ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 2, Issue 12, December 2017

Challenges Faced By the Impact of Wireless Sensor Network in Internet of Things Devices

[1] Sowmya Fernandez, [2] R. Waheetha,[3] D. Jothi Lakshmi
[1][2] Associate Professor, [3] Assisant Professor
[1][3] Dept. of Computer Science,A.P.C. Mahalaxmi College For Women
[2] Dept. of computer science,holy cross home science college.

Abstract:-- **The Internet is slowly moving from an Internet of people towards an Internet of Things (IoT). About 50 billion things may be connected to the Internet by the end of 2020.A Wireless Sensor Network (WSN) is a network comprising of several sensor nodes and each node contains a sensor which detects the physical process such as light, temperature, smell, pressure etc. A WSN is likely to be integrated with IoT and the sensor nodes connects internet dynamically in order to achieve the specified tasks. With the rapid technological development of sensors, WSNs will become the key technology for IoT. In every walk of life wireless sensor networks are increasing tremendously. Recent research work proves that the existing WSN are not suitable to support the issues related to security and user acceptance. Our proposed method designs a new framework to combine WSN of IoT that identifies the issues related to security mechanisms, users' acceptance and management of data privacy.**

Keywords:-- **Internet of Things, Sensors, Actuators, Microcontroller, Memory.**

INTRODUCTION

Wireless Sensor Networks (WSNs) is one of the growing and popular thing which catches the attraction worldwide. It is an enabler for IoT. WSN will play an important role by connecting environment and surrounding context in future. The integration of WSN with IoT is an interesting topic in scientific research. This invention can change our day to day lives. Security is one of the most important issues on WSNs for Internet of Things. The current trend, however, is to use the Internet Protocol (IP) to achieve native connectivity between WSNs and the Internet. In this way, smart objects (e.g., tiny sensors or actuators with a network interface) are interconnected in order to make an IoT, based mainly on open standards and where every device has its own IP address. The IoT will allow collecting any useful information about the physical world's smart objects to use this information in various applications during the objects' life cycle. Wireless sensor networks typically consist of large number of sensor nodes. Each node of the network has sensing ability (temperature, pressure, vibration, sound, humidity, etc.). At the same time, each node is router as well. Sensor nodes have very limited resources. They are devices that collect data from the surrounding area and transmit the data wirelessly over short distances.

Scenarios and challenges

The Internet of Things is playing more and more an important role in lot of scenarios like:

- Healthcare and goodness
- Home and building automation
- Energy efficiency
- Automation in industries
- Smart grid infrastructures
- Environmental monitoring and weather forecasting
- Flexible RFID infrastructures
- Vehicular automation and smart transport
- Agriculture
- Smart Shopping

This wide range of applications, with great differences in terms of requirements, scale and total available market, has led to a technical solutions for the embedded networking field. Smart objects have different communication, information processing capabilities and interoperability which should be maintained to provide interaction among them. Scalability is another issue for the IoT because of the large scope of communication needed to interconnect objects and people. Moreover, in a dynamic environment of ubiquitous networking, services exported by the objects must be automatically identified by means of a discovery mechanism. Confidentiality, authenticity and trustworthiness of communication are essential to guarantee personal privacy and security (for example when billing information depends on sensors' data). Even though the amount of data transferred from or to a single sensor or actuator is very limited and the overall amount of data could be huge due to the large number of objects and their frequent interaction. How to handle a big volume of data is one of the important challenges of the future Internet. Fault-tolerance is another problem of the IoT. When dealing with battery-operated smart objects, another

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 2, Issue 12, December 2017

critical aspect is their power consumption. Therefore, energy efficient communication mechanisms are essential.

General structure of the sensor node

Figure 1 shows this general structure of the sensor node, with the microcontroller, communication devices, sensors, actuators, memory and power source.

