Mini Review
Volume 11:9, 2022

International Journal of
Sensor Networks and Data Communications

ISSN: 2090-4886 Open Access

Wireless Sensors an Advanced Radio Bridge for Internet of Things (IOT)

Ritu Singh[1]*, Amarjeet Singh[2] and Rishi Kumar[3]

[1]*Department of Electronics and communication Engineering, School of Management Sciences, Lucknow, Uttar Pradesh, India*
[2]*Department of Electrical Engineering, School of Management Sciences, Lucknow, Uttar Pradesh, India*
[3]*Department of Electrical Engineering, Goel Institute of Technology and Management, Lucknow, Uttar Pradesh, India*

Abstract

Background: With the advancement of wireless technology and in-build tiny electronics increase the connection between systems and humans. Development of wireless systems based on the internet of things (IOT) revolutionizes the industrial sector and transforms the traditional lifestyle into a high tech lifestyle. The wireless sensor network (WSN) is the central element of the wireless system based on IOT because it contains a number of sensor nodes interconnected with the help of wireless channels and its capability to monitor the real world objects. Being a part of wireless systems based on IOT, in particular can be employed in multiple domains such as health, agriculture and industrial domain. The wireless system based on IOT increases the instant access of data from the surrounding environment and improves the quality of human life. Hence, the attention of this review is to shine a light on WSN and architecture classification of wireless systems based on IOT. In spite of this, we highlight the challenges associated with integration of IOT to WSN.

Keywords: WSN (Wireless Sensor Network) • IOT (Internet of Things) • Sensor node • Integration and Challenges

Introduction

Recent rapid advancement in wireless technology and in-build electronics attracted the scientific community from the past few decades towards wireless sensor network (WSN). The WSN is widely employed in multiple technical domains. A typical WSN consists of minute devices nominated as nodes including in-build CPU, few smart sensors and limited computing power. Nodes are primarily employed to record the pressure, sound, humidity, temperature and vibration from the surrounding environment. The basic components of nodes in any kind of WSN comprise a power unit, transceiver unit, sensor interface, and computing unit (Figure 1). The key function of these units is to transmit the data collected through their smart sensors. Essentiality of WSN culminates with the development of IOT (internet of things) concepts as it is the central component of IOT. IOT is defined as communication and integration between intelligent things. Actuators and sensors (eg: sensors for monitoring the environment, security cameras, and home appliances) are normally equipped with multiple kinds of micro-controller equipment, transceivers and protocol for communication of sensed data [1].

These kinds of RTMs (real time modules) interconnect with one another and transmit the data to central repositories after sensing the data where the cumulative data is deposited and users can retrieve the data with permissive access. The IOT with integration of wireless technology is much better in contrast to wireless and wired networking systems as the number of devices for communication is too high in IOT with wireless technology [2]. The use of IOT in traffic is not suitable as every device senses and transmits the obtained data to the respective server that collectively affects the efficiency of this network. The IOT based system around us consists of a heterogeneous WSN that connects a huge variety of smart sensors [3]. The key issue with these equipment's is heavy consumption of energy [4] which is reflected with a drastic rise in carbon emission and usage of energy [5]. The durability of any application depends upon the consumption of energy by smart sensors and distance of communications [6]. Integration of WSN with IOT enhances the possibility of instant access of data from the surrounding environment and improves the quality of life. Hence, the attention of this review is to shine a light on (i) WSN (ii) architecture classification of integration of IOT to WSN (iii) challenges associated with integration of IOT to WSN.

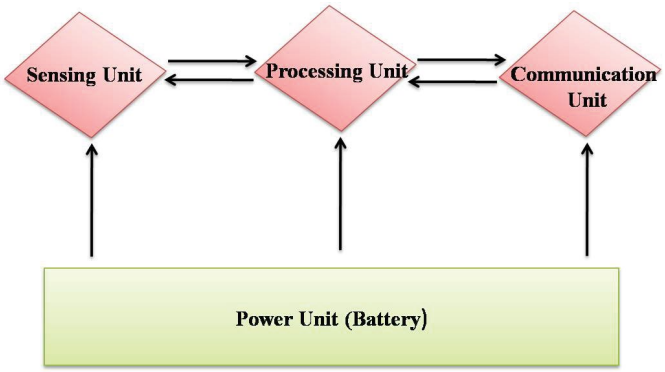

Figure 1. Basic architecture of IOT based sensor node.

