International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 1, February 2019, pp. 439~444
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i1.pp439-444

Integration of internet of things with wireless sensor network

Vandana Reddy, Gayathri P.
School of Computer Science and Engineering, Vellore Institute of Technology, India

Article Info

Article history:

Received Feb 20, 2018
Revised Aug 3, 2018
Accepted Sep 1, 2018

Keywords:

Integration
Internet of Things
WSN

ABSTRACT

The Internet of things (IoT) is a major source for technology solutions in many industries. The IoT can consider, Wireless Sensor Network (WSN) as the backbone network to reduce formation or advent of new technology. Integration of these would reduce the burden and form smart sensor node network with nodes given access to internet. WSN is already a major legacy system that has percolated into many industries. Thus by integration of IoT and WSN no huge paradigm shift is needed for the industries. .

Corresponding Author:

Gayathri P.,
School of Computer Science and Engineering,
Vellore Institute of Technology,
Vellore–632014, Tamil Nadu, India.
E-mail: pgayathri@vit.ac.in

1. INTRODUCTION

IoT is the new age revolution which is intended to connect the machines with themselves more than connecting humans to machines. This means that there would be more machine to machine communication independently which would ease the job as on 2012 8.7 million devices were connected to the internet. In 2017, 20 billion devices were connected to internet and in an estimation by 2023, 50 billion devices would be connected to the internet [1]. IoT refers to the Internet of Things. It means that the IoT consists of physical devices ranging for day to day devices such as mobiles, laptops, television and so on including the home appliances to devices used for high end calculation and processing in the industries such as whether mapping, temperature measurements, fluid density control and so on. These are the devices that have contributed to mankind in various ways. To make these devices more accountable and intelligent we have to embed them with sensors and make them communicate as a network on the whole. This is possible by integrating the IoT with Wireless Sensor Networks (WSN). The WSN consist on geographically distributed sensors that are used to monitor various physical parameter such as pressure, humidity, temperature, density and so on. These sensors would collect the data and process them by the help of centralized base station. Now is the era for digitizing the entire globe. We need to have devices communicated to each other for shrinking the entire Communication systems to the ease of human beings. One such arena that helps us to construct the communication systems globally is the Internet of Things (IoT). Using the IoT we are able to develop efficient digitized network that could possibly communicate with each other. The technology that has been developed so far has allowed us to create a network of senses that the wireless sensor networks. Using the WSN we are able to form a network of sensors that could collect data and process the data and make use of the information to develop the network. The integration of IoT with WSN has also been supported by various companies [2] such as:

a. Smart-Planet: A project on efficient water management and formation of intelligent cities initiated by IBM which makes use of the sensors as primitive device.

b. CeNSE: Central Nervous System for the earth is an initiative by HP Labs which concentrates on developing worldwide sensor network.
c. 6LowPAN standard [3]: transmitting IPv6 packets in computationally restricted networks, built by IETF.

The major challenges with integrating are data collection, data sharing and security. The scope of implementation is vast and consists of multiple dimensions of data hence data collection and sharing becomes difficult. Moreover the sensors implemented in different data collection mechanisms and bringing in sync with these data collection mechanisms Data sharing becomes difficult. After integration that will be a bulk of data in which providing data security and privacy becomes important. The integration comes with multiple problems in the present scenario such as selection of efficient topology of the network that could sustain the integration. The next concern is that the data collection frame work and also the issues related to security. The changes in the selection of topology does the following changes that is the node placement in WSN if done randomly the nodes will have flexibility to move and are also reliable. In WSN the primary concern is about the energy as they are energy constrained devices hence data aggregation ha to be done in the nodes which have less overhead of processing the data. Once the sensors are integrated the information of the sensor and the application are at stake. This is since in sensor systems with high scope, the data detailed by the neighboring hubs has some level of excess, in this way transmitting information independently in every hub while devouring data transmission and vitality of the entire sensor arrange, which abbreviates lifetime of the system. This paper provides a brief description about the existing methods and also provides relevant explanation on the better methods and modes on integration of IoT with sensor networks. The further paper is segmented into section II as Literature Survey, section III as Existing methods and section IV as scope for improvement and areas of development and at the end section V as conclusion.

