INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES
© 2004 -14 Society For Science and Nature (SFSN). All Rights Reserved
www.scienceandnature.org

CHALLENGES IN INTEGRATING WIRELESS SENSOR NETWORKS INTO THE INTERNET

Kour Tejasvit
Chandigarh Group of Colleges, Chandigrah, India

ABSTRACT

Wireless sensor networks are increasingly becoming popular day by day. Their application in every field of life is becoming evident for example health care, control networks. An important scope of wireless sensor network is its integration into the internet of things. However integration of wireless sensor networks into the internet of things poses certain challenges. This paper targets various methods of integration and the challenges related to them.

KEYWORDS: WSN, Internet of things, Security, Quality of Service,.

INTRODUCTION

A wireless sensor network basically consists of a large number of sensor nodes which are distributed over a place. These nodes measure the conditions around them like temperature, pressure and convert them into the form of signals that reveal certain information about the phenomenon. The data collected is transferred to a sink node which is also called the base station. This data is transferred to the user via a gateway, satellite or internet. The figure [1] represents a wireless sensor network. The wireless sensor nodes form the most important part of the wireless sensor network. For sufficient data management, the nodes are partitioned into clusters. Each cluster has member nodes and a coordinator called the cluster head. Clustering is done to improve network time which is a primary requirement in improving network efficiency and capability. Clustering also reduces channel contentions and packet collisions resulting in better network under high load.

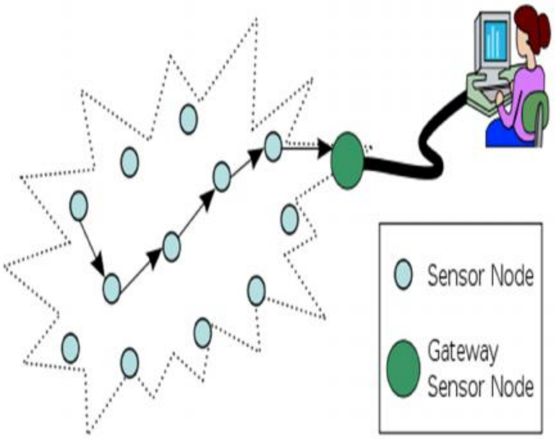


Figure – 1

Wireless sensor networks find a variety of applications like robotic landmine detection, target tracking, environment protection, wildfire detection, home, traffic monitoring, for monitoring natural phenomenon etc. There may be three ways in which the application of a wireless sensor network may be divided. They are:

a) Monitoring space
b) Monitoring objects
c) Monitoring interactions between space and objects

An example of first category is monitoring the environment. In this the sensors are placed in environments like mountains, forests and glaciers to record environment parameters over long periods. The second category includes observing particular objects. By using this breakage of bridges may be detected. The third category is a combination of both and may be applied in monitoring environmental hazards like floods, volcanic activities etc. A proposed extension application of wireless sensor networks is monitoring human beings. In this a small sensors are deployed close to the body and it may sensor certain physiological parameters like heartbeat. This may be helpful in monitoring patients at home and diagnosing bipolar patients. The integration of wireless sensor networks may be helpful in monitoring these with greater precision but certain aspects must definitely be taken into account during integration.

Internet of things means representing identifiable objects and their virtual representations in an internet like structure. Radio frequency identifiers are the key in this representation. It is possible to list and manage all objects and people if they are equipped with identifiers. The main advantage of the internet of things is that every object will have a unique identification address and information can be exchanged between them. With the advent of the internet of things it will be possible to imagine things transporting themselves for example instructing conveyer belts for its routing, analyzing data information and passing them to the required nodes.

The main issue in this is that all this requires a lot of energy to be harvested. In this process energy is required to not only collect the information but also relay the information between the objects. This calls for placing sensors everywhere even when the system is weak or absent or even if the sensors are weak or immobile.

Technology trends

With the explosion of internet of things following technology trends may be shaped in future;

The first and the foremost one is the explosion of the data collected and exchanged. This may be termed as exaflood or data deluge. This further calls for the rethinking of the current storage architecture and networking infrastructure. New ways to fetch and transfer data must be found.

