearly every area of human productivity and living, including intelligent transportation, environmental protection, public safety, IQ testing, and physical well-being. According to experts, if the Internet of Things is fully implemented, its commercial volume will be 30 times larger than it is now, making it a very big market. Real-world examples of where the Internet of Things is being used include logistics processes, distribution, food standards traceability, smart homes, digital oil fields, intelligent glasshouse monitoring, vehicle tracking, and community safety tracking. An electronic fence was installed at Pudong Airport Terminal using a sensor network that was placed in the ground outside the fence. The system will automatically broadcast recognition signals and determine the accurate location when individuals or animals approach it. [6].

The Internet of Things' implementations are now evolving quickly. For a variety of reasons, current technology cannot fully support the Internet of Things. To tackle the aforementioned issue, technological advances are being investigated. Zigbee and the 802.15.4 standard, which will be further improved in terms of channel capacity, transmission rate, and non-line-transmission ability, in particular in relation to applications for surveillance and large-scale data collection and transmission, are the main foundations for present research and practical WSN implementations. A excellent complement to ZigBee's lack of video monitoring capabilities is WiFi-based WSN. WiFi is capable of large-scale data collecting, high rates, NLOF broadcast, and more cost-effective applications. Therefore, it is crucial to conduct research on WiFi-based WSN and its applications in order to advance the global Internet of Things and Smart Grid. [7].

III. Applications of Wireless Sensor Networks in the Internet of Things

1. Application in Industrial Field

The use of wireless sensor networks in industry is very common; by removing artificial inconsistency, they enable daily operations in areas such as industrial protection, efficient traffic, security systems, logistics management, and others. The most applications are in the area of industrial protection. Consequently, wireless sensor network innovation can optimize industrial processes, lower the risk of accidents occurring in industrial activity, and even let a person use remote control rather than people to work. After interacting with the eruption of sensor nodes and optimized technology, it can be put on people have hurt environment, real-time monitoring of the safety of staff, and process line for dangerous working environment environmental parameters in time.

2. Application in the Field of Medical Care

China's population is starting to age, challenges in medical treatment are becoming more visible, and real-time monitoring of individuals' illnesses has emerged as a significant issue that has to be resolved. Wireless sensor network monitoring system, nevertheless, is quite important in this regard. In order to recognize and gather physiological data from patients in real-time and to comprehend how their circumstances are changing at any given time, doctors can implant small, precise detectors on patients. On the other side, real-time surveillance also gives medical organizations access to more reference sources. The core issues of illnesses can be discovered through the analysis and processing of many parameters, allowing for the creation of powerful medications that can save more lives.

3. Application in the Field of Smart Home

The Internet of Things has transformed into a smart home in recent years. The term "smart house" refers to an incredibly intelligent home automation system that uses a variety of high-tech system components and tools as well as artificial intelligence to enhance the safety and comfort of the home environment and, consequently, to save conserve energy and the environment. The concept behind a smart home is to link and operate home appliances by using a large number of wireless sensor network nodes to create a self-organizing connectivity. [8].

4. APPLICATION IN THE MILITARY FIELD

Rapid deployment, loose organization, high conceal ability, and high fault tolerance are just a few of the properties that make wireless sensor networks effective in the army. These characteristics make them famous on the battleground and enable them to function well in hostile conditions. In order to achieve this one key benefit, there will be a massive number of sensor nodes deployed throughout the battleground, which would include aircraft artillery, with the aim of gathering data on a variety of variables, along with terrain, voice, temperature, and moisture. Using a secure communication channel, the data will then be processed, allowing for real-time military operations evaluation and surveillance of enemy activity.

IV. CHALLENGES OF WSN IN IOT

The Internet of Things is complicated since it presents and communicates a range of heterogeneous artifacts under various conditions, which makes the deployment of security solutions more challenging. The majority of the solutions put forth in current WSN information security are intended to address arbitrary issues; they do not consider the impact of IOT ideas and functionalities. Following are a few of the challenges,

1. REAL TIME MANAGEMENT

For sensor nodes that manage their resources available, it is a difficult subject. In this case, the Internet of Things (IoT) system needs to have an efficient architecture for its service entrance in order to constantly analyze user data and limit the quantity of data that needs to be delivered. Furthermore, real-time information can only be communicated when the threshold is exceeded, which necessitates the use of intelligent data-driven middleware.

2. SECURITY AND PRIVACY

Safety, trust, and privacy are additional issues that are crucial to take into account in apps that are utilized in the real world. Different levels of safety can be attained in both difficult and simple ways. These security options are suitable for M2M implementations where the server and the module already have a mutually trusted relationship.

Sensor networks have additional responsibilities in addition to the standard sensor functionalities they offer with this "IP to the field" strategy. The sensor nodes will experience new obligations or challenges as a result of this added responsibility. As possible future duties, the issues of network configuration, service quality (QOS), and security will be highlighted.

3. SECURITY

WSNs could be able to supply data with secrecy, verification, fairness, and usability even in the absence of Internet access, depending on the degree of intricacy of the application. The attacker must take physical actions in close proximity to the WSN in order to add malicious nodes to the present network, stop them, or capture them. On the other side, the ability for malicious actors to operate anywhere in the world is made possible by the link of WSNs to the internet. As a result, the WSNs must discover a long-term fix for the issues brought on by their internet connection, such as malware and other issues. Both the key and a specialized efficient gateway are made accessible to enable that current WSNs sustain a sufficient level of security. Because of the current lack of accessible computing, energy, and memory resources, a comparable security system cannot be replicated.