Discussion

Wireless sensor networks (WSN)

WSN comprises simple and economical processing devices called as sensor nodes and WSN system is made up of three components; smart sensor nodes, RF (radiofrequency) transceiver and power unit [7]. There are different kinds of WSN with different modalities like single and multi-sensing modality. A network algorithm is not able to detect any kinds of threat in case of WSN with single sensing modality while a WSN network with multi-sensing modality is capable of detecting any kind of threat. Batteries of WSN with multi-sensing modality are rechargeable with heavy battery back-up in contrast to WSN with single sensing modality. There are two kinds of WSN with different

***Address for Correspondence:** Ritu Singh, Department of Electronics and communication Engineering, School of Management Sciences, Lucknow, Uttar Pradesh, India, E-mail: Ritusingh@smslucknow.ac.in*

Date of Submission: 03 September, 2022, Manuscript No. sndc-22-74259; **Editor Assigned:** 05 September, 2022, Pre QC No. P-74259; **Reviewed:** 17 September, 2022, QC No. Q-74259; **Revised:** 21 September, 2022, Manuscript No. R-74259; **Published:** 29 September, 2022, DOI: 10.37421/2090-4886.2022.11.178

infrastructure: Homogeneous and Heterogeneous WSN which are discussed below:

Homogeneous WSN: All nodes with similar energy efficiency and complexity of hardware are nominated as homogeneous WSN. Pure static clustering is the primary feature of homogeneous WSN where nodes of cluster head must be overloaded with transmission of long distance to remotely placed base stations and more time is needed for data aggregation and co-ordination of protocol [8]. The cluster nodes perished prior to other nodes of the sensor network. Hence, one can make sure that all nodes of the sensor network must perish at a similar time which is ensured through the rotating role of cluster head either periodically or randomly as introduced in the LEACH protocol. The most crucial shortcomings of homogeneous WSN is that all nodes of the sensor network can act as cluster head.

Heterogeneous WSN: A WSN with a wide range of sensor nodes with different capabilities like different battery functionality is nominated as heterogeneous WSN. The basic concept behind the development of heterogeneous WSN is the extra battery energy and more complex hardware to decrease the overall expense of hardware. Sensors utilized two kinds of mechanisms; single hopping and multiple hopping. In single hopping, sensor nodes that are far from cluster head utilize more energy in contrast to closest sensor nodes. Heterogeneous WSN utilize multiple hopping in which closest sensor nodes have more energy burden owing to relaying as well as existence of non-uniform energy drainage pattern [9,10].

Integration of IOT with WSN

IOT comprises a wide spectrum of physical devices like laptops, mobiles, television and other home appliances employed for precise processing and calculation in the industries like measurements of temperature, density of fluids, mapping. These physical devices help humans in different ways. To enhance the liability and smartness of these physical devices, researchers integrate these devices with sensors which are feasible owing to integration of IOT with WSN. Several companies supported the integration of WSN with IOT [11] like Smart Planet: IBM initiated this project to make an intelligent cities and management of water by use of smart sensors, CeNSE (central nervous system of earth) is initiated by HP labs that focus on to develop worldwide sensor network and 6LowPAN standard constructed by IETF that focuses on to transmit the IPv6 in to computationally restricted network [12]. Several kinds of approaches are proposed for architecture for integration of WSN with IOT like basic sensor node architecture, stack based approach, topology based approach, WSN based architecture, independent network, hybrid network and access point network.

(i) Basic sensor node architecture: This type of integration of WSN with IOT is also nominated as SSNA (smart sensor node architecture). This architecture needs to redesign some components i.e. cluster and sensor node. Sensors are usually used to aggregate data collected from various sources like temperature, pressure, sound, vibration. The node either formed of single or multiple sensing elements and number of sensors differs in their functionally and energy efficiency that depends upon the applications. Basically it is advised to use not more than two sensors but a number of sensors can be used on the node if the application is large. For a large number of sensors on nodes, each node must have its own powerful battery and signaling processing mechanism via microprocessor and microcontrollers. The most crucial component of this system is the central base station because the whole network is managed and formed from information provided by the base station. In spite of this, it also serves as connectors between the internet and network. The central base station processes the queries followed by sending the data to the destination after receiving the request for query from the node. Basically, each node of the network acquires the data from the environment and sends this data to the base station; this signaling process does not work for all times owing to hindrance in network connectivity, terrain and power supply. Distributed centralized nodes must be employed to overcome the failure of a single point. Hence, we have to form the cluster node in the network and cluster head work as a central base station [11].

(ii) Stack based approach: In this approach, the degree of integration between WSN and internet is depends upon the resemblance their network stacks like:

a. **Gateway (exchange of information with internet host):** In this approach, the base station acts as an application layer that interfaces the protocols of the below layer from one point to another. Hence, internet and sensor nodes are interconnected to exchange of information without direct access.

b. **Front end (a WSN that is completely separated from the internet):** In this approach, a sensor node directly interacts with the internet via hosting applications. WSN is totally independent and has its own sets of protocols. Communication is monitored by a central base station between the sensor node and the internet [13].

c. **TCP/IP (transmission control protocol/internet protocol):** It is a compatible network layer protocol. In this approach, sensor nodes implement TCP/IP stack that provides direct communication with the internet without use of WSN protocol.