Secondly there will be a significant reduction in the energy required to operate the intelligent devices. This is important because many data centers have already reached a maximum energy consumption value. Having a zero level of entropy where the device can harvest its energy will enable this. Another future trend is the miniaturization of devices. An ultimate limit in this is the single-electron transistor concept. Another important concept in this regard is having autonomous resources which are capable of self- healing, self-configuration, self- management. This will help improve complexity of systems. Integration of wireless sensor networks into the internet of things

There are three main approaches in which the wireless sensor networks may be connected to the internet. In the first approach both the independent wireless sensor network and the internet is connected via gateway. Figure-2 shows the integration via gateway. The main disadvantage of this approach is that the gateway failure leads to the failure of the entire system

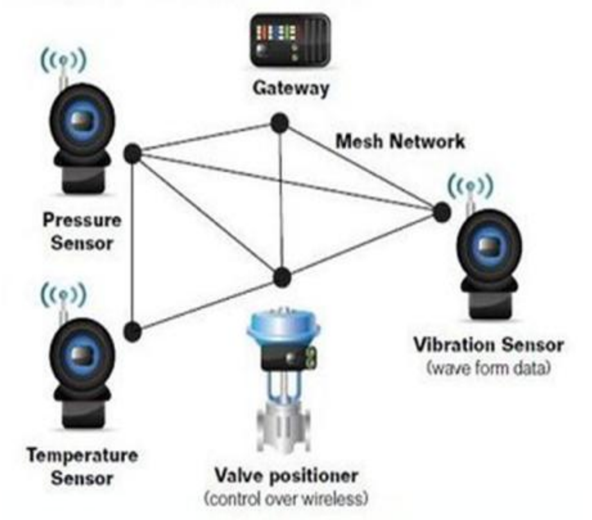

Gateway
Mesh Network
Pressure Sensor
Vibration Sensor (wave form data)
Temperature Sensor
Valve positioner (control over wireless)

Figure-2

In the second approach dual sensor nodes can access the internet. In this a hybrid network is formed but it still consists of independent nodes. In the third approach which is the access point network multiple sensor nodes can join the internet in one hop. The second and third approaches deal with the multiple gateways hence the disadvantage of the first approach is handled in these two approaches. The second approach can be considered for wireless sensor networks having mesh topology and third for those having star topology. The disadvantage of these approaches is that they support only static network configuration and a gateway reprogramming is required if a new device wants to join the internet. It further makes this process time consuming. Therefore it fails to provide the flexibility required for the internet of things for future scope

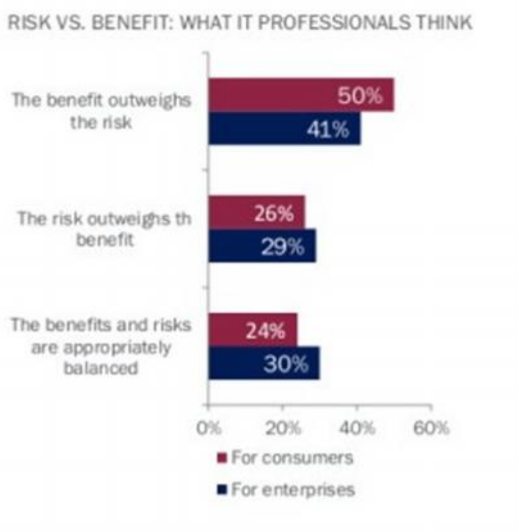


Figure-3

Figure-3 gives an overview of the benefits over risks of the integration of the internet of things. Even though the benefits are more still the risks are in a considerable amount. They need to be paid heed to and the problems of the above approaches fails to handle these risks hence we need to look for an alternative.

MATERIAL AND METHOD

Inflexibility of the three approaches should be removed and for this the IP to field model. In this model the sensor networks are considered as intelligent networks. One important advantage of this model is that the sensor nodes being intelligent are able to overcome gateway malfunctioning as the gateway functionality would be restricted to protocol translation and forwarding. Reprogramming gateway would therefore be no more required and the problem of static configuration would be solved and dynamic configuration would therefore be obtained. This model assigns additional responsibility to the nodes which presents some further challenges for successful functioning of the model the most important challenges are listed below:

Quality of service - The wireless sensor nodes in the model should be able to provide quality of service. An important way to achieve this is to increase the resource utilization of all the heterogeneous devices that are a part of future internet of things. This opens new prospects in workload distribution. The current workload may be therefore shared between the nodes. An important point to be mentioned here is that the current approaches in the internet providing quality of service cannot be applied to the wireless sensor networks. Hence it is necessary to find approaches to ensure less delay and loss.

