A Survey on the Open Issues, Limitations and Challenges in the Convergenceof WSN and IoT

Girija Vani G[1], Raj Kumar L Biradar[2]
[1]VTU RRC, Belagavi Karnataka, India
[2]GNITS, Hyderabad, India

Abstract: The Wireless Sensor Network (WSN) consists of tens of hundreds of small tiny sensors those which actively participate in creating a smart environment to gather sensitive data from an inaccessible remote environment over a low-bandwidth wireless link. The Internet of Things (IOT) creates a system of physically existing devices comprising ofautomobiles and other house hold electronics and various gadgets that allow these devices or so-called things to join, share the data and hence develops an environment that allows the direct coalescence of the computer world and the physical world.In order to directly coalescence the WSN into the IoT, lot of convergence challenges must be recognized and needs to be addressed. This paper discusses some of the technologies that may be used for the implementation of WSN and the emerging challenges while converging WSN into the IoT.

Keywords: Wireless Sensor Networks, IoT, ZigBee, 6LoWPAN.

1. Introduction

The thrust for compact, cost-effective, ease of deployment and low-power surveillance/sensing system paved the way for the augmentation of Wireless Sensor Networks. The sensor network consists of tens of hundreds of small tiny sensors capable of sensing, communication and computation. The network actively participates in creating a smart environment to gather sensitive data from an inaccessible remote environment over a low-bandwidth wireless link. The ability of sensor network lies in measuring the environmental parameters in real-time viz., temperature, humidity, pressure, light and many more. Sensor Networks are also widely used for target tracking, health monitoring, transport monitoring, pipeline monitoring, gas detection, precision agriculture, military applications, power management for office buildings, sensing tsunami & seismic events to name a few. Hence it can be stated that the sensor network has the potential to provide an extraordinary interface between the physical and the computing world. The rationale behind the integration of Wireless Sensor Networks and the Internet of Things are growing at an accelerated pace both in the field of research and industry. The convergence between the two technologies presents many challenges and advantages. Among the main challenge is the network security and the advantage is, the Internet connection without a Gateway.

A Wireless Sensor Network comprises of countless sensing nodes that are thickly covered over the environment being monitored and the position of the sensor nodes require not be planned or default. This permits the arbitrary arrangement of sensor nodes in troublesome terrain landscape. Also, the algorithms and protocols that work with WSN should possess self-configuration capabilities [1].The WSN sensor node comprises a detection module, processing algorithms, and communication components that enable the administrator the ability to monitor and respond to events in a specific situation. The important restriction in the sensor node is the requirement for low power utilization. While the traditional communication networks aim to achieve a high quality of service, WSN should focus primarily on saving energy [2].WSN are tending to join the Internet of Things IoT, which can be characterized as a worldwide system of interconnected objects with its own IP address [3], with the aim of integrating heterogeneous wired and wireless communication technologies.The integration of WSN and IoT cannot be easily achieved, since standards-based IEEE 802.15.4 (ZigBee, Wavenis, INSTEON, among others) [4] are not compatible with the Internet, so they are necessary gateway for gathering information from the Internet and communicate with WSN. Therefore, the Internet Engineering Task Force developed the standard IP version 6 over Low power Wireless Personal Area Network (6LoWPAN), characterizes the execution of the IP version 6 stack over IEEE 802.15.4 with the goal that any device can be available from the Internet Version 6 network. 6LoWPAN is based on the idea that all sensor nodes must support the TCP / IP protocols and thus join IoT.The fundamental challenge in integrating IPv6 with WSN, is the IP addressing mechanism which defines fixed header and addressing information of upto 40 bytes. The maximum of 133 byte packets including headers and 6 bytes information payload is allowed according to IEEE 802.15.4, so the translation of header information between these two heterogeneous standards is difficult.

2. Wireless Sensors Networks and The Internet of Things

2.1 Wireless Sensors Networks

A wireless sensor network comprises of a gateway (or base station) that communicates within a group of sensor nodes via RF link. The sensor node collects data, processes them and sends this information directly to the base station or uses multi-hop communication to disseminate the information [5].