4. QUALITY OF SERVICE

Each unrelated piece of equipment linked to the internet of things must contribute to the overall level of service in terms of the intelligence that is given to the sensor nodes. A workload can be divided among several nodes, each of which has access to a different set of resources, thanks to these heterogeneous devices. The currently existing QOS approaches on the internet still need to be improved because network settings are constantly changing and connections have a wide range of capabilities.

5. CONFIGURATION

Sensor nodes have a number of other responsibilities in addition to controlling QOS and maintaining network security. Among other things, these activities involve networking for a new node that is joining the network, ensuring self-healing by identifying and eliminating problematic nodes, and dealing with administration to build scalable networks. The most recent node on the Internet, nevertheless, does not automatically perform this operation as part of its normal operation. Therefore, if the user wants this network setup to work properly, they must instal the required software and take the appropriate measures to prevent malfunctions.

6. AVAILABILITY

It is possible to take use of WSNs when there are hacked nodes present. To deploy an encryption method for wireless sensor network security, more money should be budgeted. Despite this, academics have developed important strategies, some of which require altering the code so that it can be reused while others call for the use of auxiliary communications to accomplish the goals. Additionally, a number of techniques have been developed to access the data. Therefore, in order to continue the WSNs' functioning services, availability is extremely essential. Furthermore, it assists in keeping the entire system operational until it is closed down.

7. DATA INTEGRITY

A hostile node joining the network and injecting false data or a fluctuating wireless channel corrupting the data that was initially broadcast are two scenarios that could compromise a WSN's authenticity. For instance, if a mobile node added falsified information to the packets that the base station (BS) was processing, the integrity of the data may be jeopardized. However, a broken network could be to responsible for data loss or data modification. Therefore, it is crucial that the data's integrity be maintained throughout the transmission of the data packets.

8. CONFIDENTIALITY

There are a number of challenges to be solved when it comes to Internet of Things security, with maintaining anonymity being the most crucial. To protect the privacy of the data and stop illegal access, encryption capabilities including shared and common secret key cyphers like Triple DES, Blowfish, and AES block cypher are used. To guarantee the confidentiality of the data and information being communicated, the encryption procedure is insufficient on its own as a security measure. By taking advantage of a flaw in the cypher, the hacker can effectively spread sensitive information by performing a traffic analysis on the cypher data.

V. CONCLUSION

The development of WSNs, which constantly monitor the necessary parameters, has been facilitated by advances in computer technology. In latest years, the IoT-based WSN systems have attracted a lot of attention. While point-to-point communication is possible, these networks have limited bandwidth, power, and resources. One brilliant solution to this issue is data collection. How to analyze vital data in a way that uses less energy is a major issue in sensor nodes. As a result, different data aggregation algorithms can be utilized to cut down on power usage. Numerous WSN in IoT features and implementations have been covered in this research paper. Various obstacles that needed to be overcome in order to get greater results in the future have also been mentioned.

VI. ACKNOWLEDGMENT

We acknowledge that the research paper titled “Wireless Sensor Networks And IoT : A New Era of Sensor Networks” is our own work and has not been published in any other conference or journal.

REFERENCES

[1] Y. Cho, M. Kim, S. Woo, Energy Effificient IoT based on Wireless Sensor Networks for Healthcare, Int. Conf. Adv. Commun. Technol. (ICACT) (2018).

[2] Wireless Sensor Network Techniques and its Role in Internet of Things: An Overview

[3] M. Healy, T. Newe, E. Lewis, Wireless Sensor Node hardware: A review, in: 2008 IEEE Sensors, 621-624, 2008.

[4] K.I. Kim, ‘‘Clustering Scheme for (m, k)-Firm Streams in Wireless Sensor Networks,” the Journal of information and communication convergence engineering, vol.14, no. 2, pp. 84-88, 2016.

[5] Guo Dengfeng, Xu Shan, Kun, “The Internet of Things hold up Smart Grid networking technology”, North China Electric, 2010.2, pp.59-63.

[6] Li HY, Gui chao, “Application of the Internet of Things and trends”, Fujian PC, Sep.2010, pp.1-2.

[7] Li, Li; Xiaoguang, Hu; Ke, Chen; Ketai, He (2011). [IEEE 2011 6th IEEE Conference on Industrial Electronics and Applications (ICIEA) - Beijing, China (2011.06.21-2011.06.23)] 2011 6th IEEE Conference on Industrial Electronics and Applications - The applications of WiFi-based Wireless Sensor Network in Internet of Things and Smart Grid. , (), 789–793. doi:10.1109/ICIEA.2011.5975693

[8] Yao Zhang, Wanxiong Cai, “The Key Technology of Wireless Sensor Network and Its Application in the Internet of Things”, Journal of sensors, vol. 2022, Article ID 1817781, 11 pages, 2022. https://doi.org/10.1155/2022/1817781

[9] Dr K. J. Praveen Kumar, Dr. K. Divya, “Wireless Sensor Network Techniques and its Role in Internet of Things: An Overview”, *International Journal of Mechanical Engineering, ISSN: 0974-5823, Vol. 7, No. 5, May 2022.*