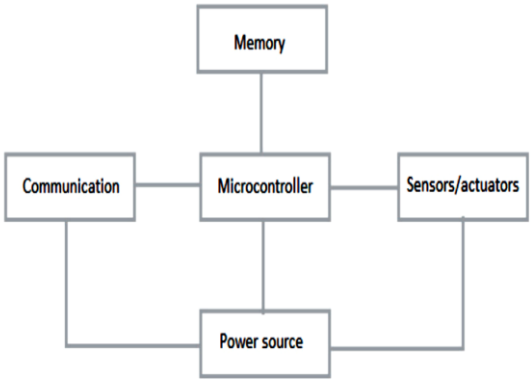

Fig.1. General structure of the sensor node

The central part of this structure is a microcontroller, general purpose processor, optimized for low power consumption. Communication block usually consists of one or more communication devices embedded on the node, such as a radio transmitter, Bluetooth, GSM/UMTS, etc. Each node has physical sensors, which can be passive or active (radar), focused (camera) or multidirectional (temperature, vibration, etc.) with different areas of coverage. Each node has one or more power sources, which need to provide as much energy as possible at lowest possible cost in terms of price, size, weight and recharge time. Charging of the batteries is not always an option in wireless sensor networks. Memory block typically depicts additional flash memory, as in the most cases available RAM memory is negligible. For the given fixed processing power, chip is becoming smaller and cheaper every year due to recent advances in semiconductor technology. These cheap wireless sensor nodes with low energy consumption can be distributed in the physical area in order to collect data about the physical phenomena under observation. They can process the data, communicate and coordinate actions with each other. In most cases, large number of distributed sensor nodes is required to overcome obstacles such as walls, optical visibility limitations, ground configuration, etc. The area under observation often does not have any existing infrastructure in terms of communications and energy sources (forests, active volcanoes, etc.). Communications between the nodes is the biggest energy consumer in wireless sensor network.

Architecture of wireless sensor networks

A wireless sensor network architecture is shown in Figure 2.

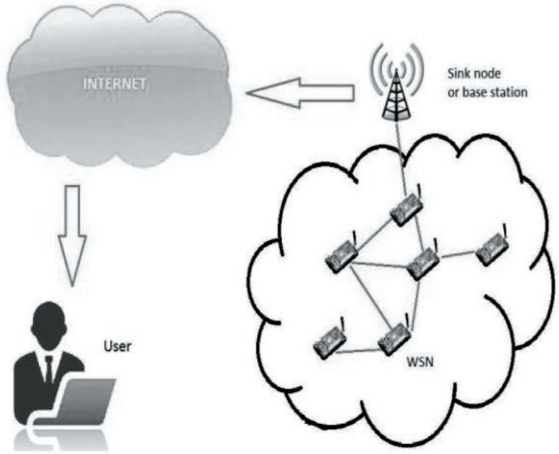

Fig.2. Architecture of wireless sensor networks

Nodes collect data and send it to the sink node, or base station. Data is then transferred to the end user via Internet network. Sensor nodes have simple microcontrollers, and miniaturization allows operation on 10 MHz with energy consumption of 1mW. Most of the components of the node can be switched off if needed, and in standby mode energy consumption is around 1 microwatt. If device is active approximately 1% of time, the average consumption is only several microwatts. These simple microcontrollers, however, have very limited storage capacity, typically less than 10 KB RAM memory for data and less than 100 KB ROM for programs, which is one million times less than average PC. Wireless sensor network formed of these low power sensor nodes, coupled with Big Data analytics and cloud computing led to a great interest and expansion of Internet of Things. With this combination of technologies, we can place multiple sensor nodes anywhere where there is valuable information which needs to be collected, even in places without proper communications and power infrastructure.

Internet of Things

(IoT) is a recent communication paradigm, where the objects of everyday life will be equipped with microcontrollers, transceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, becoming an integral part of the Internet. The IoT concept, aims at making the Internet even

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 2, Issue 12, December 2017

more immersive and pervasive. Furthermore, by enabling easy access and interaction with a wide variety of devices such as, home appliances, surveillance cameras, monitoring sensors, actuators, displays, vehicles, and so on. The IoT will foster the development of a number of applications that make use of the potentially enormous amount and variety of data generated by such objects to provide new services to citizens, companies, and public administrations. This indeed finds application in many different domains, such as home automation, industrial automation, medical aids, mobile healthcare, elderly assistance, intelligent energy management and smart grids, automotive, traffic management, and many others.

Challenges of WSN's in an internet of things

WSN is permitted to become an essential component of IoT and 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. IOT security, need to be considered from a global point of view. IoT should satisfy the needs of a user without breaking their security. It has introduced "IP to the field paradigm" 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 are security, quality of service management and network configuration.