2. LITERATURE SURVEY

There are many researches done previously to design the integration structure of IoT. Some of the industries also have launched their structure for IoT and WSN integration as mentioned previously and are conducting projects in the integrated environment. The need for integrated environment is increasing rapidly as the networking industries see huge profit out of this environment. Some of the international organizations for standards [4] have already rolled out their standards for the integration environment such as:

a. 3GPP: Successfully launched the integration environment and also launched a research team for Machine to Machine (M2M). It has given frameworks and analysis on feasibility and demands of such frameworks.
b. ETSI M2M TC: Focuses on M2M standardization, definition, examples of applications using it and analysis of demand and requirement of this technology.

As mentioned in “Application Study of Internet of Things in Home”, Tele communications Science [5], [6], [7], the centre for information aggregation is the gateway and it should be deigned with one major features such as protocol conversion for one system to another, device addressing and verification by authenticating mechanisms, collection of information, state control so on. In another proposal called “Web of Things [8]”, an intelligent gateway will be devised which will access the physical objects and turn them to RESTful resources. These resources will be used to access the external HTTP hosts. The intelligent gateways should communicate to sensors through Bluetooth connectivity where a specific URL is allocated to the sensors, then the HTTP packets are formed that consists of aggregated data that has to be sent to the web servers [9]. There are other technologies that use the RFID. These RFID’s hold the electronic details of the things such as cars, goods, accessories [10] and so on. This is made use in technologies such as pervasive computing and ubiquitous computing.

3. EXISTING METHODS

Integration architectures classification

a. Basic sensor node architecture [11]: In this approach the integration of internet and WSN is called as smart sensor node architecture. This architecture needs the redesigning of the following components: the sensor node and the node cluster. The sensor node consist of the basic modules that help in building the network. The sensor is used to aggregate data from various environment sources such as motion sensing, humidity sensing, pressure sensing, and so on. The node can be either formed with one sensor element in it or multiple of these sensing elements in it. The number of sensors in the node actually differs based on the application requirements. It is usually not advised to have more than two sensors but if the application is too large then the number of sensors on the node must also be increased. Each of these nodes must contain signal processing mechanism through micro controllers and microprocessors to sense and process information. Each of the nodes also should have a powerful battery to sustain the data processing

happening in the node. The network architecture is also framed accordingly to suite the smart sensor node architecture. The WSN is formed by several hundreds of node that are spatially distributed along a geographical area in an appropriate topology. The nodes in the network have to form a cluster on the adhoc basis to reduce the human interaction to avoid cost and other critical overheads. The most important region in this network is the central base station. This is important because the entire network is formed and managed out of the information provided by this base station. This base station also sometimes acts as the connector between the network and the internet. The base station will receive the request from node and process the quires and send the processed data to the destination. Ideally each node senses the data and sends the information to the base station. This might not work for all the times due to constraints on network connectivity, power, and terrain and so on. The solution for this could be having distributed centralized nodes to aggregate the data and avoid single point failure. Hence we must be able to form clusters in the network and the cluster head operated as the central base station.

b. Stack based approach [12]: In the stack-based approach, the degree of integration of Internet and WSN depends on the similarities between their network stacks such as:
   1) Front-End: "A Wireless Sensor Network fully abstracted from the Internet"
      According to the approach the sensor nodes can directly communicate with the internet through hosting applications. The WSN is given full freedom to implement its own set of protocols. The communications between the internet host and the sensors are monitored by central base station [13]. The base station will receive the request from node and process the quires and send the processed data to the destination.
   2) Gateway: "Exchange information with Internet hosts (*Gateway*)"
      This approach considers base station that serves as application layer gateway that translates the below layer protocols from one point to another. Hence the nodes and the internet is connected to exchange information without direct access. Even in this method we require gateway as the internet is independent of network.
   3) TCP/IP: "Compatible network-layer protocol:
      Here the sensor node implements the *TCP/IP stack and thus a direct connection is provided to the internet. We cannot make use of WSN protocol but a direct connection is established*.