2.2 Wireless Sensor Networks - Challenges and Limitations.

To meet the primary goal of communication in an WSN, is to have the design of a wireless sensor node small, cheap and enhanced processing capabilities and optimized power consumption and the most important challenges are mentioned are described below:

Energy: The most important limitation related to the design of WSN is that the sensor nodes work on restricted power. The sensor node being a microelectronic device working on a limited power source, demands energy conservation or energy efficient operation that governs several aspects of the sensor node and the network design.Power utilization can be separated into three areas: detecting which can be continuous or intermittent, data communication and data processing [6]. Among these three areas, a sensor spends maximum energy during the data communication. Energy spent on data processing is much lower compared with data communication [7]. These energy costs influence the design of protocols and algorithms for WSN.

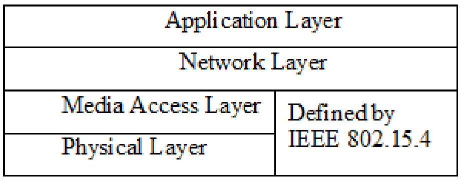
Self-Management: The idea of numerous WSN applications is that they should work in remote regions and brutal situations without the likelihood of upkeep and repair framework bolster [8]. In this way, the sensor hubs must self-manage in configuration, work and team up with different sensor nodes, adapt to the network or node failures, changes in the atmosphere surrounding it.

Fault Tolerance:A deficiency in one of the sensor nodes should not influence the general task of WSN. Fault tolerance is the ability of the network to maintain the bare minimum network services without an interruption due to abnormalities in the nodes or in the network and the extent to which the fault can be borne and depends on the implementation of the network.

Limited Hardware: In addition to the size constraints, the other restrictions on sensor nodes are extremely low energy consumption, dense spatial concentration sensor nodes, low production cost, dispensable and adaptable to the environment.Based on the exposed design challenges, different strategies work. Below are two of the most used in various applications of WSN standards, both based on the IEEE 802.15.4 (which outlines the characteristics of physical and MAC layer for LR- WPAN) with emphasis on different strategies, in order to compare the efforts of transition to the IoT.

2.3 ZigBee Standards

ZigBee- created by ZigBee Consortium, is a wireless networking technology, whose important points are simplicity in installation, reliable information exchange, limited range of operation, and a confined battery life with a protocol stack that is versatile and simple. ZigBee defines the network layer and gives a structure to programming applications in the application layer as illustrated in Fig. 1.



Application Layer	
Network Layer	
Media Access Layer	Defined by IEEE 802.15.4
Physical Layer	

Fig. 1. ZigBee Protocol Stack

The IEEE 802.15.4 physical layer supports different frequency bands: Band 1: 2450MHz (16 Channels), Band 2: 915MHz (10 channels) and Band 3: 868 MHz (single channel), uses Direct Sequence Spread Spectrum (DSSS) in all the three bands to reduce signal interference [9]. The MAC layer characterizes two sorts of nodes: Reduced Function Devices (RFDs) that can just operate as Final ZigBee device and are furnished with sensors/actuators and transducers, switches, lights, and can only communicate with FFDs [10]. The Full Function Devices (FFDs) which are furnished with a full arrangement of elements of the MAC layer, can act as coordinators or network end devices. When they act as network coordinators, FFDs manage the entire network and sends beacons to provide synchronization, communication and bonding services network. The star, tree, point to point network topologies are supported by ZigBee Technology as illustrated in Fig. 2.