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 , WSNs may address new threats such as malware and worms which is introduced by Internet and the attackers. 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. From the 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 world. Having safe interaction between objects and services is an interesting challenges in IoT.

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. Improving the quality of service, collaborative work is consequently promising for mechanisms requiring high amount of resources like security mechanisms. In WSNs, a present approach which provides quality of services in the Internet is not measured as many variations in features may lead to significant reconfiguration of the WSN topology.

Configuration

Along with the quality of service and security, sensor nodes also need to control the WSN configuration which has various tasks such as self-healing capabilities, address administration or handling their own features. Self-configuration of participating nodes is not a common feature in the Internet. 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.

Challenges and future standardization needs

WSN is an emerging technology which involves different layers and aspects of information technology. So its standardization has its unique complexity.

Disunity: Communication, coordination and unified planning are absent from different standard organizations and between each other.

Incompatibility: Since WSN involves different aspects of information technology, its standards are complex and diverse. Yet different standards developed by different standard organizations are not compatible.

Lack of harmonization: Some WSN applications have already begun to implement successively. Though different standard organizations have carried out the work from different perspective and with different depth, most of the work is still in its initial stage and is not market ready.

Divergence: Since the applications are out of synchronization and the standard development is delayed, the application constructions are not inconformity with standard development, which affects the reusability and intercommunity of the applications and impede the development of industrialization.

To resolve the above problems, it is recommended that WSN standardization should enhance the communication and coordination among different standard organizations, make unified planning, optimize resource allocation and reduce repetition of work.

Future of WSN

The future Internet, designed as an "Internet of Things" with WSN is foreseen to be "a world-wide network of interconnected objects uniquely addressable, based on

standard communication protocols". It is identified by a unique address, any object including computers, sensors, RFID tags or mobile phones will be able to dynamically join the network, collaborate and cooperate efficiently to achieve different tasks. Including WSNs in such a scenario will open new perspectives. Covering a wide application field, WSNs can play an important role by collecting surrounding context and environment information.

However, deploying WSNs configured to access the Internet raises novel challenges, which need to be tackled before taking many benefits of such integration. The main idea of this paper is as follows: We look at WSNs and the Internet, inline with the vision where WSNs will be a part of an Internet of Things. Therefore, we identify representative application scenarios for WSNs from the multidimensional of WSN space, in order to obtain the issues of integration. These representative application scenarios open up different schemes for integrating the WSNs into the Internet. A closer investigation of the integration possibilities then helps us identify critical challenges, which need to be addressed if the full potential of the integration of WSNs and the Internet has to be realized.

CONCLUSION

Integration challenges were the most important one being the privacy issue that needs to be addressed carefully. Internet of Things is not the technology of the future – it is has started happening. With the number of connected devices expected to be around 50 billion by the year 2020, the whole world is becoming one big connected thing. Integration of the wireless sensor networks with Internet of Things will bring many traditional applications of WSN to the higher level like responders and environment monitoring. It will also enable new types of WSN applications in the future. Data is collected from the different sensor networks in the real time. Data processing is also performed in real time to make time critical decisions. Cloud services are responsible for complex tasks processing and fast response to the users.

REFERENCES

[1] J. Vasseur and A. Dunkels: “Interconnecting Smart Objects with IP - The Next Internet”, Morgan Kaufmann,2010.

[2] H. S. Gol, “Integration of Wireless Sensor Network(WSN) and Internet of Things (IOT), Investigation of Its Security Challenges and Risks”, International Journal of Advanced Research in Computer Scienceand Software Engineering, Volume 6, Issue 1, pp.37-40, January 2016

[3] “Internet of Things in 2020: Roadmap for the Future,”2008, online, http://www.smart-systems-integration.org/public/internet-of-things.

[4] D. Evans, “The Internet of Things – How the Next Evolution of the Internet Is Changing Everything”, Cisco White Paper, April 2011, online:http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0 411FINAL.pdf

[5] Wood, G. Virone. T. Doan, Q. Cao. L. Selavo, Y. Wii, L. Fang. Z. He,S. Lin. and J. Stankovic. "ALARM-NET: Wireless Sensor Networks for Assisted-living and Residential Monitoring." 2006