Security - Another important factor which needs to be ensured is security as the wireless sensor networks being open to the internet become more vulnerable to attackers from everywhere. Therefore important measures need to be taken to ensure the security.

Configuration - The sensor nodes should be capable of controlling WSN configuration which may include detection and elimination of faulty nodes there by ensuring self-healing capability, management of their own configuration. The internet however does not provide self-healing capability. This again draws a line in the integration of wireless and the internet of thing and hence must be dealt accordingly.

Interoperability - A major showstopper in the integration is the problem of interoperability. This problem occurs mainly because the devices may not be interoperable even if they are following the same standard. Hence future technology requires the integration of various protocols and standards that operate at different frequencies and allow different architectures whether centralized or distributed and should be able to communicate with different networks.

Standards - they are very important for the success of internet of things. Without proper standards for example the TCP5/IP6 the internet of things cannot be applied to a level more than RFID. For this we need fully efficient global energy standards that are secure and privacy centered and use compatible protocols at different frequencies.

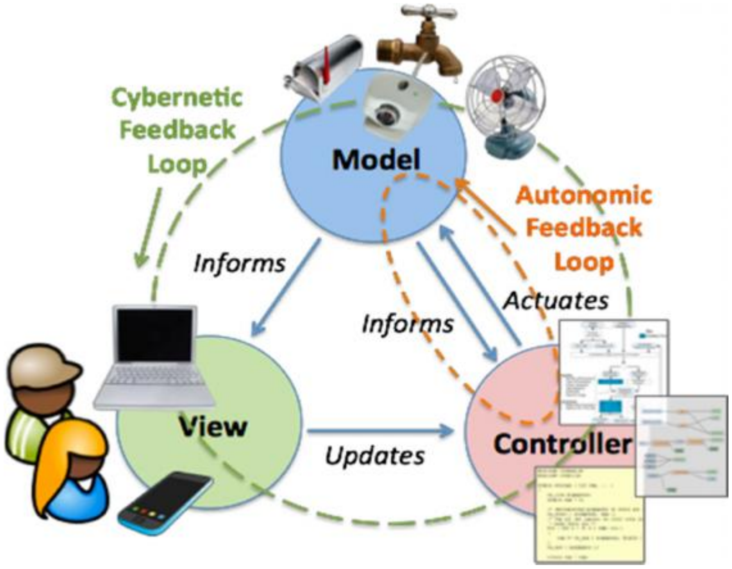


Figure - 4 describes the interoperability of the integration. It shows how the model is connected to the user and the controller.

Manufacturing: In order to implement wide scale integration manufacturing presents another constraint. To avoid this we need to reduce the cost by one percent and extreme high values of production may be achieved, the whole production process should have a minimum impact on the environment.

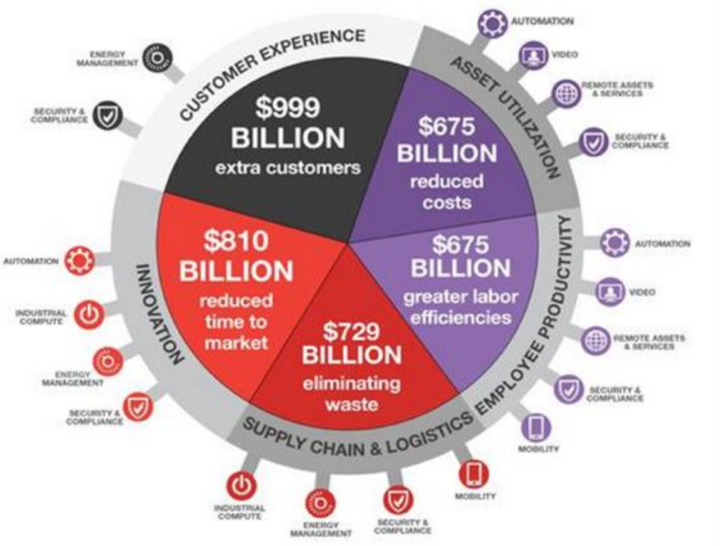


Figure - 5

Figure [5] gives the pictorial view of the manufacturing requirements of the system. All the aspects relating to customers, costs, marketing time, eliminating waste is analytically presented.

Communication: it is another constraint in the integration process. For efficient communication new smart multi frequency band antennas which are integrated on chip and are made up of new materials need to be adopted. These on chip antennas need to be prepared according to size, efficiency and cost. Various forms of such antennas like on chip antennas, printed antennas, multiple antennas which use 3D structures and different substrates could be manufactured and adopted. The communication protocols also need to be designed for web oriented architectures for the internet of things in which all objects, devices which are wireless, cameras, personal computers are combined and they analyze various aspects like the location and emotions over a network.