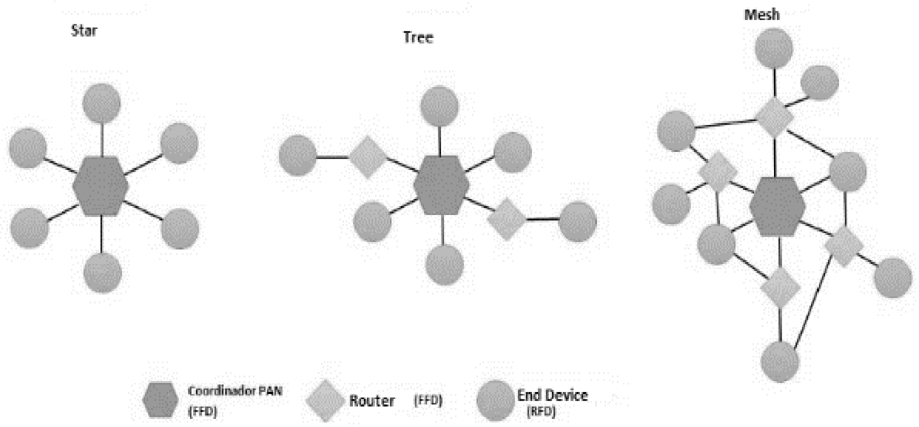


Fig. 2.ZigBee Network Topologies

The upper layers in the protocol stack are clearly standardized by the ZigBee [11]. The network layer NWL takes the responsibility of routing via a multi-hop network, route maintenance, and the APL application layer aims to provide a framework for developing distributed applications and communications.ZigBee Application Layer comprises of an arrangement of Application Objects (APOs) dispersed over various nodes on the network. Application Object is a software developed by an application engineer to control the different components available on a sensor node, such as transducer, switch, lights. The ZigBee Device Object (ZDO) is a special object that provides APOs services: these ZDOs not only discover presence of nodes on the network but also identify the available network services. The network management, security services and communication are the other services being offered. The Application sub layer (APS) enables the APOs and ZDOs to access the underlying network. The above strategies do not offer sensor nodes with the Internet connection, thus limiting the immediate integration of WSN and IoT.

2.4 IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN)

6LoWPAN is a technology developed by IETF wireless networks for low power applications and uses the IEEE 802.15.4 for definitions of physical and the MAC layer. Its architecture is shown in the Fig. 3, and the corresponding descriptions of Physical layer and MAC possess the same characteristics as in the case of ZigBee.

Application Layer	
Transport Layer	
Network Layer	
LoWPAN Layer	
Media Access Layer	Defined by IEEE 802.15.4
Physical Layer	

Fig. 3. 6LoWPAN Protocol Suite

The main changes in 6LoWPAN, is the addition of an adaptation layer between the Network layer and the corresponding IP layer [12]. This adaptation layer facilitates the transmission of datagrams over IPv6 IEEE802.15.4 defining the header compression and packet fragmentation. As for as what concerns the application layer of 6LoWPAN, is the requirement of a compatible Internet, however the typical HTTP scheme is not efficient for the restrictions imposed by IEEE 802.15.4 to overcome these difficulties, the proposed IETF RFC 7252 with an application known as COAP (constrained application protocol) which it operates over UDP and can offer similar characteristics to the requirements of the HTTP requests.So the IEEE 802.15.4 standard is adapted to be used as a means of wireless 6LoWPAN, which provides natural connectivity between WSN and the Internet, enabling smart objects involved in the IoT.

2.5 Internet of Things

The idea of IoT, is the integration of a variety of things or objects [13] (e.g, Radio Frequency tags (RFIDs), mobile phones, labels, sensors etc.) that surround us and allowing these devices to interact with each other using the unique addressing schemes and enable the cooperation among them to achieve common goals. The vision of the International Telecommunication Union (International Telecommunication Union) on IoT is anytime, anywhere connectivity for anyone who now have connectivity for anything. The Intelligence in the IoT has become an indispensable issue, hence research in this area has to be focused on making things intelligent (called Smart Objects) for better decision making and to offer reliable services to end users.The IoT architecture is structured into three layers, this architecture consists of Perception layer (Layer Sensing Technology) which is the hardware or the physical layer and is responsible to collect the data [14]. The Network Layer takes the responsibility of the connection between the perception and the application layer. The Application Layer offers services to integrate the applications and examine the information received from the other layers.Recent studies have added two layers to the existing model of Fig.4, which are the Access Gateway and the middleware Layer. The Access Gateway Layer is added to the five-layer model of IoT so along with networking layer, oversee communications, IoT surroundings and transmit messages amongst objects and frameworks. The middleware Layer is utilized to give a more adaptable interface between the equipment and applications.