(iii) Topology-based approach: In this approach, the integration degree depends upon the exact location of the sensor nodes that contribute to access the data [14].

a. **Hybrid:** In this approach, a group of sensor nodes that are placed at the edge of the network contributes to direct access of data from the internet. These sensor nodes are capable of mapping the central base station and vice-versa.

b. **Access point:** In this topology, WSN is structured in the form of a tree having multiple roots. The leaves of this tree are sensor nodes while roots are internet empowered nodes and through we confirm the one-hop mediated internet access.

(iv) WSN-based approach: This system of integrating WSN with IOT composed of four components:

a. **WSN:** WSN allowed possible employment of ZigBee that acts as a communication medium and also employed IPv6 in the network layer. IPv4 based communication occurs between gateway server, middleware and mobile clients over Wi-Fi. It allows the interaction of all devices of a system with other devices in an independent manner of communication medium.

b. **Middleware:** It is a kind of software that interconnects the external and internal equipment. It is also involved in flow error control and conservation of energy.

c. **Gateway server:** It is the critical element of the systems that pull out the data and deposits into packets. It also obtains IPv4 packets and converts it into IPv6 and vice-versa. In spite of this, it also obtains the data from WSN and transmits it to middleware [14].

d. **Mobile client:** Basically, this application is installed in the mobile phones to recognize the network as well as many other applications at anytime and anywhere from IPv4 address.

(v) Access point network (APN): It is inspired from structure of the wireless local area network (WLAN) that creates a dense 802.15.4 APN [15]. Here, WSN comprises many gateways with many sensors. Internet connected to WSN by the gateway and no single point failure occurs in this network with robust network. Direct communication and low latency are two characteristics that make this network beneficial in star topology. APN is helpful in monitoring the humans and objects and their relationship with each other.

(vi) Independent network (IN): On the basis of the degree of integration of IOT with WSN, this approach provides a high level of abstraction between WSN and internet [15]. WSN and internet both act as independent elements and interconnected with each other by the single gateway. WSN and the internet abstract the data from one another. In this approach, the internet and WSN do not recognize the

Table 1. Challenges associated with integration of WSN to IOT.

Software	Hardware	Security
Routing hole	Application server	DoS (denial of service)
Transmission of data	Energy	Privacy of data
Coordination	Processing	Unauthorized access of data
Reduction in human interaction	Wireless sensor nodes	Node compromise

services of one another; therefore it is very safe to interconnect the internet with WSN. Reduced speed is one of the concerns associated with this approach. Connectivity of the network is lost whenever the gateway fails and this approach is primarily useful to monitor the space.

(vii) Hybrid network: On the basis of the degree of integration of IOT with WSN, in this approach WSN has dual sensors that directly access the data from the internet [15]. The network is strong and single point failure is not an issue with this method and useful where coverage of area is the main concern like mesh topology. This approach is helpful in monitoring the interaction between space and objects [16].

Challenges

Integration of IOT and WSN is widely employed in different areas to benefit the human but there are some challenges associated with integration of IOT to WSN like security, hardware and software challenges (Table 1).

(i) Challenges-Software: Strong software is needed for observation of hundreds of sensor nodes that build a network. An intelligent WSN possesses a huge volume of information and transmits this information from one end to another [11,14] that requires additional energy supply processing ability in the network [17]. Another issue with software is that compromise security enhances the difficulty in transmission of data [18]. Costly software is needed to decrease human interactions. Routing holes is another challenge with software as each cluster has its own size; when it attains this size cluster does not accept more nodes resulting in connectivity issues.

(ii) Challenges-Hardware: The WSNs are fabricated with energy hampering devices [19]. The lifetime of the network decreases when we adjoin the complex operations. Complex operation is responsible for rapid draining of energy constraint devices. Processing of data from central base station to destination sensor node requires the multiple processing capabilities of the sensor as well as base station. Topology is another concern in designing the network and each technology has its own premises and shortcomings. Hence, geographical and physical positioning must be carefully considered during the design of topology of the network. In spite of this, the design of the network also must be according to application. Application servers must contain a Front End to define the input of information as application servers are centralized base stations.

(iii) Challenges-Security: The data privacy, unauthorized access, compromised node and concern with DoS are primary challenges linked to security [20]. WSN comprised multiple nodes; hence they are at high risk of threat that may be false node threat which may manipulate the data by sending to inappropriate nodes. The closest distance between nodes enhances the chances of physical malware which is an alarming issue. Un-monitoring sensor nodes leads to generation of wrong or huge volumes of information and this problem becomes huge owing to an increase in the number of unauthorized sensor nodes after connecting with the internet. Due to the huge number of sensor nodes, malicious nodes oppressed the network through flooding the network with an extensive number of requests in place of compromising the threats. Due to compromise of DoS and multiple nodes leads to no threat to data flows on the network, hence the information will be hampered and it must be passed through various security levels to warrant the correctness [21].