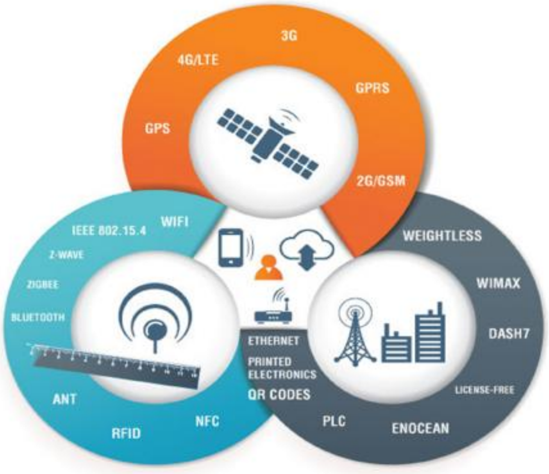
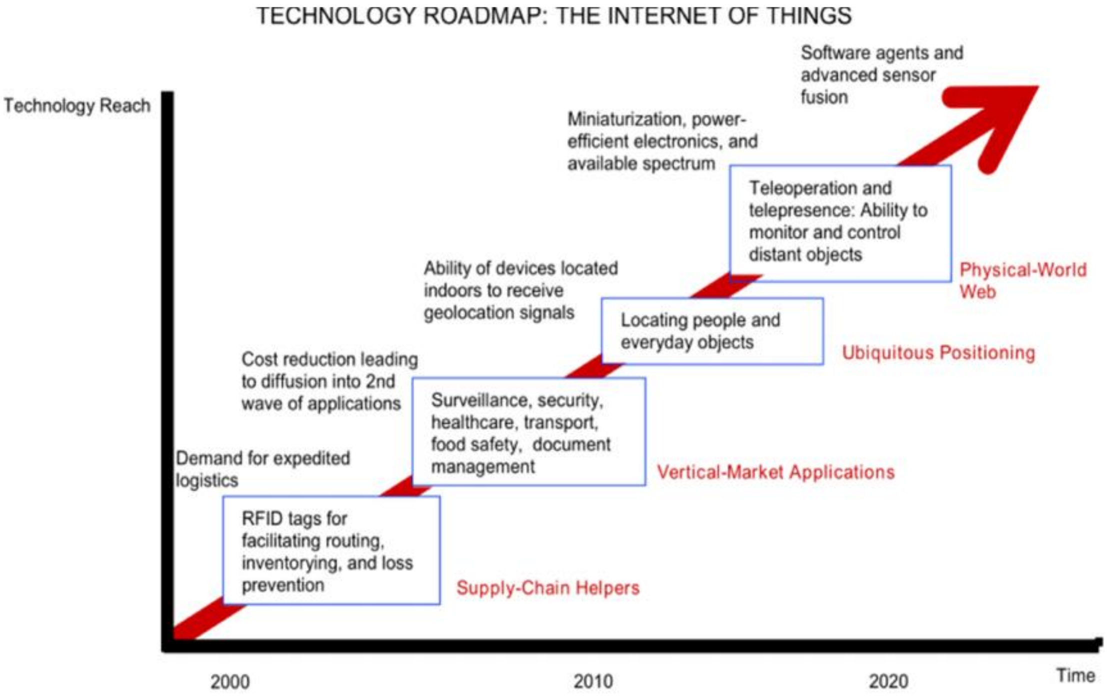


Figure-6

Figure – 6 represents the integration of communication methods to achieve proper and flawless communication.

Intelligence - Large scale integration of wireless sensor networks into the internet of things requires intelligent networks. Content awareness and communication between machines forms an important part of this. The network must be capable of handling harsh environment conditions, must provide security. To achieve this we have ultra-low power microcontrollers which are designed specifically for mobile internet of things devices. For this we may use hard programmed machines or microcontrollers. We have to choose a trade-off between flexibility, programmability, power consumption, silicon area. The devices may be one time programmable, electrically rewritable. We prefer non rewritable nonvolatile memory because it achieves high throughput during test of production, and gives the benefit of programmability and the storage of sensor data.