c. Topology based approach [14]: In the topology- based approach the degree of integration depends on the actual location of the nodes that provides access to the Internet.
   1) Hybrid: "Dual sensor nodes on WSN"
      This approach considers a group of nodes that are present at the edge of the network that provides direct access to the internet. These nodes are quickly mapped the bases station and vice versa.
   2) Access Point: "Full-fledged backbone of devices that allow sensing nodes to access the Internet in one hop:
      In this approach the WSN is formed as unbalanced tree with multiple roots. The leaves of the tree are normal sensor nodes and the roots are internet enabled nodes. By this we ensure one hop internet access.

d. WSN based architecture: The proposed system for integrating WSNs into IoT is composed of four essential blocks:
   1) WSN: The WSN makes use of Zigbee as the communication medium and also uses IPv6 in the network layer. Ccommunication among mobile client, middleware and gateway server, is based on IPv4 over Wi-Fi. This allows all devices in system to talk with all other device independent of the communication medium.
   2) Gateway server: This is the main component of the system to extract information and places into right packets. This also receives IPv4 packets and makes them as IPv6 and vice versa. It also receives sensor data from WSN and sends it to middleware [15].
   3) Middleware: It is software that is used to connect the internal and external services. It also does energy conservation and flow-error control. It mainly receives data, transforms it into require format and sent it across.
   4) Mobile client: These are the application that are installed on the mobile phones which are used to accede the network and other applications anytime from anywhere. These are accessed by IPv4 addresses.

e. Independent Network [16]: Based on the degree of integration of WSN to Internet structure. This method provides the highest abstraction between the Internet and the WSN. In this method the WSN and Internet are considered to be two different entities and are abstracted from each other. They are connected through a single gateway. Here the internet and WSN would not know each other's services directly or indirectly hence a safe way to connect WSN to internet. But this pure abstraction leads to reduced speed and interoperability between the networks. Single point failure is also a concern in this approach. If the

gateway fails the complete connectivity of the network is lost. This approach can be mainly used to monitor space.

f. Hybrid network [16]: Based on the degree of integration of WSN to Internet structure. Even in this method the WSN and internet are abstracted but in the WSN there will be some dual sensors placed that can directly access the internet. Here Single point failure does not occur and the network is robust. This method is useful for the mesh topology where distance coverage is important. This method is mainly used to monitor interactions between objects and space [17].
g. Access point network [16]: Based on the degree of integration of WSN to Internet structure. This approach is inspired from WLAN structure which forms a dense 802.15.4 access point network. Here the WSN consists of multiple gateways and each gateways are in turn connected to multiple sensors. The WSN is connected to internet through gateways. Here Single point failure does not occur and the network is robust. This approach is useful in the star topology due to low latency and direct communications. This approach is usable to monitor objects and humans and their interaction.

4. SCOPE FOR IMPROVEMENT AND AREAS FOR DEVELOPMENT

Challenges in integration as given in the Table 1.

Table 1. Challenges in Integration

Security	Hardware	Software
Node Compromise	Energy	Coordination
Unauthorized data access	Processing	Transmitting data
Denial of Service	Wireless Sensor nodes	Reduce human interaction
Data Privacy	Application Server	Coverage hole

a. Security challenges [18]
   1) Node Compromise: WSN consists of many nodes and hence is at a high risk of attacks. The nodes are also dynamically distributed and make it difficult to monitor. Some of the types of attacks that are possible are false node attacks that could send the information to wrong node and also corrupt the information. Nearer the nodes more is the chance of compromise which can introduce some malware and pose new threats. The physical attacks on the nodes are also alarmingly increasing. Physical tampering is also one of the major concerns.
   2) Unauthorized data access: Due to un-monitored nodes that data that flows in the network also is at risk as the node maliciously trap the data and generate either wrong volumes or huge volumes of data. To overcome this we can take the help of data encryption with strong schemes. When we connect to Internet the issues becomes more complex to solve due to increase in unauthorized nodes.
   3) DoS: When there are huge nodes in number rather than performing the compromise attacks in the network the malicious nodes would bring down the entire network by flooding the network with huge number of proper requests thus the network deny the services even if the request is proper. Cross authentication becomes rampant and thus acquiring more services of network. This is a tradeoff between battery and request completion in the network.
   4) Data privacy: Due to many node compromise and DoS the data that flows on the network is posed no threat. Thus the data will be corrupted and should pass through various security level checks to assure data correctness [19].
b. Hardware challenges
   1) Energy: The wireless Sensor networks are made up of energy constraint devices [20]. If we implement complex operations the network lifetime drastically decreases. Hence we have to be careful while choosing the operations that happen on the network. The energy constrained devices are often drained off with the battery upon huge operations. The Node lifetime and the networking ability is always a trade-off. Hence we have to carefully choose the network architecture and battery capability. If we have long time sensing and less processing the network should be devised accordingly. But it becomes important also for us to maintain the minimum number of operations on the network. In the recent past we have involved multiple battery technologies to overcome the network constraint on the energy. We also can make he was of scavenging devices, acoustic devices, thermal energy [21] and so on as the substitution options.
   2) Processing: if we consider the networks we can see a huge amount of process data flowing across from one into another. This data is picked up by the sensors I forwarded to the central base station. The central base station will process the data accordingly and send it across to the destination nodes.