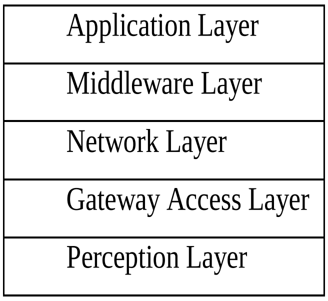


Fig. 4. IoT Protocol Stack

Many challenges need to be addressed both technologically and socially, before the idea of IoT is widely accepted. Among the main challenges are getting full interoperability between devices interconnected to achieve those devices with a higher intelligence level, as this is allowed to adapt and behave autonomously, while ensuring trust, network security and privacy.In addition, the IoT presents numerous new challenges related to aspects of networks. In fact, things that make-up IoT possesses limited resources in terms of computing power and energy. In consequence, the solutions should address especially the resource efficiency and scalability problems.Based on the summary shown in the Table.1, it is possible to identify much of the constraints imposed by a WSN and IoT in terms of computing capacity devices (things) to access in the IoT. It is important to visualize these mentioned problems as the challenges of convergence between WSN and IoT.

3. Challengesin the Convergence

IoT an ever-changing, distributed and hybrid infrastructure necessitates to consolidate various technologies, interface models and protocols with the aim of serving the end devices legitimately.Reaching a balance between safe interactions between objects and services, and the integration of security mechanisms and acceptance of users and data privacy are interesting challenges in IoT. Towards achieving a seamless integration of WSN with IoT, the WSN solutions that are working on standard IEEE 802.15.4 need to include higher layer specifications in the protocol stack, allowing the coalescence of the sensor network into the Internet [15].

This task seems to be challenging as new interconnection issues arise and the following content describes these challenges in brief.The maximum payload size of an IP packet is 64K, compared to this, the packet following the IEEE 802.15.4 has a small size of 133 bytes.Generally, the sensor nodes spend much of their time being idle to conserve energy and hence communication ceases to exist during these idle periods, prompting to new problems in IP networks, as these IP Networks are seldom found in an inactive state [16]. Currently Internet access by WSN has different ways to integrate.The first is an independent or an autonomous connection between the WSN and Internet through the use of a single gateway as shown in Fig. 5.

Table 1: Open Research Issues in IoT

Open Issues		**Description**
Mobility Protocols		Whilst there exist several protocols addressing this aspect, but there are very few which address this issue considering the adaptability, scalability, elasticity and heterogeneity in the present context of the IoT requirements.
Transport Layer Protocols		The conventional services offered by the transport layer viz., connection requirement, flow control, error control, buffering and others are almost void.
Security Issues	Authentication	With the existing limited resources and infrastructure support, it is hard to perform authentication in IoT.
	Integrity	To successful accomplishment of the data integrity relies on the length of the encryption key. However, in the IoT the key length are restricted, resulting in poor security for the data.
	Privacy	As control over the dissemination of all information is impossible with current techniques, this aspect of security needs to addressed appropriately.
QoS Requirements		New requirements are to be set inorder to cater for the diverse traffic that is unconventional for the existing Internet.

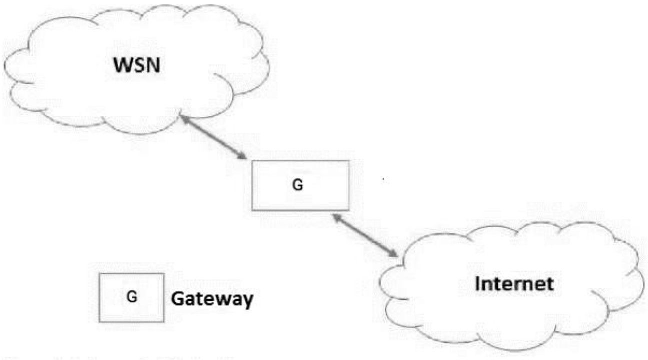


Fig. 5. Autonomous Network.