Conclusion

Revolutionary evolution in computational technology enhances the development of WSN that are capable of sensing the requisite surrounding parameters. The wireless system based IOT has attracted researchers from the past few years; however it suffers from additional need of energy supply, data privacy and security. In this review, the existence work focused on WSN, architecture classification of wireless based IOT and challenges associated with wireless based IOT is reviewed.

Conflict of Interest

There is no conflict of interest.

References

1. Cho, Youngbok, Minkang Kim and Sunghee Woo. "Energy efficient IoT based on wireless sensor networks." In 2018 20th International Conference on Advanced Communication Technology (ICACT), IEEE (2018): 294-299
2. Kim, Ho -won and Dong Kyue Kim. "IoT technology and security." 22 (2012): 7-13.
3. Abdul-Qawy, Antar Shaddad H, Nasr Musaed S. Almurisi and Srinivasulu Tadisetty. "Classification of energy saving techniques for IoT-based heterogeneous wireless nodes." 171 (2020): 2590-2599.
4. Kaur, Navroop and Sandeep K. Sood. "An energy-efficient architecture for the Internet of Things (IoT)."11 (2015): 796-805.
5. Abdul-Qawy, Antar Shaddad, P.J. Pramod, E. Magesh and T. Srinivasulu. "The internet of things (IoT): An overview." *Int J Eng Res Appl* 5 (2015): 71-82.
6. Gulati, Kamal, Raja Sarath Kumar Boddu and G. Saravanan. "A review paper on wireless sensor network techniques in Internet of Things (IoT)." *Mater Today Proc* (2021).
7. Akyildiz, Ian F., Weilian Su and Erdal Cayirci. "Wireless sensor networks: a survey." *Comput Netw* 38 (2002): 393-422.
8. Wang, Yun, Xiaodong Wang and Dharma P. Agrawal. "Intrusion detection in homogeneous and heterogeneous wireless sensor networks." 7 (2008): 698-711.
9. Liu, Benyuan, Peter Brass and Don Towsley. "Mobility improves coverage of sensor networks." In Proceedings of the 6th ACM international Symposium on Mobile ad hoc Networking and Computing (2005): 300-308
10. Zhang, Yongguang and Wenke Lee. "Intrusion detection in wireless ad-hoc networks." In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (2000): 275-283
11. Alcaraz, Cristina, Pablo Najera and Rodrigo Roman. "Wireless sensor networks and the internet of things: Do we need a complete integration?." In 1st International Workshop on the Security of the Internet of Things (2010).
12. Angioni, Andrea, Shengye Lu and Davide Della Giustina, et al. "A distributed automation architecture for distribution networks, from design to implementation." SEGAN 15 (2018): 3-13.
13. Lopez, Javier, Rodrigo Roman and Cristina Alcaraz. "Analysis of security threats, requirements, technologies and standards in wireless sensor networks." (2009): 289-338
14. Reddy, Vandana and P. Gayathri. "Integration of internet of things with wireless sensor network." *Int J Electr Comput* 9 (2019): 439.
15. Partynski, Dan, and Simon GM Koo. "Integration of smart sensor networks into internet of things: Challenges and applications." *Phys Soc Comput EEE* (2013): 1162-1167
16. Ali, Z and S.E. Esmaeili. "The design of a smart refrigerator prototype." Comput Electr *Eng 4 (2017): 579-583.*
17. Neuman, Clifford, Tom Yu, Sam Hartman, and Kenneth Raeburn. "The Kerberos network authentication service" 5(2005).
18. Smith, Mike. "Web-based monitoring & control for oil/gas industry." PGJ (2001): 20-22.

19. Lee, Dongsoo, HakJu Kim and Paudl D. Yoo. "Simulated attack on dnp3 protocol in scada system." In Proceedings of the 31th Symposium on Cryptography and Information Security (2014): 21-24

20. Kushalnagar, Nandakishore, Gabriel Montenegro, and Christian Schumacher. "IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals." (2007).

21. JordaAjn, C.E.P., B. Asare-Bediako, G.M.A. Vanalme and W.L. Kling. "Overview and comparison of leading communication standard technologies for smart home area networks enabling energy management systems." (UPEC) (2011):1-6

How to cite this article: Singh, Ritu, Amarjeet Singh and Rishi Kumar. "Wireless Sensors an Advanced Radio Bridge for Internet of Things (IOT)." *J Sens Netw Data Commun* 11 (2022): 178.