This will require multiple processing abilities of the sensor and also the base station. The goal is always to decrease the energy an increase the processing ability of the network. This results in cost effective design of the desired networks.

3) WSN: When the network is designed the major concern is about the topology of the network. Each technology has its own advantages and disadvantages. When the decision has to be made about the topology, the care has to be taken about the physical and geographical positioning of the network. The design of network is to be done according with the application it has been used on.
4) Application Servers: the application servers are basically the centralized base station that collect Data and interpret the same. This data has to be recorded in the servers. The applications that send data also should have A Front end to describe about the input of the data.

c. Software challenges

1) Coordination: a robust software system is required the monitor hundreds of nodes that form a network. A smart wireless sensor [22], [23] networks always has large volumes of data transmitting from one end of the network to another. This requires Energy add special processing capabilities in the network [24].
2) Transmitting data: As mentioned in the threats, due to security compromises the data transmission become difficult in the networks [25].
3) Reduce human interaction: the software that is required to reduce human interaction is always more cost incurring in terms of processing ability in the network. The more we concentrate on reducing the human interaction the more intelligent the node has to be. Such nodes form the gateway the bridge the network and the Internet.
4) Coverage hole: due to large Number of nodes forming network, the clustering approach may be adopted. When a cluster is forms it considers that physical location of the node. Each cluster has a size of its own, once the size is reached the cluster would not accept any more nodes and thus leaving some of the nodes not connected to any of the cluster. Those nodes that are not the part of any cluster will have connectivity issues. Along with this some region holes are also formed called as routing holes.

5. CONCUSION

The discussion in the paper about the different technologies in integration and challenges for integration has thrown new insights on the way to use the internet and the networks domestically and commercially. The overall way to integrate can be either of the stacks based or the topology based approaches

ACKNOWLEDGEMENTS

I, express my deepest gratitude to my guide Dr, Gayathri P, SCOPE, VIT University, Vellore, to constantly guide me in the correct direction to fulfill this work. Her motivation and patterns work encouraged me to peruse the research in a proper path. I would also like to thank my parents who have supported me throughput. I sincerely thank the administrative staff at VIT University, Vellore, for their persistent help.

REFERENCES

[1] Number of devices connected to Internet by www.statista.com.
[2] Cristina Alcaraz, Pablo Najera, Javier Lopez, Rodrigo Roman, "Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration? ", *1st International Workshop on the Security of the Internet of Things (SecIoT10)*, NICS Lab. Publications: https://www.nics.uma.es/publications, 2010.
[3] Modbus-IDA, The Architecture for Distributed Automation, http://www. modbus.org/, accessed on October 2010.
[4] H. Jin, WC. Liu, JT. Han and YL Ding, "Application Study of Internet of Things in Home", *Telecommunications Science*, Vol. 26, No. 2, 2010.
[5] Modbus-IDA, The Architecture for Distributed Automation, http://www. modbus.org/, accessed on October 2010.
[6] Mohd. Yazid Idris, Deris Stiawan, Nik Mohd Habibullah, Abdul Hadi Fikri, Mohd Rozaini Abd Rahim, Massolehin Dasuki, "IoT Smart Device for e-Learning Content Sharing on Hybrid Cloud Environment ",*Proc. EECSI* 2017, Yogyakarta, Indonesia, 19-21 September 2017.
[7] Suryono Suryono, Ragil Saputra, Bayu Surarso, Ali Bardadi, "Wireless Sensor System for Prediction of Carbon Monoxide Concentration using Fuzzy Time Series", *Proc. EECSI* 2017, Yogyakarta, Indonesia, 19-21 September 2017.