The second, showing the increasing degree of integration, a hybrid network formed by independent networks even when limited nodes can access the Internet as illustrated in the Fig. 6.

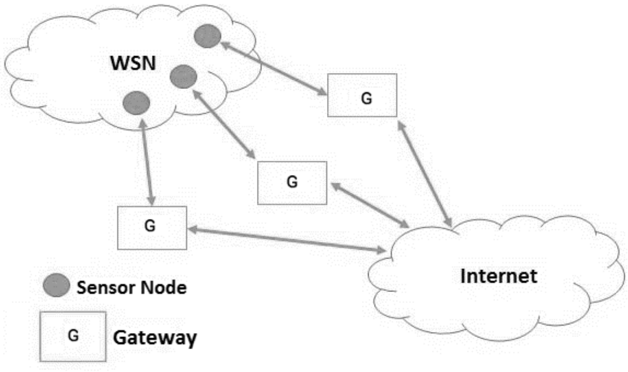


Fig. 6. A Hybrid Network.

The final technique as shown in the Fig. 7, is motivated by the current WLAN infrastructure that forms a network access point 802.15.4 using which the sensor nodes can join the Internet.This Paradigm for the sensor nodes involves assigning additional responsibility of IP besides the usual detection functionality, the most important ones being:

Security: WSN in general is a public network without access to the Internet, and the sensor nodes occupy a significant position in ensuring the secrecy, integrity, accessibility and validation subject to the requirements of the applications. The problems arising when access to information streams created by WSN has not been profoundly studied. It is believed that, once the information is recovered from the nodes, the network users will have the capability to infer the information directly through the coordinator [17].Thus, any intruder can control the sensor nodes, the surroundings, or medium for their advantage.

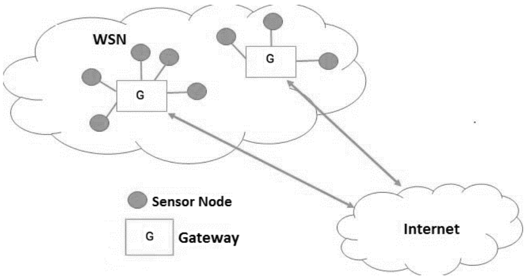


Fig. 7**:** Network using Access Points.

Besides, if such adversary manages to access to no less than one node, thereby allowing the manipulation of the information flow through these compromised nodes.Currently, for such an attack, the requirement is to have the adversary in close proximity with the WSN node. Upon connecting the WSN to the Internet, this closeness is no longer a prerequisite as the attackers will be able to threaten the WSN from everywhere. Most of the WSNs interconnected to the Internet are secured by a single gateway that ensures effective security. Nevertheless, such directly security mechanisms in sensor nodes is not possible, due to the shortage of energy, memory and computational resources. Consequently, security mechanisms should be developed in accordance with the limitations of resources to secure WSN from Internet attacks.

Quality of service: The footbridges behave as repeaters and the protocol translators are expected to contribute to the sensor nodes administration service quality by optimizing the use of resources across hybrid devices that are part of the forthcoming IoT [18]. However, existing approaches that ensure quality of service on the Internet may not be appropriate in WSN, any unexpected variations in the link attributes may induce significant reconfiguration of WSN topology, such reconfiguration focuses on minimizing energy consumption, so that the quality of link may be degraded and consequently the quality of service.

Configuration: Besides security management and quality of service, the sensor nodes also control the WSN configuration including different tasks, namely overseeing addresses to guarantee the ability of self-healing by identifying and removing malfunctioning nodes or administration.