TECHNOLOGY ROADMAP: THE INTERNET OF THINGS

Source: SRI Consulting Business Intelligence

Figure -7

Figure - 7 represents the technology roadmap of the internet of things. It shows how overcoming and achieving one factor has led to reaching the new goal. Intelligence of the system forms an important part in achieving it.

Governance - it is an important constraint to achieving integration of wireless sensor network. We cannot implement the internet of things globally without having a correct and proper governance. The governance must be kept as generic as possible because having single authority for single application field would lead to confusion, overlapping and competition between various standards and protocols.

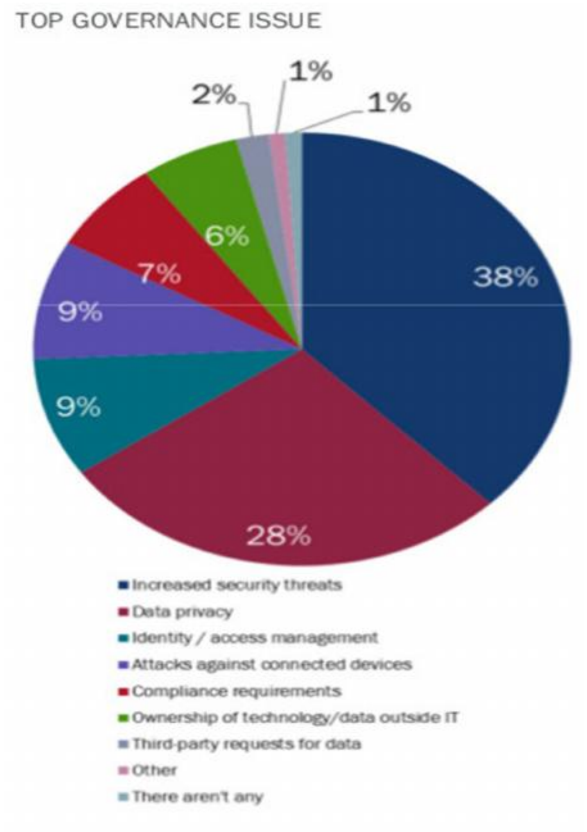


Figure-8

Figure -8 represents top governance issues. The most important is the increased security threat issue .We already discussed the vulnerability of a wireless sensor network integrated with the internet of things to the security threats. Proper measures must therefore be needed to be taken to avoid and control it. Data privacy is another important issue and comprises of almost 28 percent of the governance issues. Identity access management and attacks to connected devices forms around 9 percent of the issues. The compilation requirements needed to compile the data and transfer of data forms around 7 percent of the issues. Third party issues and others form 1 percent each.

CONCLUSION

In this paper mainly we focused on the integration and various aspects related to it. Firstly we focused on the types of application scenarios depending on which we studied the integration approaches. We studied and analyzed the three main approaches and studied their limitations. Then we analyzed the IP to field model and considered its flexibilities we concluded that certain challenges occur in achieving a flawless integration .These challenges are described in detail and their remedies are also explained to some extent. But to ensure proper integration they must be handled in a more proper way.

REFERENCES

1. "Internet of Things in 2020: Roadmap for the Future," 2008, online, http://www.smart-systems-integration.org/public/internet-of-things.

2. K. R¨omer and F. Mattern, "The Design Space of Wireless Sensor Networks," Wireless Communications, IEEE, vol. 11, no. 6, 2004.

3. D. Culler, D. Estrin, and M. Srivastava, "Guest Editors' Introduction: Overview of Sensor Networks," vol. 37, no. 8, 2004.

4. K. Martinez, R. Ong, and J. Hart, "Glacsweb: a Sensor Network for Hostile Environments," in Proceedings of the Sensor and Ad Hoc Communications and Networks Conference (SECON), 2004.

5. W. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, and M. Welsh, "Deploying a Wireless Sensor Network on an Active Volcano," IEEE Internet Computing, vol. 10, no. 2, 2006.

6. M. H. Teicher, "Actigraphy and Motion Analysis: New Tools for Psychiatry," Harvard Review of Psychiatry, vol. 3, 1995.

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

8. R. Roman and J. Lopez, "Integrating Wireless Sensor Networks and the Internet: a Security Analysis," Internet Research: Electronic Networking Applications and Policy, vol. 19, no. 2, 2009.

9. Smart Energy Alliance, online, http://www.smart-energyalliance. com/solutions/ip-to-the-field/.

10. Crossbow Technology, online, http://www.xbow.com.