[8] Delphine Christin, Andreas Reinhardt, Parag S. Mogre, Ralf Steinmetz," Wireless Sensor Networks and the Internet of Things: Selected Challenges", *Multimedia Communications Lab, Technische Universita ̈t Darmstadt Merckstr.* 25, 64283 Darmstadt, Germany.
[9] G. Irwin, J. Colandairaj and W. Scanlon, An Overview of Wireless Networks in Control and Monitoring*, ICIC, Springer*, LNAI 4114, pp 1061-1072, 2006.
[10] IEC 60870-5-104, Part 5-104: Transmission Protocols-Network Access for IEC 60870-5-101 Using Standard Transport Profiles, Second edition 06, 2006.
[11] Alcaraz, P. Najera, J. Lopez, and R. Roman, "Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?", *1st International Workshop on the Security of the Internet of Things (SecIoT10)*, pp. xxxx, NICS Lab. Publications: https://www.nics.uma.es/publications, 2010.
[12] Nacer Khalil, Mohamed Riduan Abid, Driss Benhaddou, Michael Gerndt, "Wireless Sensor Network for Internet of Things".
[13] J. Lopez, R. Roman and C. Alcaraz, "Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Network," *Foundations of Security Analysis and Design V*, LNCS 5705, pp. 289– 338, Springer, 2009.
[14] Smart Energy Alliance, online, http://www.smart- energyalliance. com/solutions/ip-to-the-field/.
[15] Cooper Power Systems' wireless Outage advisor, http://www. cooperpowereas.com/Products/SmartSensor/SmartSensors.cfm, accessed on October 2010.
[16] Dan Partynski, Simon G. M. Koo, "Integration of Smart Sensor Networks into Internet of Things: Challenges and Applications", *IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing,* 2013.
[17] *Z Ali, S. E. Esmaeili, "*The Design of a Smart Refrigerator Prototype", *Proc. EECSI 2017*, Yogyakarta, Indonesia, 19-21 September 2017.
[18] N. Kushalnagar, G. Montenegro, C. Schumacher, RFC 4919: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, *Assumptions, Problem Statement, and Goals*, 2007.
[19] Meshnetics, Meshnetics Demonstrated Integration of Wireless Sensor Data with SCADA System, http://www.meshnetics.com, accessed on October 2010.
[20] DNP3, DNP Users Group, http://www.dnp.org, accessed on October 2010.
[21] Crossbow Technology, online, http://www.xbow.com.
[22] Sensus' FlexNet SmartPoints, http://na.sensus.com/flexnet, accessed on October 2010.
[23] ZigBee Alliance, http://www.zigbee.org/, accessed on October 2010. [23] ISA100, Wireless Systems for Automation, http://www.isa.org/, Accessed on October 2010.
[24] C. Neuman, T. Yu, S. Hartman, K. Raeburn. RFC 4129: The Kerberos Network Authentication Service, 2005.
[25] M. Smith: Web-based Monitoring & Control for Oil/Gas Industry, Pipeline & Gas Journal, 2001.

BIOGRAPHIES OF AUTHORS

Vandana Reddy is working as an Assistant Professor in Christ (Deemed to be university), Bangalore, India. She has 5 years of experience in teaching. Presently Research Scholar at VIT, Vellore. Her research interest includes Wireless Sensor networks, Cloud Computing.

P. Gayathri is working as an Associate Professor in the School of Computer Science and Engineering at VIT, Vellore, Tamil Nadu, India. She received her Ph.D in Computer Science from VIT. She has 10 years of experience in teaching and research. She has published many papers in International and National Journals. She is a life member of Computer Society of India. Her research interest includes Data Mining, Information Retrieval, Big Data Analytics and Artificial Intelligence.