4. Conclusion

Integrating WSN to IoT requires that the components are integrated into the Internet and in cases of moving elements optimized in terms of energy consumption and processing power, which is reflected in the design strategies for 6LoWPAN and ZigBee. This leads naturally to a scenario in which the heterogeneity of the nodes will take an important role, where compromise between energy consumption and processing nodes will be linked to the security and quality of service and the definition of metrics applicable to WSN.Security protocols for WSN applied to IoT, where energy consumption is a metric design, are required, which opens a potential line of research in this area.

The Internet demands a certain quality of service, while optimizing WSN energy consumption the QoS is sacrificed, and upon convergence both of these parameters are affected, when sent information using IP.There is no doubt that these efforts establish a basis for the development of new strategies and new research topics, which requires the Internet of Things.

References

[1]. Priyanka Rawat, Kamal Deep Singh, Hakima Chaouchi, Jean Marie Bonnin: “Wireless sensor networks: a survey on recent developments and potential synergies”, The Journal of Supercomputing, pp. 1-48, 2014. URL http://dx.doi.org/10.1007/s11227-013-1021-9

[2]. V Garg. "Wireless Personal Area Networks Low Rate and High Rate", Wireless Communications & Networking, 2007.

[3]. L. Mainetti, L. Patrono, A. Vilei: “Evolution of wireless sensor networks towards the Internet of Things: A survey”, Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on, pp. 1-6, 2011.

[4]. C. Gomez, J. Paradells: “Wireless home automation networks: A Survey of architectures and technologies”, Communications Magazine, IEEE, pp. 92-101, 2010.

[5]. Seema Ansari, Syeda Fariha Hasnain, Adeel Ansari. "Chapter 1 Introduction and Overview of Wireless Sensor Networks", IGI Global, 2012.

[6]. Akyildiz,. "Factors Influencing WSN Design", Wireless Sensor Networks Akyildiz /Wireless Sensor Networks, 2010.

[7]. Nasser, N. "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks", Computer Communications, 2007.

[8]. Dargie. "Motivation for a Network of Wireless Sensor Nodes", Fundamentals of Wireless Sensor Networks Theory and Practice, 2011.

[9]. Anusha J Krishnan, G S Binu. "Energy efficient tree construction for ZigBee router network", 2017 2nd International Conference on Communication and Electronics Systems.

[10].Paolo Baronti, Prashant Pillai, Vince W.C. Chook, Stefano Chessa, Alberto Gotta, Y. Fun Hu: “Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards”, Computer Communications, pp. 1655 - 1695, 2007. Wired/Wireless Internet Communications.

[11].Han, Chun Guang, Yin Biao Guo, Hua Li, and Chen Jiang. "Distributed Monitoring System of Multi-Machine Tools Based on Wireless Sensor Network", Advanced Materials Research, 2010.

[12].Madanapalli, Syam. "The Internet of Things", Convergence Through All-IP Networks, 2013.

[13].Chen Wang, Bertrand David, Rene Chalon. "Dynamic road lane management: A smart city application", 2014 International Conference on Advanced Logistics and Transport (ICALT), 2014.

[14].Chun-Wei Tsai, Chin-Feng Lai, AthanasiosV. Vasilakos: “Future Internet of Things: open issues and challenges”, Wireless Networks, pp. 2201- 2217, 2014. URLhttp://dx.doi.org/10.1007/s11276-014-0731-0.

[15].Luigi Atzori, Antonio Iera, Giacomo Morabito: “The Internet of Things: A survey”, Computer Networks, pp. 2787- 2805, 2010. URLhttp://www.sciencedirect.com/science/article/pii/S1389128610001568.

[16].Atzori, L.. "The Internet of Things: A survey", Computer Networks, 20101028

[17].Rodrigo Roman, Javier Lopez: “Integrating wireless sensor networks and the Internet: a security analysis”, Internet Research, pp. 246-259, 2009.

[18].Vangelis Gazis, Konstantinos Sasloglou, Nikolaos Frangiadakis, Panayotis Kikiras. "Wireless Sensor Networking, Automation Technologies and Machine to Machine Developments on the Path to the Internet of Things", 2012 16th Panhellenic Conference on Informatics, 2012.